MREFCON
MODELO DE RASTREAMENTO DE EVIDÊNCIAS FORENSES CONTRA CRIMES ONLINE – PROPOSTA ACADÊMICA PARA INTEGRAÇÃO E AGILIZAÇÃO DE INVESTIGAÇÕES ENTRE A POLÍCIA, JUSTIÇA E PROVEDORES DE INTERNET

por
MÁRCIO LUIZ MACHADO NOGUEIRA

Niterói
2008

MÁRCIO LUIZ MACHADO NOGUEIRA

MREFCON
MODELO DE RASTREAMENTO DE EVIDÊNCIAS FORENSES CONTRA CRIMES ONLINE – PROPOSTA ACADÊMICA PARA INTEGRAÇÃO E AGILIZAÇÃO DE INVESTIGAÇÕES ENTRE A POLÍCIA, JUSTIÇA E PROVEDORES DE INTERNET

Monografia apresentada para obtenção de título de Especialista em Criptografia e Segurança em Redes no Curso de Pós-Graduação Lato Sensu em Criptografia e Segurança em Redes da Universidade Federal Fluminense.

Orientador: Dr. Luiz Manoel Figueiredo

Niterói
2008

FOLHA DE APROVAÇÃO

Márcio Luiz Machado Nogueira

MREFCON – Modelo de Rastreamento de Evidências Forenses contra Crimes Online: Proposta Acadêmica para Integração e Agilização de Investigações entre a Polícia, Justiça e Provedores de Internet

Rio de Janeiro, ____ de _____ de 2008

_____
Dr. Luiz Manoel Figueiredo

_____
Dr. Mario Olivero

_____
Dr. Paulo Roberto Trales

RESUMO

Atendendo a demanda do setor jurídico sobre a falta de recursos tecnológicos que auxiliem na coleta e validação das evidências forenses computacionais, especificamente de forma online, apresentamos uma proposta de sistema rastreador com o intuito de agilizar e integrar a investigação policial, partindo do processo de apuração até a localização do provedor de internet cujo evento teve origem; catalogando e certificando todas as evidências registradas ao longo do processo via Internet diretamente para a ordem judicial que inicia a execução do sistema e garantindo que todos os processos executados atendam as questões legais apresentadas nas leis de informática nacionais. Modelo proposto para uso conjunto entre a Polícia Federal e a Agência Brasileira de Inteligência, com trabalho colaborativo dos Provedores de Internet, e supervisão e acionamento direto pela Justiça Regional e Federal. Desenvolvendo um sistema computacional modelado nos pontos concretos onde o estado e o setor privado pode trabalhar sinergicamente a melhorar o sistema nacional de segurança na Internet, prescrevendo um ambiente virtual colaborativo, baseado em conjunto de técnicas e métodos de criptografia. Abordando o estado-da-arte da jurisprudência na informática e das técnicas de criptografia, para dar legalidade à implantação do modelo, e realizando uma comparação exaustiva, no quesito de telemática, com os sistemas Echelon e Carnivore, que monitoram de forma ambígua os meios de telecomunicação global.

Palavras-chaves: direito informático, cybercrimes, evidências computacionais, forense computacional, certificação eletrônica, criptografia, redes privativas virtuais

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

GLOSSÁRIO

ABIN – Agência Brasileira de Inteligência
AC - Autoridade Certificadora
AR - Autoridade de Registro
ARP – Protocolo de Acesso ao Meio Físico
Bits – Unidade computacional
Browser – Programa de navegação
CGI – Interface Comum de Programação
CIA – Agência Americana de Inteligência
CPU – O mesmo que processador
Crackers - Intrusos
CSCW – Trabalho Cooperativo Mediado por Computador
DNS – Serviço de Tradução de Nomes
DoS – Técnica de Negação de Serviço
Download – Baixar/Recuperar
DSS – Padrão de Assinatura Digital
Extranets – Redes Externas de Computadores
FBI – Polícia Federal Americana
Firewall – Filtro de Pacotes
FTP – Serviço de Transferência de Arquivos
Hacker - Invasor
Hash - picar, cortar, triturar
HD – Disco Rígido
Host – Computador ligado na Internet
Homepages – Páginas Pessoais na Internet
Http – Protocolo de Texto Dinâmico
ICMP – Protocolo de Troca de Mensagens
IDEA – Algoritmo de Criptografia de Dados
IDS – Sistemas de detecção de intrusos
Imap – Protocolo de
Intranet – Rede local de computadores
IPSEC – Protocolo IP Seguro
IPX – Protocolo de redes Novell
ISO – Organização de Padronização Internacional
ISP – Provedor de Internet
ITU-T X.509 – Padrão de Certificados Digitais
Kernel – Núcleo do computador
LAN – Redes locais de computadores
Links – Canais de comunicação
LOG - Registros
Loopback – Interface local do computador
Memória ram – Memória volátil
Memória Swap – Memória volátil localizada no disco rígido
NAT – Serviço de Tradução de Redes
NBR – Padrão Internacional de Certificação
NSA – Agência de Segurança Nacional Americana

Pacotes TCP – Pacotes orientados a conexão
Pacotes UDP – Pacotes não orientados a conexão
PF – Polícia Federal Brasileira
PGP – Programa de Garantia de Privacidade
PL – Projeto de Lei
Pop3 – Serviço de Recebimento de Mensagens Eletrônicas
RFC – Documentos Padronizados Internacionalmente por Comentários
Servidores proxy – Servidores de acesso entre duas ou mais redes
Scripts – Conjunto de instruções ou programação num único arquivo texto
SHA - secure hash algorithm
Site – Página na Internet
Smtp – Serviço de envio de mensagens eletrônicas
SNI - Sistema Nacional de Inteligência
Sql – Protocolo de banco de dados
Storyboard – Visão animada em papel de uma história
TCP/IP – Protocolo de comunicação em redes
WAN – Redes de computadores em longas distâncias
Web sites – Páginas com recursos multimídia na Internet
Webmail – Serviço de E-mail através do protocolo http
Upload – Envio de arquivos
Xml – Linguagem de programação para web universal

Capítulo 1 Introdução

Durante as 2 últimas décadas o mundo vivenciou um crescimento exponencial de crimes relacionados à informática, mais especificamente crimes realizados on-line, através de redes de computadores. No Brasil, o assunto ganha maior notoriedade a partir da discussão em 15/10/97, na Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados sobre crimes eletrônicos, e como os solucionar [CCTCI, 1997]. Em 2005, o lançamento do romance Fortaleza Digital [BROWN, 2005] desperta a população para o problema da liberdade individual em prol da segurança nacional, criando uma empatia social da população contra sistemas de rastreamentos online, utilizados pelos estados maiores de forma a combater o *cybercrime.*

Sistemas de seguranças capazes de deter, reter ou retaliar uma investida criminosa contra sistemas computacionais, partindo do próprio mundo virtual, a Internet, existem diversos e pode-se dizer eficientes. Contudo, acionar juridicamente o infrator e definir o objeto do direito do caso, é um processo nem sempre fácil até mesmo para especialistas da área. Há alguns anos que o setor jurídico nacional debate das condições legais para a tipificação dessas infrações, suas penas e condenações. Atualmente o estado da arte jurídica nacional resolve em sua maioria os problemas clássicos que se difundiram ao longo dos anos, problemas esses que intitularam informalmente e sem fundamentação de que a Internet seria um espaço livre sem leis (Castro, 2001). Problemas como a tipificação dos *cybercrimes*, do anonimato e da jurisprudência já tem tratamento legal cabível e prático, contudo ainda pouco difundido pelo fato de terem sido aprovados recentemente, menos de um ano.

Aliado aos avanços no judiciário as técnicas de criptografia, em específico de certificação digital, propiciam um ambiente virtual de validação de documentos eletrônicos, definidos e aceitos pelas novas leis.

A proposta do trabalho é desenvolver um modelo de arquitetura de software colaborativa virtual entre entidades responsáveis pela segurança da Internet, capaz

de integrar os órgãos responsáveis por investigações na Internet, judiciário e os repositórios de evidências existentes nos provedores, a fim de agilizar no rastreamento de evidências de *cybercrimes*. Tal integração é apelada pelo próprio judiciário federal e já existem projetos concretos fundados, como a INFOVIA [ANEXO D] e a INFOSEG [ANEXO E] na esfera de combate ao narcotráfico e a pedofilia através da Internet, os quais também serviram de motivação para o desenvolvimento deste modelo.

Essa integração objetiva principalmente a redução de cartas rogatórias necessárias em investigações de *cybercrimes*. De forma que a proposta em desenvolver um ambiente virtual entre entidades privadas e públicas é apenas um passo, que aliado às novas leis do direito, propiciam um cenário de investigação nacional prático, rastreável e legal através da Internet.

Sistemas de rastreamento e controle de comunicação não são novidades nos países desenvolvidos, literaturas e ficções já os expressam como certa banalidade, e de domínio público encontramos os sistemas americanos *Echelon* e *Carnivore*, controlados respectivamente pela *NSA* e *FBI*, com intuitos de monitorar os sistemas globais de telecomunicações e da Internet. Contudo ambos os sistemas operam de forma ambígua quanto à legalidade, lembrando o romance de [BROWN, 2005] em que toda a história se desenvolve baseada na rejeição dessa ilegalidade por parte de um funcionário. Motivo este que nos leva a apresentar todo um embasamento jurídico legal antes de adentrarmos nos méritos técnicos do modelo. A proposta técnica consiste nas extrações de dados dos logs dos provedores, técnicas de criptografias para validar o apurado e softwares para correlacionar os eventos, além de interfaces comuns de uso para todos os envolvidos.

Iniciamos o trabalho apresentando a discussão ocorrida no congresso sobre Crimes Eletrônicos e Como Soluciona-los, em 15 de Setembro de 1997, na Câmera dos Deputados em Brasília [CCTCI, 1997], aonde desde então o setor jurídico vem apelando por recursos tecnológicos que auxiliem na condenação dos *cybercrimes.* A seguir, adentraremos um pouco nos estudos dos problemas legais que inviabilizariam a proposta deste modelo há até poucos meses atrás, e das recentes conquistas pelo setor jurídico informático sobre estes temas que motivam a apresentação desta solução técnica, baseada na criação de um modelo de arquitetura de software colaborativa virtual. No capítulo 2 aprofundaremos os

estudos sobre validações, forense computacional e transporte seguro de evidências digitais. No capítulo 3 descreveremos os componentes da arquitetura de software proposta, falando dos agentes coletores, do sistema principal e da questão técnica que garante a legalidade do sistema. No capítulo 4 apresentaremos algumas aplicações e análises sobre as vantagens e desvantagens na utilização do modelo virtual em relação ao modelo tradicional. No capítulo 5 apresentaremos dois sistemas similares, ditos inicialmente inconstitucionais, e as comparações deles com o proposto. Finalmente no capítulo 6 apresentaremos as conclusões o modelo para o cenário nacional, sua análise em relação aos sistemas similares e propostas de trabalho futuro.

1.1 Cybercrimes

O primeiro assunto abordado neste trabalho consiste na definição do *cybercrime*, ou crime pela Internet, sendo este o objeto de estudo de onde se pretende identificar suas evidências e recriar o cenário para julgamento.

Apresenta [CASTRO, 2001]: “Junto com o e-commerce, o e-mail, o trabalho on line, surgiram os crimes de informática, conceituados como sendo os crimes praticados contra o sistema de informática ou através deste, abrangendo o computador, seus acessórios e a Internet.”.

Judicialmente no Brasil, os crimes de informática encontram-se tipificados nas leis 9609/98, que tutela a propriedade imaterial, e na nova lei n.° 84/99, recentemente aprovada no Congresso Nacional, e apresentada no [ANEXO B] e comentada no [ANEXO C].

A seguir apresentaremos as resoluções legais adotadas pelo Brasil no combate aos *cybercrimes* que justificam a afirmativa: A Internet não é um espaço livre sem leis. E que servirá como delimitador da tecnologia empregada para o rastreamento dos dados *online*.

1.1.1 Problemas dos Tipos de Cybercrimes

Apresenta [MARTINELLI, 2000]: “Primeiro ponto importante é a tipificação de determinadas condutas. Por princípio do Direito Penal, só é crime o que está previamente definido em lei. Portanto, as pessoas que praticaram atos pela Internet e que não sejam tipificados, apesar de toda sua reprovação, não poderão ser condenadas.”.

Segundo [ARAS, 2001]: “Os bens jurídicos ameaçados ou lesados por crimes informáticos merecerão proteção por meio de tutela reparatória e de tutela inibitória. Quando isso seja insuficiente, deve incidir a tutela penal, fundada em leis vigentes e em tratados internacionais, sempre tendo em mira o princípio da inafastabilidade da jurisdição, previsto no art. 5º, inciso XXXV, da Constituição Federal.”, ou seja, a tipificação de um crime, mesmo cometido online, deve ser analisada conforme todas as formas possíveis de leis, e não havendo a tipificação deve-se tratar conforme o art. 5°, inciso XXXV, da Constituição Federal, que reza: “a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito”, garantindo uma definição legal ao crime cometido.

1.1.2 Problemas de Jurisprudência na Internet

Como eleger o foro para reger *cybercrimes*?

Adaptando de [ARAS, 2001]: “o termo *cybercrime* é mais apropriado para identificar infrações que atinjam redes de computadores ou a própria Internet ou que sejam praticados por essas vias. Analisar as questões de tipicidade, determinação de autoria e competência jurisdicional, mormente nos delitos cometidos pela Internet e que assumem feição de crimes transnacionais, encaixa-se na classificação doutrinária de crimes à distância, e deve-se aplicar a teoria da ubiqüidade, que foi acolhida no art. 6º do Código Penal, que diz: “Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado”. Em se tratando, todavia, de crimes plurilocais (ação e consumação ocorrem em lugares diversos, mas ambos no

território nacional), incide em nosso regime a regra do art. 70, caput, do Código de Processo Penal, determinando a competência pelo lugar da consumação do crime. Conforme o Art. 42 da Lei Federal n. 5.250/67, se considera competente para o processo e julgamento o foro do local onde for impresso o jornal, periódico ou mídia de veiculação pública, como *websites*. Tais diretrizes podem servir como modelo mediante a ratificação de tratados internacionais, e quanto aos casos remanescentes, de conflito ou indeterminação de competência, o art. 5º do Código Penal, dispõe que se aplica a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional. Não exclui a possibilidade de aqui serem punidos crimes cometidos fora do território brasileiro, desde que previstos em convenções internacionais do qual o Brasil seja signatário.".

1.1.3 Problemas de Anonimato na Internet

Até onde o sigilo de informações individuais pode ser mantido, garantindo um anonimato através da Internet?

Adaptando de [ARAS, 2001]: "À proibição de interceptação de *emails* ou de comunicações telemáticas é vedada no Brasil pelo art. 5º, inciso X e XII, da Constituição Federal, salvo mediante autorização judicial para instruir inquérito policial ou processo penal, nas hipóteses da Lei Federal n. 9296/96. É o velho conflito entre ação do Estado e a intimidade do indivíduo, questão que somente se resolve por critérios de proporcionalidade e mediante a análise do valor dos bens jurídicos postos em confronto".

1.2 Ambiente Jurídico de Implantação do Modelo

Vistos os limites legais que a tecnologia precisa imbutir em sua programação para ser visto como uma ferramenta constitucional, veremos a diante o ambiente jurídico existente, objeto de resoluções por parte do modelo, de onde serão propostos módulos de atendimento para cada situação, cuja existência é parte do

atual estado da arte do judiciário informático.

1.2.1 A Omissão dos Provedores de Internet

A conduta criminal pode consistir numa ação (doloso), quando o sujeito faz alguma coisa, ou numa omissão (culposo), quando o sujeito deixa de fazer alguma coisa [DL], dessa forma o provedor de Internet pode ser interpretado como um agente culposo mesmo não tendo participação direta nos eventos.

Ressalva [BARROS, 2003]: “O provedor que não quer ser cúmplice de um crime tem que tomar precauções, perguntando ao usuário o que pretende fazer com seu espaço na Internet, catalogando seus dados a fim de que a investigação chegue à autoria do delito. Ressalte-se, porém, que a cooperação dos provedores de acesso à Internet é de vital importância para identificar os elementos necessários à comprovação da materialidade delitiva e bons indícios de autoria, pois é através dos equipamentos pertencentes a esses prestadores de serviços que o usuário divulga sua comunicação ilícita junto à comunidade virtual”.

Intimar o provedor envolvido na investigação para ter a informação sobre dados de eventos e usuários é objetivo das Cartas Rogatórias, expedidas pela justiça comum para execução pela polícia.

A não acordância do provedor mediante a intimação acarreta em multas e penalidades, mas muitos provedores alegam não manter os registros de todos os seus serviços por questões econômicas e/ou técnicas. Tal omissão contribui para o anonimato desses infratores.

Uma solução seria o juiz dar ao perito plenos poderes e autorizações específicas para operar os registros dos provedores da internet, as ligações telefônicas e os computadores das partes, tanto o do autor quanto o do réu, estabelecendo a conexão entre o envio e o recebimento do evento. O problema neste tipo de solução está no tempo hábil da investigação. Investigações muito longas podem comprometer não somente a prova, possibilitando que o infrator adquira tempo para apagar seus rastros, quanto o próprio departamento policial, onde a demanda de soluções por pequenas empresas acarretaria num congestionamento de casos.

1.2.2 A Integração de Dados para Investigações

Já alertava [MARTINELLI, 2000]: “Faz-se necessário à cooperação entre os órgãos de investigação (polícia, Ministério Público) com institutos de tecnologia para a investigação desses delitos, pois o profissional do Direito não está apto a examinar os aspectos técnicos do crime”. E comenta: “É mais do que notável que a criminalidade tecnológica evolui, assim como a preocupação que ela causa em todos os setores da sociedade. No entanto, as autoridades competentes não acompanham essa caminhada por falta de diversos recursos. Faz-se necessário investir em tecnologia e capacitação pessoal”.

Propôs [BARROS, 2003]: “Outra proposta que poderia ser pensada era a criação de uma base de dados *on line* (via Internet) de intercâmbio e divulgação de informações sobre prevenção do crime, o que de certo modo já foi delineado pelo Programa das Nações Unidas de Prevenção e de Justiça Penal”. Nesse sentido os programas INFOSEG e INFOVIA são modelos.

1.2.3 A Ausência de Recursos para Investigações

E complementa [MARTINELLI, 2000] em relação aos casos que conseguem ir a julgamento: “Mais um problema converte ao flagrante, praticamente impossível de ser obtido, pois o resultado vem muito depois do início da execução ou a vítima toma conhecimento do fato após longo intervalo de tempo porque não experimenta o prejuízo instantaneamente”. Concluindo que: “O procedimento investigatório não se apresenta trajado de provas irrefutáveis e contundentes do crime cometido. Isto acaba por ser um sintoma decorrente da falta de preparo dos agentes de investigação e da estrutura disponível”.

Em síntese, as ausências técnicas apeladas são: apuração, validação e agilização de provas digitais.

Veremos no próximo subitem quanto ao problema de agilização.

1.2.4 Os Problemas das Investigações Policiais

Numa reportagem ao jornal Estado de São Paulo e registrado no site de notícias, http://www.comunicacao.pro.br/setepontos/13/provedores.htm, em abril de 2004, o delegado Mauro Marcelo, diretor geral da ABIN vigente na época, disse que obter informações dos provedores é uma missão difícil e demorada. "Precisamos de um mandado judicial e o processo todo acaba demorando uma semana. Há ataques que passam por dezenas de provedores diferentes. Se eu demorar uma semana para rastrear o cracker em cada um deles, a investigação torna-se inviável", diz. Marcelo ainda reclama da impossibilidade de suspender um domínio que esteja sendo empregado ilegalmente. Ele dá exemplo da Fapesp que "cancela domínios por falta de pagamento, mas lava as mãos quando são utilizados de forma criminosa".

1.2.5 A Prova do Crime como Documento Eletrônico

Para que um documento eletrônico tenha validade jurídica e possa servir, por si só, de meio probatório em juízo, faz-se necessário a ocorrência de dois requisitos: impossibilidade de alteração do seu conteúdo e perfeita identificação das partes.

Para atender esses dois requisitos utilizamos a chamada certificação digital.

Em: http://www.stbrasil.com.br/principal.asp?pag=materia&mat=legis_ged, acessado em 26/03/2005, encontramos referências sobre a questão de o documento eletrônico ser válido perante a justiça:

O Governo instituiu, através da medida provisória nº 2.200-2, de 24 de agosto de 2001, a Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) com o objetivo de garantir autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Das atribuições do ICP-Brasil está a definição de um conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e

metodológicos de um sistema de certificação digital baseado em chave pública.

Completam o quadro de certificação digital a proposição PL-4906/2001, http://imagem.camara.gov.br/MostraIntegraImagem.asp?strSiglaProp=PL&intProp=4906&intAnoProp=2001&intParteProp=1&codOrgao=180, aprovada na Comissão Especial da Câmara dos Deputados, que dispõe sobre o valor probante do documento eletrônico e da assinatura digital, regula a certificação digital e conservação de documentos digitais.

Sobre a utilização de documentos eletrônicos em processos judiciais, dispõe a Lei nº 9.800, de 26 de maio de 1999:

> "Art. 1o É permitida às partes a utilização de sistema de transmissão de dados e imagens tipo fac-símile ou outro similar, para a prática de atos processuais que dependam de petição escrita."

Acrescenta [LEITAO, 2002] um âmbito internacional ao assunto:

"No direito internacional, a Lei modelo da UNCITRAL sobre comércio eletrônico (Resolução 51/162 da Assembléia Geral Das Nações Unidas – ONU – Nova York, de 16 de dezembro de 1996) , estabelece que para que o documento eletrônico tenha o mesmo valor probatório dos documentos escritos é preciso que eles tragam o mesmo grau de segurança contido nestes, sendo que para que isto aconteça é necessário o uso de recurso técnicos, o método cifrado."

Silva Neto, em seu trabalho "O e-mail como prova no direito", apresenta: Sustenta-se que o *e-mail* por si só não prova sua existência e sua integridade original. Há a necessidade de realização de uma perícia técnica que o ateste:

"*Apenas um laudo decorrente de uma perícia pode, em tese, comprovar a existência da autoria, do destinatário, do momentum e dos endereços I.P.s (protocolo de comunicação ou Internet Protocol) por onde passou a transmissão*".

"*A perícia é o mais eloqüente e adequado meio de se fazer a prova judicial de um e-mail, desde que observadas as formalidades de procedimentos cautelares próprios.*"

Para a realização da perícia é necessário que haja uma ordem judicial de busca e apreensão de natureza cautelar do computador daquele que supostamente, virtual ou presumivelmente, enviou o *e-mail* para que se constate se nele se encontram os *bits* nos quais se apóia a ação e que, por sua vez, serão objeto de perícia.

Capítulo 2 Validação de Evidências Forenses Computacionais

Estudaremos agora os artefatos técnicos que nos permitem desenvolver uma arquitetura de sistema computacional para o modelo proposto.

Apresenta [ARAS, 2001]: “No ciberespaço, há razoáveis e fundadas preocupações quanto à autenticidade dos documentos telemáticos e quanto à sua integridade. O incômodo de ter de conviver com tal cenário pode ser afastado mediante a aplicação de técnicas de criptografia na modalidade assimétrica, em que se utiliza um sistema de chaves públicas e chaves privadas, diferentes entre si, que possibilitam um elevado grau de segurança”. Tal segurança é conhecida como assinatura digital.

Afirma [ARAS, 2001]: “Tais questões se inserem no âmbito da segurança digital, preocupação constante dos analistas de sistemas e cientistas da computação, que têm a missão de desenvolver rotinas que permitam conferir autenticidade, integridade, confidencialidade, irretratabilidade e disponibilidade aos dados e informações que transitam em meio telemático. Naturalmente, tais técnicas e preocupações respondem também a necessidades do Direito Penal Informático e do decorrente processo penal. Como dito, somente os mecanismos de assinatura eletrônica e certificação digital e de análise biométrica podem conferir algum grau de certeza quanto à autoria da mensagem, da informação, ou da transmissão, se considerado o problema no prisma penal”.

Veremos neste capítulo os tipos de evidências que serão trabalhadas no escopo inicial do modelo, aprofundando em suas características técnicas a fim de podermos tomar nota sobre o grau de detalhamento passível de registro. Discutiremos em seguida entre as diferenças do estilo clássico de forense computacional em relação a nova arquitetura proposta, onde aprofundaremos os detalhes em relação ao modo como a arquitetura coleta, reconhece, preserva e correlaciona as evidências, baseados em serviços e ferramentas reais dos provedores de Internet, a fim de reconstruir eventos distintos. Por último apresentaremos as formas e ferramentas para validar todo o trabalho feito sobre a forense das evidências a fim de legitimá-las perante o judiciário.

2.1 Evidências Computacionais Online

Adaptador de [CAS, 2000] e [GEU, 2002], o termo “evidência digital” refere-se a toda e qualquer informação digital capaz de determinar que uma intrusão ocorresse ou que provê alguma ligação entre a intrusão e as vítimas ou entre a intrusão e o atacante.

Tais evidências podem ser identificadas através do processo tradicional de forense, rastreando o acesso a arquivos, pastas e dispositivos, onde aqui denominados este tipo de forense como *offline*, ou seja, a forense realizada sem a necessidade de Internet. Já o MREFCON aborda as analises sobre evidências registradas *online*, ou seja, registros de informações deixados nos provedores de internet, uma arquitetura totalmente dependente da Internet. Em outras palavras, adotou-se uma visão macro sobre a ótica da ciência forense. O Intuito é ser abrangente nos aspectos de segurança relacionada à sociedade digital e não de aspectos particulares ou individuais. Temos como missão do projeto: “Monitorar a Internet através dos provedores e não dos usuários”.

A seguir apresentaremos está macro-visão do modelo sobre a ciência da forense computacional, onde na base encontram-se os usuários propriamente ditos, excluídos de qualquer tipo de perícia computacional. Seguidos de suas ferramentas, ou computadores, donde incide a perícia forense *offline*, ou tradicional. Subindo temos toda uma camada de forense telemática, exclusiva para os provedores e serviços de telecomunicações. E por último a camada da forense computacional *online*, que implica nos servidores de Internet responsáveis por todo o provimento de serviços e comunicações *online*.

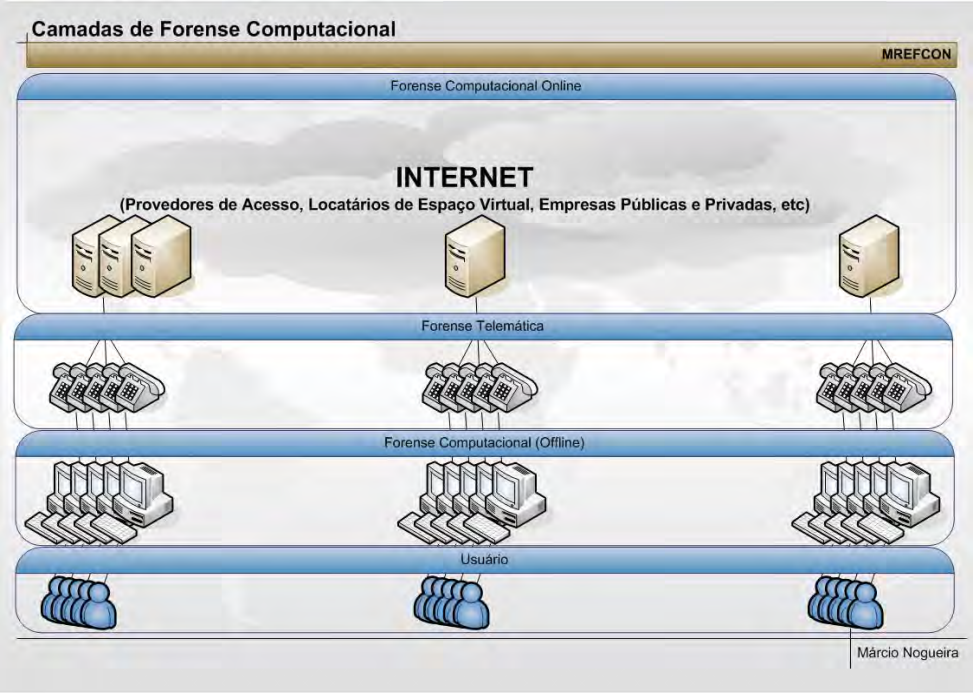


Figura 1 – Estudo da Forense Computacional para o MREFCON

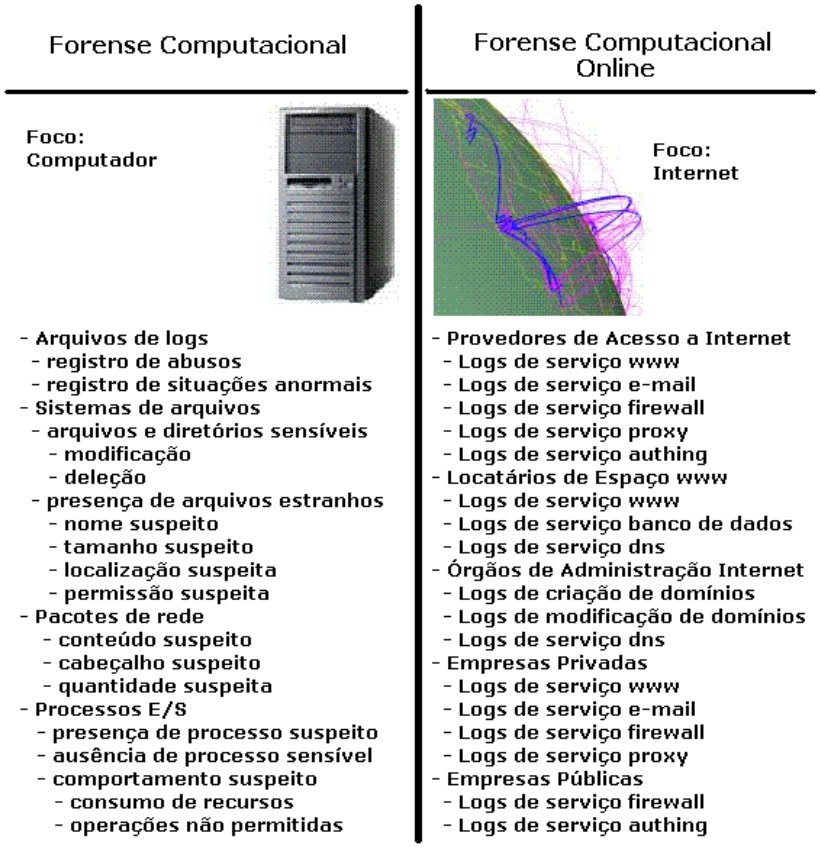


Figura 2 – Comparativo: forense [MREFCON] X [REIS]

Ao assumir essa visão geral da ciência forense observamos que muitos dos

problemas de segurança relacionados à informática também tendem a serem abstraídos, como: atividades de intrusão contra uma instituição distinta, violações através de comunicações ponto a ponto, sabotagem, espionagem e etc. O MREFCON limita-se a rastrear atividades que afetem o funcionamento geral da Internet, como em situações de: ameaça internacional, que tende a paralisar a rede através de congestionamento; ataque do tipo massivo sobre uma determinada instituição com o intuito de deixá-la inacessível; envio de mensagens não solicitadas para diversos usuários existentes ou não da Internet; publicação de um *site* clonado com o intuito da prática do estelionato, entre outros.

Focaremos para apresentação inicial do MREFCON em três eventos massivo de desordem da Internet, todos tipificados em lei, ameaças que envolvem a segurança nacional da Internet: *DDoS – Distributed Denied of Services*, Serviços de Negação Distribuídos; *SPAM* – Envio de *e-mails* não solicitados e o *PHISHING SCAM* – Clonagem, estelionato e fraude eletrônica. Suas tipificações ajudam a modelar os dados necessários que precisam ser coletados como evidências durante as forenses computacionais.

Apesar de tipificadas na nova lei de informática, contudo para o MREFCON a principal importância são as assinaturas deixadas por tais eventos, pois a possibilidade desses eventos terem analogias a outros, ou mesmo de estarem correlacionados entre si, ou mesmo terem interpretações ambíguas quanto sua tipificação na investigação são reais e freqüentes. O MREFCON propõe uma abordagem de rastreamento aberta, onde o operador informa os dados pretendidos e o sistema retorna os eventos correlacionados, independente de uma ação judicial contra *spam* ou contra *ddos*.

Tais ameaças foram escolhidas por seus perfis, onde temos o evento de *DDoS* como um tipo de ameaça por rede, *spam* como uma ameaça por conteúdo e finalmente o *SCAM* que combina essas duas formas. As demais ameaças que envolvem a Internet, e que não estão sendo tratadas nesse momento pelo trabalho, futuramente se enquadrarão num desses 3 perfis ou derivados.

A investigação das evidências, ou assinaturas, desses crimes é baseada através dos registros de informações, ou log, dos provedores de internet. Neles os serviços mais comuns de uso na Internet, são: o servidor *http*, que nomeia os *sites*, como: www.empresa.com; servidor *dns*, que traduz o nome pretendido em seu

número de identificação única, o *Internet Protocol – IP*; servidor *ftp*, responsável pela transmissão de arquivos do tipo *download* e *upload*; servidor *proxy* ou *firewall*, responsável pelo acesso a serviços que não pertençam ao provedor vinculado; servidor *smtp*, *pop3* e *imap*, responsáveis pela transmissão e recepção de mensagens eletrônicas – o *e-mail*; servidores *sql*, responsáveis pelo armazenamento de informações cruciais dos sistemas; servidor de log – *syslog*, responsável por coletar informações de eventos diversos tanto do próprio servidor quanto da *intranet*. Para esta primeira apresentação do MREFCON restringiremos o alcance das investigações a estes serviços em específico, mas registramos nossa intenção futura em ampliar os tipos de serviços bem como as variedades de versões para aumentar o poder de penetração do modelo.

2.1.1 DDoS – Distributed Denial of Service

De acordo com a definição do *CERT* (*Computer Emergency Response Team*), os ataques *DoS* (*Denial of Service*), também denominados Ataques de Negação de Serviços, consistem em tentativas de impedir usuários legítimos de utilizarem um determinado serviço de um computador. Para isso, são usadas técnicas que podem: sobrecarregar uma rede a tal ponto em que os verdadeiros usuários dela não consigam usá-la; derrubar uma conexão entre dois ou mais computadores; fazer tantas requisições a um site até que este não consiga mais ser acessado; negar acesso a um sistema ou a determinados usuários.

O *DDoS*, sigla para *Distributed Denial of Service*, é um ataque *DoS* ampliado, ou seja, que utiliza até milhares de computadores para atacar uma determinada máquina. Esse é um dos tipos mais eficazes de ataques e já prejudicou sites conhecidos, tais como os da *CNN*, *Amazon*, *Yahoo*, *Microsoft* e *eBay*.

Para que os ataques do tipo *DDoS* sejam bem-sucedidos, é necessário que se tenha um número grande de computadores para fazerem parte do ataque. Uma das melhores formas encontradas para se ter tantas máquinas, foi inserir programas de ataque *DDoS* em vírus ou em *softwares* maliciosos.

Para atingir a massa, isto é, a enorme quantidade de computadores conectados à internet, vírus foram e são criados com a intenção de disseminar

pequenos programas para ataques *DoS*. Assim, quando um vírus com tal poder contamina um computador, este fica disponível para fazer parte de um ataque *DoS* e o usuário dificilmente fica sabendo que sua máquina está sendo utilizado para tais fins. Como a quantidade de computadores que participam do ataque é grande, é praticamente impossível saber exatamente qual é a máquina principal do ataque.

Quando o computador de um internauta comum é infectado com um vírus com funções para ataques *DoS*, este computador passa a ser chamado de zumbi. Após a contaminação, os zumbis entram em contato com máquinas chamadas de mestres, que por sua vez recebem orientações (quando, em qual *site*/computador, tipo de ataque, entre outros) de um computador chamado atacante. Após receberem as ordens, os computadores mestres as repassam aos computadores zumbis, que efetivamente executam o ataque. Um computador mestre pode ter sob sua responsabilidade até milhares de computadores. Repare que nestes casos, as tarefas de ataque *DoS* são distribuídas a um "exército" de máquinas escravizadas. Daí é que surgiu o nome *Distributed Denial of Service*. A imagem abaixo ilustra a hierarquia de computadores usadas em ataques *DDoS*.

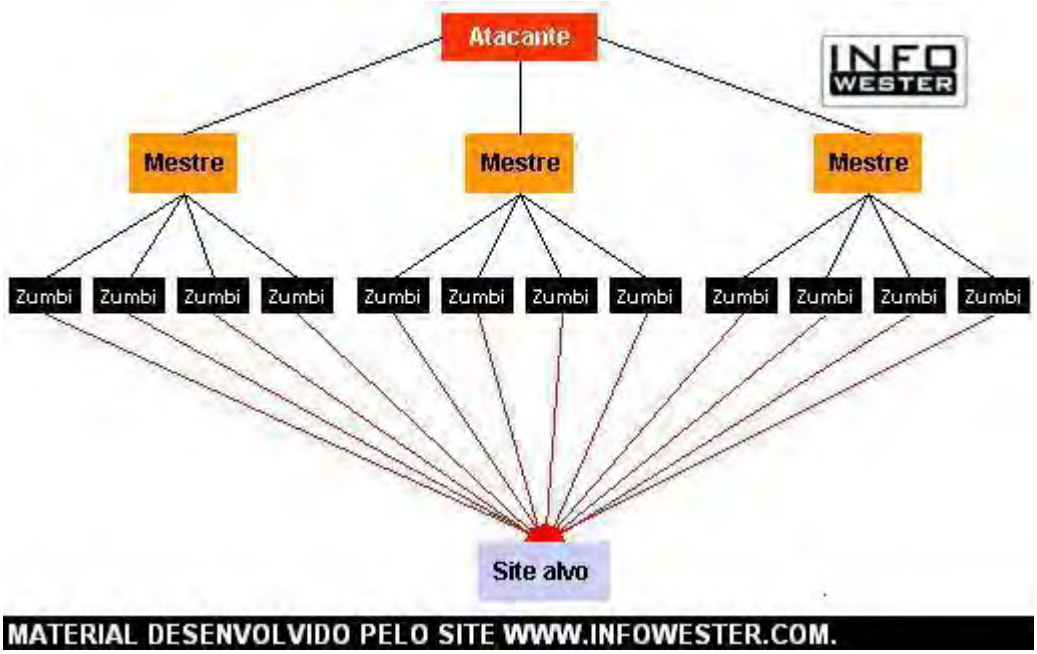


Figura 3 – Estrutura de um crime do tipo *Distributed Denied of Service*

Apesar de não existir nenhum meio que consiga impedir totalmente um

ataque *DoS*, é possível detectar a presença de ataques ou de computadores (zumbis) de uma rede que estão participando de um *DDoS*. Para isso, basta observar se está havendo mais tráfego do que o normal (principalmente em casos de sites, seja ele um menos conhecido, como o www.ufpe.br, seja ele um muito utilizado, como o *Google*), se há pacotes *TCP* e *UDP* que não fazem parte da rede ou se há pacotes com tamanho acima do normal. Outra dica importante é utilizar softwares de *IDS* (*Intrusion Detection System* - Sistema de Identificação de Intrusos) [ALECRIM , 2004].

Em resumo, as evidências online relacionadas ao evento *DDoS* podem ser caracterizadas como:

Quantidade a cima do normal de solicitações de conexões, provindos de várias localizações distintas;

Qualquer tipo de serviço do provedor é passível a este evento;

Qualquer tipo de serviço de um computador é passível a este evento;

As características dos computadores zumbis que os diferenciam para o atacante é que estes possuem rotinas de baixar de um *site* as informações de distribuição ou possuem portas abertas para acesso remoto a programação.

A forma mais simples de identificação desse evento é monitorando e quantificando a quantidade, o tamanho e tipo de informação que estão chegando da Internet para o provedor ou computador, através do *firewall* ou roteador principal.

2.1.2 SPAM – Envio de E-mails Não Solicitados

Segundo o site [INFOGUERRA] *SPAM* é: “o envio, a uma grande quantidade de pessoas de uma vez, de mensagens eletrônicas, geralmente com cunho publicitário, mas não exclusivamente”. O *spam* também é conhecido pela sigla inglesa *UCE* (*Unsolicited Commercial Email*, ou Mensagem Comercial Não-Solicitada).

Afirma: “Em plena era de Internet comercial, o *spam* é uma das principais perturbações para internautas, administradores de redes e provedores, de tal forma que o abuso desta prática já se tornou um problema de segurança de sistemas. Além disso, é também um problema financeiro, pois vem trazendo perdas

econômicas para uma boa parte dos internautas e lucro para um pequeno e obscuro grupo.”

Figura 4 – Origem do nome SPAM – Marca de Presunto

Quanto ao nome não consiste em sigla nem aspectos técnicos relacionados à informática. [INFOGUERRA] apresenta um relato que tenta justificar a origem através da marca do presunto da Hormel, que num de seus comerciais repetia a palavra *spam* para atrapalhar e aborrecer uma funcionária. Tal cena teria repercutido nos meios virtuais, em plena década de 70, para caracterizar o envio de mensagens não solicitadas e irritantes.

Segundo [TEIXEIRA], a taxonomia, em ordem cronológica, dos tipos de *spam* é: as correntes, prometendo sorte, dinheiro, saúde e etc; os boatos, contando histórias mirabolantes sobre determinado produto ou empresa, ou mesmo tentando criar um clima de pânico entre os internautas [HOAX]; os vírus, mensagens enviadas aleatoriamente com intuito de infectar o máximo possível de vítimas; os mala-direta, informativos comerciais e de marketing; as fraudes e golpes, chamados de *scams*, com intuito de enganar as vítimas e condiciona-las a entregar seus dados mediante serviços clonados; além da pornografia, ameaças e afins.

Essa grande diversidade de classificação de *spam* conduz a sistemas de proteção falhos, como o relato abaixo:

Existem diversas ferramentas de combate ao *SPAM*, contudo discorda

[INFOWESTER]: “As soluções usadas por provedores no combate ao *SPAM* são filtros ou sistemas que analisam a mensagem que chegou a um determinado usuário e, com base em regras ou em verificações de determinados itens, tentam determinar se aquele *e-mail* é *SPAM* ou não. A questão é que muitos filtros ou sistemas classificam como *SPAM* uma mensagem verdadeira ou permitem a passagem de um *e-mail* que realmente era *SPAM*. Nesse último caso, até que não se trata de um problema tão ruim, afinal, nenhum filtro é 100% eficaz. No entanto, deixar de receber uma mensagem verdadeira é o maior problema.”

Dessa forma, o *spam* não pode ser tratado conforme uma regra. É preciso analisar o comportamento dos serviços que enviam e recebem o *spam*. Em geral podemos identificar um *spam*, independente de seu tipo, através da quantidade de *e-mails* enviados por minuto a partir de um mesmo usuário na Internet. Contudo a grande maioria dos responsáveis por *spam* não utilizam os serviços de um provedor, e sim a utilização de um *software* específico para o envio das mensagens diretamente de seu computador, podendo inviabilizar o esquema de monitoração. Quando o *spammer* utiliza de um provedor para emissão de suas mensagens, a monitoração é possível através de dois serviços: o servidor de *e-mail* e o *firewall*.

Outra forma de identificação, consiste em monitorar o inverso. Muitos provedores de Internet recebendo uma mesma mensagem originada de um único usuário. Neste tipo de monitoração o rastreamento se dá diretamente nos provedores de Internet.

Outra problemática em relação ao *spam* é que ele pode ter uma constituição legal em determinados casos: O Projeto de Lei nº 1589/99 e o 2358/00 tratam do assunto de recebimento de mensagens indesejadas ou não solicitadas, mais conhecido como "spam", dispondo que aqueles que praticarem essa conduta deverão informar o caráter da mensagem, sob pena de multa (PL 2358).

O *Spam* comercial, onde pessoas estão inscritas por vontade própria, comportam-se como uma ferramenta normal de divulgação. Dessa forma é relevante a observação que nem todo envio de mensagem massiva é ilegal. É preciso analisar o conteúdo, o contexto do envio, o conjunto de destinatários e correlaciona-los.

2.1.3 Phishing Scam – Clonagem, estelionato e roubo de dados

É cediço que dentre as variantes dos tipos penais do Direito Penal Eletrônico, o Furto de Identidade é proeminência, em virtude da técnica denominada *PHISHING Scam*, utilizada por *Crackers*, na intenção de fraudulentamente conhecerem de dados da vítima de modo a obtenção de vantagens indevidas. [MILAGRE]

Completa a respeito da afirmação:

Induzem internautas na forma de envio de *e-mails* falsos que alertam sobre possíveis invasões de contas, registro como inadimplentes na SERASA, onde são solicitados aos usuários que digitem dados sobre banco, agência, conta e senhas, sendo tais informações registradas diretamente na página eletrônica e servidor utilizados pelos criminosos. Frize-se, geralmente servidor hospedado no exterior. O *e-mail* utilizado também é criado no exterior em servidores gratuitos e sem cadastro.

