Acesso forçado a sistemas remotos
OPERAÇÃO HÉRCULES

Daniel Araújo Miranda, Rodrigo Alves Carvalho

***Resumo*—A abordagem convencional utilizada pela polícia para ter acesso a indícios de crime em formato digital é a apreensão da mídia que contém os dados. Os criminosos utilizam diversos recursos para frustrar essa abordagem, entre eles a criptografia e a ocultação dos dados. Este artigo descreve o procedimento realizado pela Polícia Federal no Rio Grande do Sul na operação Hércules para acessar um sistema remoto operado por uma organização investigada pelo crime de evasão de divisas. O sistema era utilizado para armazenar a contabilidade e os documentos da organização.**

***Palavras-chave*—Polícia Federal; acesso forçado; invasão; segurança de redes; Hércules;**

1. Introdução

Devido ao uso generalizado do computador para realizar as atividades do dia-a-dia, vestígios deixados por atividades criminosas muitas vezes estão em formato digital. A abordagem convencional utilizada pela polícia para ter acesso a esses vestígios é apreender as mídias suspeitas de conter provas.

Os criminosos buscam diversas formas de proteger os registros de suas atividades. No caso dos dados digitais, já foram observados diversos casos do uso de criptografia, ocultação de mídias (discos enterrados, escondidos em cofres, pendrive na meia, etc.), ocultação de dados (esteganografia – Juan Carlos Abadia), armazenamento de dados em locais remotos (caso da casa de bingo que virava Lan House), armazenamento terceirizado de dados no exterior (operação PontoCom – roubo de senhas), armazenamento em sítios remotos próprios (operação Hércules).

A polícia utilizou estratégias diferentes em cada um desses casos para obter as provas necessárias ao processo criminal. O restante deste artigo contextualiza e descreve o acesso forçado ao sistema remoto dos investigados na operação Hércules.

2. Histórico

Foi criada a operação Hércules (deflagração em 05 de Junho de 2009), para realizar uma investigação relativa a evasão de impostos através do envio clandestino de dinheiro para o exterior.

A fraude era operada da seguinte forma:

- Uma unidade localizada no Brasil recebia dinheiro do cliente A a ser enviado para o cliente B localizado no exterior;
- Uma unidade localizada no Exterior recebia dinheiro do cliente C a ser enviado para o cliente D localizado no Brasil;
- A unidade do Brasil repassa o dinheiro do cliente A para o cliente D;
- A unidade do Exterior repassa o dinheiro do cliente C para o cliente B.

Essas transações eram contabilizadas por um sistema bancário paralelo e o dinheiro nunca era transferido através dos canais oficiais, sujeitos a auditoria pelo Banco Central e pela Receita Federal. O esquema é também conhecido por dólar-cabo.

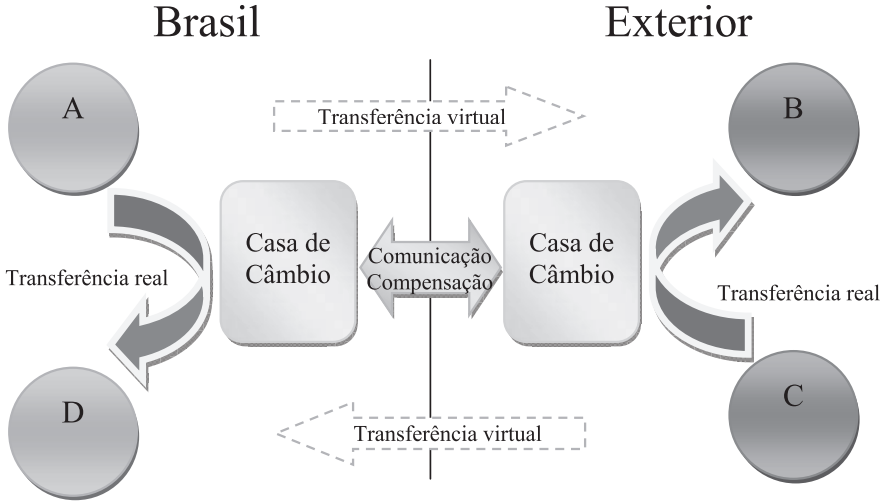

Fig. 1: Fluxo do dinheiro

Esse tipo de serviço tem diversas finalidades. Entre elas, a ocultação de dinheiro obtido ilicitamente (corrupção, furtos e fraudes) e a evasão de impostos de importação como na operação Narciso – caso Daslu: as notas são subfaturadas, o valor declarado é transferido de forma oficial pagando impostos e a diferença é enviada clandestinamente.