Em seguida desenvolvem a página "pirata" das páginas das instituições bancárias, mantendo fielmente a identidade visual, para onde os usuários são direcionados após tentarem acessar os bancos por provedor que tenha sido atacado pelos "*crackers*".

Essas condutas visam pescar as senhas dos internautas, daí, a denominação "*PHISHING*", terminologia resultante da conexão das palavras "*password*" e "*fishing*", ou seja, pescaria de senhas.

A segunda metade do *PHISHING* ocorre quando os *hackers* estão em posse das informações dos correntistas. Facilmente descobrem quais dessas estão cadastradas para serem movimentadas pela internet através da identificação, mediante simulação de transferências eletrônicas, em nome dos correntistas visados.

Em alguns casos, através de acesso não autorizado ao site de instituições de crédito, colhem-se os dados pessoais desses correntistas (RG, CPF, data de nascimento etc.).

Com as senhas do banco, código da agência, senha em letras e senha do internet banking, executam as transferências. Em caso da não obtenção da senha pelo *PHISHING*, inicia-se a exploração por tentativa de erro, valendo-se das conseqüências numéricas dos dados pessoais ou de fácil dedução (teste, 1234, data

de nascimento, etc.).

Em termos técnicos, as evidências online relacionadas ao evento *SCAM* podem ser caracterizadas como:

Quantidade a cima do normal de solicitações de conexões, provindos de um computador específico, para servidores de *e-mails* distintos, ou seja, é iniciado através de um *spam* do tipo *DDoS*;

Distingue-se do *DDoS* por apresentar o comportamento de não interromper os serviços do alvo, e sim de passar informações fraudulentas;

Em algumas situações serão utilizados *softwares* adulterados para ficar anônimo no envio do *spam*. Sendo necessário então que os logs do *firewall* sejam sincronizados com o do *e-mail*, criando uma identificação única entre eventos.

2.2 Forense Computacional

Segundo [NPP, 2000]: “Forense computacional é o ramo da criminalística que consiste no uso de métodos científicos na preservação, coleta, restauração, identificação, análise, interpretação, documentação e apresentação de evidências computacionais, quer sejam componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais. ”Seu propósito é facilitar ou possibilitar posterior reconstrução de eventos criminais, ou ajudar antecipar ações não autorizadas que se mostram anômalas a comportamentos operacionais esperados ou planejados [PAL, 2001]”.

Alguns aspectos chave que constituem as etapas do processo de análise forense de um sistema computacional [CAS, 2000]:

- Coleta de informações;
- Reconhecimento das evidências;
- Coleta, restauração, documentação e preservação das evidências;
- Correlação das evidências;
- Reconstrução dos eventos.

Toda a informação relevante deve ser coletada para análise e, conforme as evidências digitais são encontradas, elas devem ser extraídas, restauradas quando necessário (ex: evidências danificadas ou cifradas), documentadas e devidamente

preservadas. Em seguida, as evidências encontradas podem ser correlacionadas, permitindo a reconstrução dos eventos relacionados ao ato ilícito. Muitas vezes a análise das evidências (correlação e reconstrução) resulta na descoberta de novas informações, formando um ciclo no processo de análise forense [CAS, 2000].

2.2.1 Coleta de Informações

Toda informação eletrônica que entra ou sai de um provedor de internet pode ser registrada através de logs de operação. Um ponto positivo quanto à coleta de informações online é que em determinados serviços, como o *e-mail* e o servidor de páginas da *web*, a habilitação é efetivada por padrão para registrar informações de caráter crítico ao funcionamento do serviço em específico. Em contrapartida tais logs deixam de registrar informações minuciosas, para evitar o consumo dos recursos da máquina, prejudicando o nível de detalhamento técnico de um ou mais eventos.

Um serviço em especial, o *firewall*, que protege todo o tráfego que entra ou sai do provedor simbolizando um funil na arquitetura e servindo como um porteiro eletrônico, ele determina regras de acesso ou de bloqueio conforme características das informações para onde cada pacote deseja trafegar. Tais regras, quando registradas, conduzem ao real elo entre as informações de destinatário, remetente e serviço. Apesar de sua importância, contudo os registros desse tipo de serviço são na maioria das vezes desabilitados pelos provedores, por consumirem demasiadamente recursos computacionais e serem de difícil compreensão.

Chagamos na base técnica da nossa missão, a coleta de informações. Por um lado sabemos que estão nos logs dos provedores todos os dados necessários para levantamento das evidências. Por outro lado, sabemos que serviços de extrema importância para a perícia podem não estar habilitados ou estarem fora das configurações padrões. Veremos assim como achar as informações estando os logs devidamente habilitados e em seu formato padrão, posteriormente veremos como a proposta do MREFCOM lida com casos complexos, iniciaremos com os logs dos três principais serviços da Internet, o *http*, o *sendmail* e o *iptables*.

2.2.1.1 Serviço de http - Apache

Segundo Zilda Padovan, em seu trabalho Análise e Segurança de Servidores Web, www.peritocriminal.com.br/apache.htm, em 16/03/2005, o servidor *web Apache*, www.apache.org, é o servidor *web* mais utilizado no mundo; dados segundo a *Netcraft*, www.netcraft.com/survey; cerca de 60% dos servidores utilizam o *Apache*. Por ser um *software* de fonte aberta e grátis, possui estabilidade e confiabilidade e é de fácil compreensão.

Para o MREFCON a importância do servidor *apache* está nos registros armazenados em logs, que podem acusar indícios de eventos como *DDoS*, *SPAM* ou *SCAM*, vejamos como:

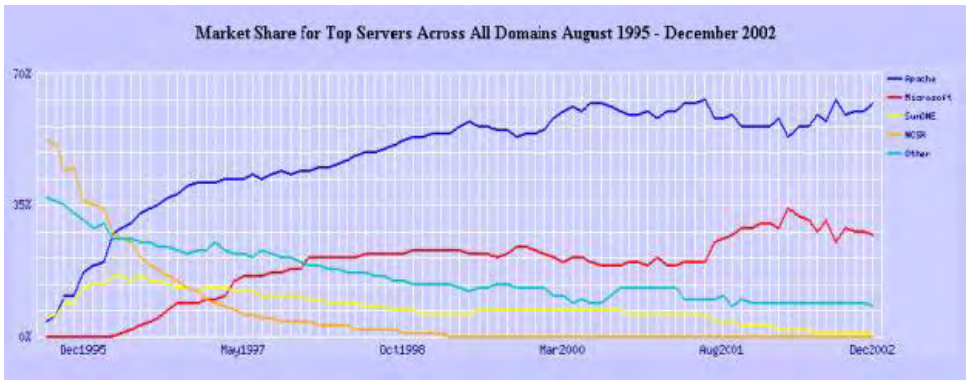


Figura 5 – Utilização do Apache entre os anos de 1995 a 2002

O *Apache* é bem flexível na especificação do que serão registrados em seus arquivos de log, possibilitando utilizar um arquivo de log único, diversos arquivos de logs registrando cada evento ocorrido no sistema (conexão, navegador, bloqueio de acesso, erros, etc) incluindo os campos que deseja em cada arquivo e a ordem dos campos em cada um deles.

O servidor httpd grava seus arquivos de log geralmente em /var/log/apache, não é possível descrever os arquivos de log usados porque tanto seus nomes como conteúdo podem ser personalizados no arquivo httpd.conf. Mesmo assim, os arquivos de log encontrados na instalação padrão do *Apache* são os seguintes:

- access.log: Registra detalhes sobre o acesso às páginas do servidor httpd.
- error.log: Registra detalhes dos erros de acesso às páginas ou erros

internos do servidor.

- agent.log: Registra o nome do navegador do cliente (campo UserAgent do cabeçalho http).

Em [FOCA] encontramos os detalhes de cada campo registrado nos logs do *apache*.

Para fazer uso do máximo de detalhamento possível de ser registrado através do servidor de páginas *web apache*, o MREFCON realiza uma pequena alteração no arquivo de inicialização deste serviço, mas de forma totalmente transparente para os administradores.

Em primeiro lugar ele copia a ferramenta http_wrapper para o diretório de utilitários do sistema operacional. Esta ferramenta foi adaptada para o modelo e possui o seguinte código:

```
 -- /bin/apache_wrapper -------------------------
#!/bin/sh

rm_file() {  rm -f $PPIDFILE }

trap 'rm_file; exit 0' 1 2 5 9 19

HTTPD=`which httpd 2>/dev/null`
PPIDFILE=/var/run/apache_wrapper.pid
USER=$2

[ X"$HTTPD" = "X" ] && exit 1
[ X"$1" = X"-U" -a X"$USER" != "X" ] && HTTPD="/usr/bin/limits -U $USER $HTTPD"

echo $$ > $PPIDFILE

while [ 1 ] ; do
  $HTTPD -F
  killall httpd
  sleep 10
  date >> /var/log/apache_wrapper.log
```

```
done

exit 0
-------------------------------------------------------
```

O apache_wrapper é responsável por monitorar todas as atividades do serviço *http*, sem interferir com o mesmo. Ou seja, é um “grampo telefônico” no serviço de páginas da *web*. Tudo o que for processado pelo servidor será registrado pela ferramenta, mesmo que as configurações originais do provedor de Internet tenham reduzido ou desabilitado os registros de informações, pois antes de serem recusadas as informações elas serão previamente monitoradas pelo uso da ferramenta.

Uma vez introduzida esta ferramenta no âmbito do sistema operacional o próximo passo e substituir a inicialização normal do serviço *http* por esta ferramenta. Após esta troca o sistema operacional estará chamando a ferramenta http_wrapper ao invés do serviço *http*, e a ferramenta será a responsável por criar o ambiente de monitoração e iniciar o serviço dentro deste ambiente.

O seguinte arquivo de inicialização deve ser substituído pelo original:

```
-- /path/to/rc.d/apache.sh ------------------------------
#!/bin/sh

case "$1" in
start)
        if [ -x /usr/local/sbin/apache_wrapper ]; then
                /usr/local/sbin/apache_wrapper -U www &
                echo -n ' apache'
        fi
        ;;
stop)
        kill `cat /var/run/apache_wrapper.pid 2>/dev/null` 2>/dev/null \
        && killall httpd && echo -n ' apache'
        rm -f /var/run/apache_wrapper.pid
```

```
        ;;
*)
        echo "Usage: `basename $0` {start|stop}" >&2
        ;;
esac

exit 0
```

Nas versões futuras do modelo pretendemos aprimorar esta rotina de inicialização de modo que não seja necessário realizar uma substituição integral do arquivo original. Já está sendo desenvolvido, porém sem muitos sucessos ainda, uma rotina que ao invés de chamar o serviço original *http* chamará o arquivo de inicialização normal. Desta forma todo o legado é aproveitado, inclusive personalizações dos próprios provedores dentro deste arquivo original de inicialização.

Vejamos agora alguns exemplos de evidências passíveis de rastreamento nos logs do *apache*, que caracterizam a chamada assinatura do evento, lembrando que não é nosso objetivo neste trabalho exaurir todas as possibilidades de coleta de informações, nosso foco é apresentar o modelo, de sua importância, de sua aceitação técnica e principalmente jurídica:

DDoS:

O evento de negação de serviço distribuído, historicamente, é atribuído diretamente ao serviço de páginas do provedor. Hoje este tipo de ataque já ganha novas proporções entre outros serviços, mas abordaremos a assunto focando o servidor de páginas onde iremos encontrar em seus logs as evidências propriamente ditas do ataque:

```
POST / HTTP/1.1
Host: Unknown
X-CCCCCCC:
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA
ÊÿD$ €|$ ué1À%D$ ÆD$
> > %d$ %D$%D$ %D$ %T$ ‹T$ % $1À°]Í€1ÉÑ,$s'1ÀPPPPÿ $Tÿ $ÿ $ÿ $ÿ $QP° Í€XXXXX<OtXXA€ù
> > uÎë½?1ÀPQP1À°ZÍ€ÿD$ €|$ uï1ÀPÆ $€4$ hBLE*h*GOB%ã°
> > PS° PP° Í€1ÀPhn/shh//bi%ãPS%áPQSP°;Í€Ì
```

Figura 6 – Exemplo de um ataque tipo DDoS registrado no log do apache – fonte: http://www.mycert.org.my/advisory/MA-044.072002.html

Como vemos a assinatura do evento está completamente inserida nos logs do *apache*, não necessitando de referências cruzadas e por conseguinte sendo suficiente para a coleta de dados.

Aprofundando um pouco mais no critério segurança podemos prever uma situação de anonimato, onde o invasor utiliza-se de *software* adulterado para enganar os logs do serviço. Desse ponto de vista, podemos querer estabelecer referência cruzada com os logs do *firewall*, a fim de determinar qual o pacote que tenha passado pelo *firewall* num determinado milisegundo e que tenha registrado o evento no log do serviço de páginas. Descobrindo ou validando o *ip* de origem do evento.

SPAM:

Existem diversas técnicas de envio de *spam*, abordaremos uma delas para exemplificar o funcionamento do MREFCON.

Atualmente é comum a atualização de contas de *e-mails* públicas, tipo yahoo.com.br, terra.com.br, ig.com.br, entre outras, para o envio de *spams*. Chegamos inclusive a analisar situações onde o infrator utiliza-se de um programa adulterado em sua própria estação de trabalho para simular a utilização de um desses provedores. O que existe de analogia entre essa técnica de distribuição é que todos precisam estar utilizando uma conta de acesso válida para ter direitos de enviar o *e-mail* através dos provedores associados.

Baseados no exposto acima, podem concluir que é uma evidência de *spam* registrada em logs do serviço *apache* o evento onde:

- É identificável o provedor de *webmail* de onde originou o evento
- É registrado em log o evento de envio das mensagens
- É registrado no log o *IP* que acessou a conta para enviar as mensagens *spam*

Mesmo em situações de furto de identidade o transgressor não estará apto a desviar do monitoramento em tempo real. Em determinados tipos de investigação a condução do caso necessita desta monitoração intensiva. Semelhante nos casos de anti-sequestro. Onde se espera a ligação do seqüestrador para rastrear em tempo real a origem da ligação. Desta forma o modelo prevê que mesmo não havendo uma coleta de dados suficientes, mas que pelo menos o monitoramento seja possível.

SCAM:

A característica principal da técnica que frauda *sites* com o intuito de roubar senhas e dados dos usuários é a clonagem de um *site* principal para um diretório hospedado noutro provedor sobre seu controle. Nesses casos nos interessam saber os *IPs* que realizaram manutenção no devido conteúdo ou *scripts* dos *sites*. Formam o conjunto de evidências para esse evento:

- Recebimento de *spam* por parte do usuário
- Identificação da origem do *spam* (primeira evidência forense)
- Monitoramento dos acessos no diretório alugado pelo infrator para hospedar o *site* clonado
- Rastreamento dos acessos de administração do *site*

As técnicas de *scam* encontram referências aos de *DDoS* e *SPAM*, onde podemos ter uma assinatura direta, registrada em logs, ou acionar um monitoramento intensivo, a fim de armar uma armadilha. É uma técnica bem mais apura que as duas primeiras, uma vez que possui um envolvimento pessoal muito mais intenso. Mas vistas as formas de combater os primeiros casos percebemos que há uma simplicidade no tratamento dos *SCAM*.

Veremos a seguir o serviço de *e-mail Sendmail* e como o mesmo se comporta perante estas mesmas evidências.

2.2.1.2 Serviço de e-mail - Sendmail

O servidor de mensagens *Sendmail*, www.sendmail.org, é o serviço de envio de *e-mails* mais antigo de todos, e um dos mais utilizados também. Por ser um *software* de fonte aberta e grátis [GNU], possui estabilidade e confiabilidade.

Como o *http*, a importância deste servidor *sendmail* está nos registros armazenados em logs, que também podem acusar indícios de eventos como *DDoS*, *SPAM* ou *SCAM*. Em parte, ao longo dos últimos 5 anos, diversos novos servidores de mensagens vêem surgindo para substituir o tão complexo *sendmail*. O objetivo de sua apresentação aqui em relação a outros é sobre a forma como iremos monitorar esse serviço. A maioria dos demais similares poderá ser “escutada” com ferramentas semelhantes às utilizadas no *http*.

O *Sendmail* é bem rígido na especificação do que será registrado em seus arquivos de log, utilizando um arquivo de log único. Diferentemente do serviço *http*, onde pudemos acoplar uma “escuta”, a complexidade do *sendmail* não permite, pelo menos nesse primeiro momento, apresentarmos uma ferramenta semelhante. Utilizaremos o próprio registro de logs do provedor para realizarmos nossa coleta, uma vez que o *sendmail* possui um padrão técnico rígido e aceitável em termos de detalhamento das informações apuradas.

Para estudarmos o nível de detalhamento do *sendmail* foi necessário compreender seu comportamento padrão, dessa forma:

- diretório de armazenamento dos logs: /var/log/maillog
- utiliza as opções de registro do serviço *syslog* configurado para “*mail*”
- o formato geral das mensagens registradas em log está na forma:

<date> <host> sendmail[pid]: <qid>: <what>=<value>, onde:

Tabela 1: Relação de campos do log sendmail

CAMPO	SIGNIFICADO
<date>	mês, dia e hora que o evento foi logado (o ano é suprimido, conforme peculiaridade do *syslog*).
<host>	O nome do computador que produziu a informação (pode ser diferente do

	computador logado)
Sendmail	literalmente, de qualquer forma que o *sendmail* seja executado esta palavra será exibida aqui.
<pid>	O número do processo invocado pelo *sendmail* que produziu a linha no log.
<qid>	O id da fila, um identificador único da mensagem do computador que produziu a linha do log.
<what>=<value>	Uma lista de conjunto de pares. Cada par aparece numa determinada linha, dependendo se a linha documenta o remetente ou o destinatário e onde o encaminhamento teve sucesso, falha ou foi descartado.

As informações aqui apresentadas neste subitem foram adaptadas de http://logreport.org/doc/gen/email/sendmail.php.

Algumas das possibilidades de combinação “<what>=<value>” relevantes para o MREFCON são:

Tabela 2: Possibilidades dos campos <what>=<value> do sendmail

<what>=	DESCRIÇÃO	OCORRÊNCIA
Class	*The queue class: the numeric value defined in the sendmail configuration file for the keyword given in the Precedence: header of the processed message.*	*Sender log records*
Ctladdr	*The "controlling" user", that is, the name of the user whose credentials we use for delivery.*	*Recipient log records*
Delay	*The total message delay: the time difference between reception and final delivery or bounce). Format is delay=HH:MM::SS for a delay of less than one day and delay=days+HH:MM::SS otherwise.*	*Recipient log records*
From	*The envelope sender. Format is from=addr, with addr defined in [2] by the "address" keyword. This can be an actual person, or also be postmaster or the value of the $n macro in the case of a bounced message.*	*Sender log records*
Mailer	*The symbolic name (defined in the sendmail configuration file) for the program (known as delivery agent) that performed the*	*Recipient log records*

	message delivery.	
Class	*The queue class: the numeric value defined in the sendmail configuration file for the keyword given in the Precedence: header of the processed message.*	*Sender log records*
Msgid	*A world-unique message identifier, defined in [2] as msgid= local-part (a) domain and the placeholders local-part and domain replaced by the respective keywords in [2]. The msgid= equate is omitted if it (incorrectly) is not defined in the configuration file.*	*Sender log records*
Nrcpts	*The number of recipients for the message, after all aliasing has taken place.*	*Sender log records*
Pri	*The initial priority assigned to the message. The priority changes each time the queued message is tried, but this equate only shows the initial value.*	*Sender log records*
Proto	*The protocol that was used when the message was received; this is either SMTP, ESMTP, or internal, or assigned with the -p command-line switch. It is stored in $r.*	*Sender log records*
Relay	*Shows which user or system sent / received the message; the format is one of relay=user(a)domain [IP], relay=user(a)localhost, or relay=fqdn host.*	*Sender and recipient log records*
Size	*The size of the incoming message in bytes during the DATA phase, including end-of-line characters. For messages received via sendmails' standard input, it is the count of the bytes received, including the newline characters.*	*Sender log records*
Stat	*The delivery status of the message. For successful delivery, stat=Sent (text) is printed, where text is the actual text that the other host printed when it accepted the message, transmitted via SMTP. For local delivery, stat=Sent is printed. Other possibilities are stat=Deferred: reason, stat=queued, or stat=User unknown. [complete list of possible values to be made]*	*Recipient log records*
To	*Address of the final recipient, after all aliasing has taken place. The format is defined in [2] by the "address" keyword.*	*Recipient log records*
Xdelay	*The total time the message took to be transmitted during final*	*Recipient log*

	delivery. This differs from the delay= equate, in that the xdelay= equate only counts the time in the actual final delivery.	*records*
To	*Address of the final recipient, after all aliasing has taken place. The format is defined in [2] by the "address" keyword.*	*Recipient log records*

A seguir apresentaremos exemplos de informações passíveis de identificação através dos campos estudados do *sendmail*. Adaptações feitas de. http://logreport.org/doc/gen/email/sendmail.php, em 21/03/2005:

Exemplo do envio com sucesso de um e-mail

"Jul 15 17:11:21 thor.foo.com sendmail[22398]: e6FFBLP22398: from=<jan(a)foo.com>, size=589, class=0, nrcpts=1, msgid=<200007151510.e6FFAC316448(a)odin.foo.com>, proto=ESMTP, daemon=MTA, relay=jan(a)odin.foo.com [192.168.1.1]"

"Jul 15 17:11:21 thor.foo.com sendmail[22400]: e6FFBLP22398: to=<gerrit(a)bar.com>, delay=00:00:00, xdelay=00:00:00, mailer=esmtp, pri=30589, relay=frigga.bar.com. [192.168.1.3], dsn=2.0.0, stat=Sent (e6FFAFv24566 Message accepted for delivery)"

As duas linhas de logs foram retiradas de um computador chamado thor.foo.com, executando o serviço *sendmail* em seu modo padrão. O significado de cada campo consiste em:

Tabela 3: Significado dos campos do log sendmail – envio com sucesso

SIGNIFICADO	CAMPO
Time	963673881
LogRelay	thor.foo.com
QueueId	e6FFBLP22398
MessageId	200007151510.e6FFAC316448(a)odin.foo.com
FromUser	Jan
FromDomain	foo.com
FromRelay	jan(a)odin.foo.com_[192.168.1.1]
Size	589
Delay	00:00:00

XDelay	00:00:00
ToUser	Gerrit
ToDomain	bar.com
ToRelay	frigga.bar.com._[192.168.1.3]
Status	Sent
XStatus	e6FFAFv24566_Message_accepted_for_delivery

O texto "e6FFAFv24566" como parte do campo *XStatus* compõe o *queue id* da mensagem no *ToRelay*. Esta informação ajuda a rastrear a mensagem através de várias máquinas. E o número **963673881** equivale a quantidade de segundos desde Jan 1 1970 1:00 até Jul 15 2000 17:11:21.

Exemplo do envio sem sucesso de um e-mail

“Jul 15 17:53:51 thor.foo.com sendmail[22493]: e6FFrpW22493: from=<jan(a)foo.com>, size=551, class=0, nrcpts=1, msgid=<200007151552.e6FFqmD16573(a)odin.foo.com>, proto=ESMTP, daemon=MTA, relay=jan(a)odin.foo.com [192.168.1.1]”

“Jul 15 17:53:51 thor.foo.com sendmail[22495]: e6FFrpW22493: to=<joost(a)magnum.bar.com>, delay=00:00:00, xdelay=00:00:00, mailer=esmtp, pri=30551, relay=frigga.bar.com. [192.168.1.3], dsn=5.1.2, stat=Host unknown (Name server: magnum.bar.com.: host not found)”

As duas linhas de logs foram retiradas do mesmo *host* do exemplo passado. O significado de cada campo é semelhante, porém apresenta informações distintas:

Tabela 4: Significado dos campos do log sendmail – erro de envio

SIGNIFICADO	CAMPO
Time	963676431
LogRelay	thor.foo.com
QueueId	e6FFrpW22493
MessageId	200007151552.e6FFqmD16573(a)odin.foo.com
FromUser	Jan
FromDomain	foo.com

FromRelay	jan(a)odin.foo.com_[192.168.1.1]
Size	551
Delay	00:00:00
XDelay	00:00:00
ToUser	Joost
ToDomain	magnum.bar.com
ToRelay	frigga.bar.com_[192.168.1.3]
Status	Host_unknown
XStatus	Name_server:_magnum.bar.com.:_host_not_found

Observamos que o motivo pelo qual a mensagem não fora enviada encontra-se no campo *XStatus*. Esta informação pode ser utilizada para determinar as causas do não envio de mensagens. Em nosso caso específico o *host* magnum.bar.com não foi encontrado.

Além dos registros de envio de mensagens podemos encontrar também nos logs:

Logs relativos a conexões

Conexões relativas ao tráfego que chega e sai da rede, de e para outros *hosts*. As categorias para o formato padrão são:

- *(potential) security problems (e.g. spamming)*
- *lost communications (network problems)*
- *protocol failures*
- *connection timeouts*
- *connection rejections*
- *VRFY and EXPN commands*

Exemplos:

“Jul 15 21:17:37 thor.foo.com sendmail[22751]: e6FJHbG22751: ruleset=check_mail, arg1=notorious(a)spammerhome.com, relay=jan(a)odin.foo.com [192.168.1.1], reject=553 5.3.0 notorious(a)spammerhome.com... Sorry, access for decent people only”

“Jul 15 21:17:37 thor.foo.com sendmail[22751]: e6FJHbG22751: from=notorious(a)spammerhome.com, size=0, class=0, nrcpts=0, proto=ESMTP,

daemon=MTA, relay=jan(a)odin.foo.com [192.168.1.1] “

“Jul 15 22:43:25 odin.foo.com sendmail[17394]: WAA17394: lost input channel from nld116-54.bar.com [172.16.123.54]
Jul 15 22:43:25 odin.foo.com sendmail[17394]: WAA17394: from=jan(a)nld116-54.foo.com, size=0, class=0, pri=0, nrcpts=1, proto=ESMTP, relay=nld116-54.foo.com [172.16.123.54] “

“Jul 15 21:21:01 thor.foo.com sendmail[22752]: NOQUEUE: jan(a)odin.foo.com [192.168.1.1] did not issue MAIL/EXPN/VRFY/ETRN during connection to MTA “

“Jul 15 21:30:54 odin.foo.com sendmail[16971]: e6FJUq016969: to=jan(a)thor.foo.com, ctladdr=jan (1003/1003), delay=00:00:02, xdelay=00:00:00, mailer=esmtp, pri=30000, relay=thor.foo.com. [192.168.1.2], dsn=4.0.0, stat=Deferred: Connection refused by thor.foo.com. “

“Jul 15 21:40:30 thor.foo.com sendmail[22850]: e6FJeUB22850: ruleset=check_rcpt, arg1=<jan(a)frigga.foo.com>, relay=jan(a)odin.foo.com [192.168.1.1], reject=550 5.7.1 <jan(a)frigga.foo.com>... Relaying denied
Jul 15 21:40:30 thor.foo.com sendmail[22850]: e6FJeUB22850: from=<jan(a)odin.foo.com>, size=0, class=0, nrcpts=0, proto=ESMTP, daemon=MTA, relay=jan(a)odin.foo.com [192.168.1.1] “

Logs relacionados as mensagens

Ítens logados a parte das mensagens enviadas com sucesso:

- *malformed addresses*
- *message collection statistics*
- *creation of error messages*
- *delivery failures (permanent errors)*
- *messages being deferred (transient errors)*

Exemplos:

“Jul 15 17:53:51 thor.foo.com sendmail[22495]: e6FFrpW22493: to=<joost(a)magnum.bar.com>, delay=00:00:00, xdelay=00:00:00, mailer=esmtp, pri=30551, relay=frigga.bar.com. [192.168.1.3], dsn=5.1.2, stat=Host unknown (Name server: magnum.bar.com.: host not found)”

“Jul 15 17:53:51 thor.foo.com sendmail[22495]: e6FFrpW22493:

e6FFrpW22495: DSN: Host unknown (Name server: magnum.bar.com.: host not found) “

“Jul 15 21:40:30 thor.foo.com sendmail[22850]: e6FJeUB22850: ruleset=check_rcpt, arg1=<jan(a)frigga.foo.com>, relay=jan(a)odin.foo.com [192.168.1.1], reject=550 5.7.1 <jan(a)frigga.foo.com>... Relaying denied “

“Jul 15 21:30:54 odin.foo.com sendmail[16971]: e6FJUq016969: to=jan(a)thor.foo.com, ctladdr=jan (1003/1003), delay=00:00:02, xdelay=00:00:00, mailer=esmtp, pri=30000, relay=thor.foo.com. [192.168.1.2], dsn=4.0.0, stat=Deferred: Connection refused by thor.foo.com.”

Como vemos existem muitas informações úteis que podem ser extraídas dos logs do *sendmail* em seu formato padrão. Veremos em resumo os tipos de evidências para este serviço que o MREFCON irá trabalhar:

DDoS:

Em eventos do tipo negação de serviços distribuídos o *sendmail* pode ser alvo imediato das investidas, reportando diversas mensagens de erros repetidas ao longo de seu log conforme visto acima.

SPAM:

O *sendmail* é utilizado como servidor *smtp* para o envio de *spam*, sua função é um elemento chave para o rastreamento deste tipo de evento. Como vimos nos detalhes dos logs o campo *MessageId* dá um identificador único para cada mensagem enviada ou recebida.

SCAM:

Utiliza o *sendmail* para propagação de seu *spam*. Passível de rastreamento nos mesmos moldes do spam.

Em termos do servidor *sendmail* as evidências estão claramente explicitadas, restando apenas compreendermos os campos nos logs para achar as informações.

2.2.1.3 Serviço de firewall - Iptables

O serviço de filtragem de pacotes, *Iptables*, www.iptables.org, é responsável pelas políticas de *firewall* em servidores Linux. Por ser um *software* de fonte aberta e grátis [GNU], possui estabilidade e confiabilidade, porém não sendo de fácil

compreensão.

No MREFCON este serviço ganha importância uma vez que podem ser registrados em seu log, indícios de eventos como *DDoS*, *SPAM* ou *SCAM*, que venham a validar dúvidas permanecentes em outros serviços, além de dirimir quesitos como adulteração de logs também de outros serviços:

Exemplo do log de um evento

"Apr 16 00:30:45 megahard kernel : NF: D(I,Priv) IN=eth1 OUT= MAC=00:80:8c:1e:12:60:00:10:76:00:2f:c2:08:00 SRC=211.251.142.65 DST=203.164.4.223 LEN=60 TOS=0x00 PREC=0x00 TTL=44 ID=31526 CE DF MF FRAG=179 OPT (072728CBA404DFCBA40253CBA4032ECBA403A2CBA4033ECBA40 2C1180746EA18074C52892734A200) PROTO=TCP SPT=4515 DPT=111 SEQ=1168094040 ACK=0 WINDOW=32120 RES=0x03 URG ACK PSH RST SYN FIN URGP=0 OPT (020405B40402080A05E3F3C40000000001030300)"

Descrição dos campos:

Tabela 5: Significado dos campos do log iptables

CAMPO	SIGNIFICADO
Apr 16 00:30:45	*syslog prefix. It is not present if you read log messages from the console.*
NF: D(I,Priv)	*Enabled with:* ***--log-prefix*** **'prefix'** *An arbitrary, user defined log prefix.* ***Including the spaces.*** *A trailing space is necessary to keep the prefix separate from the next token; this is a bug in netfilter.*
IN=eth1	*Interface the packet was received from. Empty value for locally generated packets.*
OUT=	*Interface the packet was sent to. Empty value for locally received packets.*
MAC=	*Destination MAC=00:80:8c:1e:12:60, Source MAC=00:10:76:00:2f:c2, Type=08:00 (ethernet frame carried an IPv4 datagram)*
SRC=211.251.142.65	*Source IP address*

DST=203.164.4.223	*Destination IP address*
LEN=60	*Total length of IP packet in bytes*
TOS=0x00	*Type Of Service, "Type" field. Increasingly being replaced by **DS** and **ECN**. Refer to the IP header info below.*
PREC=0x00	*Type Of Service, "Precedence" field. Increasingly being replaced by **DS** and **ECN**. Refer to the IP header info below.*
TTL=44	*remaining Time To Live is 44 hops.*
ID=31526	*Unique ID for this IP datagram, shared by all fragments if fragmented.*
CE	*Presumably the "ECN CE" flag (Congestion Experienced). This seems to be wrong because according to RFC2481, the CE bit is located in the TOS field. Refer to the IP header info below.*
DF	*"Don't Fragment" flag.*
MF	*"More Fragments following" flag.*
FRAG=179	*Fragment offset in units of "8-bytes". In this case the byte offset for data in this packet is 179*8=1432 bytes.*
OPT (0727..A200)	*Enabled with: **--log-ip-options** IP options. This variable length field is rarely used. Certain IP options, f.e. source routing, are often disallowed by netadmins. Even harmless options like "Record Route" may only be allowed if the transport protocol is ICMP, or not at all.*
PROTO=TCP	*Protocol name or number. Netfilter uses names for TCP, UDP, ICMP, AH and ESP. Other protocols are identified by number. A list is in your /etc/protocols. A complete list is in the file **protocol-numbers***
SPT=4515	*Source port (TCP and UDP). A list of port numbers is in your /etc/services. A complete list is in the file **port-numbers***
DPT=111	*Destination port (TCP and UDP). See SPT above.*
SEQ=1168094040	*Enabled with: **--log-tcp-sequence** Receive Sequence number. By cleverly chosing this number, a cryptographic "cookie" can be implemented while still satisfying TCP*

	protocol requirements. These "SYN-cookies" defeat some types of SYN-flooding DoS attacks and should be enabled on all systems running public TCP servers.echo 1 > /proc/sys/net/ipv4/tcp_syncookies
ACK=0	*Same as the Receive Sequence number, but for the other end of the TCP connection.*
WINDOW=32120	*The TCP Receive Window size. This may be scaled by bit-shifting left by a number of bits specified in the "Window Scale" TCP option. If the host supports ECN, then the TCP Receive Window size will also be controlled by that.*
RES=0x03	*Reserved bits. The ECN flags "**CWR**" and "**ECNE**" will show up in the two least significant bits of this field. Refer to the TCP header info below.*
URG	*Urgent flag. See URGP below.*
ACK	*Acknowledgement flag.*
PSH	*Push flag.*
RST	*RST (Reset) flag.*
SYN	*SYN flag, only exchanged at TCP connection establishment.*
FIN	*FIN flag, only exchanged at TCP disconnection.*
URGP=0	*The Urgent Pointer allows for urgent, "out of band" data transfer. Unfortunately not all protocol implementations agree, so this facility is hardly ever used.*
OPT (020405...300)	*Enabled with: **--log-tcp-options** TCP options. This variable length field gets a lot of use. Important options include: Window Scaling, Selective Acknowledgement and Explicit Congestion Notification. Refer to the TCP header info below.*
	Unfortunately the rule number in the chain which matched the packet is for architectural reasons not available in netfilter logs. You will have to "cook your own" by using the user-prefix feature.

Fonte: http://logi.cc/linux/netfilter-log-format.php3

2.2.2 Reconhecimento das Evidências

Vimos no sub-ítem acima o estudo de 3 serviços e como localizar dados nos mesmos, partiremos agora para a análise de evidências propriamente dita, sabendo onde e como os dados estão localizados, formando um conjunto de dados, chamado de assinatura, que nos permitirão localizar informações úteis dentro e entre o emaranhado de informações dos logs.

Apresenta [REBECCA, 2000]: “Para se automatizar o processo de analise forense é necessário um mecanismo que permita transferir parte do conhecimento do investigador para um sistema automatizado capaz de coletar, identificar e correlacionar evidências. Tal mecanismo pode ser encontrado nos sistemas de detecção de intrusão (*IDS*). A detecção de intrusão utiliza uma série de técnicas (como, por exemplo, *threshold detection*, redes neurais, sistemas especialistas e abordagens baseadas em transição de estados) que permitem “instruir" o *IDS* a reconhecer situações intrusivas”. O MREFCON utiliza-se das melhores práticas de detecção de assinatura de *IDS* (*Intrusion Detection System*) [SNORT] para dar credibilidade ao rastreamento de eventos.

Apresenta [REIS]: “A forense computacional constitui uma instância *post-mortem* de detecção de intrusão, de modo que a assinatura da invasão é representada por um conjunto de evidências correlacionadas que descreve o cenário da intrusão (vulnerabilidades exploradas, ações do invasor, *timeline* dos eventos, origem e finalidade do ataque)”. Já a forense computacional online constitui instâncias *post-mortem* e *real-time*, rastreando e monitorando ao mesmo tempo. E comenta [REIS]: “Nesse sentido, um conjunto de possíveis evidências (vestígios mais prováveis de serem encontrados, como, por exemplo, alterações em arquivos sensíveis), bem como relações entre elas, pode ser definido antecipadamente segundo experiências anteriores do investigador. Essas informações podem ser armazenadas em uma base de dados utilizada por um sistema automatizado capaz de executar as etapas de *information gathering*, busca e correlação de evidências”.

O MREFCON propõe um módulo, chamado de módulo de inteligência, composto pelo tratador de informações, o site de publicação de evidências e o repositório de evidência, mais adiante veremos a arquitetura com maiores detalhes.

É função deste módulo definir as assinaturas que serão utilizadas pelos coletores para reconhecer evidências.

Tecnicamente as assinaturas do modelo são compostas por dois grupos: assinaturas-externas e assinaturas-internas. Assinaturas externas consistem no acoplamento de regras estabelecidas pelas melhores práticas de *software* livre em segurança, ou seja, são inseridas regras de não autoria da agência de inteligência. Assinaturas internas consistem na escrita proprietária pela agência de inteligência e estão normalizadas conforme a tipificação em lei, estudos de casos oficialmente arquivados e através de autorização do judicial. Ou seja, a criação de assinaturas com o intuito de estabelecer um rastreamento personalizado dependerá de aprovação judicial, medida adotada para validar o modelo perante as leis brasileiras e evitar o rastreamento incondicional de informações violando direitos de usuários e provedores.

Veremos agora alguns exemplos dessas assinaturas de reconhecimentos de evidências.

2.2.2.1 Assinatura de Autoria Externa

Assinaturas externas fornecem o conhecimento técnico comprovado para iniciarmos nossos trabalhos. Podemos extrair tais assinaturas de fontes diversas, uma vez que a comunidade de *software* livre [GNU] já possui trabalhos exaustivos referente ao tema de traduzir em assinaturas eventos de segurança da informação. Iremos focar neste primeiro momento nas assinaturas de domínio público dos *softwares* livres: *Snort* [SNORT] e *SpamAssassin* [SPAMA].

O *Snort* é um *software* de detecção de intrusão. Sua função consiste em criar agentes monitoradores de eventos espalhados ao longo de uma rede ou mesmo de uma máquina. Ele identifica em tempo real acontecimentos que podem comprometer a estabilidade de um serviço ou servidor. Sua técnica é baseada nas mesmas coletas de dados que as citadas no subitem 2.2.1.

Em termos de forense computacional podemos classificar o *snort* como uma ferramenta de defesa, servindo para coibir eventos maliciosos. Já para o MREFCON a importância desta ferramenta consistirá em selecionar as assinaturas de eventos

relacionadas às ameaças que procuramos rastrear, por exemplo:

Tabela 6: Algumas assinaturas padrão do snort relacionadas a DDoS

SID	NAME
221	*DDOS TFN Probe*
222	*DDOS tfn2k icmp possible communication*
223	*DDOS Trin00 Daemon to Master PONG message detected*
224	*DDOS Stacheldraht server spoof*
225	*DDOS Stacheldraht gag server response*
226	*DDOS Stacheldraht server response*
227	*DDOS Stacheldraht client spoofworks*
228	*DDOS TFN client command BE*
229	*DDOS Stacheldraht client check skillz*
230	*DDOS shaft client to handler*
231	*DDOS Trin00 Daemon to Master message detected*
232	*DDOS Trin00 Daemon to Master *HELLO* message detected*
233	*DDOS Trin00 Attacker to Master default startup password*
234	*DDOS Trin00 Attacker to Master default password*
235	*DDOS Trin00 Attacker to Master default mdie password*
236	*DDOS Stacheldraht client check gag*
237	*DDOS Trin00 Master to Daemon default password attempt*
221	*DDOS TFN Probe*

Fonte: http://www.snort.org /pub-bin/sigs-search.cgi?sid=ddos

O *SpamAssasin* é um *software* livre *anti-spam*, desenvolvido e mantido pelo grupo *apache* [APACHE], os mesmos do serviço de *http apache*. Sua função consiste em monitorar em tempo real os serviços de *e-mail* com o intuito de coibir a propagação de mensagem não solicitada. Sua técnica é baseada nas mesmas coletas de dados que as citadas no subitem 2.2.1.

Em termos de forense computacional podemos classificar o *spamassassin* como uma ferramenta de defesa, servindo para coibir os eventos maliciosos. Já para

o MREFCON a importância desta ferramenta consiste em selecionar as assinaturas de eventos relacionadas às ameaças que procuramos rastrear, por exemplo:

Tabela 7: Algumas assinaturas padrão do spamassassin relacionadas a spam

SID	NAME
1	*Know non-spam mailers ("ratware")*
2	*Porn tests*
3	*Know spam mailers*
4	*URI tests*
5	*Body phrases tests*
6	*Headers tests*
7	*Scores tests*
8	*Whitlist*
9	*Meta tests*
10	*Html tests*

Fonte: http://spamassassin.apache.org

As assinaturas externas são previamente tratadas e selecionadas no módulo de inteligência. Junção, subtração e adaptação são alguns dos tratamentos realizados sobre estes arquivos. Tecnicamente este tratamento consiste num trabalho de mineração sobre os arquivos de assinaturas externas, baseado em perfis de correlação e requisitos, resultando em um meta-dado aqui denominado de assinatura do modelo.

2.2.2.2 Assinatura de Autoria Interna

Assinaturas de autoria interna visam suprir ou complementar os recursos tecnológicos de rastreamento de evidências. Por exemplo, o problema do *phising scam*, apesar de tipificado em lei, contudo não apresenta uma assinatura técnica de identificação de eventos. As ferramentas em *software* livre que abordam esse

problema, como o *spamassassim*, relatam seu tratamento como sendo causas de um *DDoS* ou uma propagação via *Spam*, ou seja, o *scam* é visto como uma conseqüência e não uma técnica, e se sita dever ser tratado combatendo-se seus dois propagadores.

Dessa forma as assinaturas desenvolvidas pela agência de inteligência devem complementar a ausência de recursos que viabilizem o uso do modelo. Por exemplo: identificar problemas de *phishing scam* rastreando diretórios virtuais (*homepages*) inidôneos, locados em provedores de internet idôneos, que estão pescando internautas através de *spam* ou de adulterações nos serviços de tradução de nomes, *dns*. São exemplos reais desse problema: *Home Banking*, *Sites* de Cartão de Crédito, *Sites* de Comércio Eletrônico, *Sites* de Provedores de Internet.

Apesar de todas as técnicas possíveis para mascarar um *site PHISHING scan* o evento ainda está passível a um rastreamento, independentemente da técnica utiliza para sua propagação. Contudo o modelo não está sendo proposto para monitorar eventos aleatórios e nem operar semelhante aos sistemas de *IDS*, de forma a aprender sozinho. Para entrar em ação o modelo necessita que sejam informados dados para uma investigação, assim como acontece com a perícia real, onde é necessário um ponto de partida, pois estamos periciando um evento como qualquer outro, distinguindo apenas da ferramenta utilizada para tal. Desta forma, rastrear toda a Internet atrás de evidências gerais de crimes, sem ordem judicial, seria desperdiçar recursos e tempo dos peritos, além de gerar questões polêmicas.

Voltemos ao problema de identificação de *sites* adulterados:

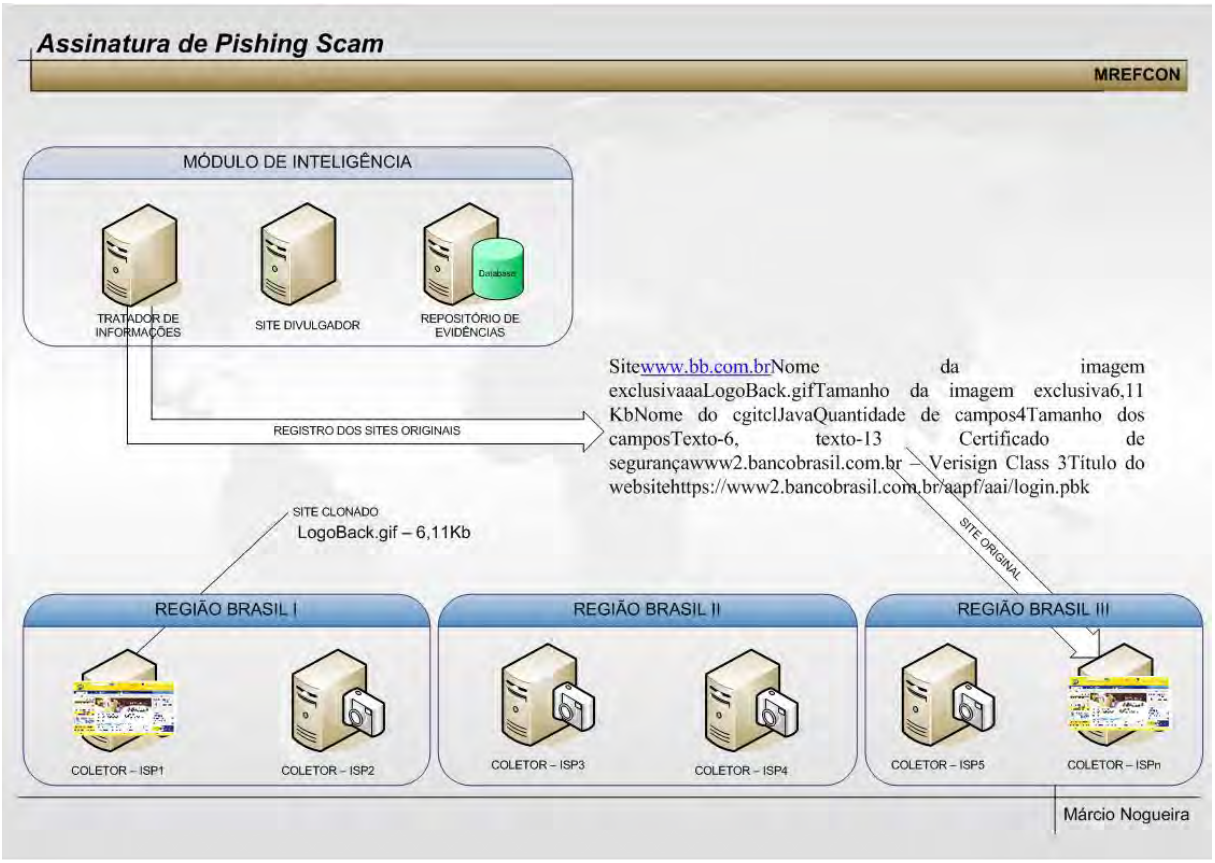


Figura 7 – Assinatura de PHISHING Scam

Observamos que tais eventos se caracterizam por utilizam algum mecanismo de registro de informações, ou *cgi´*s, e uma informação básica que irá dar partida as investigações: o endereço do próprio *site* adulterado.

Tal endereço pode ser fornecido diretamente pela própria vítima, periciado no computador da vitima, rastreado via MREFCON através dos *spams* recebidos pela vítima ou rastreado via MREFCON através de problemas semelhantes, acionados judicialmente, onde o ponto de partida fora estabelecido.

Uma vez identificada a melhor assinatura que corresponde a identificação de um evento o MREFCON realiza o rastreamento nos logs do provedor conveniado. Identificado um possível usuário o modelo termina o rastreamento, se não estabelece comunicação com o próximo coletor apontado pelo evento para continuar o rastreamento recursivo. No capítulo 4 apresentamos algumas aplicações sobre estudos de casos.

2.2.3 Preservação das Evidências Encontradas

Adaptando a apresentação de [SANTOS] quanto à apuração pericial de evidências digitais, temos:

Para garantir que o material apurado através de uma ação pericial não sofra nenhuma alteração ou troca de conteúdo adoutou-se o uso da criptografia como fator de confiabilidade. A criptografia por sua vez, basea-se na função matemática *hash*, que é o método de autenticação pelo qual, através de um algoritmo, atestamos a autenticidade de um documento.

"*Hash*" em inglês significa picar, cortar miúdo, triturar. Essas funções são diferentes das funções normais de encriptação, por não possuírem uma chave. O procedimento da função *hash* é bastante simples, utiliza-se uma função matemática padrão que aceite como parâmetro um documento a ser criptografado. O resultado da função é um cifra na forma de letras e números. A grande vantagem da função *hash* é seu *modus operandi*, onde não é possível a partir do resultado da função chegar aos dados iniciais, ou seja é irreversível [CARVALHO, 2000].

Adotaremos o software SHA, ou mais conhecido como sha1sum, disponibilizado através de licença gnu, e encontrado na maioria dos servidores linux e com versões amplamente distribuídas para os sistemas operacionais mais utilizados, como forma de implementar a função *hash*. Este software adota os conceitos da família de funções hashes *SHA.*

O *SHA* (*Secure Hash Algorithm)*, foi desenvolvido pelo governo dos Estados Unidos, em 1994, para fazer parte do seu *DSS*. Ele foi desenvolvido baseando-se no *MD4*, outro algoritmo de blocos muito utilizado para criptografia, e assim como o *MD5*, sucessor do *MD4*, é mais seguro que o *MD4*. Sua vantagem sobre o *MD5* é um sumário, ou cifra, de 160 *bits* em relação aos 128 *bits* [CARVALHO, 2000].

Para exemplificar sua utilização, iremos utilizar o seguinte: teste.txt, com o seguinte conteúdo: "Teste de criptografia através do *software sha*.".

Para gerar uma assinatura de integridade para o teste.txt utilizamos o *software sha* da seguinte forma:

```
# \usr\bin\sha teste.txt
# 07e660bb bfb4cb85 1aa3367e fa5c4bd6 2c42ea46
```

Como vimos acima após a execução do *software* o programa retorna uma cifra do documento original, tal cifra só é válida para o arquivo em questão.

Vamos supor que haja uma modificação no arquivo original, ficando com o seguinte conteúdo: “Teste de criptografia através do *software sha*”, observem que o ponto ao final da frase foi suprimido. Vejamos agora o resultado da criptografia:

\usr\bin\sha teste.txt

58095d3e 42b2cee0 15f6a7e7 af53b02b 84db94b9

Comparando-se as duas cifras verificamos visivelmente que houve algum tipo de adulteração no documento original.

Os riscos quanto a utilização das funções matemáticas de *hash* é a possibilidade de arquivos diferentes gerarem a mesma cifra, contudo tal possibilidade além de remota é imprevisível.

2.2.4 Correlação das Evidências

Até aqui temos um pacote de assinaturas sendo informado por uma entidade hierarquicamente superior a uma massiva quantidade de receptores. Tais assinaturas serão responsáveis por informar a cada um desses receptores o tipo de dado que deverá ser retornada a fonte. Uma vez apurados todos os dados diversos é hora de correlacionarmos estas evidências a fim de montarmos o cenário do nosso incidente.

Apresenta [MARTINS] quanto ao assunto: “A obtenção de evidências deve ser qualitativamente aceitáveis, que fundamentem o trabalho de forma objetiva. A qualidade das evidências é considerada satisfatória quando reúne as características de suficiência, adequação e pertinência. A suficiência ocorre quando, mediante a aplicação de testes que resultem na obtenção de uma ou várias provas, os dados levam a um grau razoável de convencimento a respeito da realidade ou veracidade dos fatos examinados. A adequação entende-se como tal, quando os testes ou exames realizados são apropriados à natureza e características dos fatos examinados. A pertinência ocorre quando há coerência com as observações, conclusões e recomendações eventualmente formuladas”.

A correlação de evidências no MREFCON está relacionada a funções

matematicamente recursivas, onde ao dar início a uma investigação o sistema só termina ao receber informações de todos os coletores, vejamos em exemplos:

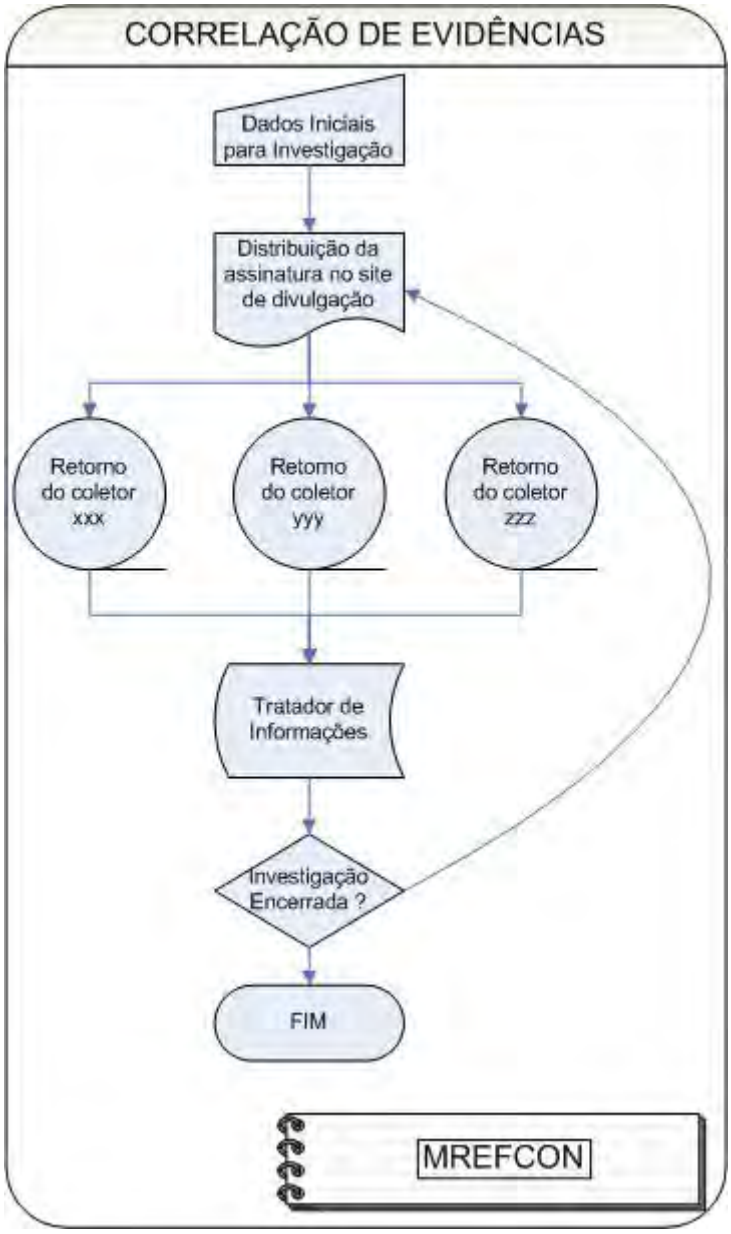


Figura 8 – Correlação de Evidências

1. É iniciado um processo de investigação qualquer

2. Todos os coletores recebem as assinaturas a serem analisadas

3. Havendo qualquer indício de evidência no coletor o mesmo reportará ao *site* de divulgação as informações investigadas

4. Analisando as evidências de um determinado coletor, se forem suficientes

para determinar um único usuário de forma distinta então a investigação está encerrada. Caso aponte para outros *sites* o tratador de informações correlaciona os coletores associados aos próximos *sites* e reinicia a investigação até alcançar o *status* de encerrado. Caso aponte para mais de um usuário apresenta uma informação de que os dados para investigação foram insuficientes, apresenta a relação de suspeitos e questiona se deseja refinar a investigação ou monitorar os suspeitos. Caso o sistema entre no modo de monitoração o encerramento se dará por prazo, suficiência das provas ou encerramento do caso através de uma segunda investigação conclusiva.

Para determinar o grau de suficiência dos dados elaboramos um processo em camadas determinando níveis de correlação:

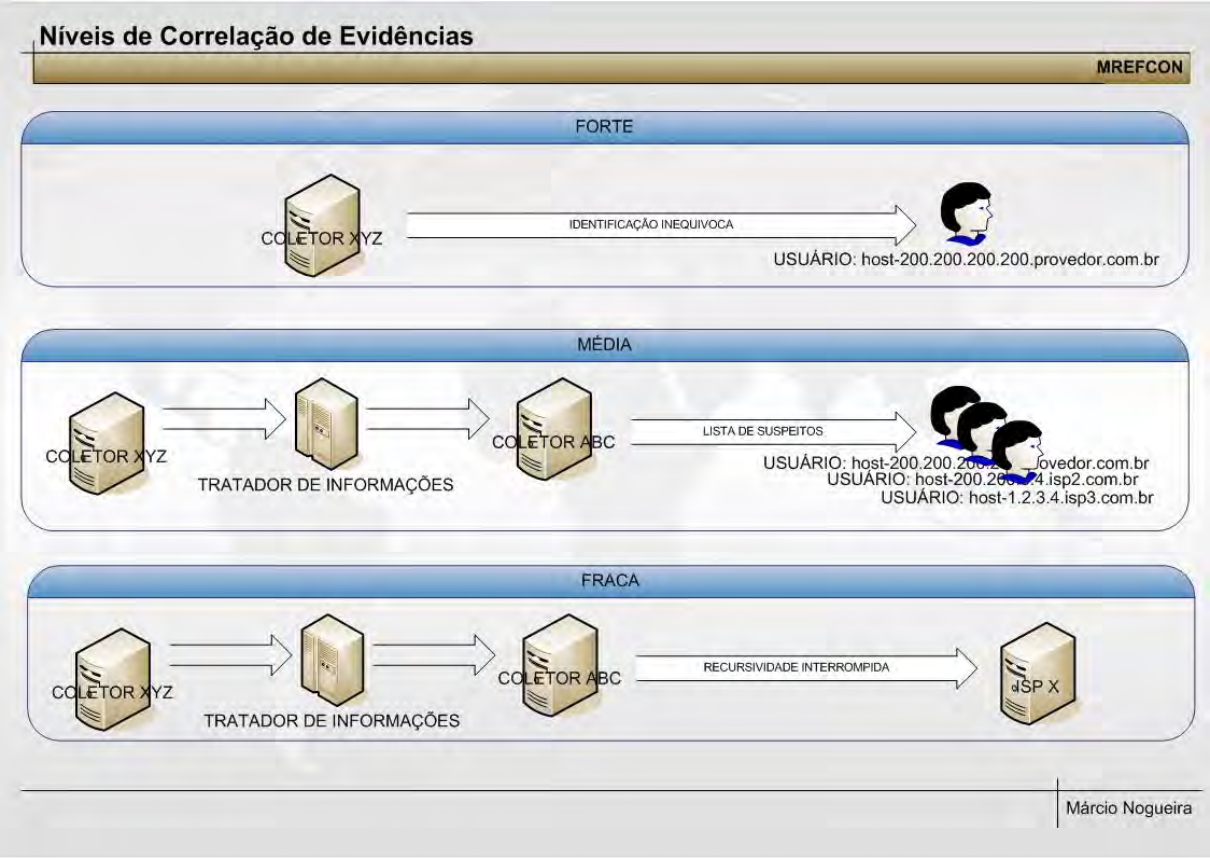


Figura 9 – Níveis de Correlação de Evidências

O nível forte determina com precisão e inequivocadamente a localização do transgressor. O nível médio, por sua vez, não consegue concluir com precisão a investigação, retornando uma lista de possíveis suspeitos que através de outros tipos de perícia precisarão ser analisados. O nível fraco indica que a investigação foi

interrompida por não haver recursos para a investigação eletrônica, normalmente ocasionada pela presença de um provedor não conveniado ao projeto do MREFCON. Tal investigação poderá ter continuidade mediante a instalação do MREFCON por parte do provedor identificado ou mesmo sendo informado os dados recolhidos por perícia física no mesmo.

O modelo encerra sua investigação uma vez que alcança o nível forte ou que por exaustão não consegue alcança-lo. Uma investigação é dita conclusiva quando alcança o nível forte, médio ou fraco, quando nenhum desses níveis é alcançado o modelo retorna a informação de que os dados iniciais foram insuficientes para a investigação.

2.2.5 Reconstrução de Eventos

A reconstrução dos eventos está relacionada a todos os dados coletados e correlacionados de uma investigação, apontando acontecimentos realizados antes, durante e após o evento. Em determinados casos a reconstrução é insuficiente para provar algum delito, sendo necessário acionar uma monitoração de eventos sobre determinada lista de suspeitos para indicar ou correlacionar com nível forte o verdadeiro transgressor.

Tecnicamente a reconstrução só é possível mediante um sincronismo de horário entre todos os coletores envolvidos e o sistema principal, do contrário haveria ambigüidade e incertezas a respeito do evento.

A assinatura inicial da investigação muitas vezes também será insuficiente para determinar todos os eventos associados a um determinado suspeito. Dessa forma, uma investigação poderá demandar uma quantidade razoável de interações até obter todos os dados necessários. Utilizando o mesmo algoritmo de correlação de evidências, vejamos um exemplo mais complexo para demonstrar o grau de aprofundamento suportado pelo modelo:

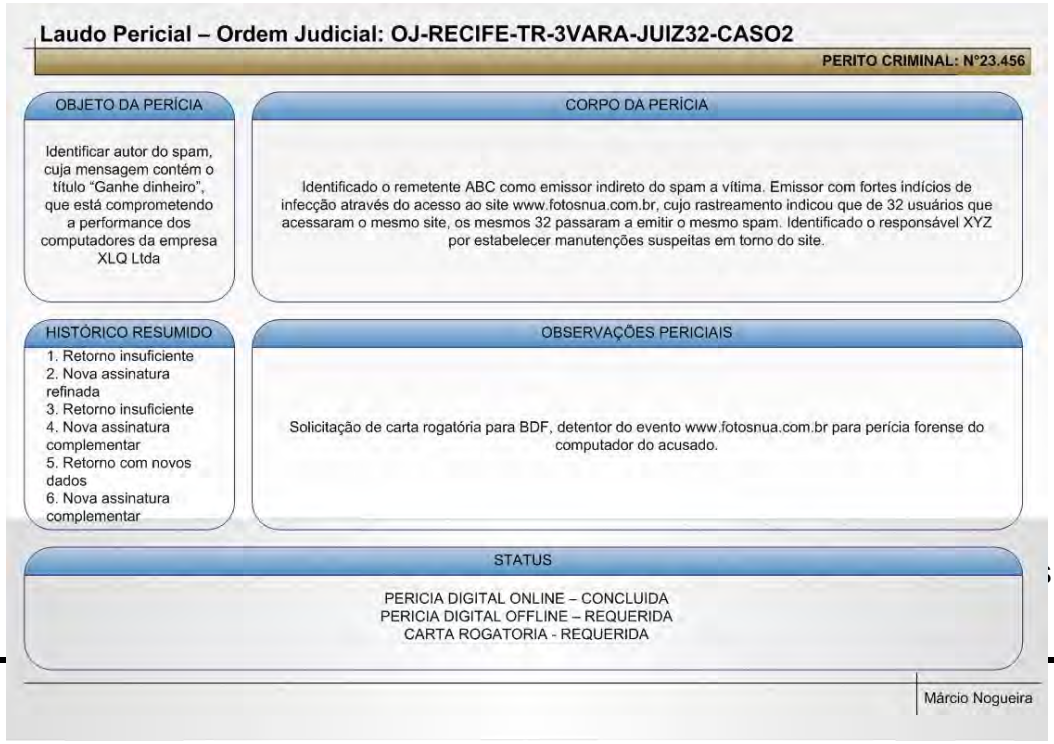
Tabela 8: Exemplo da reconstrução de um evento do tipo spam

PASSO	AÇÂO	DESCRIÇÃO

1	Assinatura	Identificar autor de spam cujo título do e-mail seja “Ganhe dinheiro”
2	Retorno	6.432 coletores registram usuários remetendo mensagens com esse título
3	Nova assinatura refinada	Identificar o primeiro autor de spam cujo título do e-mail seja “Ganhe dinheiro”
4	Retorno	Em 12-2-2003, as 15:20:34 usuário 200.200.200.23 remeteu mensagem com o referido título
5	Nova assinatura complementar	Analisar histórico de comportamento do usuário 200.200.200.23 em 12-2-2003
6	Retorno	Registrado no coletor “X” o horário da conexão de 15:13:20 – 12-2-2003 até 16:50:45 – 12-2-2003; acessou os seguintes sites: www.porn.com; www.google.com.br, www.bol.com.br; comunicou-se com os seguintes serviços: ftp, www, smtp; realizou cronologicamente as seguintes ações na Internet: www.bol.com.br/webmail.exe?login=fulano, www.google.com.br/search?”fotos”&”nua”; www.fotosnua.com.br; ftp://200.65.34.12; telnet www.site1.com.br smtp – mailto: fulano@site1.com.br; telnet www.site2.com.br smtp – mailto:fulano@site2.com.br ; telnet ... ; telnet www.siteN.com.br smtp – mailto:fulano@siteN.com.br; Registrado no coletor “Y”, detentor do evento “ftp://200.65.34.12” , as seguintes atividades para 200.200.200.23: user:jashd, cmd: cd\klasd\asdasd\ooer, get: .$$; Registrado no coletor “Y”, detentor do evento “telnet www.site1.com.br smtp – mailto:fulano@site1.com.br”, tamanho do e-mail: 34k, remetente: no-replay@site1.com.br, attached: sorte.pif; ... ; registrado no coletor “N”, detentor do evento “telnet www.siteN.com.br smtp – mailto:fulano@siteN.com.br”, tamanho do e-mail: 34k,

		remetente: no-replay@siteN.com.br, attached: sorte.pif
7	Nova assinatura complementar	Analisar comportamento e histórico do site www.fotosnua.com.br
8	Retorno	Coletor “W”, detentor do evento www.fotosnua.com.br, relata: data de criação 01-01-2003, ultimas 5 atualizações: 01-01-2003, as 12:34:23 por 200.199.5.1, 01-01-2003, as 16:29:21 por 200.199.5.75, 02-01-2003, as 14:23:21 por 200.199.5.32; Usuários que acessaram este site: 200.143.5.34, 200.5.3.67, 200.4.6.23, ..., 200.123.234.234
9	Nova assinatura complementar	Analisar evento “ftp://get:.$$” por parte dos usuários 200.143.5.34, 200.5.3.67, 200.4.6.23, ..., 200.123.234.234
10	Retorno	32 usuários responderam a assinatura
11	Nova assinatura complementar	correlacionar sites semelhantes acessados pelos usuários: 200.143.5.34, 200.5.3.67, 200.4.6.23, ..., 200.123.234.234, quando data de acesso = horário do evento “ftp://get:.$$ “
12	Retorno	32 usuários = www.fotosnua.com.br, 19 usuários = www.google.com.br

Finalmente o relatório de conclusão da investigação:



2.3 Validação das Evidências

Vimos no subitem 2.2.3, sobre preservação de evidências, que o algoritmo de blocos de dados *SHA* é utilizado para implementação da função matemática *hash*, responsável por autenticar as evidências rastreadas pelos coletores. Essa função compõe um dos elementos principais dentro do tema de certificação digital. Veremos agora como o estado-da-arte da criptografia pode ser utilizado para a implementação do MREFCON, integrando todas as entidades envolvidas pela segurança da Internet.

2.3.1 Criptografia

O MREFCON utiliza uma combinação das melhores práticas das chaves simétrica, assimétricas e da função autenticadora *hash*, promovendo níveis de assinaturas seguras das evidências em cada etapa do processo de forense: coleta, validação, correlação, reconstrução e transporte. Além de canais de comunicação seguros entre todos os módulos do sistema.

A imagem a seguir ilustra um resumo dos níveis de segurança proposto pelo MREFCON para validação de todo o processo de investigação digital:

Figura 11 – Níveis de Criptografia do MREFCON

Observamos a presença de 5 níveis onde cada um se distingue pela técnica de criptografia adotada. Na primeira camada de coleta, estaremos utilizando o *software sha1sum* como ferramenta de criptografia do tipo *hash* e o *software pgp*, a fim de assinar digitalmente o arquivo contendo os dados apurados. Na segunda camada de transporte, estaremos utilizando por padrão o conceito de *vpn*, utilizando para isso o pacote de *softwares isakmp*, *ah*, *esp* e *ipsec*, e *httpproxy* e *redir* como contingência. Na terceira camada de reconhecimento, teremos o trabalho inverso ao realizado na segunda camada, onde iremos traduzir as informações recebidas, os *softwares* utilizados são os mesmos. Na quarta camada de reconstrução, é gerado um novo arquivo, com as mesmas técnicas da segunda camada, mas contendo o relatório pericial. Na última camada de armazenamento, as informações táticas decorridas em todo o processo são catalogadas e fechadas num único diretório, que por sua vez será compactado e criptografado baseado nas mesmas técnicas da função *hash,* onde teremos no final de todo o processo um banco de dados com registros criptografados com chaves públicas e privadas.

2.3.2 Assinatura Digital

Adaptando de [CARVALHO, 2000]: As assinaturas digitais, ou eletrônicas, são feitas para que uma entidade possa, digitalmente, “assinar” um documento. Apresentando as mesmas características de uma assinatura real:

- Fácil de produzir para quem assina
- Fácil de verificar por qualquer um
- Muito difícil de ser falsificada
- Tenha uma vida útil apropriada (de modo que quem assine não possa negar ter assinado)

E que proporcione as seguintes características:

- Confidencialidade
- Integridade
- Não-repudiação

Utilizaremos os *softwares* livres *GnuPG* e *Wget*, num ambiente linux, para exemplificar a utilização da criptografia sobre a ótica dos coletores.

O *GNU PRIVACY GUARD, GnuPG*, é uma completa e livre reposição ao *PGP*. Devido não utilizar o algoritmo patenteado *IDEA*, ele pode ser utilizado sem nenhuma restrição, modificado e distribuído conforme os termos da *GNU – General Public License* [GNU]. *GnuPG* é um aplicativo compatível com a *RFC2440* (*OpenPGP*), http://www.gnupg.org.

O *GNU Wget* é um programa não interativo para buscar arquivos da rede. Já incluído por padrão na maioria dos sistemas linux.

Vejamos agora o exemplo:

1. Assinatura de investigação disponibilizada no *site*: “Identificar origem do evento de *DDoS* que está impedindo que o *site* www.livrariaimportante.com.br opere normalmente, cuja característica inicial é sua distribuição em forma de anexo virótico por *e-mail*. Ordem Judicial 19.345, Tribunal Regional de Pernambuco, 8° Vara Civil, Comarca 4. Perito registrado n° 8746362. Média urgência na perícia. Data de acontecimento do evento em 23/03/2005, data de publicação da assinatura em 27/03/2005. Rastrear informações desde 01/01/2005. Pesquisar regiões Norte, Nordeste, e Centro-Oeste”. Importante observar que neste ponto do trabalho ainda

estamos escrevendo a assinatura do evento na forma por extensa para facilitar a compreensão, veremos mais adiante na modelagem que as assinaturas serão escritas de forma técnica, obedecendo a campos tabelados.

2. Os coletores baixam a informação do site:

Observamos aqui a utilização do *software wget* para baixar do *site* www.sitedistribuidor.com.br/<dia>/assinaturas.txt. O arquivo foi recebido com sucesso.

3. O arquivo baixado encontra-se criptografado com a chave privada do *site*, iremos utilizar a chave pública, que já se encontra no próprio coletor, para descriptografar a mensagem:

Figura 13 – Exemplo de descriptografia das assinaturas de evidência

4. O coletor analisa a assinatura, executa a solicitação, compacta a evidência e gera a autenticação do arquivo:

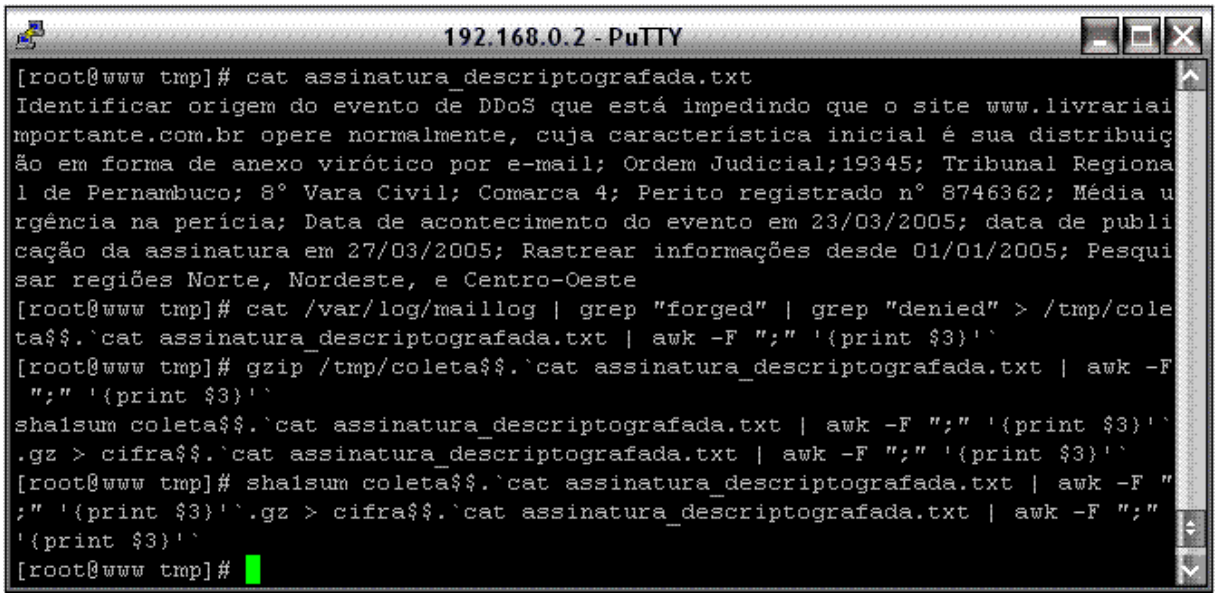


Figura 14 – Exemplo de geração da autenticação da evidência

5. A cifra da autenticação armazenada no arquivo é criptografada utilizando-se uma chave privada, única para cada coletor.

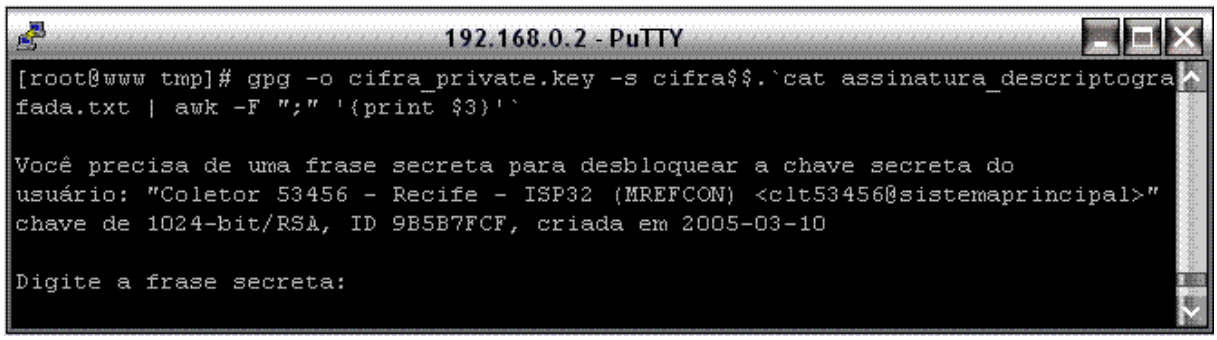


Figura 15 – Exemplo do arquivo contendo o valor de autenticação

6. O arquivo contento a evidência rastreada é criptografado utilizando-se uma chave simétrica randômica, que é muito mais rápida de ser gerada além de consumir recursos mínimos da máquina:

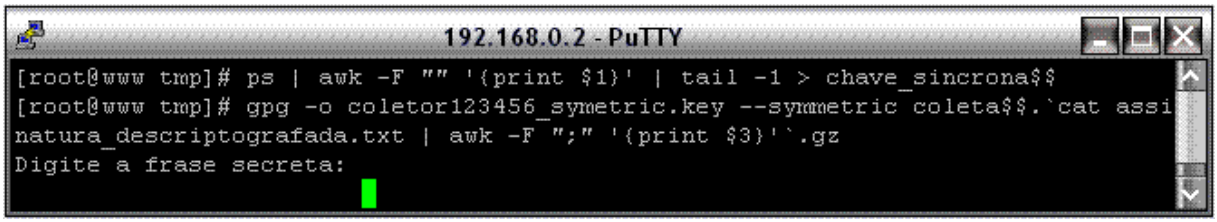


Figura 16 – Exemplo de utilização da chave simétrica aleatória

7. Realizaremos agora a criptografia da chave simétrica, utilizando a chave pública do sistema principal, utilizada para criptografar a evidência:

8. Juntaremos todos os arquivos gerados para formar um único arquivo de transmissão:

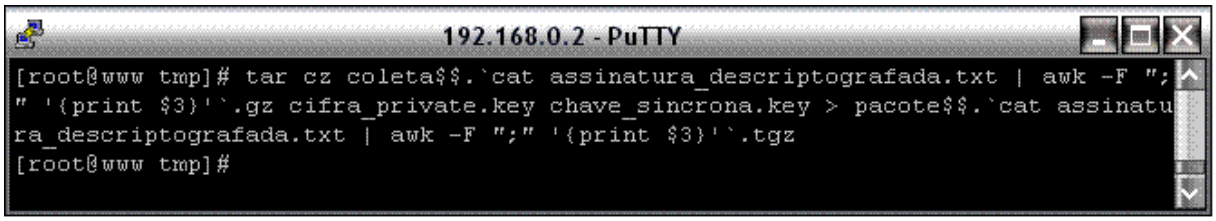


Figura 18 – Exemplo de geração do pacote final por coletor

9. Finalmente enviaremos o arquivo gerado para o devido tratamento junto à agência de inteligência. Para isso o seguinte comando será utilizado: wget www.siteprincipal.com.br/mrefcon.cgi --post-file=pacote$$.`cat assinatura_descriptografada.txt | awk –F “;” ‘{print $3}’`.tgz

Vimos em exemplos o funcionamento da camada de coleta, utilizando técnicas de criptografia *hash* para gerar um pacote inadulterável e chaves públicas e privadas para garantir a confidencialidade sobre o receptor e o transmissor. Na próxima sessão apresentaremos os detalhes do funcionamento do esquema de certificação digital, a fim de validar as chaves públicas e privadas de forma que não fiquem em posse de uma única entidade privada.

2.3.3 Certificação Digital

Vimos no subitem anterior exemplos práticos de como aplicar uma assinatura digital nos coletores atendendo aos critérios de confidencialidade, integridade e não-repudiação. Veremos agora como aplicar os mesmos conceitos ampliando para o

sistema principal.

Um certificado é um documento digital contendo informações de identificação e uma chave pública. Em geral, os certificados têm um formato comum, normalmente baseados no padrão *ITU-T X.509*. Mas ainda não podemos ter certeza de que o certificado é genuíno e não é falso. Uma forma de descobrir isso é utilizar autoridades de certificação ou *CAs* [CRIPTY].

Uma autoridade de certificação assina certificados de chave pública digitalmente. Ao assinar um certificado, a *CA* garante sua validade. No entanto um problema persiste: como a chave pública da *CA* é distribuída? Também existem muitas estratégias para esse problema. Em uma delas, se a *CA* for muito conhecida, como é o caso do serviço postal americano, ele poderá divulgar amplamente sua chave pública. Outro método seria que a *CA* tivesse seu próprio certificado assinado por outra *CA*, também conhecida pelo destinatário. Essa idéia de encadeamento de certificação pode avançar ainda mais, com várias *CA* organizadas em uma hierarquia onde cada *CA* subordinada valida sua assinatura com a assinatura de uma *CA* mais alta na hierarquia. Obviamente, as *CA* de nível mais alto deverão reverter para o método de divulgação direta [CRIPTY].

A nível nacional a *CA* de mais alto nível corresponde a AC-Raiz da ICP-Brasil. Este certificado contém a chave pública correspondente à chave privada da AC Raiz, utilizada para assinar o seu próprio certificado, os certificados das AC de nível imediatamente subseqüente ao seu e sua LCR (Lista de Certificados Revogados) [ICP, 2001].

Além das *CA* temos as autoridades de registro, AR, cuja função é credenciar novas AC sobre sua hierarquia.

Quanto a autoridades de registro, AR, do ICP-Brasil: a atividade de identificação e cadastramento das AC de nível imediatamente subseqüente ao da AC Raiz será realizada junto com o processo de credenciamento, não havendo Autoridades de Registro, AR, no âmbito da AC Raiz da ICP-Brasil. Os certificados emitidos pela AC Raiz da ICP-Brasil têm como titulares a própria AC Raiz ou as AC de nível imediatamente subseqüente ao seu.

A utilização de certificados pelo MREFCON segue em moldes a resolução n° 21.740, instrução n° 85, classe 12° de Brasília [RESOLUCAO21740], que dispõe sobre a assinatura digital dos programas fontes e programas executáveis que

compõem os sistemas informatizados das eleições 2004, sobre sua conferência e a dos dados das urnas eletrônicas, onde:

Art. 4º Os programas referidos no art. 1º desta instrução serão assinados digitalmente pelos representantes da Justiça Eleitoral, por meio de programa de propriedade do Tribunal Superior Eleitoral, cujos códigos e mecanismos poderão ser auditados na oportunidade prevista no § 1º do art. 16 da Instrução nº 79 e deverão seguir, no que cabível, a regulamentação expedida pelo Comitê Gestor da Infra-estrutura de chaves Públicas Brasileira (ICP-Brasil).

§ 1º As chaves privadas e públicas que serão utilizadas pela Justiça Eleitoral serão geradas pelo Tribunal Superior Eleitoral.

§ 2º As chaves privadas serão geradas sempre pelo próprio titular e serão de seu exclusivo controle, uso e conhecimento.

O formato ténico do certificado utilizado pelo MREFCON segue as recomendações do próprio ICP-Brasil, em sua resolução n° 1, onde:

7.2 Perfil de Certificado da AC de nível subseqüente ao da AC Raiz

O formato de todos os certificados emitidos pela AC Raiz está em conformidade com o padrão ITU X.509 ou ISO/IEC 9594.

O certificado da AC de nível subseqüente ao da AC Raiz é assinado pela AC Raiz, e possui validade de no máximo 5 (cinco) anos, podendo este prazo ser revisto de acordo com as definições estabelecidas pelo CG da ICP Brasil.

Número(s) de versão

O certificado da AC de nível imediatamente subseqüente ao da AC Raiz implementa a versão 3 de certificado do padrão ITU X.509.

Extensões de certificado

O certificado da AC de nível imediatamente subseqüente ao da AC Raiz pode implementar quaisquer das extensões previstas na versão 3 do padrão ITU X.509.

Identificadores de algoritmo

O certificado de AC de nível subseqüente ao da AC Raiz é assinado com o uso do algoritmo RSA com o SHA-1 como função *Hash*, conforme o padrão PKCS#1.

Veremos mais adiante na arquitetura do MREFCON que está previsto uma camada intermediária entre o sistema principal e os coletores, chamado de Sistema de Certificação Digital Federal, que consiste em:

Entidade Divulgadora AR: Responsável por credenciar os coletores.

Entidade Certificadora AC: Responsável por validar os certificados.

Repositório de Certificados: Local seguro de armazenamento dos AR

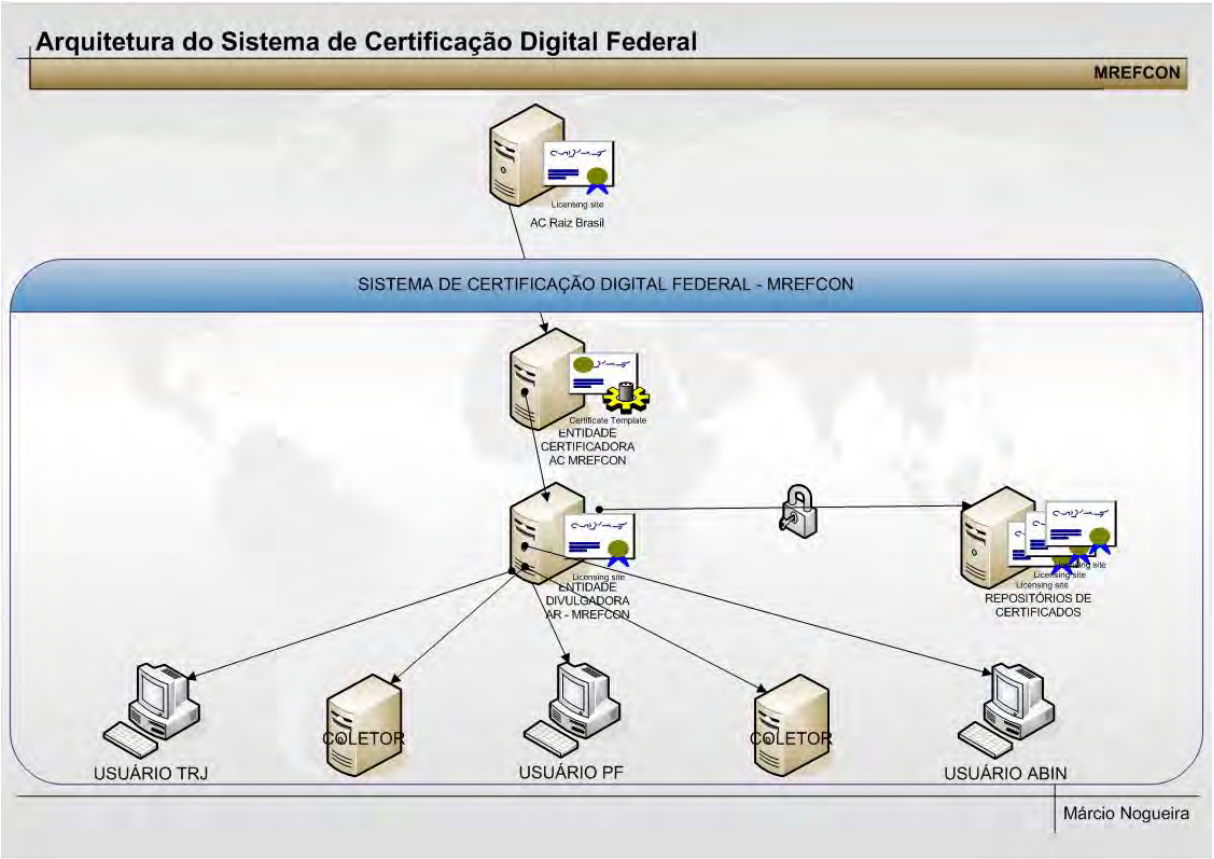


Figura 19 – Arquitetura do Sistema de Certificação Digital Federal do MREFCON

2.3.4 Transporte Seguro de Evidências

Adaptamos dos artigos de [ARQIPSEC, 1999] e [IPSECVPN, 1998] para:

A idéia de utilizar uma rede pública como a Internet em vez de linhas privativas para implementar redes corporativas é denominada de *Virtual Private Network* (*VPN*) ou Rede Privada Virtual [ORTIS, 2003]. As VPN são túneis de criptografia entre pontos autorizados, criados através da Internet ou outras redes públicas e/ou privadas para transferência de informações, de modo seguro, entre redes corporativas ou usuários remotos.

A segurança é a primeira e mais importante função da *VPN*. Uma vez que dados privados serão transmitidos pela Internet, que é um meio de transmissão inseguro, eles devem ser protegidos de forma a não permitir que sejam modificados ou interceptados.

Outro serviço oferecido pelas *VPN* é a conexão entre corporações (*Extranets*) através da Internet, além de possibilitar conexões discadas criptografadas que podem ser muito úteis para usuários móveis ou remotos, bem como filiais distantes de uma empresa.

Uma das grandes vantagens decorrentes do uso das *VPN* é a redução de custos com comunicações corporativas, pois elimina a necessidade de *links* dedicados de longa distância que podem ser substituídos pela Internet. As *LAN* podem, através de *links* dedicados ou discados, conectar-se a algum provedor de acesso local e interligar-se a outras *LAN*, possibilitando o fluxo de dados através da Internet. Esta solução pode ser bastante interessante sob o ponto de vista econômico, sobretudo nos casos em que enlaces internacionais ou nacionais de longa distância estão envolvidos. Outro fator que simplifica a operacionalização da *WAN* é que a conexão *LAN-Internet-LAN* fica parcialmente a cargo dos provedores de acesso.