A investigação obteve mandados judiciais e coletou informações através de escutas, vigilância e monitoramento telemático. Descobriu-se que uma das instituições investigadas armazenava todas as suas informações em um sítio remoto. Caso fosse utilizada a abordagem convencional o material apreendido não possuiria nenhum dado relevante.

A proposta inicial foi realizar uma entrada tática e impedir que os usuários desligassem os computadores. As dificuldades para essa ação eram muitas:

- A entrada deveria ser feita com o sistema em uso, ou seja, durante o horário de expediente.
- Segurança física das instalações do alvo. A casa de câmbio tinha grades, portas reforçadas e câmeras de segurança.
- Haveria muito tempo para o alvo desligar os computadores. Para a entrada ser realizada na velocidade suficiente seria necessário utilizar explosivos.
- Desconhecimento do sistema até o momento da entrada. Grande possibilidade de imprevistos e sem garantias que a informação poderia ser obtida.

Diante da situação, o comando da operação consultou a perícia de informática e forneceu muitas informações sobre o caso:

- Arquivos provenientes do monitoramento telemático
- Seleção de áudios pelo pessoal da inteligência
- Informações sobre a natureza do sistema e forma de utilização pela quadrilha

3. Método

3.1. Exame dos dados da interceptação

Analisando-se os dados do monitoramento constatou-se que:

- A maioria do tráfego estava criptografado (pacotes SSL) e era dirigido a um único IP;
- O servidor ficava sempre ligado. Durante o horário comercial de trabalho verificava-se uma concentração de utilização da banda. No horário de almoço essa utilização caía bastante e, durante os finais de semana, era mínima.

3.2. Sondagem do sistema remoto

Foi realizada uma pesquisa sem nenhum procedimento de quebra de segurança ou acesso a dados.

Ao pesquisar em um serviço de DNS reverso, descobriu-se a URL associada àquele IP. Ainda, ao consultar um serviço WHOIS, chegou-se aos dados do responsável administrativo pelo domínio e à localização do servidor. Nenhum serviço de anonimato em pesquisas WHOIS era utilizado.

Após a descoberta do IP remoto, levantou-se o máximo de informação possível acerca do servidor. Para isso, utilizando um IP anônimo, e durante um horário adequado, foi realizado um mapeamento do servidor. O objetivo era descobrir portas abertas e/ou serviços ativos, o sistema operacional em execução, existência de firewalls, entre outras informações. A ferramenta NMAP se mostrou bastante útil. Apenas scans convencionais foram utilizados, para não levantar suspeitas.

Em paralelo, foram realizados acessos à máquina apontada pelo IP via HTTP. Surgiu na tela a front-end do aplicativo Sun Secure Global Desktop, com campos para inserção de usuário e senha. Como o próprio nome diz, trata-se de um servidor remoto seguro, multiplataforma (Windows, Linux, MacOS) e que provê um bom nível de segurança, pois todo o tráfego entre servidor e cliente é criptografado. Não foi feita tentativa de login.

3.3. Testes de laboratório

A próxima etapa do exame consistiu em tentar obter na internet um instalador dessa aplicação. O site oficial, na época, disponibilizava uma versão com funcionalidade completa para avaliação por um prazo de poucas semanas. Assim, foi possível simular o ambiente tal qual o do servidor alvo, para tentar sanar algumas dúvidas:

- Descobrir se tentativas frustadas de login eram armazenadas ou explicitamente advertidas;
- Descobrir se, após um login bem sucedido com senha, poderiam serem exigidas outras senhas ou formas de autenticação;
- Estudar os meios e aplicativos que viabilizassem a transferência de um grande volume de dados, de dentro do ambiente para o exterior.
- Com o auxílio do Wireshark, analisar a fundo tanto os pacotes de requisição de login quanto as respostas de "falha de autenticação" e "login bem sucedido", para posterior confecção de pacotes e análise de pacotes de resposta.

Entre outras informações adquiridas, descobriu-se que a cada 100 tentativas de conexão mal sucedidas, o SSGD derrubava a conexão. Ainda, que era possível ativar vários threads paralelos: o SSGD tratava todas as requisições, respeitando, porém, o limite de tentativas mal sucedidas por conexão. Além disso, as tentativas frustradas de login eram armazenadas em logs, porém nenhum alerta era enviado ao administrador. Era necessário verificar o arquivo de log periodicamente.

3.4. Elaboração do ataque

Depois de estudar bastante o sistema, conhecendo e avaliando as situações que poderiam ser encontradas no

sistema alvo, iniciou-se a preparação para o ataque. Tal preparação envolveu:

- Geração de um dicionário de senhas, derivado das informações obtidas pela escuta telefônica – descobriram-se 6 caracteres, de uma senha de 9 caracteres no total. Tais caracteres seriam letras, e o nome de usuário seria uma derivação unívoca da senha. Assim, um ataque de força bruta ficou viável: o dicionário conteve apenas 20.000 candidatos, aproximadamente.
- Implementação de script em Python para criação dos pacotes de requisição de login, utilizando as senhas do dicionário, e avaliação da resposta do servidor. Ao encontrar uma senha válida, o script armazenava a mesma e continuava testando o dicionário até o final.
- Pesquisa e definição das ferramentas de infra-estrutura para o ataque:
    - *socat*: estabelecimento de socket com a aplicação remota;
    - *cryptcat*: similar ao *netcat*, porém criptografa os dados transmitidos;
    - *7zip*: compactação das pastas "Documents And Settings" dos usuários e volumes de discos encontrados.

3.5. Ataque em laboratório

A técnica desenvolvida para ataque foi testada no aplicativo instalado em laboratório. Uma das preocupações era de que o ataque alertaria o administrador do sistema. Esse comportamento não foi observado em laboratório, as tentativas mal sucedidas eram registradas em um arquivo de log discreto. Não foi ativado nenhum alerta para o administrador.

O ataque funcionou localmente, descobrindo a senha de acesso do servidor. Em seguida foi testada uma técnica para retirar os arquivos.

Os aplicativos utilizados para retirar os arquivos foram o *tar,* o *cryptcat* e o *7zip*. O *tar* foi utilizado para acondicionar vários arquivos em um só, preservando os caminhos e as datas de modificação dos arquivos. O *7zip* foi utilizado como alternativa, caso fosse mais interessante comprimir os dados antes do envio. O cryptcat foi utilizado para transferir o arquivo gerado pelo *tar* via rede em uma conexão criptografada. Isso gera mais uma dificuldade para o administrador do sistema – supondo que ele estivesse monitorando o tráfego, seria mais difícil de perceber o que estava acontecendo e, se percebesse, seria difícil descobrir que dados estavam sendo transferidos.

Foi criada uma conta anônima no gmail para conter os arquivos que seriam usados no ataque.

Por fim, a técnica foi ensaiada para ser realizada com rapidez: as linhas de comando foram anotadas, as pastas que seriam criadas foram fixadas e foi ensaiado o apagamento dos rastros de navegação e dos arquivos temporários gerados.

3.6. Preparação

Os dados do monitoramento foram analisados para definir o período em que uma cópia massiva de dados geraria menos suspeita. O fim de semana era o período em que se observava o menor tráfego para o servidor, portanto o início do ataque foi agendado para o sábado de manhã.

Foi obtido um mandado judicial autorizando explicitamente o acesso forçado ao servidor remoto.

3.7. Ataque

De posse de mandado judicial explícito, foi iniciada a tentativa de acesso. O ataque começou no dia 30 de maio de 2009, sábado, por volta das 11:00 da manhã. Em aproximadamente 15 minutos a senha foi descoberta.

A senha foi utilizada para acessar o sistema. Ao acessar a área de trabalho remota, um cliente MSN foi iniciado automaticamente, e foi prontamente desligado para evitar que o atacante aparecesse "on-line" para os contatos do alvo.

Foi encontrada uma máquina virtual com pastas de rede montadas; o desktop acessado era o de uma máquina virtual em uma rede com NAT (Natural Address Translation), portanto sem endereço IP válido na internet. Foi feita uma breve busca por arquivos e sistemas de interesse.

Obstáculo 1: Não era possível realizar uma conexão com o *cryptcat* pois tanto a máquina remota como a máquina dos peritos não possuíam endereços IP válidos na internet.

A estratégia passou a ser conectar da máquina alvo para uma máquina com ip válido controlada pelos peritos.

Foi feito "logout" do ambiente remoto para que a máquina com ip válido fosse providenciada. A solução à mão, no momento do ataque, foi utilizar a internet pessoal de um dos peritos do setor.

Após providenciar uma máquina com ip válido, os peritos ficaram separados em dois locais: um no escritório controlando a máquina do alvo e outro em uma residência, para receber os dados.

As ferramentas (*tar* e *cryptcat*) foram transferidas para o alvo através de uma conta de e-mail do Gmail.

Obstáculo 2: O antivírus do alvo não permitiu a execução da ferramenta *cryptcat*.

A solução encontrada foi alterar o arquivo binário do *cryptcat* – apenas um byte em uma região não relevante no início do arquivo. O antivírus parou de criar problemas.