São características da *VPN* que atendem o MREFCON:

- Verificação da identidade do usuário, restringindo o acesso às pessoas autorizadas. Dispondo de mecanismos de auditoria, provendo informações referentes aos acessos efetuados - quem acessou, o quê e quando foi acessado.
- O endereço do cliente na sua rede privada não é divulgado, adotando-se endereços fictícios e estáticos para o tráfego externo.
- Os dados trafegam na rede pública ou privada num formato cifrado e, caso sejam interceptados por usuários não autorizados, não são decodificados, garantindo a privacidade da informação. O reconhecimento do conteúdo das mensagens deve ser exclusivo dos usuários autorizados.
- O uso de chaves garante a segurança das mensagens criptografadas funcionando como um segredo compartilhado exclusivamente entre as partes envolvidas. O gerenciamento garante a troca periódica das

mesmas, visando manter a comunicação de forma segura.

- O suporte a diversidade de protocolos garante que o modelo seja expansível a uma solução proprietária

As redes virtuais privadas baseiam-se na tecnologia de tunelamento cuja existência é anterior às *VPN*. Ele pode ser definido como processo de encapsular um protocolo dentro de outro. O uso do tunelamento nas *VPN* incorpora um novo componente a esta técnica: antes de encapsular o pacote que será transportado, este é criptografado de forma a ficar ilegível caso seja interceptado durante o seu transporte. O pacote criptografado e encapsulado viaja através da Internet até alcançar seu destino onde é desencapsulado e decriptografado, retornando ao seu formato original. Uma característica importante é que pacotes de um determinado protocolo podem ser encapsulados em pacotes de protocolos diferentes. Por exemplo, pacotes de protocolo *IPX* podem ser encapsulados e transportados dentro de pacotes *TCP/IP*.

Dentro das características técnicas de *VPN* apresentaremos a seguir as que descrevem o MREFCON:

- Protocolo aberto de tunelamento nível 3 – Rede – (*IP* sobre *IP*), *IPSEC* da *IETF* (*Internet Engineering Task Force*), que compõe parte dos protocolos que servem a plataforma aberta da *IP Security Mode,* conforme a *RFC* 2411, do que define:
- Autenticação mútua de usuários entre as duas extremidades do túnel através do protocolo *EAP* (*Extensible Authentication Protocol*), que utiliza os *softwares AH* (*Authentication Header*), *RFC* 2402, para provê integridade e autenticação de cabeçalhos *IP*, utilizando o algorítimo de criptografia *HMAC-SHA-1*, *RFC* 2404.
- Confidencialidade garantida para que apenas usuários autorizados entendam o conteúdo transportado, utilizando o *software ESP* (*Encapsulation Security Payload*), *RFC* 2406, que também utilizam o algorítimo de criptografia *HMAC-SHA-1*.
- Utiliza a autenticação através de chave pública durante a negociação de parâmetro feito pelos *softwares ISAKMP* (*Internet Security Association and Key Management Protocol*), *RFC* 2408, *IKE* (*Internet*

Key Exchange)*, RFC* 2409, e *OAKLEY*, *RFC* 2412.

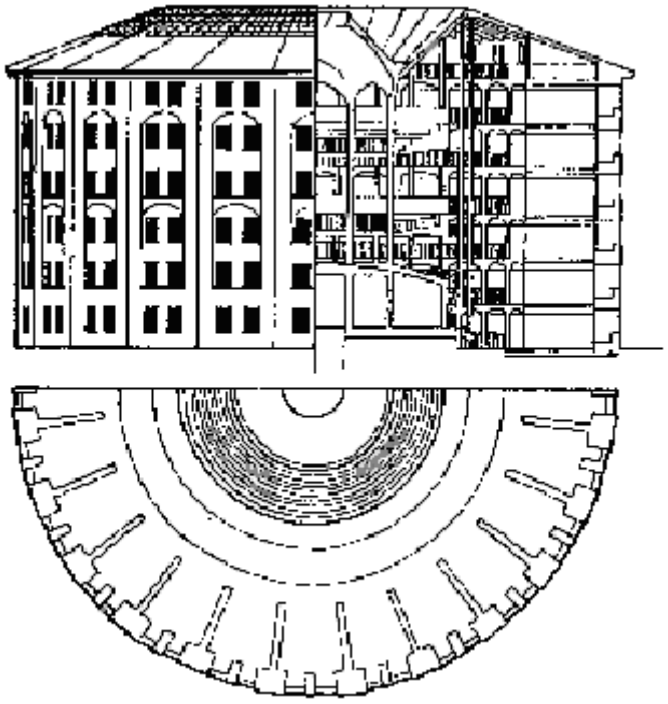
- Endereçamento estático requerido antes da inicialização do túnel
- Compressão de dados através do *IP*, definido pelo *IETF*, *RFC* 2393.
- A criptografia de dados *RSA* é executado durante a faze do *ISAKMP*
- O gerenciamento de chaves é estabelecido pelo *ISAKMP*, negociando inicialmente uma chave comum e periodicamente realizando atualizações.
- Túneis voluntários são criados sempre que um coletor precisa remeter as evidências, através de um software cliente de vpn.
- Suporte a conexões discadas.

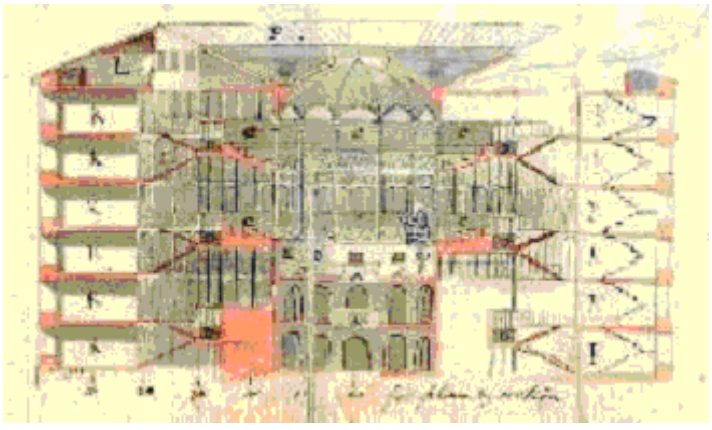
Além dessas características, o modelo prevê ainda um sistema de contigência no modo de transporte, de forma que havendo quaisquer restrições técnicas nos provedores de internet referente a utilização dos túneis do *ipsec* que um pacote de ferramentas alteranativas seja possível de estabelecer a comunicação e garantir a segurança das informações. Inicialmente foram testadas as ferramentas *httpproxy* e *redir*, que funcionam criando túneis virtuais tanto sobre a aplicação *http* quanto demais aplicações que tiverem acesso a Internet.

Essas ferramentas de contingências, apesar de possuírem um bom nível de segurança, contudo são ferramentas que exigem maiores consumos computacionais das máquinas virtuais, dando vez ao conjunto de ferramentas *ipsec*.

Capítulo 3 Arquitetura para Rastreamento das Evidências

O Trabalho de [KAMINSKY, 2003] apresenta uma idéia conceitual sobre vigilância constante, onde: Bentham desenvolveu, em 1787, uma idéia de prisão – a qual chamou de pan-óptica – onde as celas são dispostas em um círculo e a parte interna de cada cela, voltada para dentro do círculo, é feita de vidro. A torre de guarda é colocada no centro do círculo, de onde cada cela pode ser inteiramente observada. O efeito, naturalmente, não é duplo: os prisioneiros não podem ver o guarda na torre.





A prisão pan-óptica funcionaria como uma máquina de vigilância permanente. Sua arquitetura garantiria que nenhum prisioneiro pudesse ver o "inspetor" que efetuasse a vigilância a partir da localização central privilegiada. O prisioneiro nunca poderia saber se efetivamente estava ou não sendo vigiado – e essa incerteza mental seria suficiente para manter a disciplina, na medida em que o prisioneiro, acreditando na possibilidade de estar sendo vigiado, ajustaria seu comportamento.

Evidentemente, a coleta de informações por governos, agências governamentais e corporações privadas não representa um fenômeno novo, pois já existe há muito tempo. A diferença que a era tecnológica traz pode ser resumida em cinco fatores: a maior quantidade de informações disponíveis, os diversos tipos de informações disponíveis, a enorme facilidade e maior escala de intercâmbio de informações, os efeitos potencializados de informações errôneas e a duração perpétua dos registros.

Aparentemente, essa coleta desenfreada de informações não se assemelha tanto à prisão pan-óptica sugerida por Bentham, já que não há uma única instituição privada ou um único governo controlando tais informações. Geralmente, dados de uma determinada espécie são mantidos em cadastros separados de dados de outras categorias, o que cria a ilusão de que o monitoramento, ainda que constante, não é centralizado.

No entanto, ainda que as informações sejam coletadas por instituições diversas e de forma fragmentada, a tecnologia atual permite a combinação de todos estes dados. Notadamente no setor privado, o cruzamento de dados é largamente utilizado, possibilitando conhecer todo o perfil de um determinado indivíduo.

Em nosso país, excetuando-se os preceitos do artigo 43 do Código de Defesa do Consumidor, que regula os bancos de dados e cadastros de consumidores, e a proteção constitucional genérica do "*habeas data*" prevista no artigo 5.º, inciso LXII, não há praticamente legislação que controle a criação de bancos de dados, o que dá margens a criação de sistemas de monitoramento inconstitucionais.

O MREFCON é baseado em leis concretas e ferramentas que dão apoio tecnológico efetivo, sem segundos caminhos, para a validação de evidências forenses online. A arquitetura proposta, tema principal deste capítulo apresenta um sistema computacional, restrito em determinados pontos chaves, para prevalescer a constitucionalidade em detrimento das técnicas de programação de computadores.

O objetivo da arquitetura é a construção de um sistema de monitoramento constante e em tempo-real. Com analogia a prisão pan-óptica sendo um monitoramento obscuro, onde o observado conhece a presença do observador, mas não interage diretamente com o mesmo. Apesar dessa característica de “ilusão” é proposta uma arquitetura de *software* colaborativa mediada por computador, onde os resultados e os próprios termos da investigação, mesmo que acionados remotamente, são apresentados para os responsáveis legais do provedor de internet investigado, não sendo possível a divulgação dos dados para técnicos ou especialistas do mesmo.

A figura a seguir resume o esquema geral proposto:

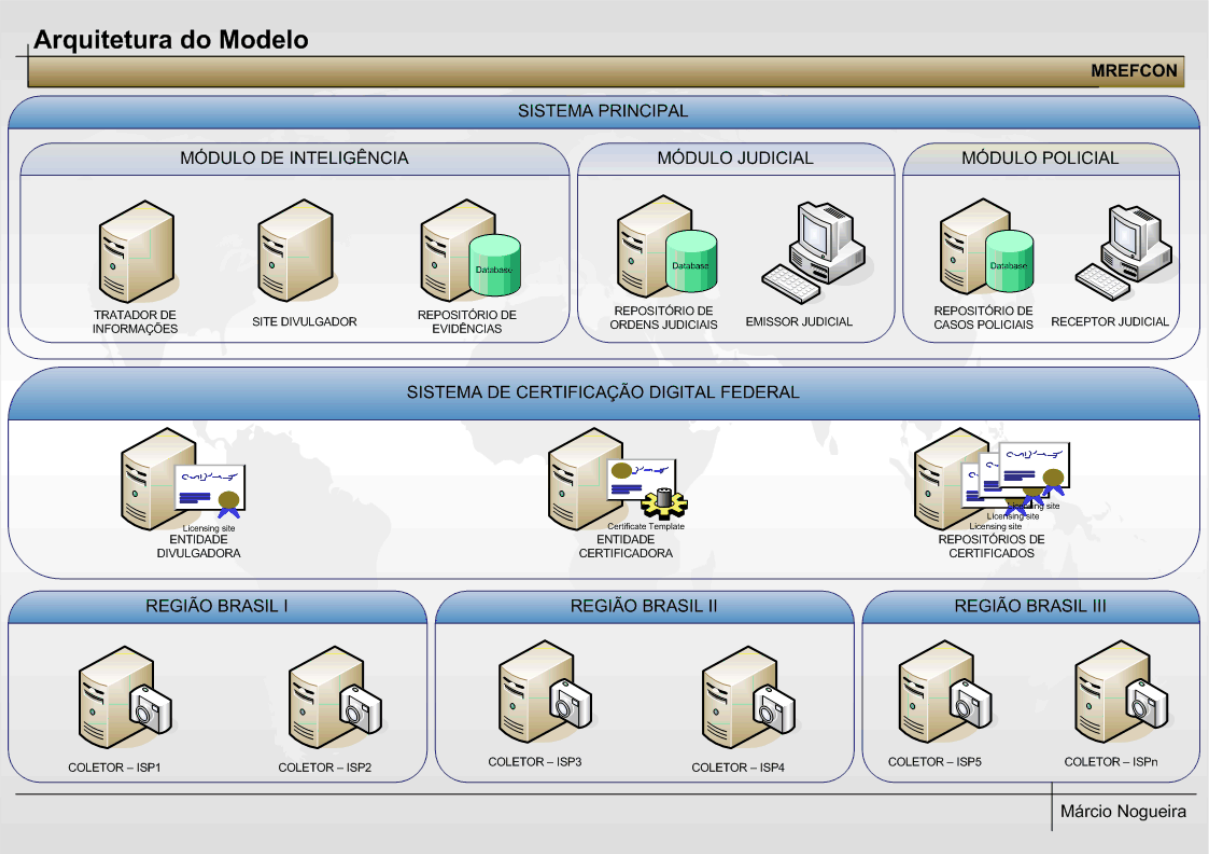


Figura 20 – Arquitetura do MREFCON

Onde observamos a existência de trêis níveis principais: o sistema principal, o sistema de certificação digital e o conjunto de coletores agrupados por regiões federais. Sobre o sistema de certificação digital, já apresentado com detalhes no sub-ítem 2.3, resumimos como sendo uma camada de transporte das informações coletadas, tratadas e finalizadas, e tendo como característica principal o uso da

criptografia em todas as suas fases. Responsável por estabelecer e manter toda a parte de confidencialidade, não-repudio e integridade das mensagens trocadas, valida de forma constitucional as evidências apuradas nos coletores e o armazenamento e tratamento das mesmas junto ao sistema principal. Veremos os detalhes das próximas duas camadas, responsáveis pela coleta propriamente dita, o tratamento dos apurados até a reconstrução e armazenamento de um caso judicial.

3.1 Dos Agentes Coletores

Os objetivos dos coletores são:

- Garantir a integridade das informações apurada pelos logs dos provedores;
- Estabelecer e manter o canal de comunicação entre o provedor de internet e o sistema principal;
- Sincronizar os horários das informações transientes nos provedores com o relógio do sistema principal;
- Registrar e reportar as informações transitórias nos logs dos provedores conforme a assinatura de evento requisitada pelo sistema principal;
- Ser elemento, ou serviço, de baixo consumo de recursos computacionais, prevalecendo todas as demais atividades do servidor de internet sobre a necessidade de uma investigação, salvo critérios.

Quanto a sua constituição os coletores são uns pacotes de ferramentas em código livre, que possibilitam a extração transparente dos dados, apresentando seu consumo real dos recursos computacionais, porém não sendo passível de interação direta ou indireta com operadores do servidor. Ferramentas caracterizadas pelo tipo de operação em linha de comando, processadas em modo “*batch*” (várias linhas de comando num único arquivo, onde a resposta de uma linha é utilizada como parâmetro para a próxima), ausência de documentação de uso, versões personalizadas para

o uso do modelo, configurações pré-determinadas e com insuficiência para alterações. Tais características visam diminuir ao máximo possível as interações com operadores ou administradores dos servidores de Internet, ao mesmo tempo em que garante a possibilidade de acompanhamento da utilização de recursos e o próprio documento jurídico para o responsável legal pelo provedor.

Os agentes coletores possuem forte analogia com os sistemas de detecção de intrusos, conhecidos como *IDS* [SORT], de *Intrusion Detection Systems*. Os *IDS* visam à monitoração em tempo real de recursos computacionais a fim de determinar novas assinaturas maliciosas ou de alertar mediante a presença de uma assinatura já conhecida. Porém muito mais restrito em seu conceito por trabalhar unicamente na detecção de assinaturas disponibilizadas por um servidor central e não possuir recursos inteligentes autônomos para elaboração de novas fontes de informações. Tal característica visa transferir toda carga de processamento de dados dos agentes coletores para o sistema principal, além de garantir ao provedor de internet, parceiro colaborador do modelo, que não terá recursos demasiados ocupados por serviços não relevantes a sua atividade.

3.1.1 Características Técnicas

Dividimos as características técnicas dos coletores nos seguintes grupos: Integridade, Comunicação, Sincronização, Extração e Correlação de Dados, Disponibilidade e Priorização.

Em integridade apresentaremos a base de funcionamento dos coletores, do pacote de softwares e da lógica de integração dos aplicativos.

Em comunicação apresentaremos as diversas formas de estabelecimento de canais de troca de informações, prevendo adversidades e dispondo de contingências.

Em sincronização apresentaremos a forma de manter uma configuração de

data e hora para toda a rede de coletores.

Em extração e correlação apresentaremos as formas que os coletores irão extrair, armazenar, correlacionar e por último enviar os dados para o sistema principal.

Finalmente em disponibilização e priorização apresentaremos a forma técnica em que os coletores irão operar. Consumindo o mínimo de recursos possíveis dos servidores, baseado em padrões pré-estabelecidos, e garantindo disponibilidade absoluta em relação ao fornecimento de informações para o sistema principal.

3.1.1.1 Integridade

Os arquivos de logs apresentam uma vulnerabilidade evidente: fragilidade. Pelo fato de serem armazenados localmente no próprio sistema do servidor, uma intrusão em nível de acesso ao sistema operacional acarreta na adulteração ou exclusão dos mesmos. Tal ameaça é ainda mais comprometedora visto que *softwares* de invasão já automatizam esta atividade sem interagir com o intrusor. A solução empregada para erradicar tais ameaças, conceito básico dos sistemas de detecção de intrusão é através do conceito de *loghost*.

O *loghost* é um servidor de rede, exclusivo em receber e armazenar registros de logs de todos os demais servidores e estações de trabalho da rede. Sua segurança deve ser garantida adotando-se medidas simples de segurança, como: atualização periódica do sistema operacional, ausência de contas de acesso remota e *firewall* configurado para receber unicamente informações do serviço de logs, bloqueando todos os demais tráfegos.

No MREFCON, para alcançarmos o mesmo grau de segurança e integridade dos *loghosts* nos baseamos nos seguintes *softwares*:

- Um emulador, ou máquina virtual, que é um *software* capaz de criar uma segunda instância totalmente distinta da primeira em termos de sistema operacional. Ou seja, é possível ter dois sistemas operacionais funcionando simultaneamente totalmente distintos entre si, tanto em desempenho quanto em funcionalidade. Através deste segundo sistema operacional estaremos garantindo que o servidor local

continue a armazenar suas informações e que cópias dessas informações sejam enviadas via rede de computadores para um segundo computador, no nosso caso emulado pelo *software*, onde tal sistema é totalmente inviolável baseado nos preceitos de *loghost*. Na prática este tipo de *software* divide os recursos computacionais, de forma a atender os dois sistemas operacionais. Estaremos utilizando uma configuração onde o máximo de consumo de processador não ultrapasse em 10% do total, e memória *ram* fixa em 4Mb. Tal *software* é utilizado para evitar que o servidor onde os logs estejam sendo armazenados sofra qualquer tipo de invasão comprometendo a integridade das informações. Este *software* é o Xen, http://www.cl.cam.ac.uk/Research/SRG/netos/xen/, baseado em código livre [GNU], plataforma linux e operação em linha de comando (*batch*).

- Uma imagem de um sistema operacional desenvolvida exclusivamente para o modelo MREFCON. Uma imagem é um arquivo, geralmente com extensão ".iso", semelhante aos arquivos compactados, mas que possui na verdade uma cópia fiel de um *cd-rom* ou disquete. Geralmente empregada para realizar múltiplas cópias de *cd-rom* ou disquete. Tal imagem possui uma versão compacta e reduzida de um sistema operacional linux, servindo como parâmetro para o *software* emulador. Onde o mesmo irá emular esta imagem na memória e a partir de então teremos dois sistemas operacionais funcionando na mesma máquina. Para a criação da imagem estaremos utilizando o *software BYLD*, http://byld.sourceforge.net, baseado em *software* livre e com código fonte distribuído. Como modelo e ponto de partida para a criação da imagem estaremos utilizando o código fonte da distribuição linux em disquete da *Trinux*, http://www.trinux.org, conhecida como a melhor mini-distribuição linux em disquete para segurança da informação, onde estaremos personalizando e mantendo o seguinte conjunto de ferramentas:

Tabela 9: Pacote de Ferramentas do Coletor

AÇÂO	DESCRIÇÃO
ngrep.tgz	aplica expressões regulares sobre tráfego de rede
arping.tgz	envia ARP e/ou ICMP para verificar se um host/interface está ativo
snort.tgz	IDS para leitura de assinaturas do sistema principal
desproof.tgz	ferramenta para detectar pacotes falsos
hping2.tgz	verifica se o sistema principal está disponível
irpas.tgz	para verificar o sistema principal mesmo estando atrás de um firewall
nasl.tgz	outro leitor de assinaturas complementar ao snor
httptunl.tgz	cria túneis virtuais para tráfego tcp sobre http
nconvert.tgz	facilita a comunicação entre computadores
redir.tgz	mudança dinâmica das configurações de rede do provedor de internet
tunnel.tgz	ferramenta de criação de túneis virtuais entre coletor e sistema principal
dropbear.tgz	um servidor ssh2 com criptografia
gnupg.tgz	envio de mensagens baseado em chaves públicas e privadas
ncrypt.tgz	ferramenta de criptografia de arquivos
openssh.tgz	cliente para servidores ssh
ssldump.tgz	um analisador de conteúdo criptografado SSL
stunnel.tgz	cria túneis virtuais baseado em certificados
openssl.tgz	cria certificados e realiza todas as criptografias conhecidas
zebedee.tgz	contingência de serviços de criptografia
frgroutr.tgz	fragmenta os pacotes para evitar congestionamentos de rede
zodiac.tgz	ultrapassar os limites dos servidores de dns do provedor de internet
sentinel.tgz	evitar que o tráfego entre coletor e sistema principal seja monitorado
hunt.tgz	f evita técnicas de ludibriação do coletor em relação ao sistema principal, como ARP Spoofing, TCP Session Hijacking e sniffers
curl.tgz	um cliente web que suporta downloads através de http, ftp e https
netconf.tgz	pacote clássico de configuração de rede
bind.tgz	servidor cache dns para uso interno
echoping.tgz	análise, medição e controle do fluxo de dados a serem transmitidos
perlbin.tgz	personalizar ações do sistema operacional do coletor
phpcgi.tgz	personalizar ações do coletor para o sistema principal

Ext2tools.tgz	para operar no sistema de arquivos linux
netfilter.tgz	módulos do kernel para firelwall
iptables.tgz	firewall específico do kernel
linux-fs.tgz	para operar outros sistemas de arquivos linux
sysutil.tgz	ferramenta que monitora o estatus do sistema operacional
kernel-2.4.tgz	Mini Kernel 2.4 para aplicações em disquete
Apt-get.tgz	para atualizações automáticas do sistema
xntpd.tgz	cliente de configuração de hora e data, extra ao pacote original do trinux
logwatch.tgz	tratador de logs
syslogd.tgz	pacote extra para prover um servidor de registro de logs – *loghost*

3.1.1.2 Comunicação

A comunicação dos coletores está subdividida em dois grupos: a comunicação da máquina virtual com o servidor de internet e a comunicação da máquina virtual com a Internet.

No primeiro grupo temos a problemática de como a máquina virtual, que se trata de um segundo sistema operacional, irá se comunicar com o servidor de internet para receber os dados dos logs. Em resposta a esta questão utilizaremos a configuração de *TCP/IP* do próprio *software* da máquina virtual, onde o novo sistema operacional irá emular uma nova placa de rede configurada para operar no modo ponto-a-ponto com o servidor de internet, ou seja, equivalendo a uma comunicação do tipo computador-a-computador, onde a ligação física é estabelecida através de um cabo entre os dois computadores. Nas configurações do *TCP/IP* utilizaremos a configuração privada universal de rede 127.0.0.x/255.255.255.0, ou seja, a comunicação será tratada no nível de *loopback*, um modo de configuração que não permite que outros computadores, mesmo conectados ao servidor de internet, possam se comunicar com a máquina virtual. A figura a seguir resume o explanado:

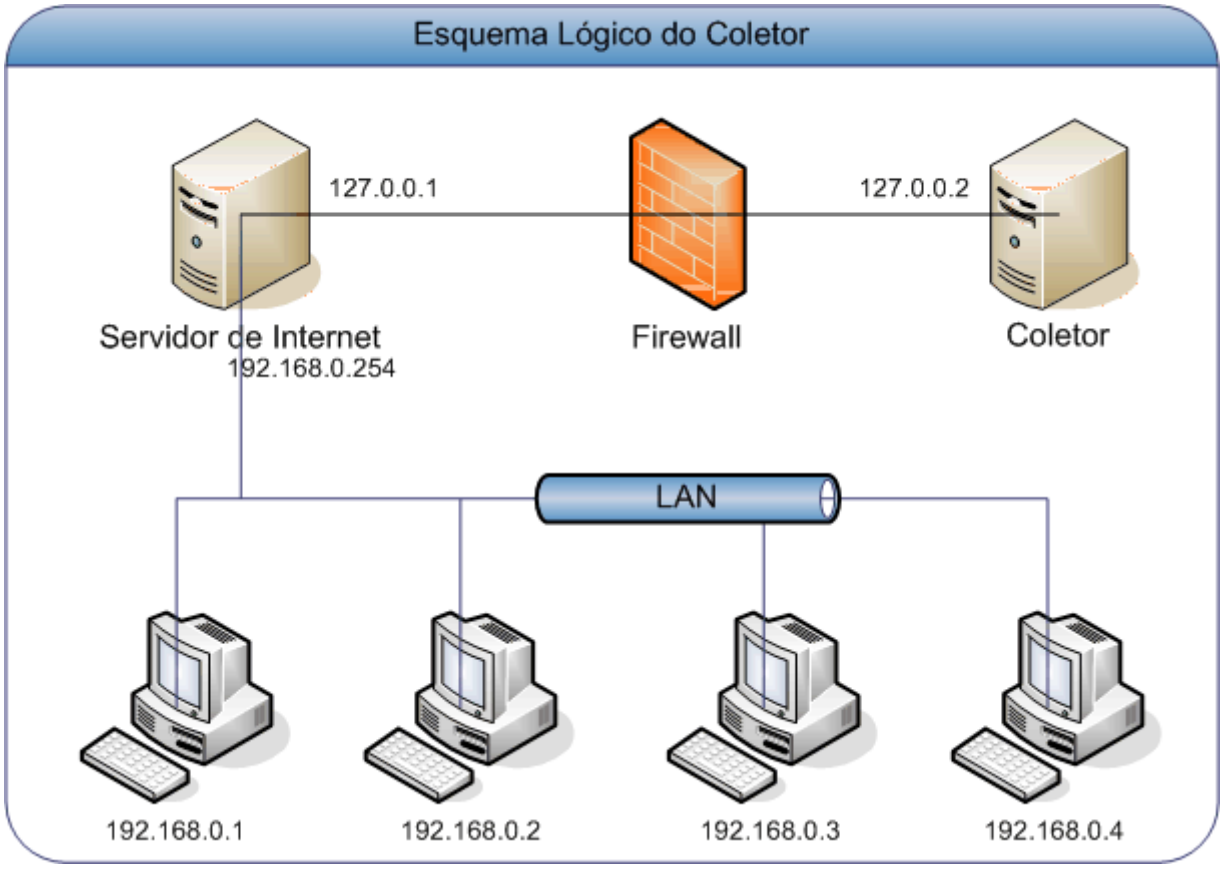


Figura 21 – Esquema Lógico dos Coletores

No segundo grupo temos a problemática de como a máquina virtual irá se comunicar com a Internet. Para isso voltaremos a utilizar as opções do próprio *software* de máquina virtual com algumas configurações extra. Inicialmente habilitaremos a opção de *NAT*, uma característica técnica que permite que o tráfego de uma rede seja transportado para outra – *Network Address Translation*. O *NAT* será habilitado na interface de rede do servidor de Internet que mantém contato com a máquina virtual, no nosso caso a interface de *IP* 127.0.0.1. Feito isso todo o tráfego de dados que saia da máquina virtual em direção a Internet será redirecionado para a placa de rede do servidor de Internet que possui comunicação direta com a Internet. Como extra, tratamos a questão do servidor de Internet possuir um *firewall* habilitado. Nesse caso será acrescentada automaticamente, necessitando ou não, uma linha de configuração no *firewall* do servidor que permita a passagem do tráfego da máquina virtual para a Internet. Em sua versão inicial os coletores estarão preparados para habilitar automaticamente os servidores de

Internet linux que operarem com as seguintes ferramentas de *firewall*: *iptables*, *ipchains* e *ipfwd*. A figura a seguir resume o explanado:

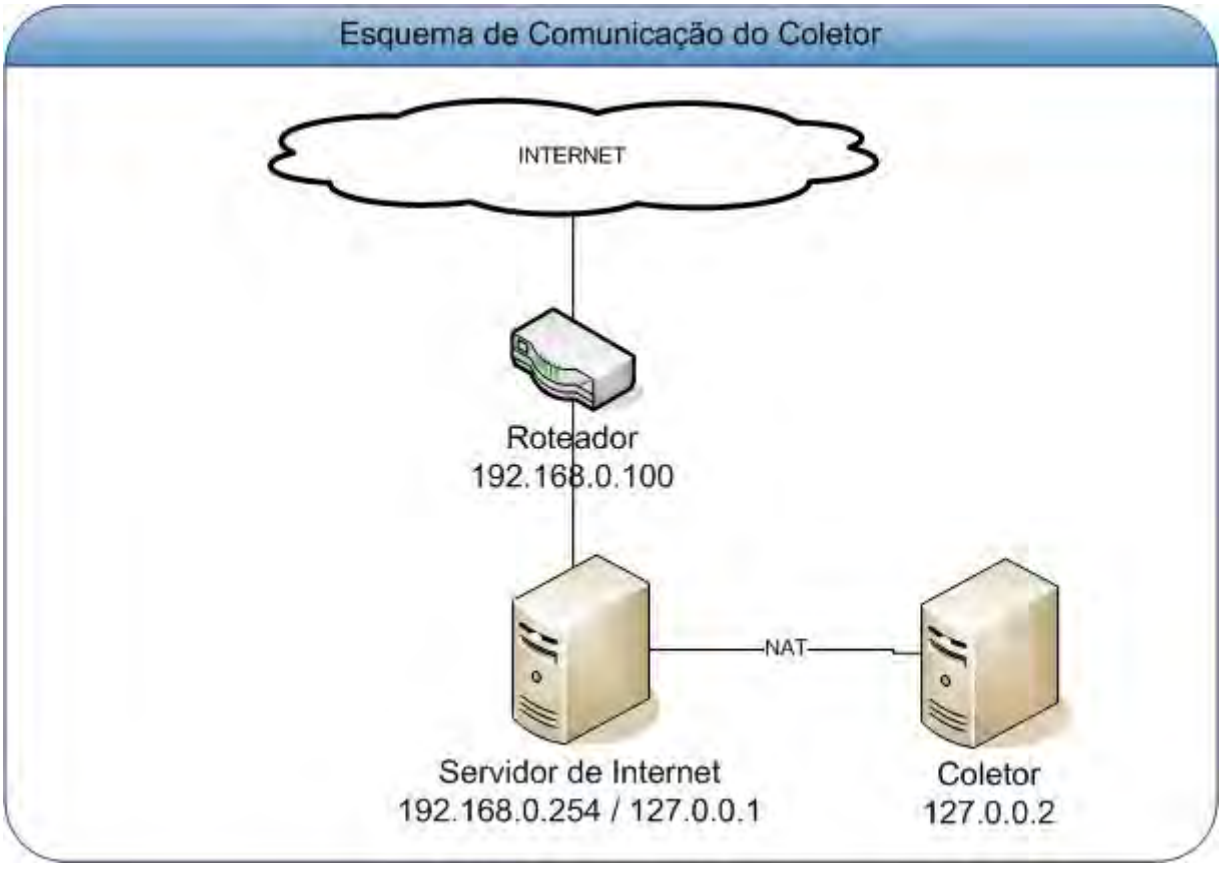


Figura 22 – Esquema de Comunicação dos Coletores

Apresentaremos agora as diversas formas de criação de canais de comunicação entre os coletores e o sistema principal, utilizando para isso técnicas de criação de túneis virtuais criptografados, conhecidos basicamente pela nomenclatura técnica de *VPN* [ORTIS, 2003]. Tais canais serão criados a partir de ferramentas distintas, a depender unicamente do tipo de canal disponível no servidor. Tais ferramentas serão apresentadas em ordem de prioridade, previamente configurado nos coletores, onde o não estabelecimento de comunicação por uma ferramenta implica em nova tentativa através da ferramenta seguinte da lista.

- httptunl.tgz – cria túneis virtuais para tráfego *tcp* sobre *http*;
- nconvert.tgz – facilita a comunicação entre computadores;
- redir.tgz – possibilita a mudança dinâmica das configurações de rede do provedor de internet sem que comprometa a

comunicação do coletor;

- tunnel.tgz – ferramenta de criação dos túneis virtuais de comunicação entre o coletor e o sistema principal;
- stunnel.tgz – cria túneis virtuais baseado em certificados;

E por último os aplicativos responsáveis por determinar qual a ferramenta de criptografia e criação dos canais virtuais será empregada:

- irpas.tgz – para verificar o sistema principal mesmo estando atrás de um firewall;
- arping.tgz – envia *ARP* e/ou *ICMP* para verificar se um *host*/interface está ativo;
- hping2.tgz – verifica se o sistema principal está disponível;

3.1.1.3 Sincronização

A sincronização é a chave de funcionamento do coletor. Havendo falhas e ou ausência de comunicação entre o coletor e o sistema principal a transmissão dos dados é suspensa ou interrompida.

A sincronização é a primeira ação realizada após o estabelecimento da comunicação. Sendo repetida a cada evento de transmissão de informações do coletor para o sistema principal. Tal medida visa garantir que os dados enviados estejam no mesmo formato de data e hora que toda a rede de coletores.

A ferramenta utilizada para a sincronização é um cliente de servidor de tempo universal, distribuído na forma de código aberto, que compõe o pacote de *softwares* na imagem emulada pela máquina virtual, chamado *xntpd*, http://www.ntp.org.

Uma segunda primícia em relação à sincronização é a questão da autenticação. Independente do tipo de canal virtual estabelecido na fase da comunicação o coletor necessitará validar sua chave pública com o sistema principal a fim de estabelecer os parâmetros de sincronização. A figura a seguir resume a explanação:

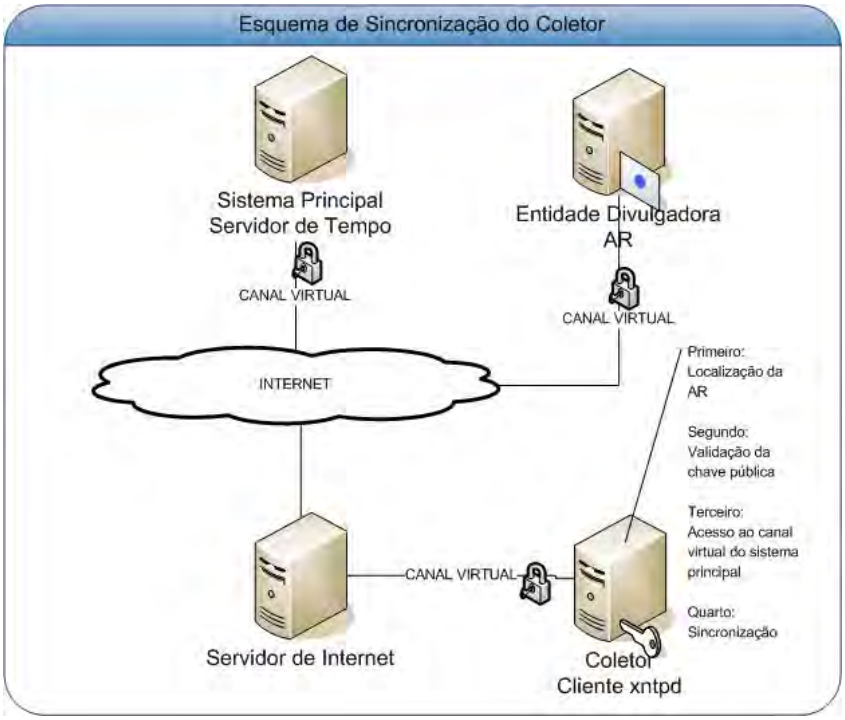


Figura 23 – Esquema de Sincronização dos Coletores

Observa-se no esquema acima a criação dos canais virtuais através da fase de comunicação, contudo, o coletor só terá acesso a realizar a sincronização de horários caso esteja com o seu certificado em dia, ou seja, o coletor precisa estar registrado na rede MREFCON para funcionar. Uma segunda característica observada é a constante necessidade de sincronização entre o coletor e o sistema principal, reforçando critérios rígidos de segurança, onde o coletor precisa estar registrado na rede para poder realizar qualquer ação.

Esse rígido esquema de sincronização garante que as partes envolvidas troquem constantemente informações de autenticação, validação e certificação o que garante a legitimidade dos coletores, ausência de chaves furtadas, coletores comprometidos e riscos de invasão na rede. Associada a esta política tem-se a troca dinâmica das chaves públicas e privadas dos coletores, acrescentando uma última camada de segurança no critério de não-repudio das informações.

3.1.1.4 Extração e Correlação de Dados

Uma vez estabelecida e validada a comunicação é hora de ativarmos as ferramentas que justificam a presença do coletor, são elas: *syslogd*, o servidor de logs que irá receber todas as informações necessárias para a extração, e o *wget*, utilitário responsável por importar as assinaturas disponibilizadas no sistema principal e exportar os dados correlacionados da extração.

O *syslogd* irá atuar no coletor como o único serviço de rede disponível no sistema operacional. Nessa fase a configuração deste serviço será de receber toda e qualquer informação e direcioná-las para a ferramenta de tratamento *logwatch*.

Através de uma versão aprimorada para o MREFCON da ferramenta *logwatch* é garantido que não haja desperdício de espaço em disco rígido, sejam registradas apenas informações úteis às análises e que o histórico de eventos sejam catalogado de forma econômica. Essa integração de ferramentas possibilita que o coletor extraia volumosas quantidades de dados do servidor de Internet e resuma-as para a correlação. Em termos estatísticos tem-se alcançado o percentual de compactação de todos os dados extraídos para a ordem de 10% em resumos para correlação, ou seja, a cada 10*Mbytes* extraídos pelo coletor apenas 1*Mbyte* é arquivado. A figura a seguir resume o esquema geral da ferramenta *logwatch*:

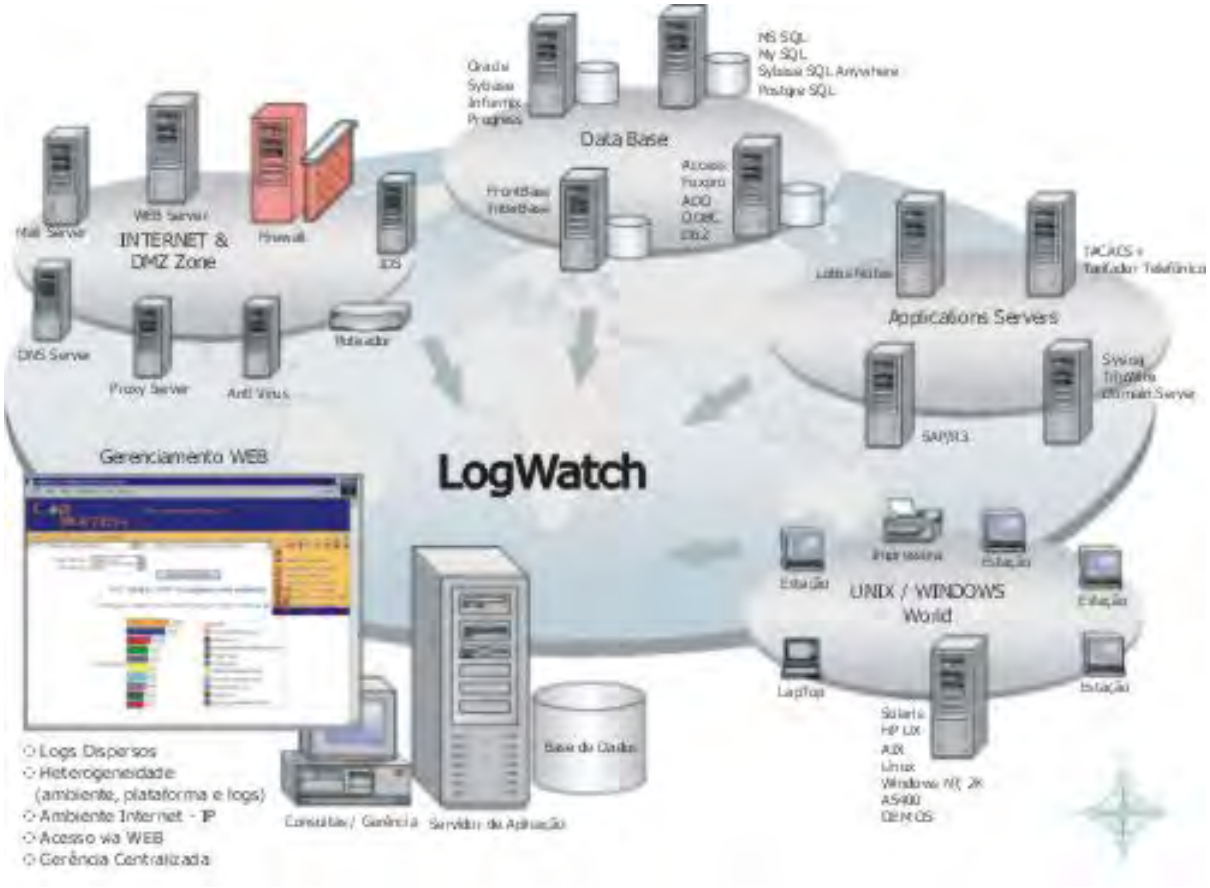


Figura 24 – Esquema Tradicional do LogWatch
http://www.3elos.com.br/produtos/logwatch/descricao.php

Ainda assim é bastante crítico a disponibilização do coletor para um provedor de internet cujo espaço em disco seja a essência do negócio, onde podemos levantar um cenário de extração na ordem de 1*Gbyte* de informações por dia, o que implicaria na necessidade de consumo de 100*Mbytes* de espaço em disco, inviabilizando o modelo MREFCON.

Para erradicar essa ameaça ao modelo aprimoramos o esquema de extração de dados incluindo fases de extração, a figura a seguir apresenta o novo esquema:

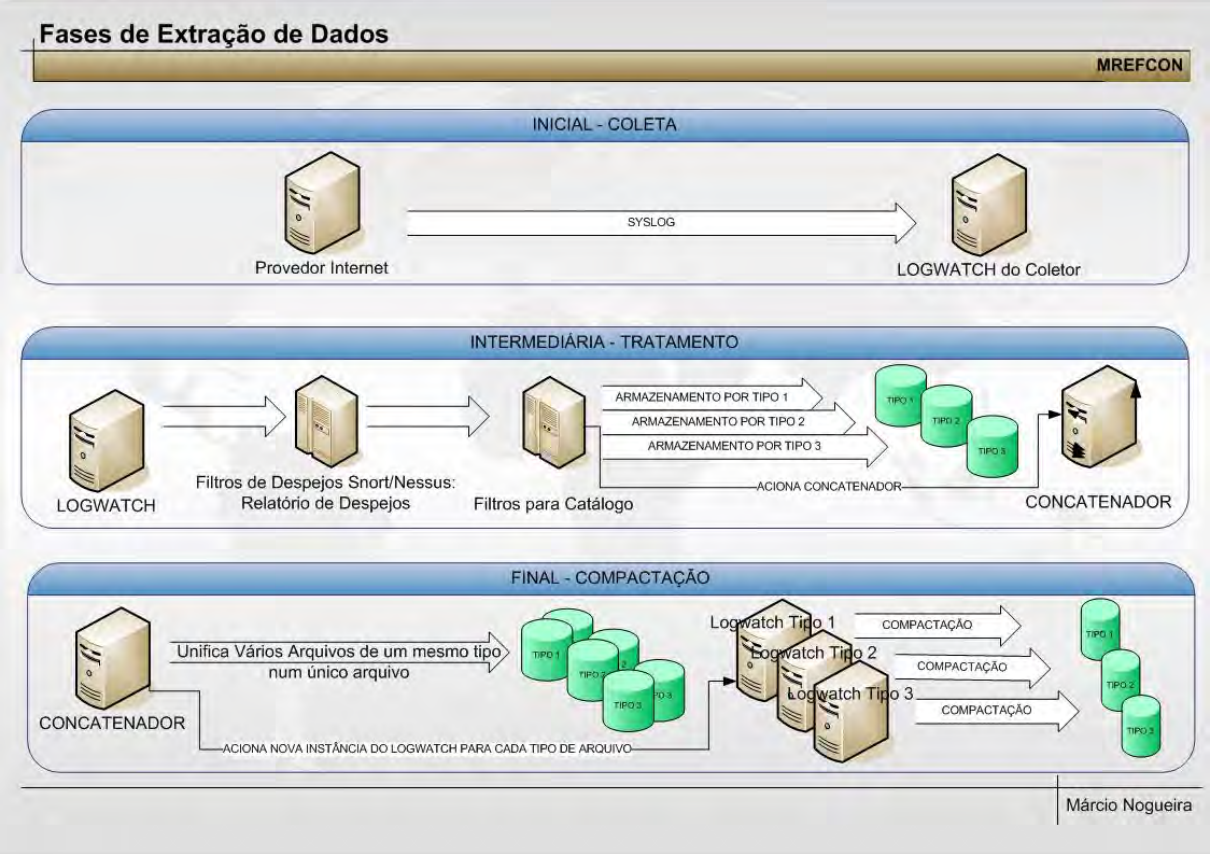


Figura 25 – Esquema de Extração dos Coletores

O esquema apresenta 2 novas fases em relação ao modelo padrão do *logwatch*. Após a fase inicial de coleta os dados apurados passarão por uma nova fase, denominada aqui de fase intermediária de tratamento. Nesta o excesso de informações nos dados serão descartados e protocolados através de um relatório de despejos. Esse relatório tem a função de informar ao sistema principal o tipo de informação que está sendo ignorada, apresentando um resumo sintético com dados, como: quantidade de registros ignorados por tipo de informação, horário de exclusão das informações, regra que motivou o despejo da informação.

Tanto o filtro de despejo quanto o filtro de catálogo são atualizados periodicamente. A cada sincronização entre o coletor e o sistema principal, novos filtros e novas assinaturas de evidências são repassados para o coletor. Após passagem por ambos os filtros os registros restantes são catalogados em arquivos distintos, conforme o tipo de dados, como: *e-mail, http, https, firewall, proxy, sql, ldap*, etc. Após o catálogo um novo evento é acionado

automaticamente, o concatenador.

O concatenador é uma rotina desenvolvida no próprio sistema operacional servindo para unificar dois ou mais arquivos de um mesmo tipo num só. Essa rotina será de grande importância uma vez que permitirá eliminar registros duplicados ao longo de dias, semanas e meses. Permitindo que possamos armazenar o máximo de informações ao longo do maior tempo possível economizando o máximo de espaço em disco. Essa é função da fase final, ou compactação, onde aplicaremos novamente os filtros existentes sobre os arquivos concatenados e por último aplicaremos uma compactação a fim de ganhar espaço em disco.

Experiências mostraram que a cada 100*Mbyte*s extraídos do servidor de Internet 2*Mbyte*s permanecem catalogados nos coletores. E mais, 1*Gbyte* de dados extraídos ao longo de uma semana resultam em 10*Mbyte*s de arquivos catalogados nos coletores. Isso só é possível mediante 2 fatos: a flexibilidade dos filtros e uma segunda rotina que apresentaremos agora.

A característica de filtrar, catalogar e compactar informações está diretamente relacionada a ação de descartar dados. O descarte de certos tipos de informações, em algumas situações, pode comprometer totalmente a investigação. Baseado nas próprias estatísticas dos modelos de filtros adotados, são eles: os filtros do *snort*, http://www.snort.org, e os filtros do *nessus*, http://www.nessus.org. Ambos os *softwares* de código aberto [GNU], que compõe parte do pacote de ferramentas da imagem emulada. O *snort* possui filtros especializados em detecção de intrusos baseado em assinaturas, com especialidades para eventos acontecidos na própria máquina ou rede. Já o nessus possui filtros especializados em análise de segurança baseado também em assinaturas, com especialidades para realizar auditoria em computadores remotos. A combinação dessas duas ferramentas garante a total cobertura do perímetro onde o modelo MREFCON estiver implantado, além de utilizar técnicas já consolidadas por toda a comunidade de segurança internacional e ser flexível o suficiente para o desenvolvimento de assinaturas próprias, exigências do modelo. A economia proporcionada por esses filtros aponta que estatisticamente menos de 5% do que foi descartado serviria para auditorias.

Contudo, ainda é possível que dentro desse universo de 5% de

informações esteja a solução para algum grande caso nacional. Analisado esse fato o modelo ainda apresenta uma alternativa de consulta aos logs originais do servidor de Internet, a fim de realizar uma consulta inversa às regras dos filtros, ou seja, será realizada uma extração personalizada a fim de localizar unicamente os dados filtrados. A forma encontrada para esta solução de contingência é aplicando um servidor de acesso remoto, conhecido através da ferramenta de código aberto *ssh*, dentro do próprio *software* de máquina virtual. A incorporação dessa ferramenta dentro do código fonte do *software* da máquina virtual permite que o coletor realize um acesso remoto ao servidor de Internet com acessos a ler e enviar os dados dos logs para o coletor.

Para garantir a segurança do servidor, em casos de violação do coletor, é garantido que a conta utilizada para o acesso remoto não seja um usuário normal do sistema operacional, e sim um *script*, cuja rotina é unicamente acessar os diretórios de logs do servidor de internet, extrair os dados segundo o inverso dos filtros e envia-los através do *syslog*.

Uma segunda garantia que o provedor de internet possui em relação ao acesso remoto que o coletor realiza é que não existem contas de usuários no sistema operacional do coletor para propiciar uma invasão remota. Dessa forma, mesmo que o sistema do coletor seja comprometido, que uma intrusão tenha sido concretizada e que o invasor tenha ganhado acesso privilegiado como administrador do coletor, ainda assim o invasor não estará autorizado a realizar uma conexão remota com o servidor de Internet, pois o *software* emulador do sistema principal do coletor comprometido, não sendo possível de invasão, evita qualquer tipo de acesso da conta privilegiada para fora da máquina emulada. A figura a seguir resume a explanação dada:

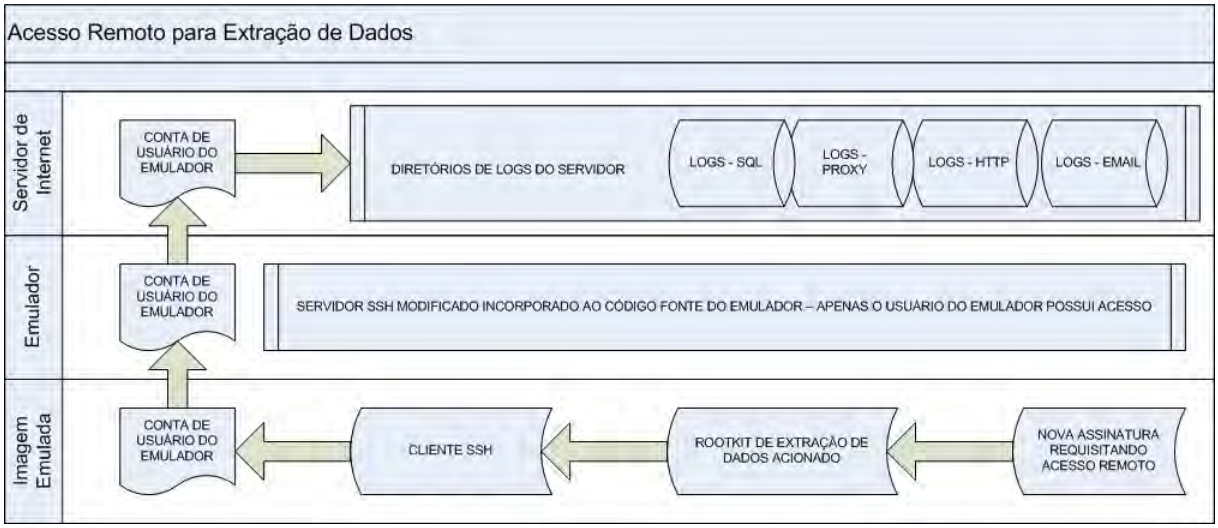


Figura 26 – Algoritmo de Acesso Remoto ao Servidor de Internet

3.1.1.5 Disponibilidade e Priorização

É chegado o momento onde temos coletores tecnicamente prontos, restando apenas garantir aos provedores de Internet, parceiros do modelo, que o sistema proposto não comprometerá a integridade nem estabilidade de seus servidores. Para isso desenvolveremos nessa sessão a questão da priorização, utilizando as características técnicas do próprio *software* emulador.

Por ser de domínio público, a forma de medir o consumo do *Xen* junto ao sistema onde o mesmo encontra-se instalado é popular. Baseados nessa afirmativa apresentamos uma sínteses dos números equivalentes ao consumo do servidor de Internet, localizado em /etc/xen.conf:

- Memória *RAM* Consumida: de 2 a 4 *Mbytes*
- Processador Consumido: Picos máximos de 10% da capacidade total
- Espaço em *HD* para instalação do coletor: 35*Mbytes*
- Espaço em *HD* necessário para o tratamento: Máximo de 100*Mbytes*
- Memória *SWAP* Consumida: máximo de 10% da capacidade total

Priorização acarreta num problema chamado disponibilidade, se os índices de priorização foram ínfimos o suficiente a ponto de não conseguirem processar as informações a tempo, a função do coletor passa a ser de um processo morto na memória do servidor de Internet consumindo recursos desnecessariamente.

Para evitar essas situações desenvolvemos o conceito de disponibilidade à priorização, onde as ferramentas dos coletores serão trocadas dinamicamente a fim de acompanhar a demanda de consumo.

Utilizaremos a ferramenta *sysutil.tgz*, responsável por monitorar o *status* do sistema operacional, para informar ao sistema principal do coletor o conjunto de ferramentas que devem ser utilizadas para minimizar ou maximizar suas atividades.

A forma de utilização dessa ferramenta se dará em duas camadas. A primeira no próprio sistema operacional do servidor de Internet, onde o consumo de recursos será monitorado em tempo-real. A segunda no sistema operacional do coletor, a fim de mensurar o esforço realizado pelo coletor num determinado instante.

Exemplificando: Estando o servidor de Internet com recursos consumidos em ordem inferior a 50% do total, são maximizadas as ferramentas do coletor a fim de que os recursos computacionais deste alcancem ordem superior a 75% da capacidade de recursos do coletor. Por outro lado, estando o servidor de internet com recursos consumidos acima de 50% da capacidade total, ou seja, trabalhando num modo forçado, então se minimizam as ferramentas no coletor para que o mesmo não ultrapasse 50% da capacidade computacional do coletor.

Este ajuste de carga se trata da escolha do aplicativo que será utilizado para realizar a filtragem e compactação dos dados. Enquanto que o *logwach* pode ser configurado para reduzir o consumo de processamento à medida que a carga do processador da máquina virtual esteja aumentando, utilizaremos *softwares* mais rápidos para filtragem e compactação em contrapartida a uma maior utilização do processador do sistema emulado, bem como utilizaremos ferramentas mais lentas que proporcionem um menor consumo de *cpu*. Em resumo:

Se, uso da *CPU* do servidor de internet maior que 50%:

- coletor deve trocar ferramentas de compactação para diminuir o consumo de *CPU* do coletor para menos de 50%.

Se, uso da *CPU* do servidor de internet menor que 50%:

- coletor deve usar ferramentas padrões de compactação a fim de maximizar os trabalhas, consumindo o máximo de *CPU* do coletor.

3.1.2 Estudos de Casos

Apresentaremos agora um exemplo de coletor funcionando, recebendo um pacote de assinaturas para verificação, correlacionando as assinaturas aos dados extraídos e transmitindo a apuração para o sistema principal.

Partiremos do pressuposto que o coletor esteja devidamente instalado.

Em /etc/xen/ encontramos o arquivo de configuração xmmerfcon, cujo conteúdo é:

kernel = "/boot/vmlinuz-2.6.9-b6-mrefcon"

memory = 4

name = "trinux"

nics = 1

ip = "127.0.0.2"

disk = ['file:/usr/packages/mrefcon/trinux/rootfs,sda1,w']

root = "/dev/sda1 ro"

Para iniciar o Xen no modo de teste utilizamos o seguinte comando:

xm create xmmerfcon –c

xm -> é o programa que administra a utilização das máquinas virtuais

create -> parâmetro utilizado pelo xm para iniciar uma máquina virtual

xmmrefcon -> arquivo de configuração da máquina virtual

-c -> modo interativo, não disponível na versão oficial disponibilizada aos provedores de Internet

Após a emulação da imagem, será apresentada uma tela para podermos acessar o coletor:

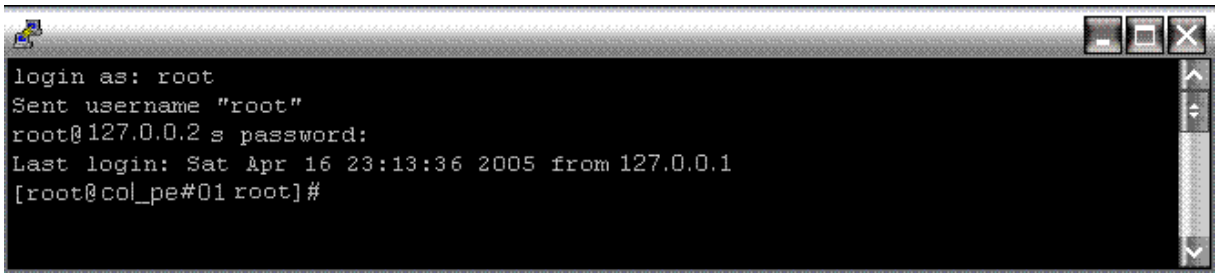


Figura 27 – Prompt de comando do coletor

A primeira tarefa a ser realizada pelo coletor condiz com a fase de comunicação, dessa forma iremos executar a lista de ferramentas que determinam o tipo de conexão e em seguida efetivar a conexão. No coletor oficial essa lista será automaticamente disparada na inicialização do sistema operacional através de uma rotina conhecida no linux por *initd*. A seguir apresentamos o serviço que executa a verificação do tipo de comunicação disponível na rede.

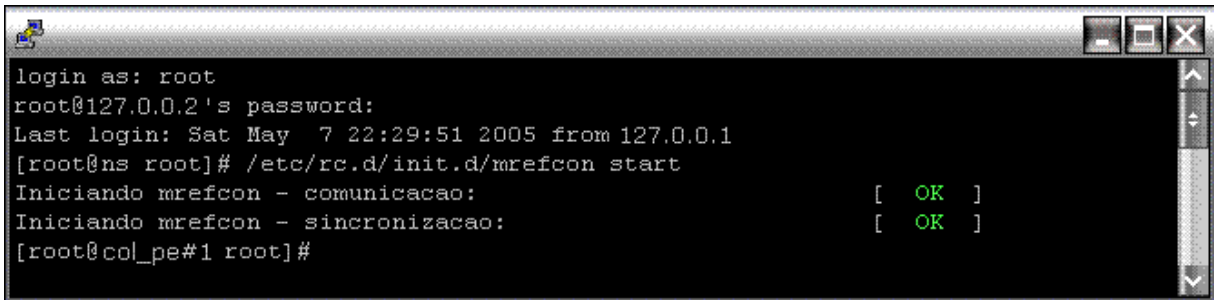


Figura 28 – Iniciando comunicação no coletor

Podemos verificar o tipo de comunicação estabelecida e tempo decorrido após a última sincronização através do comando:

Figura 29 – Verificando o status da comunicação e sincronização

O processo de recebimento de um pacote de assinaturas é acompanhado logo em seguida ao processo de comunicação. Resolvemos separa-los aqui para mera demonstração das sucessivas etapas. A tarefa executada pelo coletor para recebimento de novas assinaturas encontra-se descrito nas figuras 14, 15 e 16 deste mesmo trabalho.

A figura 16, em especial, apresenta um exemplo conceitual do que poderia ser a assinatura, traduzimos agora do conceitual para o técnico validando o esquema final de recebimento das assinaturas:

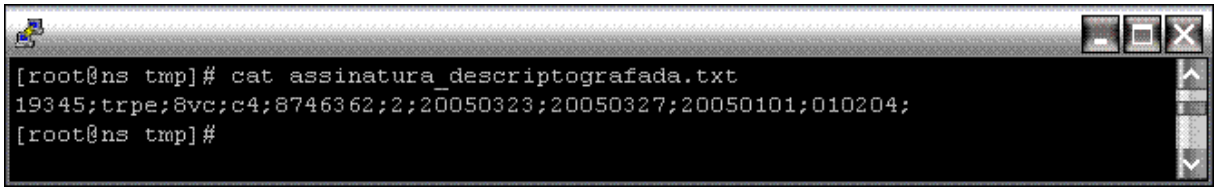


Figura 30 – Arquivo de Assinatura

O exemplo acima apenas denota o que seria um cabeçalho padrão, moldado em exemplificar um esquema assinatura. A seguinte tabela descreve os campos:

Tabela 10: Descrições dos campos do arquivo de assinatura

AÇÂO	DESCRIÇÃO
1	N° da Ordem Judicial que Autoriza a Investigação
2	Tribunal Emissor da Ordem
3	Vara do Juiz Responsável
4	Informações Extras sobre a Vara
5	N° de Registro do Perito Responsável pela Investigação
6	Grau de Importância do Caso: (1) Urgente, (2) Médio, (3) Normal, (0) Monitoramento
7	Data de ocorrência do Evento
8	Data de publicação da assinatura
9	Data para inicio do rastreamento
10	Regiões investigadas: (01) Norte, (02) Nordeste, (03) Centro, (04) Centro-Oeste, (05) Sudeste, (06) Sul
11	Tipo de Log: (01) Email, (02) Firewall, (03) http, (04) imap, (05) mysql, (06) radius, (07) ssl, (08) dns

12	Palavra(s) chave(s)
13	Tipo de ordenação: (1) Cronológica, (2) por coluna, (03) por log
14	Tipo de processo: (0) local, (1) remoto

De posse da assinatura o coletor finalmente estará apto a realizar o trabalho pelo qual foi criado: extrair e correlacionar as evidências. Para extrair as evidências baseados no esquema apresentado na figura 27, partiremos da seguinte assinatura:

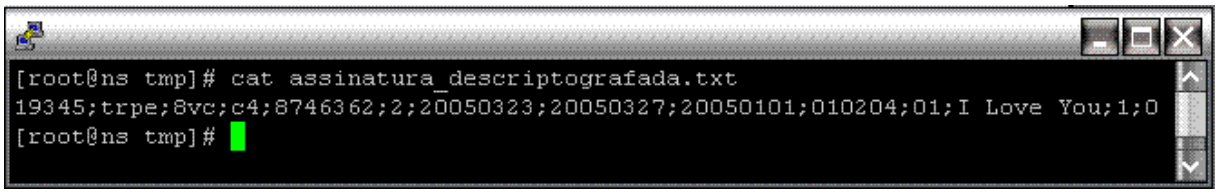


Figura 31 – Arquivo de Assinatura Completa

O responsável por verificar a existência de novas assinaturas é a ferramenta *wget*. Essa ferramenta é iniciada junto ao sistema através do serviço de comunicação /etc/rc.d/init.d/mrefcon. Em tempos de 20 minutos a ferramenta é automaticamente chamada pelo sistema, através do serviço de agendamento de tarefas padrão do linux, *crontab*. O serviço *contrab*, ao executar o *wget*, verifica através de uma rotina desenvolvida, a existência de um novo pacote de assinaturas. Havendo, o mesmo se encarrega de assinar os serviços de extração para dar inicio ao trabalho.

Os serviços de extração correspondem a um conjunto de rotinas desenvolvidas exclusivamente para o mrefcon. Essas rotinas realizam operações de busca, comparação e correlação, sobre os logs da etapa final de extração, que correspondem aos arquivos compactados por tipo.

Entre as rotinas de extração utilizam-se trechos de códigos das ferramentas *ext2tools* e *ngrep*, além de comandos em *perl* e *php*.

Após a extração e correlação das informações através dos diversos logs agrupados crontab conclui sua tarefa acionando o envio das informações coletadas para o sistema principal.

O envio condiz com o que foi apresentado nas figuras 17, 18, 19 e 20. Não sendo necessário repetir novamente.

3.1.3 Formas de Instalação

Sendo o coletor uma das etapas finais da arquitetura proposta, é importante apresentarmos as formas pelos quais serão instaladas para dirimir quaisquer dúvidas técnicas.

Utilizaremos mais uma vez das características padrões do *software* de máquina virtual, *xen*, para explanarmos nossas idéias.

O *xen* utiliza um sistema de gerenciamento de *hardware*, conhecido como *kernel*, próprio, necessitando com isso inserir nas configurações de inicio, ou *boot*, do servidor de internet, as informações referentes a sua inicialização. Para isso o *xen* acrescentará no lilo.conf ou grub.conf as seguintes informações:

```
title Xen 2.0 / XenMrefcon 2.6.9-mn-32
  kernel /boot/xen.gz dom0_mem=4028
  module /boot/vmlinuz-2.6.9-mn-32-xen0 root=/dev/sda4 ro
```

As informações acima refletem na utilização do *kernel*, personalizado para o MREFCON, vmlinuz-2.6.9-mn-32-xen0, padrão para todos os coletores. Reserva o espaço de memória volátil de 4*Mbytes* que se localiza em /dev/sda4 e configura o sistema para o modo de apenas leitura, *ready only*.

Em seguida, informaremos ao sistema operacional do servidor de Internet como executar o software de máquina virtual.

Através do módulo mrefcon_initrd.gz, também inserido no arquivo que carrega os módulos do sistema operacional na memória *ram*, conhecido como /etc/conf.modules, o sistema poderá ser acionado como um outro serviço qualquer. Podendo ser interrompido e re-iniciado.

Este procedimento de instalação dos coletores é padrão. Para instalar o coletor em plataformas distintas, com personalizações e novas tecnologias, o modelo requer que o provedor de internet interessado em adotar a solução baixe no site do MREFCON um coletor específico para sua versão de sistema operacional. Ao baixar a versão do coletor que mais se aproxime do seu sistema operacional o *software* irá tentar identificar automaticamente todas as informações necessárias para que o coletor funcione corretamente. Baseados neste modelo de *software* o coletor não possui dependências em relação ao sistema operacional do provedor.

Uma vez instalado o *software* de emulação o coletor irá trabalhar de forma totalmente auto-suficiente. Já o processo de instalação do emulador requer características mínimas para sua operação, sendo coletadas automaticamente pelo *software* de instalação.

3.2 Do Sistema Principal

Os objetivos do sistema principal são:

- Interagir colaborativamente entre as entidades federais e regionais envolvidas no modelo;
- Apresentar uma interface comum entre um jurista e um perito informático a fim de traduzir numa assinatura técnica a ordem judicial expedida;
- Apurar os dados coletados ao longo dos provedores de Internet, correlacionando-os com a assinatura da ordem judicial;
- Remontar o ocorrido criminal baseado nas apurações feitas;
- Segmentar por regiões federais os diversos coletores a fim de assegurar as jurisprudências regionais, garantindo que investigações regionais não necessitem de intervenção federal;
- Relatar o laudo pericial eletronicamente para o jurista da ordem judicial;
- Enviar os dados rogatórios da investigação para os responsáveis legais pelo provedor de internet investigado;
- Garantir os devidos níveis de acesso distinguidos conforme a entidade envolvida

Quanto a sua constituição o sistema principal é um conjunto de servidores de Internet, baseado na plataforma em código livre linux, distribuídos entre as entidades envolvidas, conforme a Figura-22, cada qual com objetivos, funções e responsabilidades distintas. Utilizamos para representar o modelo a distribuição linux conectiva versão 10, http://www.conectiva.com.br, por possuir suporte regional em quase todos os estados da federação brasileira.

Entendemos por servidor de Internet o computador que proverá serviços de Internet, como: *http, e-mail,* banco de dados, *ftp* e etc.

As figuras a seguir ilustram o ambiente virtual proposto na camada principal do MREFCON:

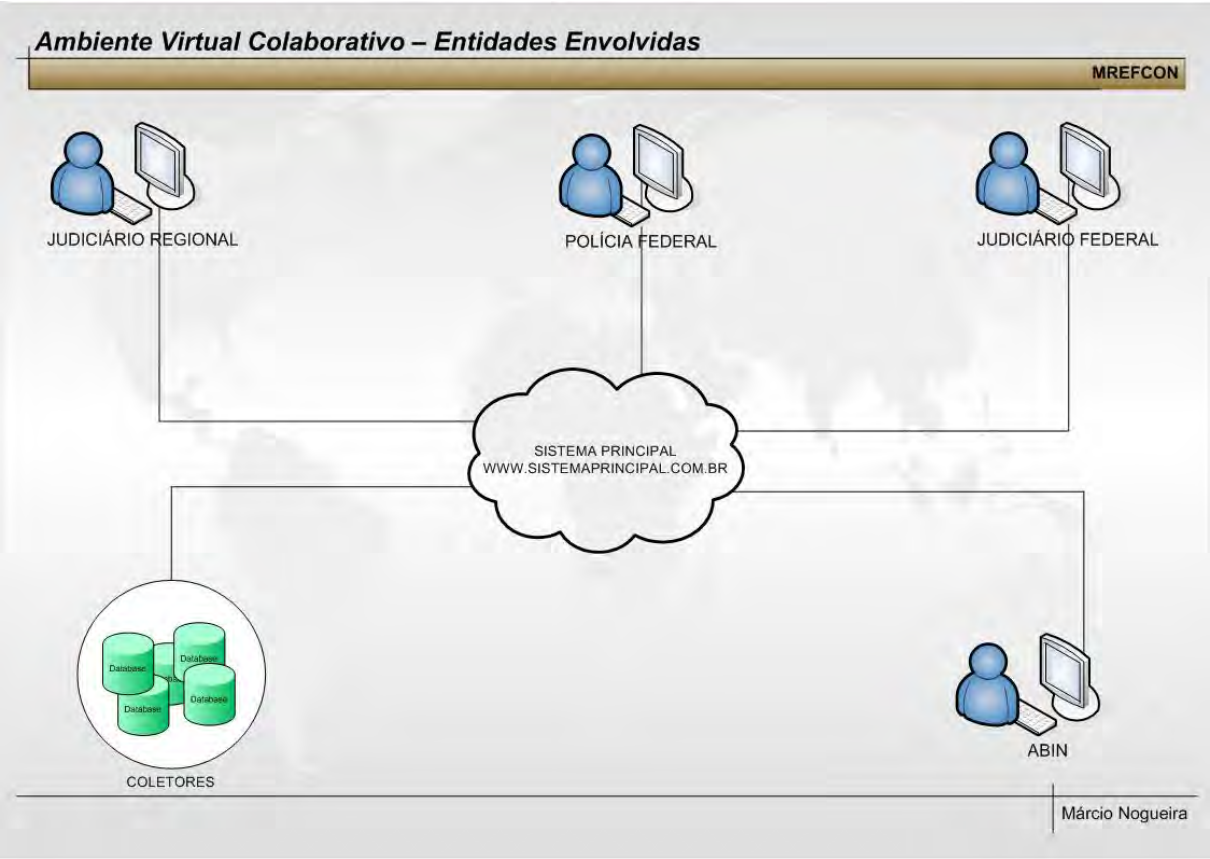


Figura 32 – Entidades envolvidas no sistema principal

A figura acima ilustra o esquema de comunicação centralizada do modelo, onde toda e qualquer informação trocada é direcionada para o sistema principal. Ressaltando que a comunicação entre as entidades só pode ser estabelecida mediante aprovação pelo sistema de certificação digital federal, ou seja, a imagem ilustra o que seria a comunicação final após todos estar devidamente certificados e autenticados perante o sistema.

Para garantir a autonomia institucional de cada entidade envolvida o modelo MREFCON propõe a seguinte arquitetura computacional:

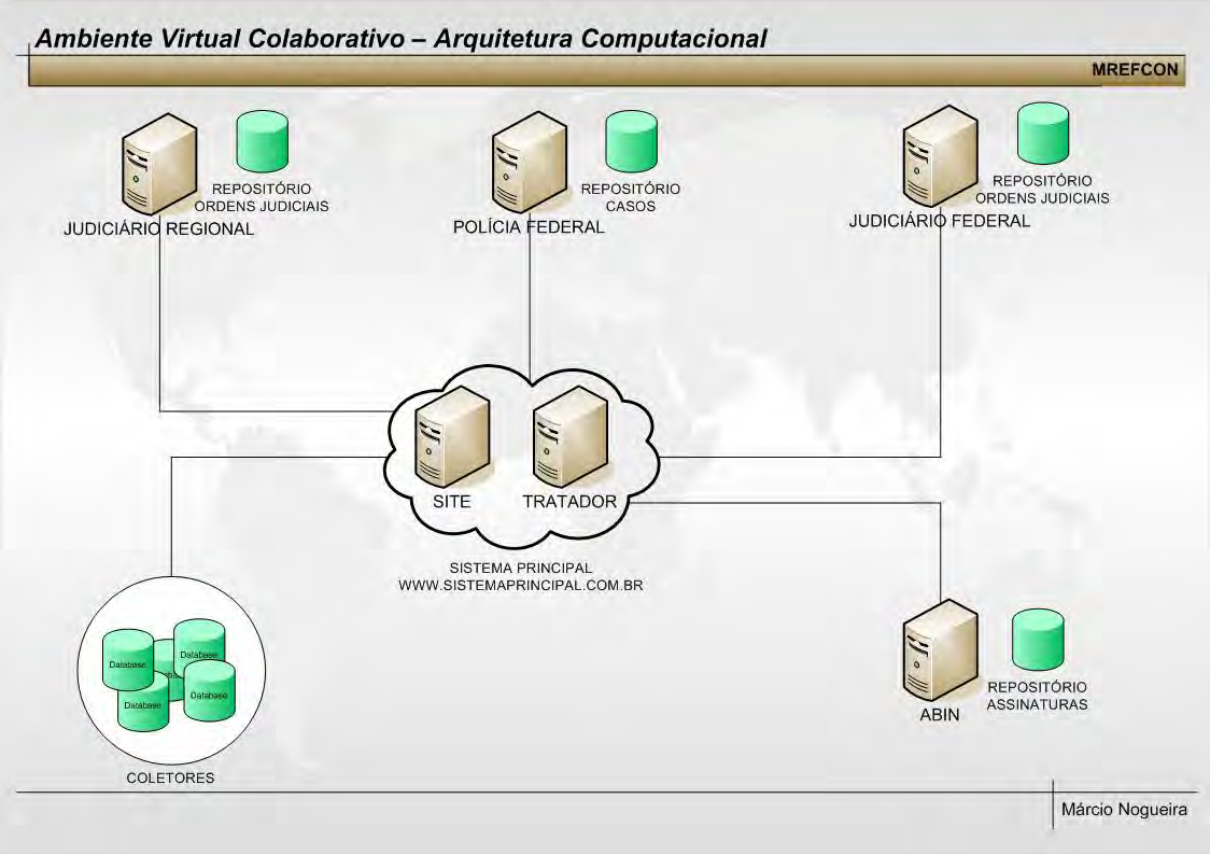


Figura 33 – Arquitetura Computacional do Sistema Principal

A arquitetura proposta garante que as informações desenvolvidas por cada entidade sejam protegidas de outras entidades e delas mesmas. Ou seja, havendo problemas de segurança numa determinada entidade o intrusor só terá acesso ao banco de dados daquela entidade. Mesmo em posse do banco de dados o intrusor terá em suas mãos informações criptografadas, cuja leitura só é possível mediante acesso autorizado no sistema principal para obtenção da chave pública de leitura.

O modelo proposto de arquitetura conduz a necessidade dos sistemas estarem sempre *online*, pois mediante ausência de comunicação o recebimento da chave pública para leitura dos bancos de dados não se processa e a entidade não obtem o acesso aos seus próprios dados. E denota a necessidade de esforços colaborativos entre todas as entidades, pois a ausência de um inviabiliza todo o processo para os demais.

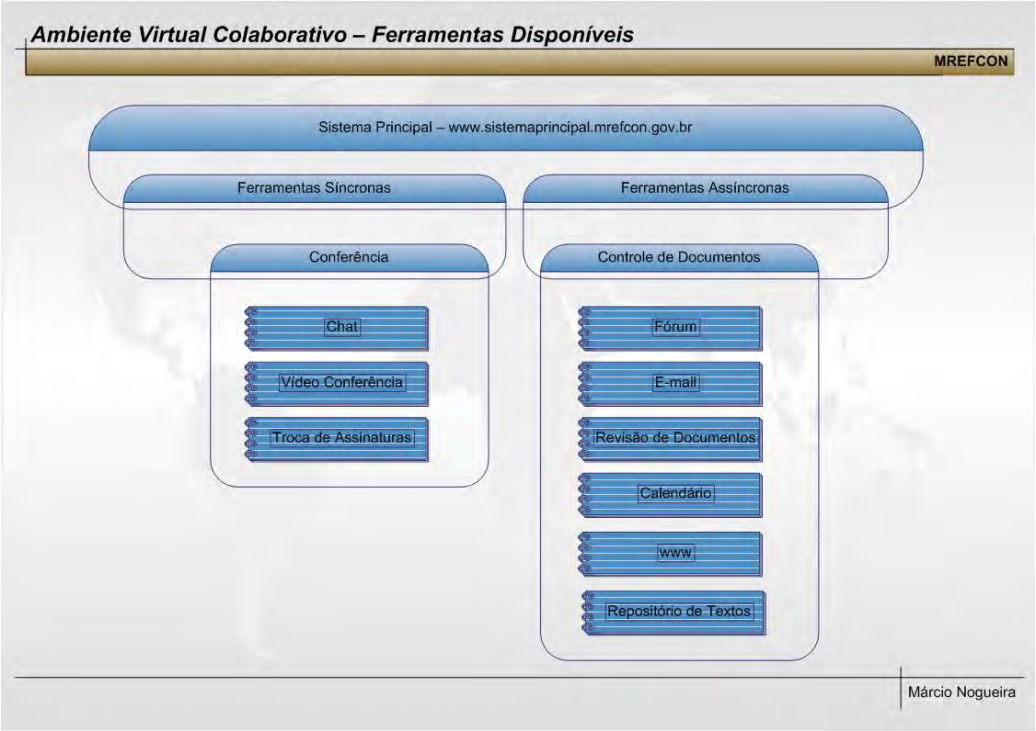


Figura 34 – Ferramentas disponíveis no sistema principal

A figura ilustra as ferramentas disponíveis através de uma interface comum de operação entre todos os envolvidos, independente do nível de acesso que o usuário tenha, podendo inclusive ser de acesso público para a Internet. Observa-se que o sistema principal é acessado através de um *site* na Internet, de onde classificamos nossas interfaces como cliente-servidor.

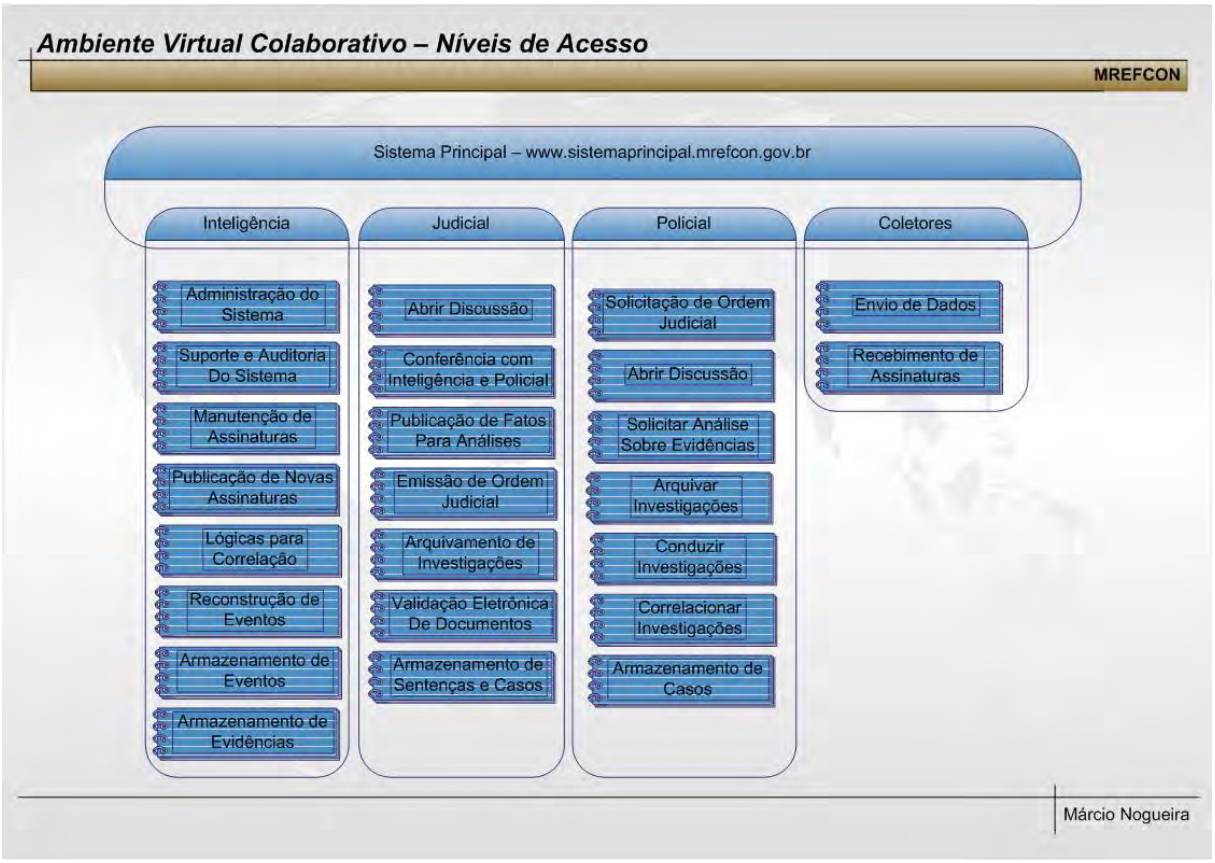


Figura 35 – Níveis de acesso ao sistema principal

Ilustramos acima as ferramentas disponíveis conforme o nível de acesso que o usuário tenha. O sistema é único para todos os envolvidos, garantindo sua acessibilidade em qualquer parte do mundo, desde que atenda os critérios de segurança exigidos.

Os critérios de segurança se resumem no estabelecimento de uma comunicação privada, chamada de *VPN*, semelhante a fase de comunicação dos coletores.

O *site* público visa a publicação e informações sobre este projeto federal. A intranet, que é a rede de dados estabelecida pelas *vpn*, visa o funcionamento do sistema entre as entidades envolvidas.

No lado das entidades policial e judicial o acesso ao MREFCON se dará através do *site* público. Aparecerá uma tela em especial para cada entidade envolvida solicitando um usuário e senha para o sistema.

Ao informar usuário e senha, o envolvido ganha os níveis de acesso ao qual seu usuário está restrito. Tal acesso pode ser realizado remotamente em qualquer

lugar do mundo, necessitando apenas que o usuário esteja na Internet.

Ao ganhar as credenciais para acesso ao sistema o *site* exigirá do usuário que o mesmo instale um programa específico para o modelo, que se trata do cliente *vpn* para acesso a rede privada. Esse cliente *vpn* é único para cada sessão de usuário, sendo necessária sua reinstalação a cada novo acesso ao *site*. Dessa forma garantimos a autenticidade do usuário e sigilo do sistema interno.

Figura 36 – Instalação do Cliente VPN ActiveX

Na prática esse cliente *vpn* é um programa desenvolvido com a tecnologia *activex*, de objetos dinâmicos e multimídia para *web*, que realiza uma troca de chaves públicas e privadas entre o computador do usuário e o servidor do sistema principal. Observa-se aqui outro requerimento para acesso ao *site*, uma chave privada. Não basta somente o usuário ter uma senha ele precisa dispor também de um certificado. Na fase atual de desenvolvimento do MREFCON este certificado classifica-se nos critérios padrões de certificados digitais, mas já apto para operar no modo de identificação biométrica. Em posse do usuário, senha e certificado o programa em *activex* cria o túnel virtual que dará acesso a *intranet* do MREFCON.

No capítulo 4 apresentaremos com maiores detalhes aplicações do modelo, utilizando para isso telas, formas de operar e funções do sistema principal.

Em resumo, o sistema principal é um conjunto de servidores linux integrados a partir de interfaces comuns de uso, desenvolvidas com tecnologia de páginas dinâmicas *xml*, segurança aplicada através de um cliente *vpn*, que muda a cada vez que o usuário abre o *broswer*.

3.3 Da Constitucionalidade

Tecnicamente a criação do MREFCON exige uma forte bagagem técnica no que diz respeito a programação, criptografia, certificados digitais e *vpn*, contudo a arquitetura proposta de integração dessas ferramentas, a fim de solucionar um problema comum entre entidades físicas distintas, basea-se não apenas numa proposta colaborativa virtual, mas sim numa integração técnica baseada nos princípios constitucionais aos quais cada entidade está restrita, ou seja, modelamos o sistema de forma que a constituição vigente da época limite a autonomia de cada entidade envolvida. Essa característica técnica, respaldada por uma solução de código aberto, possibilita que o MREFCON seja uma ferramenta juridicamente legal.

As principais restrições do sistema, baseado nas leis brasileiras, são:

3.3.1 Autenticação do Operador

Vimos anteriormente o macro esquema do sistema principal, contudo é no detalhe do módulo de autenticação do operador que faremos prevalecer os itens apontados na subseção anterior sobre a constitucionalidade.

Vimos também que cada usuário envolvido necessita de um nome, senha e certificado para ter acesso, mas essas informações são insuficientes para garantir que um perito policial ou qualquer outro indivíduo não realize investigações e monitoramentos em âmbito pessoal. Principalmente para dirimir essa possibilidade que o MREFCON distribui sua arquitetura computacional junto a todas as entidades

envolvidas, conforme vimos na figura 35. Dessa forma, para um indivíduo ter acesso ao banco de dados dos casos em andamento numa determinada cidade, ele necessitará: ser um usuário legítimo e com credenciais da polícia federal. Nenhum outro usuário conseguirá obter tais informações, mesmo realizando uma intrusão na sede da polícia federal, capturando os dados do banco de dados e conseguindo se autenticar junto ao sistema principal como um juiz ou perito da ABIN. A chave pública liberada pelo sistema para leitura do banco de dados da polícia federal só acontece mediante um perfil de usuário da polícia federal.

De forma similar, porém com grau de autenticidade dobrado, uma investigação policial, por menor que seja, necessitará:

1. Apresentação do caso e solicitação de recursos investigativos através de um perfil policial
2. Autorização da investigação através de uma ordem judicial
3. Execução da investigação através de um perfil policial

Através desse processo em três passos garantimos que nenhuma investigação seja realizada sem o consentimento da justiça. Na prática, o esquema dos três passos é:

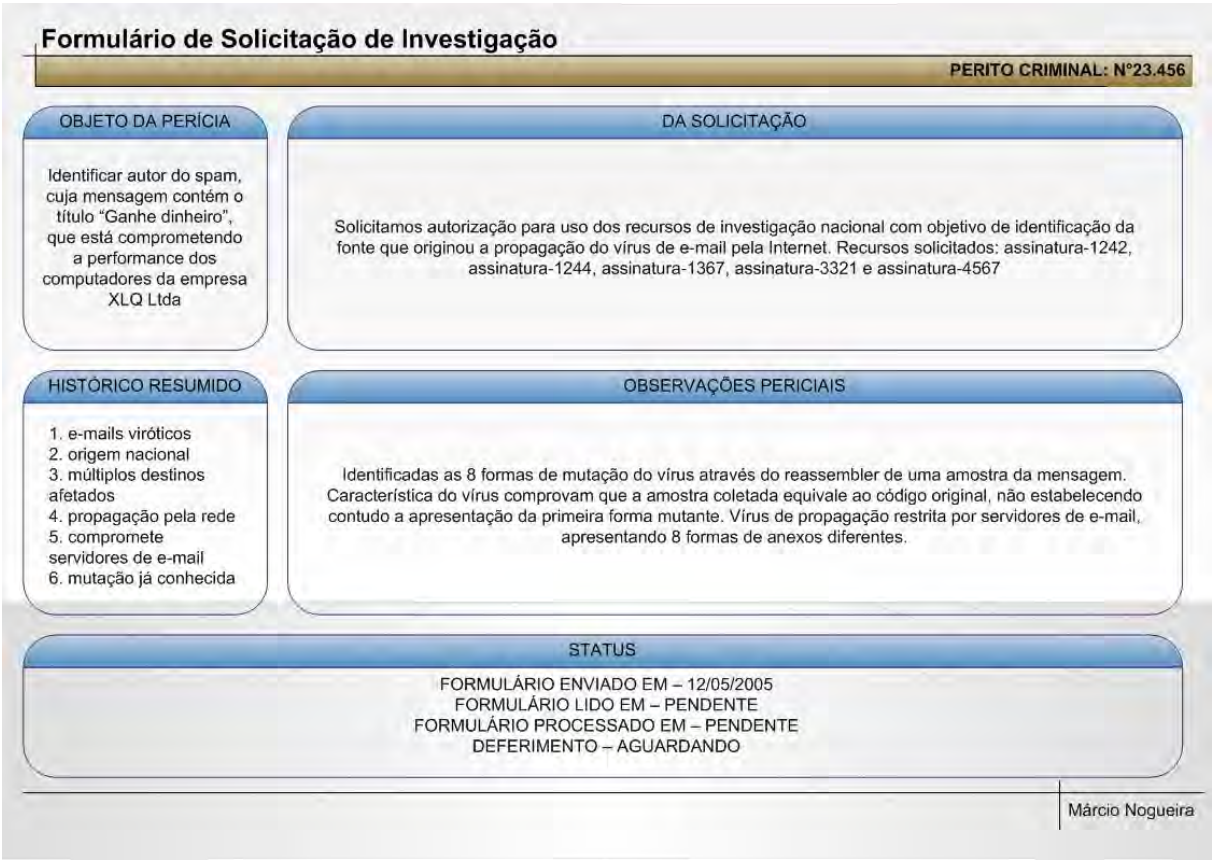


Figura 37 – Formulário de Solicitação de Investigação Policial

Polícia solicita através do formulário de investigação autorização para o uso de determinadas assinaturas do sistema principal. Tais assinaturas serão melhores apresentadas no próximo capítulo, sobre a modelagem, mas a princípio cada assinatura realiza um tipo de investigação técnica, o conjunto de assinaturas para um caso determinará a assinatura final a ser enviada para os coletores.

Todas as informações preenchidas no formulário condizem com as mesmas informações que teriam que ser apresentadas numa decorrência judicial normal. Acrescidas dos detalhamentos técnicos que justificam a solicitação das assinaturas.

Após a solicitação o perito aguarda pelo deferimento para poder realizar a investigação:

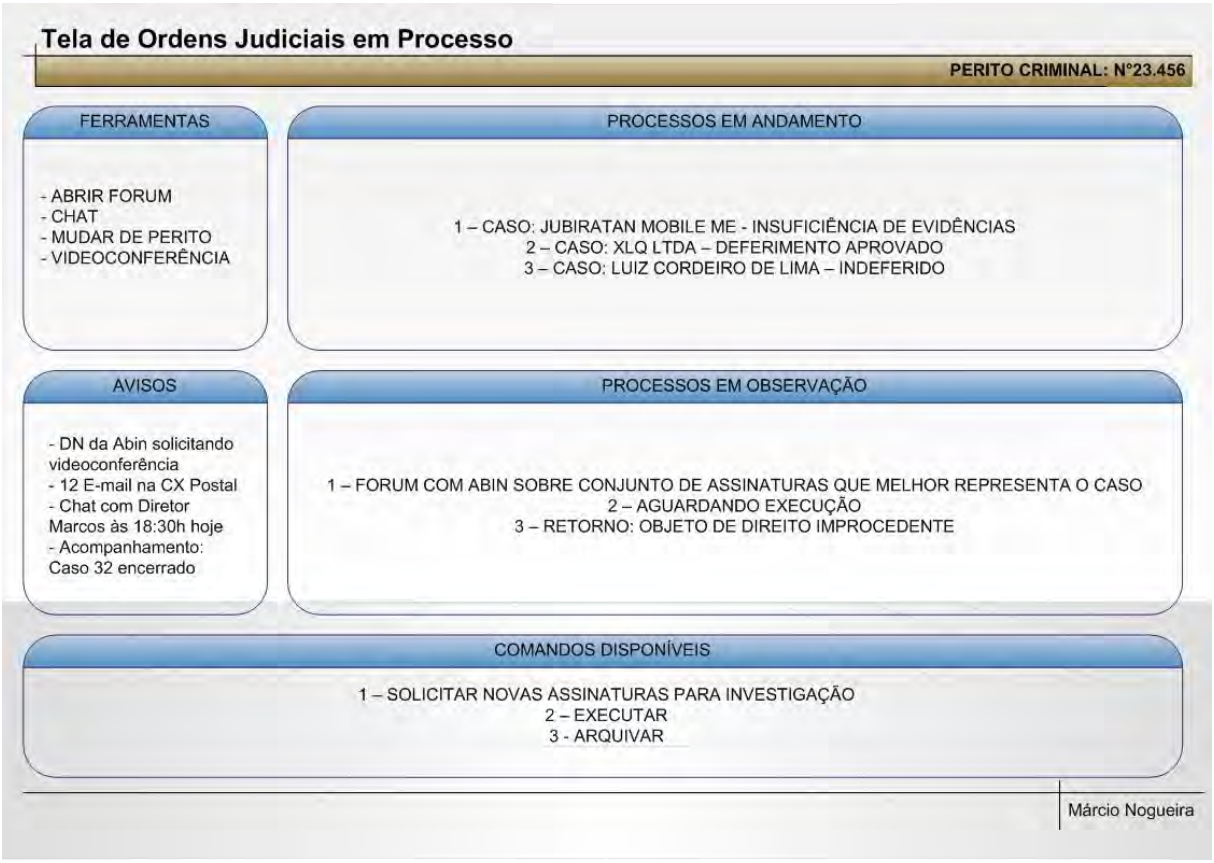


Figura 38 – Tela Policial de Ordens Judiciais em Andamento

Como podemos observar a opção de execução de uma investigação só está disponível para o usuário após seu deferimento junto à justiça. Na tela observamos outras características como a visão macro sobre todos os casos em andamento, observações e que ações o policial pode tomar.

O nível de abstração técnica para juízes e policiais é garantido através de interfaces comuns, estudadas com aspectos cognitivos [SOUZA], baseadas em *softwares* de educação à distância e ferramentas de *CSCW* [BARROS, 1994].

3.3.2 Validação da Ordem Judicial

Como garantir que a informação sobre a ordem judicial, ou mesmo que uma determinada ordem judicial, não tenha sido adulterada durante o processo de comunicação?

A indagação acima procede do fato de estarmos operando através de uma

rede pública de comunicações, disfarçados na forma de canais criptografados, sujeitos às ameaças diversas. Para haver a adulteração de uma ordem judicial, decorrendo num processo de investigação fraudulento, pelo menos um dos seguintes pontos precisam ser violados:

- Direto na fonte do judiciário: computador do juiz violado e ordem adulterada;
- Direto na fonte do judiciário: banco de dados violado e adulterado;
- Através do sistema principal: informação está correta no banco de dados do judiciário, porém apresenta outra informação quando acessado pelas entidades policiais;
- Direto no destinatário da polícia: banco de dados violado e adulterado;
- Direto no destinatário da polícia: computador do perito violado e ordem adulterada;

Sobre esses pontos, o MREFCON responde:

1. Os dados sobre uma ordem judicial estão armazenados num único repositório, da justiça;
2. Todas as telas de acesso ao sistema principal são dotadas de criptografia por sessão, garantindo que qualquer violação de tela acarreta na insuficiência de comunicação com o sistema principal;
3. Cada tela de sessão apresenta características únicas que inviabilizam qualquer tentativa de clonagem;

Essas três colocações são o suficiente para descartarmos as possibilidades de adulteração através do banco de dados da polícia, no computador do perito e no sistema principal. Quanto ao banco de dados do judicial, o fato do banco estar criptografado, necessitar de chave pública que só o sistema principal possui, e requerer um perfil de acesso autorizado, garante que adulterações no banco somente através de pessoal autorizado.

A única ameaça pelo qual o sistema não possui proteção é quanto as credenciais de acesso de um usuário legítimo. No caso em questão, tendo os dados de: nome, senha e certificado roubados, o acesso será normalmente concedido.

Antecedendo esse tipo de problemática o MREFCON já incorpora as técnicas

de acesso por biometria, em substituição pelos certificados, contudo esse projeto não será apresentado neste trabalho para ganhar espaço em teses posteriores.

Esse nível de segurança adotado na arquitetura do modelo, aliado aos requisitos transcritos das leis apresentadas no capítulo 1, garantem que o sistema possua uma chave única para processar as investigações: a ordem judicial.

Essa abordagem garante ao MREFCON ser tratado como um legítimo ambiente virtual, condizente com o ambiente presencial.

Capítulo 4 Aplicações e Análises sobre o Modelo

Vimos até aqui as questões legais que validam o modelo, as ferramentas individuais utilizadas por cada elemento da arquitetura, a lógica de integração entre elas e um pouco sobre o que seria um exemplo de cenário de produção.

Apresentaremos agora algumas aplicações estudadas em laboratório, que validam o esquema técnico proposto, e análises comparativas sobre os resultados obtidos em relação a uma investigação normal.

Iniciaremos os estudos com um caso de uso sobre um incidente de grande repercussão mundial na Internet, a propagação do vírus *Blaster* versão 2, registrado no final do ano 2003. Em seguida um estudo de caso sobre o último grande escândalo de golpes fraudulentos envolvendo a clonagem de *internet bankings*.

4.1 Investigando um *DDoS* mascarado por *SPAM*

Em 11/08/2003 a empresa americana *Symantec*, www.symantec.com, uma das maiores empresas de antivírus do mundo, anunciou as características técnicas de um novo vírus de computador, o *W32.Blaster.Worm*, ou simplesmente *Blaster*, http://www.symantec.com.br/region/br/avcenter/data/w32.blaster.worm.html.

O vírus, apresentado como uma ameaça de alto grau de distribuição e médio grau de dano propagou-se tão rapidamente pelo Brasil que ganhou destaque em todas as mídias. Caracterizado por provocar instabilidade no sistema, levando ao travamento dos computadores, e comprometer as configurações de segurança, ocultando uma ferramenta que possibilitava que hackers acessassem o computador da vítima.

Apesar dos detalhes técnicos não surpreenderem a comunidade de informática, que já conheciam as vulnerabilidades dos sistemas os quais o vírus explorava para se propagar, contudo os usuários leigos foram massivamente enganados e iludidos.

O *Blaster* inicialmente apresentava uma única forma de propagação, diretamente através da rede de computadores, estabelecendo comunicações direta com outros computadores e enviando pacotes de *DDoS* para o servidor do *Windows Update*, www.windowsupdate.com. Servidor responsável por disponibilizar as correções para os sistemas operacionais não ficarem vulneráveis a este vírus.

O detalhe, que designou o *Blaster* como uma ameaça de dano médio, foi que para cada tentativa de conexão sem sucesso o processo do vírus não saia da memória. Como o vírus iniciava dezenas de tentativas de conexões por minutos era muito comum que dezenas desses processos ficassem ocupando o processador até que o mesmo trava-se. Contudo, o sistema operacional possuindo uma defesa própria para esse tipo de acontecimento, informava um erro, exibindo uma mensagem que o computador precisaria ser reiniciado em 60 segundos, sem deixar possibilidades ao usuário de interromper o processo de reiniciar o computador.

Como a informática, o *Blaster* também evoluiu. *Hackers* perceberam que os provedores de Internet estavam bloqueando através de seus *firewalls* as formas de propagação do vírus. Em contra ataque os *hackers* desenvolveram uma nova forma de propagação para o vírus, através do *e-mail*. Deste ponto em diante cada nova máquina contaminada pelo *Blaster* adquiriu uma rotina extra ao código original fazendo com que o vírus enviasse automaticamente uma cópia de si próprio para todos os *e-mails* que estivessem registrados no catálogo de endereços da máquina infectada. E mais, além desses *e-mails* o vírus também se auto enviava para uma relação fixa de nomes populares, de todos os domínios registrados no catálogo de endereços do computador, sempre alterando o e-mail de origem como se fossem as

pessoas do catálogo que estivem enviando o vírus, e não o proprietário do computador.

Foi-nos proposto a resolução do seguinte caso envolvendo o vírus *Blaster*:

Uma entidade de ensino particular, detentora de mais de 100 computadores, entre eles 2 laboratórios de acesso público para os alunos. Está sendo acusada de danificar o computador de um diretor comercial de televisão. Segundo o réu, sua equipe de informática identificou a origem do invasor através do cabeçalho do *e-mail* recebido um dia antes do incidente. O qual o diretor suspeitou do *e-mail* e solicitou análise. Tanto o réu quanto o acusado residem na mesma cidade. O acusado alega desconhecer o fato e se julga inocente, ameaçando processar o diretor comercial por calúnia e difamação caso não se prove a acusação.

A justiça local encaminhou uma investigação policial a ser realizada em torno de todos os possíveis envolvidos na situação. Tradicionalmente essa solicitação seria encaminhada para o departamento de investigações da polícia civil, contudo, o tribunal regional possuía acesso ao MREFCON, vejamos o caso em *storyboard*:

Figura 39 – Tela de Acesso ao Sistema Principal

1. O Juiz, ou encarregado judicial, acessa a tela inicial do sistema principal e informa seu usuário e senha.

2. Antes de validar seu usuário e senha o sistema solicita o certificado digital de acesso a rede:

Figura 40 – Tela de Solicitação do Certificado Pessoal

3. Após validar o certificado o sistema irá instalar o *software* de acesso remoto a rede do MREFCON:

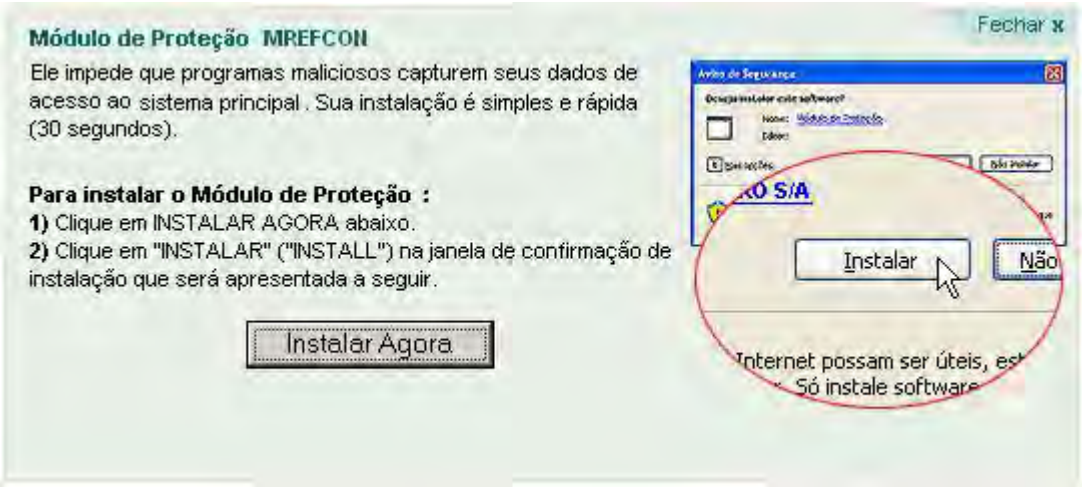


Figura 41 – Tela de Informação sobre a Instalação do VPN Cliente

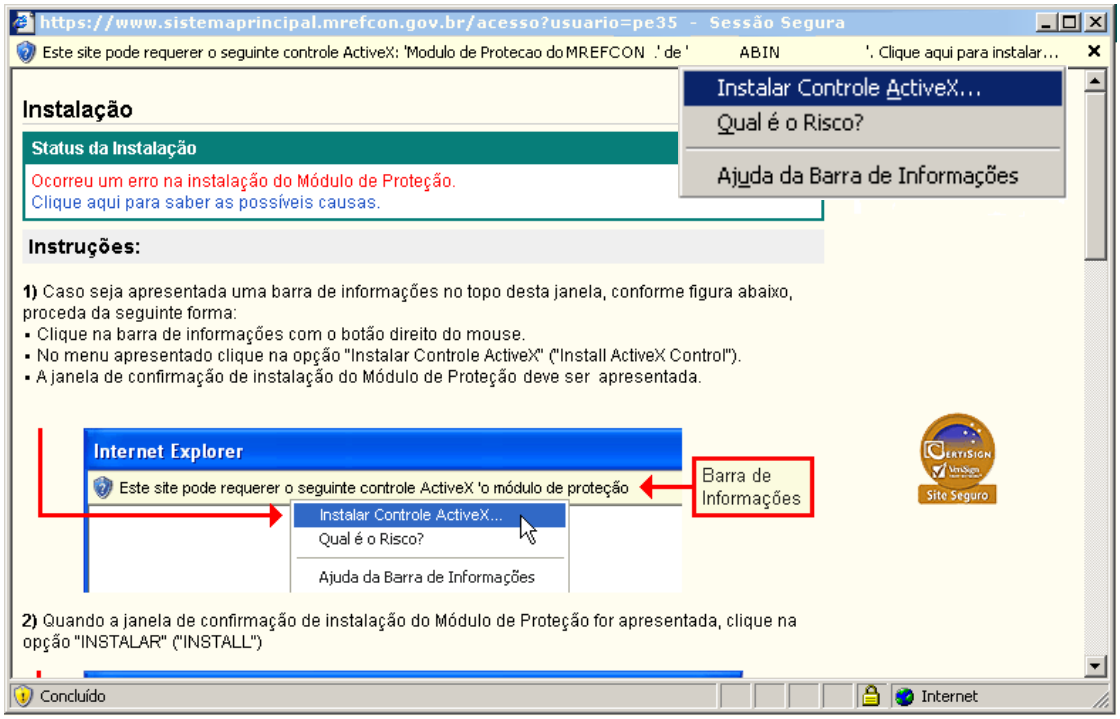


Figura 42 – Instalação do Controlador ActiveX

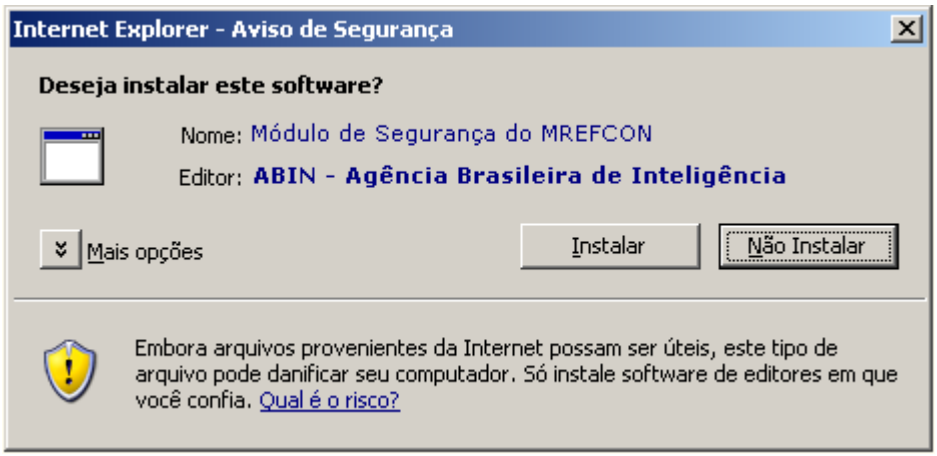


Figura 43 – Instalação do Controlador ActiveX

4. Uma vez validado pelo sistema principal o juiz terá acesso as ferramentas de seu perfil judicial:

Figura 44 – Tela de Ferramentas no Perfil Jurídico

Atentemos para o detalhe que agora o navegador da Internet ao invés de informar o *site* do sistema informa um *IP* do tipo inválido, ou seja, somente aquela janela possui acesso ao sistema.

5. Estando no sistema, o juiz irá acessar o item de “Publicação de Fatos para Análises”. Esse item será o responsável em delegar o próximo perito informático disponível no sistema:

Figura 45 – Publicando um Fato para Análise

6. Na Polícia Federal, o plantonista dos peritos informáticos da vez, irá receber na tela do computador a solicitação de análises logo após o envio pelo judiciário:

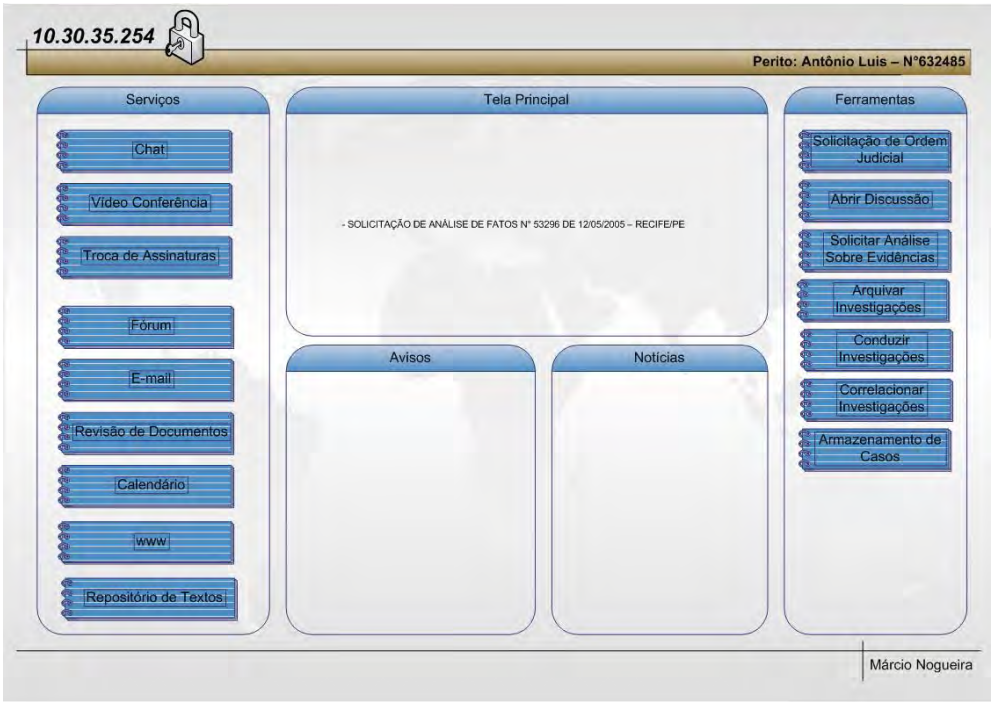


Figura 46 – Tela de Ferramentas no Perfil Policial

7. O perito analisa todos os fatos e provas disponíveis pelo judiciário e monta uma investigação inicial baseados nas assinaturas existentes no sistema, para isso ele acessa a ferramenta de “Solicitação de Ordem Judicial”. Ele solicita a seguinte investigação: Relatório resumido, sintético, sobre todos os logs de *e-mail* e *firewall* da cidade de Recife, cujo endereço destinatário *ip* 200.200.200.1 tenha sido envolvido posteriormente a data de 10/05/2005:

Figura 47 – Perito montando uma Investigação

8. Cerca de meia hora após a solicitação pelo judiciário, o juiz receberá em sua tela a primeira solicitação de ordem judicial para inícios das investigações, nessa solicitação constarão as assinaturas utilizadas pelo perito bem como a justificativa para uso de cada uma delas:

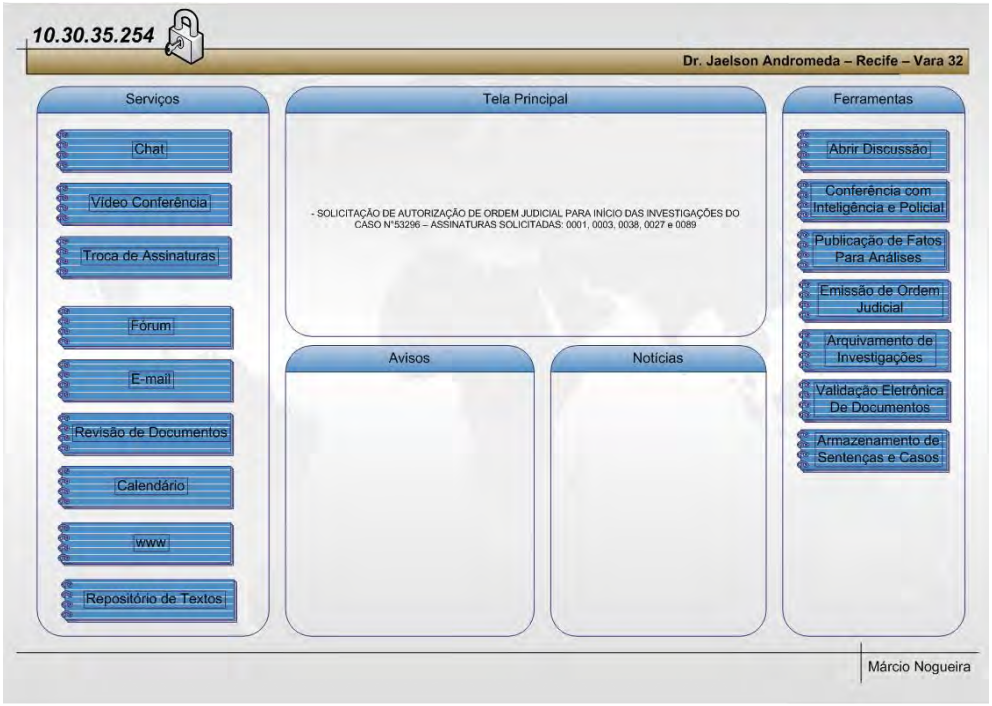


Figura 48 – Autorização de uma Ordem Judicial

9. O perito recebe a autorização de investigação imediatamente após o juiz clicar na mensagem:

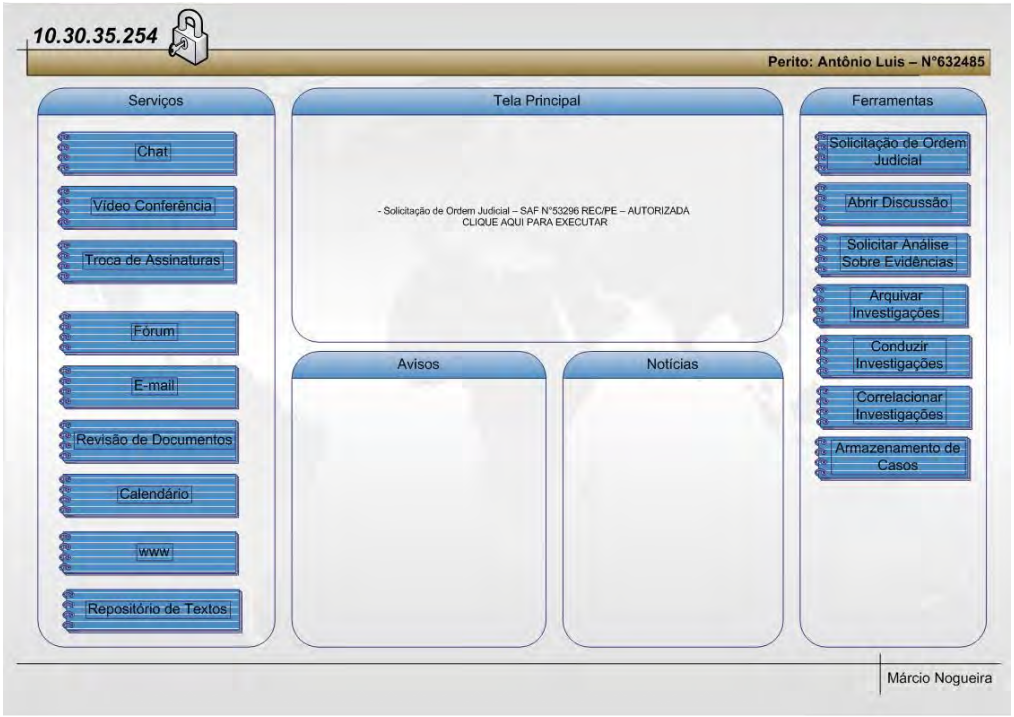


Figura 49 – Execução de uma Ordem Judicial

10. A execução da investigação retorna para o perito todas as informações solicitadas. Em geral a primeira análise serve apenas para nortear o início

das investigações, sendo necessárias várias outras investigações até o término do caso. O sistema principal irá agora publicar o pacote de assinaturas para que os coletores retornem os dados. O sistema detém a informação que para a cidade de Recife existem cadastrados 23 coletores (dado fictício para o exemplo, baseado no número dos principais provedores da cidade). O sistema aguardará até 1h para que 100% dos coletores anunciem o recebimento das assinaturas e respondam suas extrações. Havendo até 5% de coletores que não tenham informado o recebimento ou que estejam processando, o sistema aguarda mais uma hora. Após este prazo o sistema retorna as análises sobre os dados dos primeiros coletores e uma nota para o perito informando que ainda restam apurar um determinado número de coletores. Coletores que não responderem a uma ordem em até 24h serão contatados pelos técnicos do modelo para averiguação. Por padrão as assinaturas consideradas básicas recolhem apenas informações consideradas anômalas ao tráfego normal da Internet, sendo a troca de *e-mails* uma atividade comum, é esperado que o sistema não localize nenhuma informação relevante. Nesses casos o sistema irá apurar as informações dos relatórios de despejos, que são as informações resumidas sobre o tráfego normal. O relatório final do perito constará então de informações resumidas sobre quem envio *e-mails* para o réu, o tamanho desses e *e-mails* e a data:

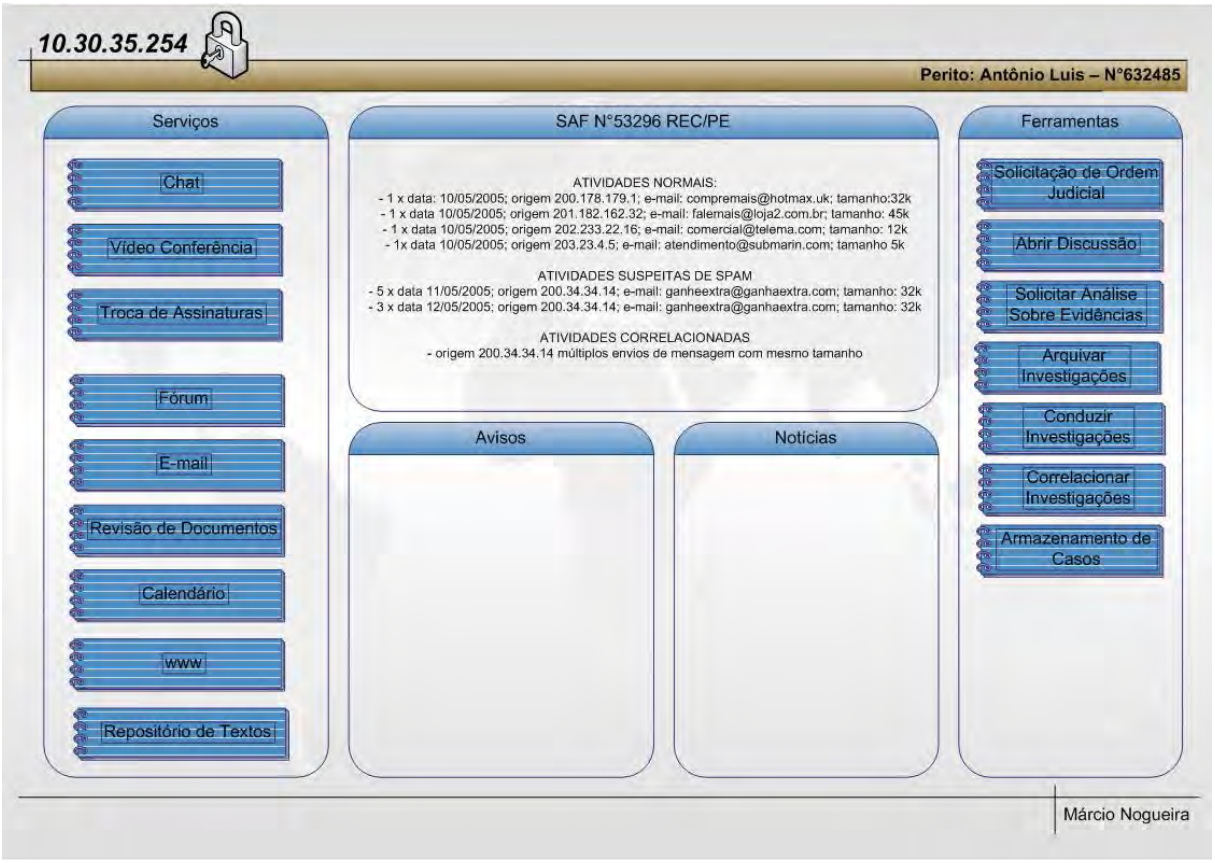


Figura 50 – Relatório de Análise da Investigação

11. A análise retornada pelo sistema já se apresenta na forma de relatório, informando dados normais coletados, possíveis problemas de segurança e correlacionando as extrações com casos semelhantes durante o mesmo período de análise. Com isso o perito minimiza esforços para identificação dos eventos. No caso em questão o relatório apontou um problema de *spam* de uma determinada origem. O próximo passo do perito é solicitar uma nova investigação para acompanhar o fluxo de dados emitido por essa origem e constatar o envio do *SPAM*. Constatado o *SPAM*, e constatado que o vírus *Blaster* foi propagado por este *SPAM* fica confirmado que o acusado foi fonte de envio do vírus que prejudicou o réu. Contudo, o sistema também analisará fontes de infecção pelo acusado. Achando, desenvolverá uma rotina recursiva até encontrar pontos de envio do vírus que não sofreram infecções, ou seja, fontes primárias que originaram a infecção na Internet:

O estudo deste caso mostra que o MREFCON possui um poder de

investigação muito além de uma simples investigação do tipo cliente para cliente. Sua aplicação é indicada para visualizar um cenário maior da Internet e identificar focos de problemas gerais.

4.2 Investigando um PHISHING Scam

Em janeiro de 2005 a revista Veja publicou uma matéria sobre a captura de *hackers* envolvidos em fraudar contas do banco do Brasil através da Internet. Os fraudadores utilizaram uma clonagem perfeita do site do banco e enviaram *spams* na Internet a espera que usuários pescassem a idéia deles.

A operação da polícia federal resultou na captura de mais de 40 acusados no Pará e durou cerca de 6 meses.

Se o MREFCON estivesse disponível na época deste evento certamente este prazo de 6 meses poderia ser reduzido significativamente, vejamos como:

1. Para ter início a investigação bastaria uma única denúncia, feita por *e-mail* para a polícia federal, relatando que *spams* estariam veiculando na Internet induzindo usuários a acessar um *site* pirata do banco do Brasil. Partindo desta denúncia a policia iria solicitar da justiça a seguinte ordem judicial:

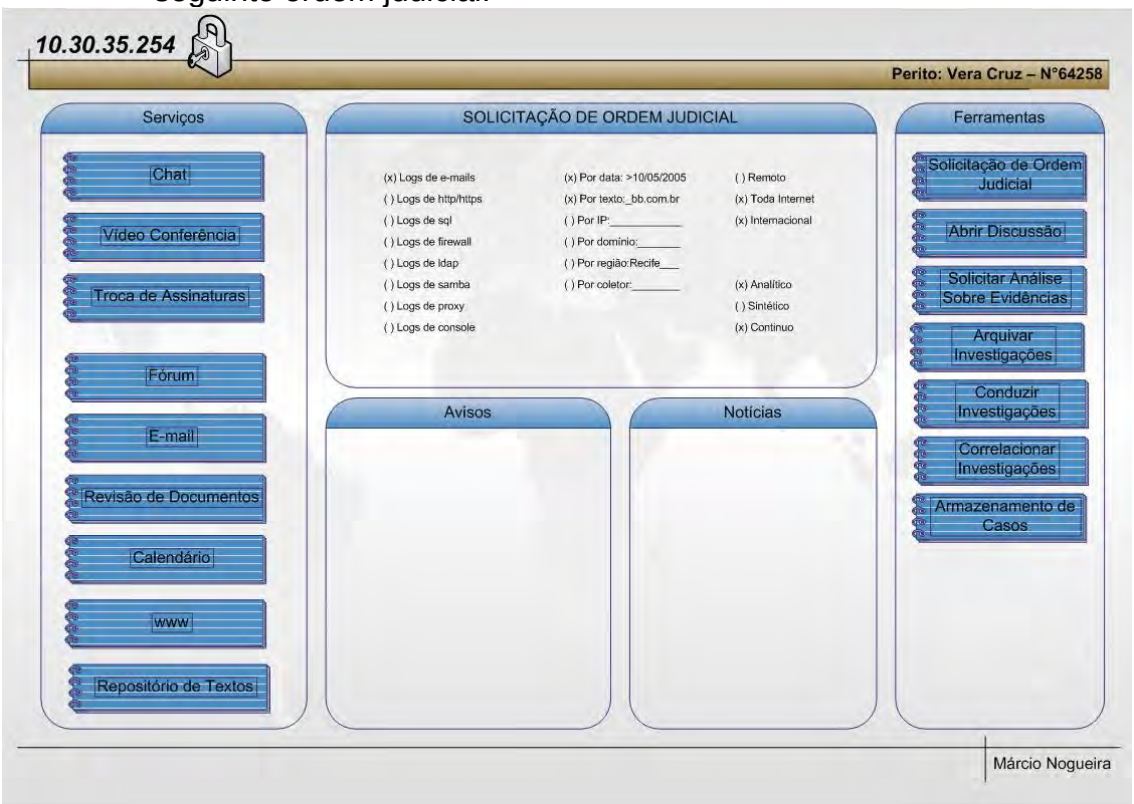


Figura 51 – Requisição de Ordem Judicial partindo de Denúncias

2. A solicitação informa que irá monitorar toda a Internet, nos logs dos *e-mails*, rastreando todas as mensagens que contiverem o conteúdo “bb.com.br”. Como o sistema opera de forma recursiva irá identificar todas as fontes que tiveram em seu conteúdo esta expressão e não todas as mensagens recebidas. Também serão apresentados todos os pontos na Internet de onde foram recebidas mensagens porém não foram registradas informações de envio
3. Observamos aqui que o rastreamento de evento do tipo *phising scam* é mais simples de ser acionado judicialmente e que o retorno pode ocorrer de forma imediata ou ficar em monitoração contínua.

4.3 Investigação Virtual X Investigação Presencial

Observamos através de duas aplicações que o modelo apresenta vantagens e desvantagens em relação a uma investigação conduzida de forma presencial. Resumiremos estes pontos através das seguintes tabelas:

Tabela 11: Investigação Virtual x Presencial

QUESITO	VIRTUAL	PRESENCIAL
Inquéritos envolvendo vários provedores	Tempo máximo de conclusão em 1 semana	Exige várias cartas rogatórias, acarretando em várias semanas
Inquérito envolvendo até 3 provedores	Excessos de dados podem atrapalhar a visão do caso	Geralmente com duas cartas rogatórias resolve o caso
Monitoração de eventos suspeitos em andamento	Eficiente e eficaz	Incapaz de processar esse tipo de investigação
Rastreamento de eventos passados	Falta de dados podem inviabilizar o modelo	Extremamente custoso, mas passível a uma solução
Inteligência em correlacionar eventos	Limitado as experiências da ABIN	Fator humano é bem mais eficiente que o virtual

Onde observamos que o modelo virtual completa o presencial agilizando e não substituindo.

Capítulo 5 Comparações ao *Echelon* e *Carnivore*

O militante dos direitos humanos, Dermi Azevedo, escreveu um artigo acusando o sistema *Echelon* de rastreamento de realizar monitoramento inconstitucional de diversas áreas no mundo, em http://www.dhnet.org.br/direitos/militantes/dermiazevedo/echelon_espionagem.htm, acessado em 12/05/2005, encontramos a seguinte afirmação: “Talvez você não saiba, mas tudo o que você fala pelo telefone ou transmite pela Internet e fax, é controlado, em tempo integral, via satélite, pelo Sistema *Echelon*, uma sofisticada máquina cibernética de espionagem, criada e mantida pela Agência de Segurança Nacional (*NSA*) dos Estados Unidos, com a participação direta do Reino Unido, Canadá, da Austrália e da Nova Zelândia”.

Acrescenta também um breve histórico:

Com suas atividades iniciadas nos anos 80, o *Echelon* tem como embrião histórico, o Pacto denominado *Ukusa*, firmado secretamente pela Grã-Bretanha e pelos EUA, no início da Guerra Fria.

Destinado à coleta e troca de informações, o Pacto *Ukusa* resultou, nos anos 70, na instalação de estações de rastreamento de mensagens enviadas desde e para a Terra por satélites das redes *Intelsat* (*International Telecommunications Satellite Organisation*) e *Inmarsat*.

Outros satélites de observação foram enviados ao espaço para a escuta das ondas de rádio, de celulares e para o registro de mensagens de correios eletrônicos.

Além disto, já sob o guarda-chuva do *Echelon*, são captadas as mensagens de telecomunicações, inclusive de cabos submarinos e da rede mundial de computadores, a lnternet. Em linguagem técnica, o objetivo dessa rede (*network*) é o de captar sinais de inteligência, conhecidos como *sigint*.

O segredo tecnológico do *Echelon* consiste na interconexão de todos os sistemas de escuta. A massa de informações é espetacular e, para ser tratada, requer uma triagem pelos serviços de espionagem dos países envolvidos, por meio de instrumentos da inteligência artificial.

“A chave da interpretação — afirma Nicky Hager; pesquisador do tema — reside em poderosos computadores que perscrutam e analisam a massa de

mensagens para delas extraírem aquelas que apresentam algum interesse. As estações de interceptação recebem milhões de mensagens destinadas às estações terrestres credenciadas e utilizam computadores para decifrar as informações que contêm endereços ou textos baseados em palavras-chaves pré-programadas".

De forma totalmente extralegal, a *NSA* utilizou a rede *Echelon* para espionar todos os movimentos do *Greenpeace* por ocasião dos protestos contra os ensaios nucleares franceses, no Atol de Mururoa, no Pacífico Sul.

O Brasil também participa da história secreta do sistema: por meio da rede, o governo norte-americano interceptou as negociações entre o governo FHC, no primeiro mandato, e a empresa francesa Thomson, para a compra dos equipamentos de vigilância da Amazônia, através do Sivam.

Com base nos dados coletados, a Casa Branca e o complexo industrial estadunidense conseguiram derrubar Thomson e, finalmente, a empresa norte-americana Raytheon acabou ganhando a concorrência internacional.

As comunicações dos países e dos cidadãos latino-americanos são processadas na estação de Sabana Seca, em Porto Rico. Na Inglaterra, o órgão governamental associado à *NSA* é a *GCHQ* (*Britain's Government Communications Headquarters*).

A maior base eletrônica de espionagem no mundo é a *Field Station* F83, da *NSA* e se situa em Menwith Hill, Yorkshire, nos EUA.

Um projeto de lei aprovado pelo Congresso americano amplia o poder policial de investigação eletrônica.
Pela lei atual, "grampos" de internet são permitidos só com ordem judicial que explicite os limites da espionagem "O *Carnivore* é como um filtro gigantesco, que, segundo o *FBI*, deixa passar algumas informações e retém outras, que ficam guardadas num arquivo para serem analisadas", disse Coralee Whitcomb, presidente da organização Profissionais da Computação pela Responsabilidade Social.(Folha de S.Paulo/Mundo/07/10/01).

Em 23/11/2001 Guilherme Kujawski, Paula Pacheco e Sérgio Lírio escreveram um artigo para o *site* Infoguerra, http://www.infoguerra.com.br/infonews/talk/1006552142,29890,.shtml, comentando sobre o sistema *Carnivore*, onde:

'Após os ataques terroristas, a polícia federal americana ganhou argumentos

para vasculhar a internet ao redor do planeta".

O monitoramento de funcionários pode ser feito com *softwares* encontrados nas boas casas do ramo. A lista é enorme: *SurfControl, Websense, MIMEsweeper*, entre outros. Já o programa de espionagem do *FBI*, a polícia federal americana, o *Carnivore*, transcende seus pares, pois espreita de maneira avassaladora qualquer esfera da sociedade.

Sua existência não corre mais o risco de ser ficcional, dada a quantidade de documentos, artigos e demonstrações práticas, como a realizada recentemente por um agente do *FBI* para a associação de administradores de rede nos EUA. Apesar disso, a agência continua recusando-se a falar sobre o assunto.

Carnivore é o nome do programa capaz de interceptar qualquer informação enviada ou recebida pela internet, tanto uma carta de amor, como uma correspondência corporativa ou a cópia de uma canção. O nome "*carnívoro*" é reconhecidamente inadequado, muito mais que o "poema" acróstico designado para representar a nova Lei Antiterrorismo: *USA PATRIOT*. Para extirpar o título predatório, a agência o renomeou com uma sigla mais inofensiva: *DCS1000*.

O *Carnivore* faz parte da terceira geração de instrumentos voltados para grampear a internet. A primeira foi baseada num famoso *software* comercial chamado *Etherpeek*, que auxilia administradores a fazer diagnósticos de redes com o objetivo de detectar problemas técnicos.

A segunda geração, mais sofisticada, era conhecida como *Omnivore* e, em seguida, como *DragonWare Suite*, um conjunto de funções que originou o *Carnivore* propriamente dito. Os recursos do programa nunca foram novidade, pelo menos para a comunidade da área de tecnologia. O que causa estranheza é a maneira pouco transparente de sua aplicação nesse formato policial.

Teoricamente, o *FBI* pode apenas interceptar dados de pessoas que tenham antecedentes em atos de terrorismo, pedofilia, espionagem e fraude. Se um provedor de acesso fornecer inadvertidamente uma conta a uma pessoa que está na lista de suspeitos, deverá ceder, mediante um mandado de busca, uma cópia dos arquivos de registro de tráfego ao *FBI*.

Caso não existam esses arquivos, a agência instala no provedor uma máquina *Carnivore* para monitorar as atividades do suspeito. O detalhe é que,

quando a agência instala este computador, qualquer assinante está sujeito a ser espionado. "Depois dos ataques terroristas, alguns provedores não estão mais nem exigindo um mandado de busca. A tendência agora, aqui, é valorizar a segurança em detrimento da privacidade", diz Gerald L. Kovacich, um especialista americano em segurança.

"Independentemente de serem democráticos ou não, os governos hoje precisam ter um controle sobre o fluxo de informação. Por isso, além do *Echelon*, existem outras formas de espionagem, como o *Frenchelon*, *SORM2* e, claro, as ferramentas chinesas", continua *Kovacich*.

Maiores detalhes sobre o *Echelon* e *Carnivore* estão no [ANEXO A].

Comparando estes dois sistemas com o MREFCON, temos:

Tabela 12: Investigação Virtual x Presencial

DESCRIÇÃO	ECHELON	CARNIVORE	MREFCON
Cobertura	Mundial	Federal USA	Federal BRA
Código Fonte	Privado	Privado	Aberto
Constitucionalidade	Ilegal	Legal	Legal
Confidencialidade	Secreto	Público	Público
Monitoramento	Global	Internet	Internet
Ambiente	Fechado	Fechado	Colaborativo
Pro Hospedeiro	Invisível	Parasita	Simbiose
Autenticação	NSA	FBI	Diversas Entidades
Segurança	Proprietária	Nenhuma	Certificados Digitais
Topologia	Difusão	Sniffer	VPN
Visão	Espionagem	Segurança	Segurança

Capítulo 6 Conclusões

Em relação aos demais sistemas rastreadores apresentados o MREFCON é o único que apresenta características de proteção ao cidadão. Com regras definidas pelas leis federais e aplicação através de suas entidades responsáveis. Não sendo, portanto passível a ilegalidades nas investigações, violando a liberdade individual.

Como inovação de arquitetura o modelo apresenta uma integração simbiótica com os servidores dos provedores de Internet. A instalação de uma máquina virtual em oposição à instalação de uma máquina física garante flexibilidade do sistema. Onde não mais se faz necessário a presença de um perito no provedor de Internet e questões como vigilância indiscriminada de dados são substituídas por regras de programação e acesso a arquivos exclusivos para investigação.

Destacamos ainda, em termos de recursos técnicos, o controle simbiótico de produção, onde o modelo garante ao provedor parceiro que o *software* coletor não prejudique seus serviços, utilizando o máximo de recursos quando disponíveis pela máquina servidor do provedor e minimizando quando a mesma estiver operando com capacidade limitada; os canais virtuais de comunicação, responsáveis por garantir a segurança de todo o modelo, tanto nos coletores quanto no sistema principal; e as interfaces comum de uso baseada em estudos cognitivos e *CSCW*.

Apesar do MREFCON ser um modelo acadêmico, desenvolvido baseado em experiências de laboratório, a aplicação individual de cada ferramenta citada fora testada e analisada conforme apresentação. Para futuro estaremos desenvolvendo novas teses sobre a aplicação desse modelo, apresentando novas tipificações de *cybercrimes*, acrescentando biometria como requisito de validação para acesso ao sistema principal e coletores para plataformas proprietárias.

REFERÊNCIAS BIBLIOGRÁFICAS

[CCTCI, 1997] Crimes eletrônicos e como soluciona-los . Câmera dos Deputados, Brasília, discussão 15 out. 1997. Disponível em: <http://wwww.cg.org.br/infoteca/debates/debate1.htm>. Acesso em: 28/09/2004.

[BROWN, 2005] Dan. Fortaleza Digital. Sextante. Rio de Janeiro, 2005, isbn: 85-754-2161-1

[CASTRO, 2001] Carla Rodrigues Araújo de. Impunidade na Internet . Jus Navigandi, Teresina, a. 6, n. 52, nov. 2001. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=2327>. Acesso em: 06 fev. 2005.

[ARAS, 2001] Vladimir. Crimes de informática. Uma nova criminalidade. Jus Navigandi, Teresina, a. 5, n. 51, out. 2001. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=2250>. Acesso em: 06/02/2005.

[MARTINELLI, 2000] João Paulo Orsini. Aspectos relevantes da criminalidade na Internet . Jus Navigandi, Teresina, a. 4, n. 46, out. 2000. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=1829>. Acesso em: 06/02/2005.

[BARROS, 2003] Lucivaldo Vasconcelos. O crime na era da inform@ção . Jus Navigandi, Teresina, a. 7, n. 61, jan. 2003. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=3675>. Acesso em: 06/02/2005.

[LEONARDI, 2004] Marcel. Vigilância tecnológica, bancos de dados, Internet e privacidade . Jus Navigandi, Teresina, a. 9, n. 499, 18 nov. 2004. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=5899>. Acesso em: 07/02/2005.

[KAMINSKY, 2003] Omar. Bancos de dados e habeas data. Projeto de lei do Senado . Jus Navigandi, Teresina, a. 7, n. 61, jan. 2003. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=3658>. Acesso em: 07/02/2005.

[DL] Direito e Legislação, isbn: 8502-02054-4

[LEITAO, 2002] Júnior, Esdras Avelino. O e-mail como prova no Direito . Jus Navigandi, Teresina, a. 6, n. 57, jul. 2002. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=3025>. Acesso em: 07/02/2005.

[REINALDO, 2004] Demócrito Filho. O projeto de lei sobre crimes tecnológicos (PL nº 84/99). Notas ao parecer do Senador Marcello Crivella. Jus Navigandi, Teresina, a. 8, n. 375, 17 jul. 2004. Disponível em:

<http://www1.jus.com.br/doutrina/texto.asp?id=5447>. Acesso em: 06/02/2005.

[CAS, 2000] Casey, E. *Digital Evidence and Computer Crime.* Academic Press, San Diego, California, 2000, isbn: 01-216-288-5X

[GEU, 2002] Geus, P. L., Reis, M. A. Análise forense de intrusões em sistemas computacionais: técnicas, procedimentos e ferramentas. *Anais do I Seminário Nacional de Perícia em Crimes de Informática*. Maceió. AL. 2002.

[ALECRIM, 2004] Emerson. Disponível em: http://www.infowester.com/col091004.php. Acesso em: 09/10/2004

[INFOGUERRA] Disponível em: http://informatica.terra.com.br/virusecia/spam/interna/0,,OI195623-EI2403,00.html. Acesso em 15/03/2005

[TEIXEIRA] - Renata Cicilini. Características e tipos de Spam. Disponível em: http://informatica.terra.com.br/virusecia/spam/interna/0,,OI195557-EI2403,00.html . Acesso em 15/03/2005

[HOAX] Disponível em: http://hoaxbusters.ciac.org. Acesso em: 15/03/2005

[MILAGRE] José Antonio. Disponível em: http://www.imasters.com.br/artigo.php?cn=3059&cc=215. Acesso em 14/03/2005

[NPP, 2000] Noblett, M., Pollitt, M., Presley, L. (2000). *Recovering and Examining Computer Forensic Evidence.* Forensic Science Communications, Outubro 2000, Volume 2, Número 4. U.S. Department of Justice, FBI. Disponível em: http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm. Acesso em 08/2003.

[PAL, 2001] Palmer, G. *A Road Map for Digital Forensic Research*. In: Digital Forensic Research Workshop (DFRWS). *Report.* 2001. Disponível em: http://vip.poly.edu/kulesh/forensics/docs/DFRWS_RM_Final.pdf. Acesso em: 05/03/2005

[INFOWESTER] Disponível em: http://www.infowester.com/col270205.php. Acesso em: 15/03/2005

[FOCA] Guia Foca GNU/Linux Avançado – Capítulo 12.10. Disponível em: http://focalinux.cipsga.org.br/guia/avancado/ch-s-apache.htm#s-s-apache-logs. Acesso em 20/03/2005

[GNU] GNU/GPL – "*The GNU Project and the Free Software Foundation*". Disponível em: http://www.gnu.org. Acesso em 26/03/2005

[REBECCA, 2000] Bace. Intrusion Detection. Macmillan Technical Publishing,

Indianapolis, IN, 2000.

[SNORT] *Snort IDS* – "*Snort – Network Intrusion Detection System"*. Disponível em: http;//www.snort.org. Acesso em 25/03/2005

[REIS] Reis, Marcelo Abdalla e Geus, Paulo Lício. Modelagem de um Sistema Automatizado de Análise Forense: Arquitetura Extensível e Protótipo Inicial, Campinas/SP.

[SPAMA] *The Apache SpamAssassin Project*. Disponível em: http://spamassassin.apache.org. Acesso em 26/03/2005

[APACHE] Disponível em: http://www.apache.org. Acesso em: 15/03/2005

[SANTOS] Santos, Claudemir C. Funções Hash. Disponível em: http://www.peritocriminal.com.br/hash.htm. Acesso em 16/03/2005

[CARVALHO, 2000] Carvalho, Daniel Balparda de. Segurança de Dados com Criptografia: Métodos e Algorítimos. Book Éxpress. Rio de Janeiro, 2000, isbn: 85-868-4638-4

[UNIX] *Practical UNIX and Internet Security*, isbn: 1-56592-148-8

[MARTINS] Martins, Raildy Azevedo Costa. Conselho Nacional de Assistência Social – Reunião de Comissões Temáticas. Em: A operacionalização do Controle Social. Ministério do Desenvolvimento Social e Combate à Fome. Disponível em: http://www.mds.gov.br/conselhos/down_cnas/18_capacitacao/controle_social_raildy martin.pps#256,1. Aceso em 26/03/2005

[CRIPTY] Disponível em: http://www.absoluta.org/cripty/algoritmos.htm. Acesso em 28/03/2005

[ICP, 2001] Disponível em: http://www.icpbrasil.gov.br/RES_ICP1.htm. Acesso em: 15/03/2005

[RESOLUCAO21740] Disponível em: http://www.tse.gov.br/servicos_online/instrucoes/res21740.htm. Acesso em: 15/03/2005

[ARQIPSEC, 1999] Adailton J. S. Silva **,** Renata Cicilini Teixeira, em: Boletim bimestral sobre tecnologia de redes, RNP – Rede Nacional de Ensino e Pesquisa, 28 de Julho de 1999 | volume 3, número 4, ISSN 1518-5974. Disponível em: http://www.rnp.br/newsgen/9907/ipsec3.html. Acesso em 12/05/2005

[IPSECVPN, 1998] Liou Kuo Chin**,** em: Boletim bimestral sobre tecnologia de redes,

RNP – Rede Nacional de Ensino e Pesquisa, 13 de Novembro de 1998 | volume 2, número 8, ISSN 1518-5974. Disponível em: http://www.rnp.br/newsgen/9811/vpn.html. Acesso em 12/05/2005

[ORTIS, 2003] Eduardo Bellincanta, Ed Wilson Tavares Ferreira. VPN: Implementando Soluções com Linux. São Paulo: Érika, 2003, isbn: 85-7194-952-2

[SOUZA] Souza, Clarisse Sieckenius de; Leite, Jair Cavalcanti ; Prates, Raquel Oliveira; Barbosa, Simone D.J., em: Projeto de Interface de Usuários, Perspectivas Cognitivas e Semióticas. Disponível em: http://www.dimap.ufrn.br/~jair/piu/JAI_Apostila.pdf. Acesso em 17/05/2005

[BARROS, 1994] L. A. Suporte a Ambientes Distribuídos para Aprendizagem Cooperativa. Rio de Janeiro, 1994. Tese (Doutorado). Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia (COPPE), UFRJ.

ANEXOS

Anexo A – Os Sistemas Echelon e Carnivore

[LEONARDI, 2004] Leonardi, Marcel. Vigilância tecnológica, bancos de dados, Internet e privacidade . Jus Navigandi, Teresina, a. 9, n. 499, 18 nov. 2004. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=5899>. Acesso em: 07/02/2005.

6. O monitoramento governamental global: sistemas Echelon e Carnivore.

Após uma série de relatórios e suspeitas sobre a existência de um sistema global de interceptação de comunicações com o nome de código ECHELON, o Parlamento Europeu decidiu, em 5 de junho de 2000, constituir uma comissão temporária encarregada de averiguar sua existência e funcionalidade.

O longo e detalhado relatório elaborado por Gerhard Schmid concluiu que *"a existência de um sistema de escuta das comunicações que opera a nível mundial com a participação dos Estados Unidos da América, do Reino Unido, do Canadá, da Austrália e da Nova Zelândia, no quadro do acordo UKUSA, deixou já de constituir objeto de dúvidas. Com base nos indícios disponíveis, bem como em inúmeras declarações coincidentes oriundas de círculos muito diferenciados, incluindo fontes americanas, pode presumir-se que, pelos menos durante algum tempo, tenha sido dado ao sistema ou a partes do mesmo o nome de código ´´ECHELON´´. Importante afigura-se o fato de o mesmo ser utilizado para fins de escuta das comunicações privadas e econômicas, mas não militares"* .

Entre as características do sistema ECHELON, destaca-se sua capacidade praticamente global de vigilância, através da utilização de estações receptoras que operam via satélite e de satélites de espionagem, os quais permitem a interceptação de qualquer comunicação e de seu respectivo conteúdo, desde que seja efetuada por telefone, fax, Internet ou e-mail, emitida por quem quer que seja.

O ECHELON funciona a nível mundial graças a uma cooperação entre os citados Estados UKUSA, representados pelo Reino Unido, Canadá, Estados Unidos da América, Austrália e Nova Zelândia, os quais podem disponibilizar reciprocamente os respectivos dispositivos de interceptação e escutas, partilhar entre si os encargos e utilizar em comum os resultados obtidos. Interessante destacar que o governo norte-americano se recusa a admitir a existência do sistema ECHELON até a presente data, apesar das inúmeras provas em contrário.

Como destaca o relator, *"a ameaça que o ECHELON encerra para a vida privada e a economia não deve ser vista apenas em função do poderoso sistema de vigilância que representa, mas também pelo facto de operar num espaço praticamente à margem da lei. Um sistema de escutas das comunicações internacionais não incide, na maioria dos casos, nos habitantes do próprio país. O visado não dispõe assim, enquanto estrangeiro, de qualquer forma de protecção jurídica nacional, ficando desse modo inteiramente à mercê deste sistema (...)"* .

O problema da utilização do ECHELON no âmbito global resulta no fato de que o sistema tem sido utilizado para favorecer empresas pertencentes aos Estados UKUSA. Os serviços de informações dos Estados Unidos não se limitam a investigar assuntos de interesse econômico geral, interceptando também as comunicações entre empresas, sobretudo no quadro da concessão de contratos, justificando essa interceptação com o propósito de combater tentativas de corrupção.

O Brasil já foi alvo da espionagem concorrencial norte-americana em 1994, quando da contratação de empresa especializada para o projeto SIVAM (Sistema de Vigilância da Amazônia). O sistema ECHELON foi utilizado pela CIA/NSA para escutar as comunicações entre a empresa vencedora da contratação, a francesa Thomson-CSF, as quais revelaram a suposta existência de corrupção no procedimento, tendo havido pagamento de subornos aos julgadores. Com isto, o governo Clinton formalizou queixa junto ao governo brasileiro, acarretando a transferência do contrato a favor da empresa norte-americana Raytheon. A informação a respeito desse episódio encontrava-se disponível no web site dessa companhia, mas foi removida para evitar maiores controvérsias.

Inúmeros outros exemplos de utilização do sistema ECHELON encontram-se citadas no Relatório, destacando-se, entre outras, a revelação de

suborno na concorrência do consórcio europeu Airbus com o governo da Arábia Saudita, uma transação de 6 bilhões de dólares que acabou por ser concedida à empresa norte-americana McDonnel-Douglas, também no ano de 1994.

A justificativa para a utilização de tal sistema, como se vê, é o suposto combate à corrupção em procedimentos de contratação entre grandes empresas e governos. Evidentemente, no caso de uma interceptação pormenorizada, existe o risco de as informações não serem utilizadas para a luta contra a corrupção, mas sim para a espionagem dos concorrentes, ainda que os Estados Unidos e o Reino Unido declarem que não o fazem.

Apresenta-se de fundamental importância a análise efetuada pelo Parlamento Europeu no que tange à compatibilidade da utilização do sistema ECHELON com o direito da União Européia, bem como com o direito fundamental ao respeito da vida privada e familiar, previsto no artigo 8.º da Convenção Européia dos Direitos do Homem, em destaque nos capítulos 7 e 8 do Relatório elaborado. Resumidamente, o Parlamento Europeu entendeu que (grifamos):

"No atinente à questão da compatibilidade de um sistema do tipo ECHELON com o direito da UE, impõe-se estabelecer a seguinte diferenciação: se o sistema for apenas utilizado para fins de informação, não se observa qualquer contradição com o direito da UE, na medida em que as actividades ao serviço da segurança do Estado não são abrangidas pelo Tratado CE, sendo-lhes aplicável o título V do Tratado UE (PESC), que não contém ainda qualquer disposição nesta matéria, pelo que não se observa qualquer colisão. Se, pelo contrário, o sistema é objecto de utilização abusiva para espionar a concorrência, é o mesmo contrário à obrigação de lealdade que vincula os Estados-Membros e à concepção de um mercado comum em que a concorrência é livre. Se um Estado-Membro nele participa, viola, assim a legislação da União.

Na sua reunião de 30 de Março de 2000, o Conselho declarou não poder aceitar a instituição ou a existência de um sistema de intercepção que não respeite a ordem jurídica dos Estados-Membros e que constitua uma violação dos princípios fundamentais do respeito pela dignidade humana. (...)

Todas as operações de intercepção de comunicações constituem uma grave ingerência na vida privada da pessoa humana. O artigo 8º da Convenção dos Direitos do Homem, que protege a vida privada, apenas permite uma tal ingerência

quando esteja em causa garantir a segurança nacional, desde que a mesma se encontre prevista em disposições do direito nacional, disposições essas que sejam de acesso geral e estabeleçam em que circunstâncias e condições os poderes públicos a ela podem recorrer. Tais ingerências devem ser proporcionadas, razão pela qual se impõe ponderar os interesses em jogo. Não é suficiente que a intervenção seja meramente oportuna ou desejável.

Um sistema de informações que, aleatória e sistematicamente, interceptasse todas e quaisquer comunicações, infringiria o princípio da proporcionalidade e seria, por conseguinte, contrário à Convenção dos Direitos do Homem. Observar-se-ia igualmente uma violação da Convenção se as disposições por força das quais a vigilância das comunicações tem lugar fossem desprovidas de base jurídica, caso esta não fosse acessível a todos ou se se encontrasse formulada de molde a que qualquer indivíduo não pudesse prever as suas consequências. Dado que as disposições com base nas quais os serviços de informações norte-americanos operam no estrangeiro são, em grande parte, secretas, o respeito do princípio da proporcionalidade afigura-se, no mínimo, questionável. Observa-se manifestamente uma violação dos princípios de acesso ao direito e de previsibilidade dos seus efeitos. Embora os EUA não sejam partes contratantes na Convenção relativa aos Direitos do Homem, os Estados-Membros devem proceder à sua observância. Não podem, com efeito, subtrair-se às obrigações que a mesma lhes impõe autorizando os serviços de informações de outros países submetidos a disposições menos rigorosas a operarem no seu território. Caso contrário, o princípio da legalidade e as suas duas componentes (acesso e previsibilidade) seria privado dos seus efeitos e a jurisprudência do Tribunal dos Direitos do Homem seria destituída de conteúdo.

A conformidade com os direitos fundamentais de uma actividade legalmente legitimada de serviços de informações exige, além disso, a existência de suficientes mecanismos de controlo, a fim de equilibrar os riscos inerentes à acção secreta levada a efeito por uma parte do aparelho administrativo. Atendendo a que o Tribunal Europeu dos Direitos do Homem salientou expressamente a importância de um sistema de controlo eficaz no domínio das actividades dos serviços de informações, afigura-se preocupante que alguns Estados-Membros não disponham de órgãos parlamentares de controlo dos serviços secretos".

Assim como o Parlamento Europeu, também entendemos que a utilização do sistema ECHELON para quaisquer outros fins que não a obtenção de informações de interesses de segurança nacional viola frontalmente o direito à privacidade dos indivíduos.

Como se não bastasse, o governo norte-americano utiliza ainda o sistema Carnivore para interceptar toda a transmissão de dados efetuada através da Internet, fazendo-o para combater atividades criminais específicas, incluindo a espionagem, a pornografia infantil e o terrorismo.

Os primeiros relatos sobre o sistema circularam nos EUA em 11 de julho de 2000. Um pedido de informações sobre o funcionamento do sistema formulado pelo Electronic Privacy Information Center (EPIC) foi indeferido, o que motivou a propositura de ação judicial para obrigar o FBI norte-americano a revelar as informações solicitadas. Até então, a agência governamental recusava-se a admitir a existência do sistema.

O material fornecido pelo FBI foi estudado, a pedido do Departamento de Justiça norte-americano, por revisores independentes (IIT Research Institute e Illinois Institute of Technology Chicago-Kent College of Law), os quais analisaram detalhadamente o funcionamento do sistema, em relatório que se encontra disponível no web site do Electronic Privacy Information Center.

Resumidamente, os revisores independentes concluíram que o sistema Carnivore é composto de uma ferramenta de software capaz de examinar todos os pacotes de Protocolo de Internet (IP) em uma rede e registrar apenas aqueles pacotes ou pedaços de pacotes contendo um parâmetro pré-determinado em filtros.

Quando instalado junto a um provedor de acesso à Internet, o software recebe todos os pacotes do segmento da rede em que está conectado e registra os pacotes ou pedaços que contenham informações pré-estabelecidas em um filtro. O Carnivore não transmite dados pela rede e também não pode fazer nada com os pacotes além de filtrá-los e, opcionalmente, registrá-los. O sistema apenas lê os dados recebidos, não alterando os pacotes destinados a outros computadores nem tampouco iniciando quaisquer transmissões, não interferindo, portanto, no tráfego regular da rede.

Em tese, o sistema é utilizado para efetuar a vigilância de

comunicações via Internet, de sorte a investigar crimes determinados, mediante ordem judicial específica, e apenas quando outros métodos de obtenção de informação não bastem para atender às necessidades da investigação ou às restrições impostas pelo Judiciário.

Antes da utilização do Carnivore, é necessária uma autorização do Departamento de Justiça e do FBI norte-americanos, sendo possível ao juiz prolator da ordem, a qualquer tempo, verificar se o tráfego sendo coletado efetivamente se restringe àquele que foi autorizado. Além disto, o sistema somente é colocado em utilização após a investigação criminal respectiva não ter obtido resultados através dos métodos normais de coleta de informações, o que deve ser devidamente demonstrado.

Todas as informações coletadas pelo sistema são gravadas em formato ininteligível ao usuário comum, necessitando de outro software específico para análise humana. Tais informações só podem ser acessadas pelo próprio FBI, sendo interessante observar que os agentes que configuram o sistema e estabelecem os filtros de dados não são os mesmos agentes que posteriormente analisam o material coletado, o que, em princípio, assegura a lisura do procedimento. As configurações utilizadas (contendo os filtros estabelecidos) podem ser analisadas separadamente, permitindo, assim, verificar se obedeceram rigorosamente aos parâmetros previstos na ordem judicial.

Corretamente utilizado, o sistema Carnivore é um excelente recurso à disposição das autoridades norte-americanas para realizar a interceptação de informações transmitidas através da Internet que possam, porventura, ter utilidade no combate ao crime organizado e ao terrorismo.

Boa parte da controvérsia envolvendo o sistema Carnivore reside no fato de que o sistema acessa e processa boa parte do tráfego de um provedor de acesso à Internet, sujeitando a grande maioria dos usuários – que não são objeto da vigilância – ao controle do FBI. Todas as comunicações privadas dos usuários de um provedor de acesso onde o Carnivore esteja sendo utilizado estarão sujeitos ao monitoramento, o que evidentemente cria grandes riscos para sua privacidade.

O sistema Carnivore pode, efetivamente, coletar mais informações do que aquelas autorizadas pela Justiça. Quando o sistema está adequadamente configurado, apenas registra o tráfego que está de acordo com os filtros

estabelecidos. Em caso contrário, o sistema é capaz de registrar todo o tráfego que monitora. Esta característica pode ser abusada por investigadores pouco éticos, notadamente quando se observa que o sistema não identifica os agentes que estabeleceram os filtros.

De fato, não é possível determinar quem, dentro de um grupo de agentes com senha de acesso ao sistema, estabeleceu ou modificou os parâmetros do filtro. Em verdade, qualquer procedimento adotado pelo Carnivore pode ser determinado por qualquer pessoa que conheça a senha de acesso do administrador do sistema, sendo impossível rastrear o usuário específico que o utilizou, fato que, evidentemente, também propicia abusos.

Em outras palavras, o funcionamento do sistema e sua adequação à ordem judicial prolatada dependem exclusivamente da correta utilização dos filtros de dados. Configurado incorretamente, o sistema pode coletar todo o tráfego da rede onde está instalado.

Há ainda o risco de que pessoas não-autorizadas pertencentes ao quadro de funcionários da empresa provedora de acesso à Internet utilizem o sistema ou observem-no em funcionamento. Ainda que o computador encarregado da coleta de dados não tenha monitor de vídeo, teclado nem mouse, as entradas respectivas não são protegidas. O FBI apenas isola a área em que o computador que coleta as informações está instalado, o que pode ser insuficiente para assegurar que nenhum terceiro tenha acesso ao sistema.

A utilização do Carnivore interessa aos usuários de Internet de todo o planeta, e não apenas aos norte-americanos, na medida em que o sistema pode ser empregado para monitorar todo o tráfego de dados que circula naquele território. Considerando-se que o tráfego da Internet circula pelos caminhos que estiverem disponíveis, o que é da própria natureza da rede, pode-se dizer que a maioria das comunicações transmitidas através da Internet passa ou pode passar pelos equipamentos norte-americanos, sujeitando-se, nesse passo, ao monitoramento pelo sistema Carnivore.

Observe-se, ainda, que inúmeros outros sistemas de vigilância eletrônica são utilizados pelas agências governamentais de diversos países, sempre sob o argumento de combate ao terrorismo e ao crime organizado. Resta saber se são efetivamente utilizados apenas para esses nobres fins.

Anexo B – Projeto de Lei N° 84/99

COMISSÃO DE CONSTITUIÇÃO E JUSTIÇA E DE REDAÇÃO

PROJETO DE LEI Nº 84, DE 1999

Dispõe sobre os crimes cometidos na área de informática, suas penalidades, e dá outras providências.

Autor: Deputado Luiz Piauhylino

Relator: Deputado Léo Alcântara

I - RELATÓRIO

O Projeto de Lei em epígrafe intenta disciplinar as relações no campo da informática, tipificando condutas e instituindo penas, além de disciplinar o uso de bancos de dados em computador contendo informações privadas.

Justifica-o o ilustre Autor afirmando, em síntese, que a sua proposta foi fruto do trabalho de um grupo de juristas; e que, no nosso ordenamento jurídico, não dispomos de lei que trate especificamente do tema e que regule os crimes de informática.

O Projeto foi aprovado pela Comissão de Ciência e Tecnologia, Comunicação e Informática.

Não foram apresentadas emendas no prazo regimental.

Foram apensados os Projetos de Lei nºs 2.557 e 2.558, de 2000, ambos do ilustre Deputado Alberto Fraga, e 3.796, de 2.000 do nobre Deputado Luciano Castro.

O de nº 2.557,de 2000, visa acrescentar ao Código Penal Militar, Decreto-Lei 1.001, de 21 de outubro de 1969, crimes relativos à violação indevida de banco de dados, ou interceptação de comunicação militar entre redes de comunicação eletrônica.

O PL 2.558, de 2000, visa acrescentar o mesmo tipo legal, só que no Código

Penal, Decreto-Lei 2.848, de 7 de dezembro de 1940.

O PL 3.796, de 2000, acrescenta um Capítulo ao Título II do Código Penal, prevendo condutas delituosas na área de informática.

A esta Comissão de Constituição e Justiça e de Redação cabe analisá-los sob os aspectos de constitucionalidade, juridicidade, técnica legislativa e mérito, sendo a apreciação final do Plenário da Casa.

É o relatório.

II - ANÁLISE

Os Projetos de Lei nºs 84/99, 2.557, 2.558, e 3.796 de 2.000, não apresentam vícios de natureza constitucional, de juridicidade ou de técnica legislativa.

No mérito, as Propostas vêm ao encontro do desamparo que se encontra nossa sociedade, que reclama por providências legislativas na área de crimes de computador. Diariamente temos notícias de fraudes, e de prejuízos de grande monta, resultantes de ações praticadas por meio de computadores, ou contra sistemas de computadores. Invariavelmente, tais notícias vêm acompanhadas de queixas sobre a dificuldade ou impossibilidade de punir várias dessas ações, por falta de uma legislação específica.

Alguns especialistas posicionam-se contra a criação de novos tipos legais para parte das condutas aqui tipificadas, entendendo já estarem contempladas na legislação penal vigente. Segundo eles, , por exemplo, o dano ocasionado a dado ou programa de computador, enquadra-se no dano feito em coisa alheia, tipificado no Código Penal no seu art. 163. que dispõe:

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia:

Pena – detenção, de um mês a seis meses, ou multa.

Não haveria necessidade, portanto, de novo tipo penal, para cuidar de tal conduta.

Todavia, tendo em vista a exigência constitucional de lei anterior para definir o crime e impor a respectiva pena, não sendo admissível o uso de analogia ou ampliações para incriminar determinada conduta, preferimos adotar uma postura de prudência, reconhecendo como legítima a postulação de tal matéria em lei nova. É inegável a existência de dificuldades na punição das ações aqui enfocadas. Dando-lhes tratamento específico, colmatamos qualquer lacuna que porventura pudesse vir a ser invocada pelos agentes da conduta para evadir-se à justa sanção da

sociedade, e eliminamos as referidas dificuldades.

Vislumbramos, todavia, que as penas estabelecidas para os crimes ora tipificados não estão em perfeita consonância com o sistema de gradação das penas adotado pelo nosso Código Penal. Basta comparar a pena estabelecida no Código para o já mencionado crime de dano, – detenção de um mês a seis meses, e multa – , com aquela instituída pelo art. 8º do presente projeto para o crime de dano a dado ou programa – detenção de um ano a três anos, e multa. Não deveria haver tal desproporção, uma vez que o bem jurídico protegido é o mesmo, e os delitos são semelhantes. Procedemos, portanto, à devida adequação.

Por outro lado, verificamos que exatamente o mesmo conjunto de circunstâncias qualificadoras é previsto para cada um dos crimes, numa repetição perfeitamente eliminável, pela inclusão de um único artigo dispondo sobre a sua aplicação a todos os crimes ali tipificados.

Analisando o projeto à luz da Lei Complementar nº 95, de 26 de fevereiro de 1998, que rege a elaboração, redação e alteração das leis, constatamos a necessidade de incluir um primeiro artigo indicando o objeto da lei, bem como a de alongar o prazo para a sua entrada em vigor, contemplando um período proporcional à repercussão da lei.

Embora fosse recomendável elencar no bojo do Código Penal os crimes de que trata este projeto, afigura-se correta a iniciativa para introdução de lei extravagante. Isso ocorre porque a proposição trata também de assuntos que não poderiam ser inseridos naquele Código. Desse modo, somente em legislação esparsa poderemos ver tipificadas as condutas criminosas relativas à informática.

Essa mesma multiplicidade de temas impõe a modificação da ementa, que passa a expressar o tratamento desses outros assuntos além dos crimes de informática.

Ademais, note-se que, em nosso Código Penal, a quantidade da pena in abstracto vem especificada simultaneamente em números e por extenso e, ainda, que a Lei Complementar determina, em seu art. 11, II, f, que qualquer referência a número ou percentual deve ser feita por extenso. Por tal motivo, modificamos a redação das penas previstas.

Alteramos a ordem dos artigos que tratam dos crimes, para que a seqüência refletisse a ordem provável dos atos de um agente desse tipo de crime, bem como

uma possível gradação da gravidade dos delitos cometidos.

Finalmente, sugerimos a supressão dos arts. 14 e 18, com a conseqüente renumeração dos demais.

O art. 14 regulamentava a veiculação de material pornográfico em rede de computadores. Considerando o uso intensivo que atualmente crianças e adolescentes fazem do computador, cujo uso se encontra cada vez mais associado a atividades educativas e culturais, não há porquê transformá-lo em meio de divulgação de pornografia. O controle do acesso ao computador por usuários menores de idade é mais difícil do que o controle do conteúdo divulgado, sendo, portanto, mais produtivo proibir a veiculação de material pornográfico do que o acesso a ele.

O art. 18 contraria a norma constitucional consagrada no art. 84, IV, que estabelece como competência privativa do Presidente da República a regulamentação das leis. Conseqüentemente, ao estabelecer prazo ao Poder Executivo para realização de tal tarefa, está avançando na sua competência constitucional. Realmente, não faria sentido o Legislativo impor a duração desse processo, pois este envolve tratamento de detalhes de operacionalização que são da alçada exclusiva do Executivo, que sobre eles tem melhor compreensão, de vez que os gerencia. Nesse sentido já se pronunciou o Supremo, em sede de ação direta de inconstitucionalidade, declarando a inconstitucionalidade de se assinalar tal prazo.

Todavia, no que concerne às Proposições de Lei nºs 2.557 e 2.558, de 2000, cremos que não há necessidade de alterações no Códigos Penal e no Código Penal Militar, como sugerido. Eis que, uma vez aprovado o presente Projeto de Lei nº 84/99, as hipóteses naqueles ventiladas já estão neste contempladas, sendo aplicadas erga omnes.

O Projeto de Lei nº 3.796, de 2000, cuidando da mesma matéria elencada pela Proposição principal e pelas mesmas razões apontadas acima, não pode ser aprovado.

III – VOTO

Ante o exposto, voto pela constitucionalidade, juridicidade, boa técnica legislativa das Proposições analisadas; e, no mérito, pela aprovação do Projeto de Lei nº 84, de 1999, na forma do Substitutivo que apresento, e pela rejeição dos de

nºs 2.557, 2.558, e 3.796 de 2.000.

Deputado LEO ALCÂNTARA (Relator)

COMISSÃO DE CONSTITUIÇÃO E JUSTIÇA E DE REDAÇÃO

PROJETO DE LEI Nº 84, DE 1999 (SUBSTITUTIVO)

Regula o uso de bancos de dados, a prestação de serviços por redes de computadores, dispõe sobre os crimes cometidos na área de informática, e dá outras providências.

O CONGRESSO NACIONAL decreta:

1. Art. 1º Esta Lei regula o uso de bancos de dados e a prestação de serviços por redes de computadores, dispõe sobre os crimes cometidos na área de informática, e dá outras providências.

CAPÍTULO I

DOS PRINCÍPIOS QUE REGULAM A PRESTAÇÃO DE SERVIÇO

POR REDES DE COMPUTADORES

Art. 2º O acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede.

Art. 3º É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições específicas reguladas em lei.

CAPÍTULO II

DO USO DE INFORMAÇÕES DISPONÍVEIS EM COMPUTADORES

OU REDES DE COMPUTADORES

Art. 4° Para fins desta Lei, entendem-se por informações privadas aquelas relativas à pessoa física ou jurídica identificada ou identificável.

Parágrafo único. É identificável a pessoa cuja individuação não envolva

custos ou prazos desproporcionados.

Art. 5° Ninguém será obrigado a fornecer informações sobre si ou sobre terceiros, salvo nos casos previstos em lei.

Art. 6° A coleta, o processamento e a distribuição, com finalidades comerciais, de informações privadas ficam sujeitas à prévia aquiescência da pessoa a que se referem, que poderá retirá-la a qualquer momento, ressalvando-se o pagamento de indenizações a terceiros, quando couberem.
§ 1° Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.
§ 2° A toda pessoa cadastrada dar-se-á conhecimento das informações privadas armazenadas a ela referentes, bem como das respectivas fontes, ficando-lhe assegurado o direito à retificação gratuita de qualquer informação privada incorreta.
§ 3° Qualquer pessoa, física ou jurídica, tem o direito de interpelar o proprietário de rede de computadores ou provedor de serviço para saber se mantém informações a seu respeito, e o respectivo teor.

Art. 7º As entidades que coletam, armazenam, processam, distribuem ou comercializam informações privadas, ou utilizam tais informações para fins comerciais ou para prestação de serviço de qualquer natureza, ficam obrigadas a explicitar, desde o início de tais atividades:
I - os fins para os quais se destinam tais informações; e
II os limites de suas responsabilidades no caso de fraude ou utilização imprópria das informações sob sua custódia, bem como as medidas adotadas para garantir a integridade dos dados armazenados e a segurança dos sistemas de informação.

Art. 8° As entidades mencionadas no artigo anterior não poderão divulgar ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente,

à origem racial, opinião política, filosófica ou religiosa, crenças, ideologias, saúde física ou mental, vida sexual, registros policiais, assuntos familiares ou profissionais, vida privada, honra e imagem das pessoas, informações nominais restritivas de crédito, oriundas de títulos ou documentos de dívida que não tenham sido regularmente protestados, bem como as relativas a ações, processos e feitos ajuizados, cujas decisões não tenham transitado em julgado e que a lei definir como sigilosas, salvo por ordem judicial ou com anuência expressa da pessoa a que se referem ou do seu representante legal.

CAPÍTULO III

DOS CRIMES DE INFORMÁTICA

Seção I

Acesso indevido ou, não autorizado

Art. 9° Acesso, indevido ou não autorizado, a dados ou informações armazenadas no computador ou em rede de computadores.

Pena – detenção, de um mês a um ano, e multa.

Parágrafo único. Na mesma pena incorre quem, sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro meio de acesso a computador ou rede de computadores.

Seção II

Alteração de senha ou meio de acesso a
programa de computador ou dados

Art. 10. Apagar, destruir, alterar, ou de qualquer forma inutilizar, senha ou qualquer outro meio de acesso a computador, programa de computador ou de dados, de forma indevida ou não autorizada.

Pena – detenção, de seis meses a dois anos, e multa.

Seção III

Obtenção, manutenção ou fornecimento indevido, ou não autorizado, de
dado ou instrução de computador

Art. 11. Obter, manter ou fornecer, de forma indevida ou não autorizada, dado

ou instrução de computador.

Pena – detenção, de um mês a um ano, e multa.

Seção IV

Dano a dado ou programa de computador

Art. 12. Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.

Pena: detenção, de um a seis meses, e multa.

Seção V

Criação, desenvolvimento ou inserção em computador de dados ou programa de computador com fins nocivos

Art. 13. Criar, desenvolver, inserir ou fazer inserir, dado ou programa de computador, em computador ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador, ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores, ou o acesso a estes.

Pena – detenção, de um ano a dois anos, e multa.

Seção VI

Violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar

Art. 14. Obter ou fornecer segredos, de indústria ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.

Pena: detenção, de seis meses a dois anos, e multa.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 15. Se qualquer dos crimes previstos nesta Lei é praticado no exercício

de atividade profissional ou funcional, a pena é aumentada de um sexto até a metade.

Art. 16. Se qualquer dos crimes previstos nesta Lei, é cometido:
I – contra a União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II – com considerável prejuízo para a vitima;
III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV – com abuso de confiança;
V – por motivo fútil;
VI – com o uso indevido de senha ou processo de identificação de terceiro; ou
VII – com a utilização de qualquer outro meio fraudulento.
Pena – reclusão, de dois a seis anos, e multa.

Art. 17. Nos crimes definidos nesta Lei, somente se procede mediante queixa ou representação do ofendido, salvo se cometidos contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundações instituídas ou mantidas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo poder público, casos em que a ação é pública incondicionada.

Art. 18. Esta Lei regula os crimes relativos à informática sem prejuízo das demais cominações legais.

Art. 19. Revogam-se os arts. da Lei nº 9.507, de 12 de novembro de1997.

Art. 20. Esta Lei entra em vigor no prazo de noventa dias decorridos de sua publicação.

Anexo C – Comentários sobre o PL84/99

O Projeto de Lei sobre crimes tecnológicos (PL n. 84/99) – notas ao parecer do Senador Marcello Crivella

Demócrito Ramos Reinaldo Filho*

O Senador Marcelo Crivella apresentou seu relatório quanto ao PLC n. 89/2003, na condição de membro da Comissão de Constituição, Justiça e Cidadania do Senado Federal. O projeto em questão, originário da Câmara (PL n. 84/99), de autoria do Dep. Luiz Piauhylino, altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), dispondo sobre os crimes cometidos no campo da informática e suas penalidades.

Trata-se da superação de mais uma fase da longa caminhada que o projeto vem percorrendo. Só na Câmara dos Deputados passou por quatro comissões temáticas, recebeu várias emendas, apensamentos a outros projetos e substitutivos. Chegou ao Senado no dia 13-11-2003, tendo sido enviado para a CCJ no dia seguinte, onde ainda se encontra para ser votado pelos membros da comissão e, em seguida, pelo plenário da casa legislativa.

O projeto tem a virtude de pretender se tornar a primeira lei brasileira que trata de uma maneira ampla e sistematizada dos crimes cometidos através dos meios informáticos (1). Não apenas cria tipos penais novos, mas estende o campo de incidência de algumas figuras já previstas no CP para novos fenômenos ocorrentes nos meios desmaterializados - impossíveis de ter sido previstos pelo legislador de 1940, ano de edição do atual Código Penal. Como se sabe, persistiu uma discussão doutrinária se a legislação brasileira precisava ser reformada ou se ela já satisfazia e era suficiente para punir os comportamentos criminosos que ocorrem nos ambientes desmaterializados dos sistemas informáticos e das redes telemáticas. Para alguns, os chamados "crimes informáticos" são apenas uma faceta

de realidades já conhecidas, crimes e condutas já tipificadas em sua definição material que apenas são cometidos com o auxílio de outros recursos (os elementos informáticos). A grande verdade, porém, é que determinadas condutas surgidas nesses ambientes são inteiramente novas, e não guardam relação ou similitude com tipos já descritos na lei atual, havendo uma necessidade de sua reformulação para "acompanhar os novos tempos - a Era Digital", como ressaltou o Sen. Marcelo Crivella em seu parecer (2). Por isso o projeto de lei em comento cria novos tipos penais, não se limitando a reformular conceitos legais existentes.

O projeto, na versão aprovada pelo Plenário da Câmara (em novembro de 2003), criava os seguintes tipos penais, cometidos contra sistemas informáticos ou por meio deles: a) acesso indevido a meio eletrônico (art. 154-A); b) manipulação indevida de informação eletrônica (art. 154-B); c) pornografia infantil (art. 218-A); d) difusão de vírus eletrônico (art. 163, § 3º); e e) falsificação de telefone celular ou meio de acesso a sistema informático (art. 298-A) (3). O projeto também elaborava os conceitos legais de "meio eletrônico" e "sistema informatizado", para efeitos penais (art. 154-C). Além disso, produzia as seguintes alterações em figuras penais já existentes: a) acrescentava a "telecomunicação" no tipo penal de *atentado contra a segurança de serviço de utilidade pública* (art. 265 do CP) e no de *interrupção ou perturbação de serviço telegráfico ou telefônico* (art. 266 do CP); b) estendia a definição de *dano* do art. 163 do CP (crime de dano), por meio da equiparação à noção de "coisa" de elementos de informática como "dados", "informação" e "senha", sob a nova rubrica do dano eletrônico (acrescentando o § 2º, I e II); c) equiparava o cartão de crédito a documento particular no tipo *falsificação de documento particular*, acrescentando um parágrafo único ao art. 298 do CP, sob a rubrica de falsificação de cartão de crédito; e d) permitia a interceptação do fluxo de comunicações em sistema de informática ou telemática, mesmo para crimes punidos apenas com detenção, por meio do acréscimo de um § 2º ao art. 2º da Lei n. 9.296, de 24 de julho de 1996 (esta regula a interceptação das comunicações telefônica, informática e telemática).

O Sen. Marcelo Crivella, muito apropriadamente, entendeu que o projeto necessitava de alguns aperfeiçoamentos. É claro que isso se deve ao longo tempo de maturação que o projeto ficou na Câmara, mas também é fato de que o projeto original não contemplava algumas condutas já previstas em legislações de outros

países, como bem lembrou o Senador. Nesse sentido, apresentou algumas emendas criando novas figuras delituais, tais como os crimes de falsidade informática (art. 154-C) e de sabotagem informática, com a emenda relativa a eles assim redigida:

"Falsidade Informática

Art. 154-C. Introduzir, modificar, apagar ou suprimir dado ou sistema informatizado, ou, de qualquer forma, interferir no tratamento informático de dados, com o fim de obter, para si ou para outrem, vantagem indevida de qualquer natureza, induzindo a erro os usuários ou destinatários.

Pena - detenção, de um a dois anos, e multa.

Parágrafo único. Nas mesmas incorre quem, com a mesma finalidade, cria, disponibiliza ou divulga comunicação eletrônica falsa.

Sabotagem Informática

Art. 154-D. Introduzir, modificar, apagar ou suprimir dado ou sistema informatizado, ou, de qualquer forma, interferir em sistema informatizado, com o fim de desorientar, embaraçar, dificultar ou obstar o funcionamento de um sistema informatizado ou de comunicação de dados à distância.

Pena - detenção, de um a dois anos, e multa".

O acréscimo dessas duas figuras (4) traz inegáveis avanços ao projeto e o atualiza em relação às novas espécies de crimes informáticos cometidos por meio de redes eletrônicas.

A definição do crime de *falsidade informática*, e em especial a subespécie da *comunicação eletrônica falsa* (encapsulada no parágrafo único do art. 154-C), vem em boa hora diante do fenômeno que se tornou a marca cada vez mais comum dos crimes cometidos nos ambientes das redes informáticas: a associação entre fraudadores e *spammers*. A nova faceta de um problema que cada vez mais assola os usuários, o recebimento de mensagens não solicitadas (*spams*), agora vem adicionado às tentativas de fraudes eletrônicas (*scams*). Não se trata somente das tradicionais mensagens eletrônicas enganosas, contendo texto com as famosas "correntes" ou promessas de recompensa. Agora, elas costumam vir adicionadas de "programas maléficos" atachados à própria mensagem de *e-mail*. Uma vez abertos esses arquivos anexos, eles instalam programas espiões no computador do

destinatário da mensagem, do tipo *spyware* ou *trojan* (cavalo de tróia), que permite que o agente criminoso tenha acesso remoto a todo o sistema do computador atacado (5). Um tipo específico desses programas espiões (o *keylogger*) tem capacidade para registrar qualquer tecla pressionada pelo usuário do computador infectado, bem como alguns movimentos do *mouse*, e enviar esses dados (por *e-mail*) para o agente criminoso que opera um computador remoto, tudo sem o conhecimento da vítima. Esse tipo de programa permite capturar informações críticas, como senhas e números de contas bancárias.

Um tipo de estelionato eletrônico que teve um incremento muito grande no último ano (de 2003) e começo deste foi o conhecido como *phishing scam*. Nessa subcategoria de fraude através de comunicação eletrônica falsa (*scam*), os *e-mails* têm na indicação da origem um remetente aparentemente confiável, a exemplo de uma instituição bancária, um órgão do governo, uma administradora de cartão de crédito ou um conhecido *site* de comércio eletrônico (6). A nota característica, portanto, dos *phishing scams* é que o estelionatário se faz passar por uma confiável fonte e usa geralmente o endereço de e-mail dessa fonte (ou endereço eletrônico ligeiramente parecido, mas suficiente a confundir o destinatário) ou falseia seu endereço na *Web* (7), prática conhecida como *spoofing*. A mensagem falsa contém uma solicitação de informações pessoais ou um *link* para um endereço falso onde deve ser preenchido um formulário. No *website* falso, a pessoa é solicitada a fornecer número do cartão de crédito, dados de contas bancárias e números de documento de identidade, entre outros. De posse desses dados, os estelionatários (*scammers*) transferem os recursos das vítimas para suas próprias contas (8).

A redação do dispositivo em comento (art. 154-C), a ser introduzido no CP, pretende abarcar todas essas modalidades de fraudes eletrônicas, ao prever que incorre no tipo penal de *falsidade informática* todo aquele que "de qualquer forma interferir no tratamento informático de dados, com o fito de obter, para si ou para outrem, vantagem indevida de qualquer natureza, induzindo a erro os usuários ou destinatários" (*caput*). As fraudes eletrônicas perpetradas por *e-mail*, ainda que sem a utilização de programas espiões, também não escapam da regulamentação, na medida em que o parágrafo único esclarece que "nas mesmas penas incorre quem, com a mesma finalidade, cria, disponibiliza ou divulga comunicação eletrônica falsa" - na verdade o parágrafo único estabelece a figura do crime de *comunicação*

eletrônica falsa, como já observamos acima.

É suficiente, portanto, o simples envio de uma mensagem eletrônica falsa, com a finalidade de obter vantagem indevida, mediante a indução do operador ou usuário de um sistema informático a erro. O artifício ou meio fraudulento necessário à caracterização do crime pode ser exclusivamente a mensagem eletrônica falsa, desde que daí surta um duplo resultado: a vantagem indevida (ilícita) e o prejuízo alheio (da vítima). A consumação propriamente dita exige esses dois elementos (vantagem ilícita e dano patrimonial), mas a figura do crime de *falsidade informática* admite a tentativa, da mesma forma como o estelionato tradicional (do art. 171 do CP). Em outras palavras, aquele que envia mensagem eletrônica falsa, com essa finalidade (a obtenção de vantagem indevida), ainda que não se concretize o prejuízo do destinatário, responde pelo crime na modalidade tentada, até porque, nessa hipótese, a fraude já estaria caracterizada.

Entendemos que a pena prevista para esse tipo de crime está muito atenuada, pois o limite é de 2 anos de detenção (e multa). A *falsidade informática* pode gerar imensos prejuízos patrimoniais para empresas e pessoas físicas, em escala ampliada. Observe-se que para o crime de estelionato tradicional a pena é de reclusão até 5 anos. Não há motivo, portanto, para que sua versão eletrônica tenha previsão de pena mais branda, na medida em que o seu potencial de lesão é muito mais acentuado.

É importante também destacar que a regra do art. 154-C, que se pretende introduzir no CP por meio do projeto, não objetiva e nem tampouco resolveria o problema específico do *spam* - o envio de mensagens não solicitadas. A questão do *spam* deve ser tratada em uma lei específica, contendo uma regulamentação completa e exaustiva sobre o problema, que estabeleça os tipos penais, as exceções (os casos em que se legitima o envio de mensagens comerciais não solicitadas), atribua poderes a agências governamentais para fiscalizar e aplicar multas, contenha previsão das sanções civis e penais, dos limites das penas pecuniárias, atribua recompensa a quem prestar informações que auxiliem a desvendar identidades dos criminosos, entre outras medidas. Algumas leis estrangeiras editadas recentemente sobre *spam* têm mais de cem dispositivos (9). Além do mais, a questão do *spam* é objeto de vários projetos que estão tramitando atualmente no Congresso Nacional. O futuro art. 154-C se limita, como

se disse antes, ao problema das fraudes eletrônicas, quer sejam elas cometidas com ou sem a utilização de *e-mail*. Trata-se de uma ferramenta legal para combater os *scammers*, e não propriamente os *spammers*.

A figura do crime de *sabotagem informática*, delineado no descritor normativo do art. 154-D, pretende por sua vez alcançar outras modalidades de crimes informáticos cometidos em rede, a exemplo do conhecido *denial-of-service attack*, um tipo de delito que pode resultar em significante perda de tempo e dinheiro para as vítimas, em geral empresas que operam serviços na Internet ou em outras redes de arquitetura aberta.

O principal objetivo nesse tipo de ataque é impossibilitar a vítima (um sistema informático) de ter acesso a um particular recurso ou serviço. Em geral, não somente o operador do sistema atacado fica impossibilitado de fazer uso dele, mas também seus legítimos usuários. Por exemplo, existem *hackers* que atuam inundando uma rede informática por meio do envio de massivos pacotes de informações, impedindo assim o tráfico na rede (ainda que temporariamente) de todos os seus usuários; em outros casos, atuam tentando romper a conexão entre o computador do usuário ao do seu provedor, obstaculizando o acesso a um serviço prestado por esse último. Em suma, esse tipo de ataque essencialmente visa a desabilitar o computador da vítima ou a rede informática que ela usa para prestar ou receber um serviço. O pior é que esse tipo de ataque pode ser executado com limitados equipamentos contra sofisticados *sites* e sistemas informáticos. Usando um velho e simples PC e uma conexão à Internet de baixa velocidade, um *hacker* consegue incapacitar máquinas e redes informáticas tecnicamente sofisticadas.

Os modos de ataque são os mais variados possíveis, atingindo a velocidade do tráfico de informações na rede, a memória ou espaço em disco do sistema informático ou sua estruturação de dados.

Boa parte dos ataques que se enquadram nessa categoria (*denial-of-service*) são cometidos contra a velocidade ("banda") de conexão à rede. O objetivo, nesse caso, é prevenir o provedor ou mantenedor da rede de se comunicar com outras redes ou sistemas informáticos. Explico: o *hacker* executa seu ataque por meio do estabelecimento de uma conexão com a máquina do servidor-vítima, mas o faz de tal maneira que a conexão não se completa. Nesse meio tempo, ele impede que os usuários legítimos do sistema se comuniquem com o servidor, pois este está

ocupado tentando completar a conexão semi-aberta (10). A velocidade da conexão à rede também pode ser afetada por meio do envio de extenso pacote de informações diretamente para ela. Esse tipo de ataque às vezes não ocorre de um único computador, pois ele pode coordenar ou cooptar o ataque simultâneo de muitas outras máquinas contra o servidor ou sistema-vítima.

Outros recursos informáticos podem ser atingidos, como se disse, além da "banda" de conexão à rede. Por exemplo, muitos sistemas são estruturalmente desenhados para processar os dados que os alimentam. Um intruso pode simplesmente alterar seu funcionamento por meio da inclusão de um pequeno programa que não faça absolutamente nada, a não ser reproduzir-se automaticamente, consumindo assim todos os recursos de processamento de dados do sistema-vítima.

Também é comum de o ataque consumir espaço em disco do computador-vítima, colocando arquivos FTP em áreas da rede disponibilizadas aos usuários. Em geral, os servidores se previnem desse tipo de ataque limitando o espaço em disco que pode ser utilizado para a colocação de dados, mas os *hackers* às vezes têm como eliminar esse tipo de controle.

Alguém pode sugerir que esses tipos de ataques a sistemas informatizados já estariam cobertos pela figura do *dano eletrônico*, que a versão original (proveniente da Câmara) já pretendia criar (§ 2º do art. 163 do CP). Só que esses ataques podem ser feitos sem necessariamente destruir o sistema informático (vítima do ataque) ou sequer alterar sua configuração de dados. Daí que a redação do dispositivo referente ao crime de *sabotagem informática* incrimina o ato que "de qualquer forma, interferir em sistema informatizado, com o fim de desorientar, embaraçar, dificultar ou obstar o funcionamento de um sistema informatizado ou de comunicação de dados à distância".

O parecer do Senador Crivella também estabelece a obrigação de todos os provedores de Internet armazenarem os registros de movimentação de seus usuários, pelo prazo de três anos (11). Trata-se de medida inadiável e indispensável para possibilitar a investigação de delitos cometidos na rede mundial. Sem esses registros de conexão e navegação é impossível qualquer investigação criminal de delitos informáticos. O projeto, nesse sentido, segue uma tendência global, pois praticamente todos os países desenvolvidos já incluíram esse tipo de obrigação legal

em seus sistemas jurídicos, sobretudo depois que o combate ao terrorismo se tornou assunto de política geral. Essa providência, aliás, já deveria ter sido implementada por via infralegal, através de alguma agência reguladora, a exemplo da Anatel. O Comitê Gestor da Internet (CGI) no Brasil apenas recomenda aos provedores nacionais, dada a ausência de lei nesse sentido, que guardem por até três anos os registros de conexão dos usuários (12).

O parecer ainda faz outros ajustes ao projeto original, como, por exemplo, a eliminação da figura do art. 218-A (pornografia infantil), cuja inclusão não é mais necessária, uma vez que a Lei n. 10.764, de 12 de novembro de 2003, já criou esse tipo de delito (por meio do aperfeiçoamento da redação do art. 241 do ECA, que agora já pune a difusão desse tipo de material ilícito na Internet). Além disso, aperfeiçoa a redação do art. 298-A (crime de falsificação de telefone celular ou meio de acesso a sistema informático), de que trata o Projeto de Lei da Câmara (13), e acrescenta um parágrafo único ao art. 46 do CP, de modo a possibilitar a aplicação de penas restritivas de direito a *hackers*, aproveitando seus conhecimentos técnicos em cursos de instituições públicas ou outras atividades equivalentes (14).

O parecer do senador Crivella segue para votação na Comissão de Constituição, Justiça e Cidadania do Senado Federal. Caso seja aprovado, a matéria seguirá para a apreciação da Comissão de Educação da Casa. Após análise nessa comissão, ele retornará para Comissão originária para receber parecer definitivo.

De um modo geral, o parecer promove alterações importantes ao projeto originário da Câmara. É claro que o combate aos *cybercrimes* não se resolverá na sua aprovação. O grande problema desse tipo de crime é que quase sempre é muito difícil determinar sua origem. A identificação do agente responsável direto pelo ato envolve a necessidade de cooperação com o provedor de Internet ou do administrador das *networks* afetadas. É preciso dotar os órgãos policiais e ministeriais com pessoal e meios técnicos para promover o rastreamento desses crimes. Nos EUA, o próprio FBI auxilia na investigação de alguns casos, inclusive possibilitando o contato para pessoas que estão situadas fora daquele país (15). Além disso, é necessário que o nosso país assine tratados de cooperação, que simplifiquem procedimentos de extradição, já que esses crimes são cometidos de maneira transnacional. Apesar disso tudo, a definição legal das práticas criminosas é realmente o primeiro passo na luta contra o problema. Em respeito ao princípio da

legalidade estrita que impera no campo penal, é imprescindível a descrição de forma antecedente (na lei) para que se possa, então, punir as condutas.

Agora, o que não podemos é retardar ainda mais a aprovação do projeto e, a cada passo, ficar acrescentado novas figuras à sua redação original. É melhor uma lei que não preveja todos os delitos de possível ocorrência no ciberespaço do que nenhuma. A existência de um vácuo na legislação penal dificulta a luta contra os *cybercrimes*. Parece-me que o correto, no momento, reside em apressar a votação do projeto com os crimes já incluídos e analisados nas diversas comissões (tanto na Câmara como no Senado), até porque, nos ambientes das redes de comunicação, novas modalidades de crime surgem a cada dia; é impossível se prever todas elas. A aprovação do projeto é um primeiro passo; no futuro se pode criminalizar outras condutas que forem surgindo. Nos EUA existe uma lei de crimes informáticos há 14 anos, o *Computer Misuse Act* (*CMA*). O debate que se trava lá no momento é sobre a necessidade de atualizá-la, sobretudo para fazer face aos crimes cometidos em redes informáticas abertas. Mas ela é uma lei básica, que vem servindo (pelo menos até agora) eficazmente.

Precisamos de um estatuto básico sobre crimes informáticos em nosso país, e o projeto originalmente apresentado pelo Dep. Luis Piauhylino cumpre bem esse papel.

Notas:

(1) Antes dele, apenas a Lei n. 9.983, de 14-7-2000, havia introduzido no Código Penal Brasileiro a figura qualificada do crime de divulgação de segredo (art. 153, § 1º-A), cujo tipo prevê pena de detenção de um a quatro anos e multa para aquele que divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública. Essa Lei introduziu, ainda, o chamado "peculato eletrônico", ao acrescentar no Código Penal os arts. 313-A e 313-B, os quais contêm a previsão de punição para o funcionário público que praticar a inserção de dados falsos em sistemas de informações (art. 313-A) - a pena prevista é de reclusão de dois a doze anos e multa -, bem como para aquele que modificar ou alterar sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente (art. 313-B), sendo a pena neste caso de detenção de três

meses a dois anos e multa. Também a Lei n. 10.764, de 12-11-2003, alterou a redação do art. 241 do Estatuto da Criança e do Adolescente, ampliando o descritor normativo do crime de pornografia infantil, para proibir a divulgação e publicação na Internet de fotografias e imagens contendo cenas de sexo explícito envolvendo criança ou adolescente, com pena de reclusão de dois a seis anos, além de multa.

Essas duas leis anteriores, como se vê, trataram de definir de forma isolada tipos específicos de "crimes informáticos", possuindo ambas outros dispositivos que tratam de figuras delitivas que não se incluem nessa denominação. Não foram elaboradas, portanto, com a finalidade de criar um texto sistematizado e geral sobre delitos no campo da informática, objetivo a que se propõe o projeto de lei ora em comento.

(2) Como consta do parecer do Senador, para essas novas condutas ilícitas "não havia remediação hermenêutica possível para inclusão nos dispositivos penais tradicionais".

(3) Essa numeração atribuída a cada um desses crimes é a que o projeto pretende introduzir no Código Penal.

(4) O parecer do Senador Marcelo Crivella modifica o art. 2º do PLC, que aborda os crimes contra a inviolabilidade dos sistemas informatizados e acrescenta outros na "Seção V do Capítulo VI do Título I do Código Penal". Assim, o atual art. 154-C do PLC é transformado em 154-E, para que sejam acrescidos os dois novos artigos (o do crime de *falsidade informática* e o do crime de *sabotagem informática*).

(5) Recentemente foi registrado o envio em massa de uma mensagem a internautas brasileiros, oferecendo um produto para aumento do pênis - item tradicional na lista dos *spammers*. Só que tudo não passava de uma farsa, pois a mensagem visava a instalar um arquivo espião no computador do destinatário. O *e-mail*, supostamente de uma empresa chamada "DoutorPenis.com", vem em português e promete um manual para "aumentar permanentemente o órgão sexual masculino em até 40% do comprimento e diâmetro".

Um "cavalo de tróia", contendo um formulário para inscrição no *Big Brother Brasil* 4, também circulou intensamente meses atrás no braço brasileiro da Internet.

Outro tipo bastante comum de fraudes eletrônicas são as cometidas por meio do envio de mensagens com ofertas falsas de antivírus, mas que na verdade, quando aberto o arquivo anexo, descarregam um *trojan* no computador da vítima.

(6) Através dessa prática de se fazer passar por um banco ou *site* comercial conhecido, os *scammers* conseguem enganar as pessoas com mais facilidade, segundo dados estatísticos. Já existe inclusive uma organização mundial que combate esse tipo específico de prática, o *Anti-Phishing Working Group*, cujo *site* é www.antiphishing.org. O FBI também mantém um serviço que visa a combater fraudes eletrônicas, o *Internet Fraud Complaint Center* - www.ifccfbi.gov.

(7) Todo *site* tem um endereço de localização na Web (a *World Wide Web*), o canal gráfico da Internet.

(8) De acordo com pesquisa digulgada pelo *Gartner Group*, os *phishing attacks*, embora não sendo uma coisa nova na Internet, explodiram em número nos últimos seis meses. 76% dos ataques registrados foram lançados de outubro de 2003 pra cá. Outros 16% foram executados nos seis meses anteriores, significando que 92% de todos os ataques foram conduzidos no ano passado. Ou seja: embora sendo um tipo de fraude já antiga (em termos de Internet), os *phishing scams* adquiriram uma dimensão preocupante apenas a partir do ano passado. De acordo com essa mesma pesquisa, 57 milhões de cidadãos americanos foram vítimas de tentativas de fraudes desse tipo. De acordo com Avivah Litan, Diretor de pesquisas do *Gartner Group*, e autor de um estudo baseado na mesma pesquisa, as tentativas de fraudes eletrônicas (*phishing scams*) não são executadas por *hackers* amadores, mas pelo crime organizado, em particular por cartéis de drogas da Europa oriental, que descobriram que o furto de identidade (*identity theft*) e dados pessoais, e a fraude eletrônica em geral, pode ser um "negócio" bastante lucrativo. Ele estima que o prejuízo causado às companhias de cartões de crédito e bancos americanos só ano passado (2003) foi da ordem de US$ 1.2 bilhões. E o pior, nesse tipo de prática, é que os criminosos têm uma chance de uma em 700 de serem pegos, segundo ele avalia. Se os *phishing attacks* continuarem, estima ele, o resultado vai ser um decréscimo na taxa de confiança nas transações comerciais *on line*. A não ser que governos e empresas tomem providências, a taxa de crescimento do comércio eletrônico, que atualmente é de 20% anual, irá decair rapidamente. Ele estima que, pelo ano de 2007, a taxa de crescimento do comércio eletrônico nos EUA caia para 10% ou mais, se essas medidas não forem tomadas. Os dados da pequisa foram divulgados em entrevista publicada no *site* InternetWeek.com - www.internetwk.com.

(9) É o caso da lei americana (o *CAN-SPAM Act*) e da lei australiana (o *Spam*

Act 2003).

(10) Para esse tipo de conexão, usa-se o termo *half-open connection*.

(11) O parecer traz emenda que acrescenta um parágrafo único ao art. 11 do projeto da Câmara (PLC n. 89/2003).

(12) Tal recomendação está prevista no item 3.2 ("Manutenção de Dados de Conexão") do documento "Recomendações para o Desenvolvimento e Operação da Internet no Brasil", criado pelo Comitê Gestor.

(13) O art. 298-A, proposto pelo projeto, cria o crime de falsificação de telefone celular ou meio de acesso a sistema informático. O parecer sugere emenda para deixá-lo com a seguinte redação:

"Art. 298-A. Criar, copiar, interceptar, usar, indevidamente ou sem autorização, ou falsificar senha, código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de radiofreqüência ou telefonia celular ou qualquer instrumento que permita o acesso a meio eletrônico ou sistema informatizado.

Pena: reclusão, de um a cinco anos, e multa" .

A redação anterior não era clara sobre a conduta bastante comum de "quebra de senhas", o que demandava um aperfeiçoamento do art. 298-A, agora incluída pelo parecer do Sen. Marcelo Crivella.

(14) A emenda proposta tem a seguinte redação:

"Dê-se ao art. 5º do Projeto de Lei da Câmara n. 89, de 2003, a seguinte redação:

Art. 5º O art. 46 do Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar acrescido do seguinte parágrafo:

"No crime praticado contra ou por meio de meio eletrônico ou sistema informatizado, o juiz poderá aproveitar as habilidades e conhecimentos do condenado para a ministração de cursos ou trabalhos de criação de sistemas informatizados em empresas ou instituições públicas, ou para qualquer tipo de prestação de serviços equivalentes" (NR).

(15) A página com informações para contato: http://www.fbi.gov/contactus.htm

* Juiz integrante do Colégio Recursal dos Juizados Especiais Cíveis e Juiz Auxiliar da Corregedoria-Geral de Justiça de Pernambuco, Professor da Escola Superior da Magistratura de Pernambuco e da Faculdade de Direito de Caruaru.

Fonte: <www.saraivadata.com.br> Acesso em: 25 de jun. 2004

Anexo D – INFOSEG

Programa de Integração Nacional de Informações de Justiça e Segurança Pública

Estender para todos os Estados a disponibilização dos dados atuais do INFOSEG nas áreas de segurança e justiça, de forma a permitir a integração e o acesso das informações de identidade criminal, de mandados de prisão e população carcerária entre todas as unidades federadas.

PREMISSAS

Manter a autonomia dos Estados

Controlar acesso às informações

Garantir sigilo das informações

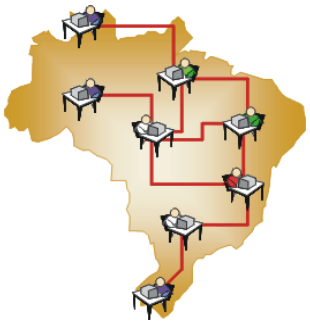
Implementar rotinas de auditoria

Diferentes níveis de autorização

Utilização de recursos gráficos

Apresentação de fotografia e impressões digitais

Permitir a troca de informações não estruturadas



OBJETIVOS

Integrar e disponibilizar informações de:

inquéritos policiais

mandados de prisão

armas de fogo

processos criminais

Veículos

Histórico

O Decreto de 26/09/95 do Presidente Fernando Henrique Cardoso criou o "Programa de Integração das Informações Criminais", constituído pelos Cadastros Nacionais e Estaduais de Informações Criminais, de Mandados de Prisão, de Armas de Fogo e de Veículos Furtados e Roubados, complementado e regulamentado pela Portaria do Exmo. Sr Ministro da Justiça, de 07/12/95. (O primeiro publicado no DOU n° 186-27/09/95 e o segundo no DOU n° 235 de 08/12/95).

O projeto INFOSEG tem por objetivo principal a disponibilização e integração das informações de inquéritos policiais, processos judiciais criminais, de mandados de prisão, de armas de fogo, população carcerária, informações sobre penitenciárias, veículos, passaportes e estrangeiros, entre todos os Estados da nação, através de uma rede de informações operando a nível nacional.

Descrição do Projeto

O projeto disponibiliza as informações de Justiça e Segurança Pública através de uma rede de computadores, utilizando catálogos que servem de Índices Nacionais. O índice de indivíduos possui informações sobre indivíduos indiciados em inquéritos policiais, com processos judiciais criminais, que possuam mandado de prisão em aberto, ou que façam parte da população carcerária. O índice de veículos possui informações sobre veículos da frota nacional. O índice de armas possui informações sobre todas as armas registradas legalmente ou que foram apreendidas pelas Polícias Civil e Federal ou pela Justiça. Também serão disponibilizadas informações sobre as penitenciárias do país, passaporte e cadastro de estrangeiros registrados na Polícia Federal.

O resultado da consulta ao Índice Nacional é uma relação de objetos com ponteiros para as Bases de Dados estaduais onde estão armazenadas as informações completas e detalhadas.

Os dados armazenados nos Índices Nacionais tem a finalidade de auxiliar na individualização do objeto que se deseja consultar. O Banco de Dados INFOSEG armazena além do Índice Nacional, o cadastro de usuários com suas permissões, as informações de auditoria dos acessos aos dados do Índice e consultas realizadas

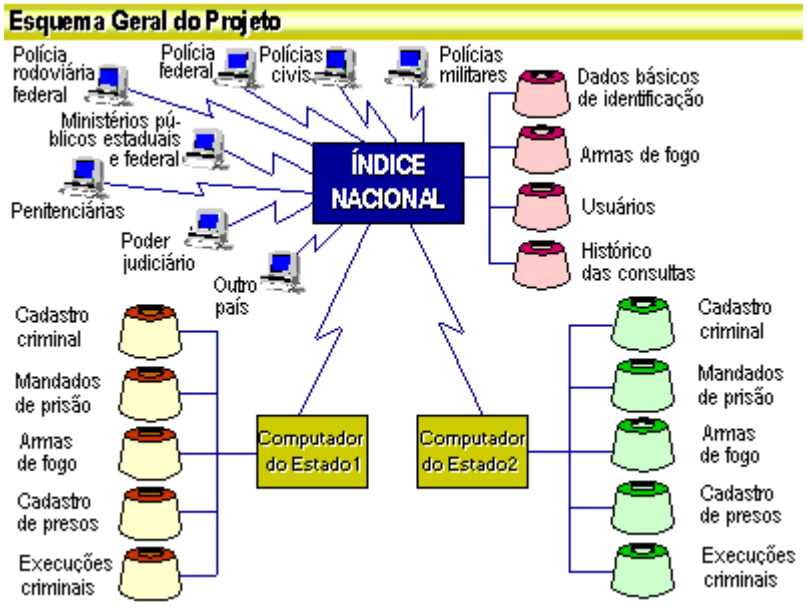
aos Estados.

Para obter informações detalhadas de um objeto solicita-se uma consulta à Base de Dados do órgão responsável por esta informação.

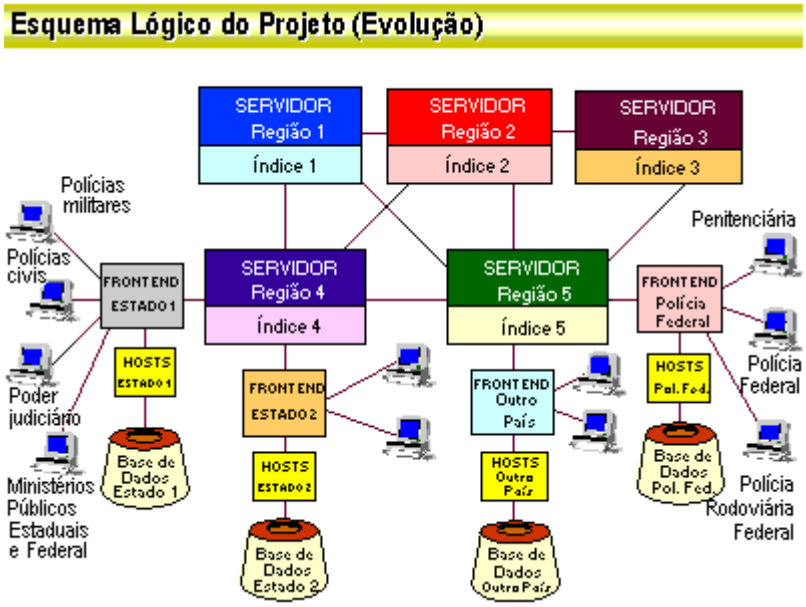
As manutenções do Índice Nacional de indivíduos são de responsabilidade dos Estados que enviam periodicamente as informações atualizadas por seus sistemas para a instalação central responsável pela administração do índice (PROCERGS/RS). Também será de responsabilidade dos Estados as informações disponibilizadas nas consultas através desta rede.

Os Índices Nacionais de veículos e armas são mantidos , respectivamente, pela aplicação RENAVAN e SINARM, hoje já implantadas nos Estados.

Arquitetura do Sistema



Topologia da rede



Módulos do sistema

Módulo 1 - Montagem do Índice Nacional

Este módulo consiste na implementação de rotinas para geração inicial (carga), consulta ao Índice Nacional, e auditagens das consultas realizadas.

As manutenções do Índice Nacional são de responsabilidade dos Estados que enviarão diariamente as informações atualizadas por seus sistemas para a instalação central responsável pela administração dos índices (PROCERGS/RS).

Nesta fase o Estado deve desenvolver as rotinas de criação dos arquivos de movimento com os dados para carga e atualização do Índice Nacional da sua região, conforme especificações definidas pela PROCERGS e PRODESP.

Todos os acessos ao índice serão registrados pelo sistema, armazenando informações sobre os usuários que consultaram informações sobre determinado indivíduo (auditoria).

Faz parte também da implementação deste módulo a montagem de toda a infra-estrutura de comunicações para interligação dos Estados.

Módulo 2 - Acesso às Bases de Dados dos Estados

Este módulo consiste no desenvolvimento (programação), pelos Estados, de rotinas para consulta aos Bancos de Dados estaduais , com informações mais detalhadas sobre: indivíduo, armas, inquéritos policiais, processos judiciais criminais e histórico penitenciário.

Módulo 3 - Replicação do Índice Nacional

Este módulo consiste na implementação de rotinas para a replicação do

Índice Nacional.

O sistema prevê a existência de cinco (5) Índices Nacionais, localizados em cinco Estados. Toda modificação nas informações de um índice tem que ser automaticamente repassada para os demais índices. Este mecanismo de sincronização das atualizações é denominado de replicação.

No INFOSEG a replicação da atualização das informações dos Índices Nacionais é feita a partir de um único Índice Nacional (Master), num Estado, que a partir daqui chamaremos de Estado Master. Os Estados remetem seus arquivos para este site centralizador (o Estado Master), que atualiza o seu índice e propaga as alterações para os demais Índices Nacionais.

Módulo 4 - Correio Eletrônico

Para facilitar a obtenção de informações não estruturadas, será disponibilizado na Rede Nacional INFOSEG um correio eletrônico. Com ele os usuários poderão solicitar/trocar informações de uma forma ágil e segura, sem a necessidade de utilizar outros meios de comunicação.

Módulo 5 - Consolidação dos itens de Segurança

Neste módulo, serão implementados, no projeto INFOSEG, os itens de segurança definidos pelo Ministério do Planejamento,Orçamento e Gestão, para a rede do Governo Federal.

Níveis de acesso dos operadores

O INFOSEG tem dois níveis para controlar o tipo de acesso às informações (nível 1 e 2) e três níveis para controlar as funções de administração do cadastro de operadores (nível 3, 4 e 5).

Nível 1 e 2 – referente ao acesso às informações

Hoje permite o acesso a todas as informações tanto do Índice Nacional como das bases de dados disponibilizadas no sistema.

No início do Projeto existiam diferenças de acesso do Nível 1 para o Nível 2.

O nível 1 acessava todas as informações do Índice Nacional e o acesso às bases de dados estaduais estava liberado somente para indivíduos com mandado de prisão em aberto.

O nível 2 acessava todas as informações do Índice Nacional e das bases de dados estaduais.

Esta situação foi modificada devido a várias solicitações recebidas pelo

Ministério da Justiça dos usuários do sistema.

Nível 3 - referente ao acesso às informações e a autorização de administração do cadastro de operadores

Permite acesso a todas as informações do sistema e tem autorização para administrar o cadastro de operadores do mesmo órgão em que o operador administrador está cadastrado.

Nível 4 - referente ao acesso às informações e a autorização de administração do cadastro de operadores

Permite acesso a todas as informações do sistema e tem autorização para administrar o cadastro de operadores do Estado em que o operador administrador está cadastrado.

Nível 5 - referente ao acesso às informações e a autorização de administração do cadastro de operadores

Permite acesso a todas as informações do sistema e tem autorização para administrar o cadastro de operadores de todo o país.

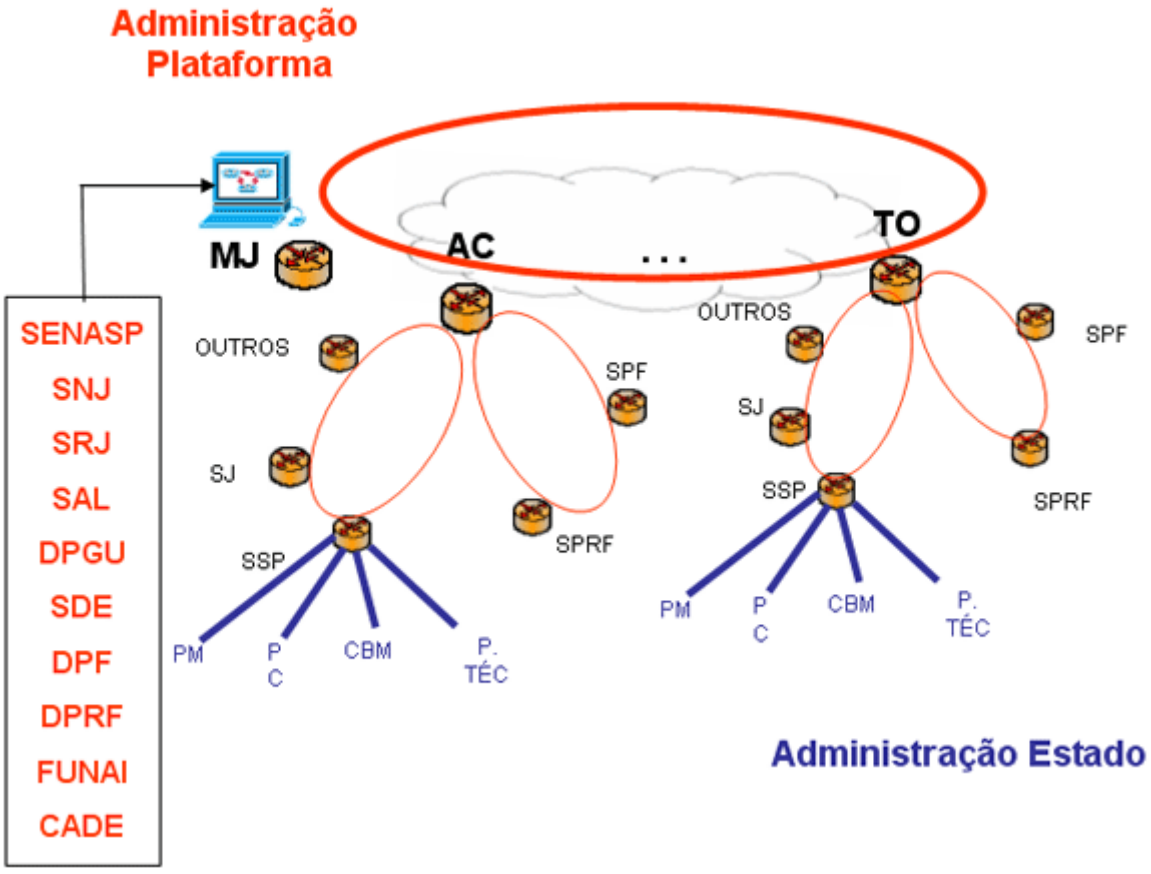
Este nível é utilizado pelo Ministério da Justiça.

A Secretaria Nacional de Segurança Pública - SENASP informa que o INFOSEG (Sistema Nacional de Integração de Informações em Justiça e Segurança Pública) é um sistema de uso restrito dos órgãos que compõem a área da justiça e da segurança pública tendo como escopo integrar todos os bancos de dados existentes no país, com **o objetivo de** facilitar a atuação das polícias brasileiras na identificação de pessoas que estejam com pendências criminais junto a justiça.

Anexo E – INFOVIA

A Plataforma Nacional de Informações sobre Justiça e Segurança Pública é uma Infovia de rede, voz e imagem que irá ligar o Ministério da Justiça aos Operadores de Segurança Pública e Justiça do país.

CONCEITO_____



O combate à criminalidade pode ser encarado segundo uma gestão subdividida em três esferas:

Prevenção **-** por intermédio da adoção de políticas públicas integradas.

Intervenção **-** por intermédio de ferramentas que viabilizem a inteligência policial e criminal.

Detenção - por intermédio da adoção de políticas eficazes de ressocialização.

A obtenção da eficiência e eficácia nessas três dimensões passará, dentre outras coisas, pela otimização dos recursos de comunicação de dados, voz e imagem empregados pelos operadores de justiça e segurança pública do país. O quadro atual é composto por operadores circunscritos operacionalmente a "ilhas de informação" ou, quando muito, fracamente interligadas ou compartilhadas. Em última instância, isso implica em se reagir às demandas de segurança pública em tempo aquém das expectativas da sociedade.
A resposta do Ministério da Justiça a essa lacuna será o estabelecimento de uma "Infovia", capaz de trafegar dados, voz e imagem entre os diversos operadores do país. Essa "Infovia" será denominada **Plataforma Nacional de Informações sobre Justiça e Segurança Pública**.

Meta: estabelecer uma plataforma nacional de informação integrada (infovia) capaz de atuar como instrumento de controle, gestão e combate da criminalidade.

Objetivos principais:

- Integrar e disponibilizar informações, em âmbito nacional, sobre criminalidade, segurança pública e justiça;
- Permitir que qualquer operador de segurança pública e justiça tenha acesso a estas informações;
- Permitir que, de qualquer pondo do Brasil, ou exterior, se tenha acesso controlado a estas informações;
- Permitir a interligação necessária a implementação das seguintes ações:

Ação 1: Integração das Organizações Básicas Policiais

Ação 2: Integração das Unidades Móveis

Ação 3: Integração dos Patrulheiros

Ação 4: Integração das Informações dos Cartórios de Registro Civil de Pessoas Naturais

Ação 5: Integração dos Institutos de Identificação

Ação 6: Integração dos Institutos de Criminalística e Institutos Médicos Legais

Ação 7: Criação de Centrais Integradas de Planejamento Tático e Despacho

Ação 8: Monitoramento de Logradouros Públicos

Ação 9: Integração do Sistema Penitenciário

Ação 10: Integração do Poder Judiciário e Ministério Público

Ação 11: Ensino à Distância

Ação 12: Integração do Sistema Brasileiro da Concorrência

Ação 13: Integração Nacional de Informações de Defesa do Consumidor

Ação 14: Integração das unidades da FUNAI

Ação 1: Integração das Organizações Básicas Policiais

Objetivos: Imprimir uma maior eficácia e eficiência às intervenções policiais, diminuindo o tempo de resposta ao cidadão e oferecendo ferramentas de pronto atendimento que assegurem um maior controle da criminalidade e, ao mesmo tempo seja uma garantia dos direitos e garantias individuais.

.....

Ação 2: Integração das Unidades Móveis

Objetivos: Prover ferramentas de consulta junto aos veículos de patrulhamento ostensivo e de investigação policial que possibilitem uma maior eficácia das respectivas ações.

.....

Ação 3: Integração dos Patrulheiros

Objetivos: Prover o policial de ferramentas que otimizem seu trabalho no campo preventivo e repressivo, melhor integrando-o em estratégias de polícia comunitária.

.....

Ação 4: Integração das Informações dos Cartórios de Registro Civil de Pessoas Naturais

Objetivos: Prover informações complementares ao sistema nacional de visando a completude da geração de conhecimento.

.....

Ação 5: Integração dos Institutos de Identificação

Objetivos: Geração e integração de informações sobre impressões digitais e imagens individuais ao sistema nacional.

.....

Ação 6: Integração dos Institutos de Criminalística e Institutos Médicos Legais

Objetivos: Vincular dados e informações de laudos periciais, inquéritos policiais, processos judiciais, execuções de sentenças, imagens e sons a partir do BON - ciclo de justiça criminal. Possibilitar o acesso ao SINIP - Sistema Nacional de Identificação de Projéteis.

.....

Ação 7: Criação de Centrais Integradas de Planejamento Tático e Despacho

Objetivos: Instituir centros que integrem as atividades das polícias estaduais e de defesa civil, interligados a outras agencias governamentais, visando a racionalização dos serviços e a diminuição do tempo de resposta das intervenções.

.....

Ação 8: Monitoramento de Logradouros Públicos

Objetivos: Controlar a criminalidade a partir da observação de indivíduos e veículos em locais estratégicos.

.....

Ação 9: Integração do Sistema Penitenciário

Objetivos: Possibilitar o acesso *on-line* de informações constantes do prontuário individual do condenado.

.....

Ação 10: Integração do Poder Judiciário e Ministério Público

Objetivos: Possibilitar o intercâmbio de informações entre os organismos policiais, o Ministério Público e o Poder Judiciário, além de outras agências governamentais, a avaliação pro-ativa da eficácia e eficiência do sistema de justiça criminal, notadamente através da agilização dos processos judiciais, da maior adequação na dosimetria das penas impostas e do acompanhamento efetivo de sua execução.

.....

Ação 11: Ensino à Distância

Objetivos: Criar nas organizações policiais salas de aula, equipadas adequadamente, possibilitando a formação continuada, à distância, de policiais, via Internet.

Ação 12: Integração do Sistema Brasileiro de Defesa da Concorrência

Objetivo: Integrar os sistemas aplicativos e banco de dados dos órgãos que compõem o Sistema Brasileiro de Defesa da Concorrência, com o objetivo de proporcionar maior agilidade no trâmite processual e estimulando a migração para as melhores práticas de Governo Eletrônico, como a substituição de documentos em papel por documentos eletrônicos certificados.

Ação 13: Integração do Sistema Nacional de Informações de Defesa do Consumidor

Objetivo: Integrar as unidades do PROCON com o propósito de dinamizar e potencializar os procedimentos já existentes, almejando a harmonização necessária para a criação da base de dados nacional.

.....

Ação 14: Integração das Unidades da FUNAI

Objetivo: Integrar as unidades da FUNAI com o propósito de dinamizar o atendimento às necessidades das comunidades indígenas espalhadas pelo país.

.....

GESTÃO_____

O Ministro da Justiça, Márcio Thomaz Bastos, por intermédio da Portaria n. 1806, de 21 de novembro de 2003, instituiu o Comitê Gestor da Plataforma Nacional de Informações sobre Justiça e Segurança Pública, com o objetivo de estabelecer diretrizes, promover, priorizar e supervisionar programas, projetos e atividades no âmbito da Plataforma Nacional de Informações sobre Justiça e Segurança Pública do Ministério da Justiça.

Os seguintes órgãos fazem parte do Comitê Gestor da Plataforma Nacional:

- **SENASP** - Secretaria Nacional de Segurança Pública;
- **DPF** - Departamento de Polícia Federal;
- **DPRF** - Departamento de Polícia Rodoviária Federal;
- **FUNAI** - Fundação Nacional do Índio;
- **CADE** - Conselho Administrativo de Defesa Econômica;
- **SNJ** - Secretaria Nacional de Justiça;
- **DPGU** - Defensoria Pública Geral da União;
- **SAL** - Secretaria de Assuntos Legislativos;

- **SRJ** - Secretaria de Reforma do Judiciário;
- **SDE** - Secretaria de Direito Econômico.