Depois de resolver os problemas de transmissão de dados, foi utilizado o aplicativo *tar* enviando os dados direto para o *cryptcat*. Cada conexão suportava no máximo 50Kbps, ficou muito lento para transferir os dados sem compressão. Optou-se por gravar arquivos *.tar* e comprimi-los para envio.

Obstáculo 3: Não havia espaço suficiente no disco da máquina virtual para criar os arquivos temporários.

A alternativa foi armazenar os dados temporariamente na pasta de rede. Foi criado um diretório com nome similar aos já existentes.

Obstáculo 4: Não foi possível utilizar o aplicativo *tar* para gerar arquivos para uma pasta de rede.

O aplicativo *7zip* foi baixado da internet e utilizado tanto para criação de um arquivo único como para compressão.

Foram levantados cerca de 3GB de informação, que foram comprimidos em diversos arquivos. Devido à limitação de banda por conexão individual, esse conteúdo foi dividido em vários arquivos que foram enviados simultaneamente em várias conexões.

Os dados foram transferidos do sábado de manhã até depois do meio dia do domingo, sem interrupção.

As pastas, os arquivos, os programas e o histórico de navegação foram apagados.

No dia 01 de junho de 2009 (segunda-feira) à noite foi explorada uma extrapolação da regra de formação da senha, que levou à descoberta de senhas de outros usuários, por tentativa e erro; foram baixados os dados desses usuários.

3.8. Dados obtidos

Foi realizada uma cópia de segurança e foi calculado o hash SHA-256 de cada arquivo assim que a transferência do servidor foi finalizada.

Após a descompressão e análise dos arquivos, foram identificados:

- Sistema gerencial e contábil, contendo mais de 3500 relatórios contábeis de 2480 clientes, que faziam transações em até 7 moedas;
- Milhares de digitalizações e documentos em formato DOC, DOCX, PDF e TXT, contendo:
  - Documentos manuscritos;
  - Comprovantes de depósitos e transferências entre contas;
  - Ordens e recibos de pagamentos;
  - Documentos swift – documentos contendo dados para controle de transações interbancárias internacionais. A rede onde as mensagens eletrônicas contendo tais dados transitam é chamada de rede swift;
  - Documentos de identidade;
  - Emails;
  - Relatórios do sistema gerencial e contábil;
  - Invoices – documentos comerciais trocados entre comprador e vendedor, contendo dados como natureza, quantidade e preço acordado de produtos, condições para pagamento, entre outros dados;
- Registros criptografados de conversas MSN – software utilizado: Secway Simp Pro. As chaves criptográficas foram baixadas do servidor remoto. Ainda, ficou claro que alguns usuários ou colocavam senha em branco, ou utilizavam a mesma senha para acesso ao sistema gerencial.
- Foram desenvolvidos 2 scripts do AutoIt para realizar procedimentos específicos em alguns dados:
  - Extrair relatórios do sistema gerencial em arquivos PDFs, separados por cliente e tipo moeda. No total, foram gerados mais de 3500 documentos PDF.
  - Descriptografar as conversas MSN (arquivos com extensão slk) gerando documentos RTF únicos para cada contato.

4. Conclusão

Todo o procedimento envolveu riscos calculados. A sondagem e o ataque poderiam ter alertado o administrador, que poderia ter tirado o sistema do ar ou feito alterações. Como as interações com o alvo foram realizadas utilizando o menor tempo possível, em horários favoráveis e de forma a simular um atacante comum, o risco foi avaliado como baixo, fazendo o procedimento valer a pena mesmo que não fosse bem-sucedido.

O sucesso do procedimento dependeu da solução rápida de problemas. É esperado que, em procedimentos desse tipo, sejam encontrados imprevistos, pois o invasor não conhece *a priori* o ambiente invadido.

Os resultados foram apresentados via documento sigiloso (Informação Técnica), com anexos em DVD criptografados. Tal sigilo era necessário, pois a operação ainda não tinha sido deflagrada.

O *feedback* de delegados e promotores mostrou que esse foi um trabalho importante para a valorização da perícia. Foram feitos vários comentários do tipo "eu não esperava que vocês fossem conseguir", "esses peritos são hackers", "vamos demorar anos para analisar toda essa informação", "toda a operação do alvo está aí".

O resultado desse trabalho foi fruto do diálogo e cooperação dentro da Polícia Federal, algo que deve ser incentivado para que esse sucesso se repita sempre.

Agradecimentos

À chefia do Setor Técnico-Científico - RS, pelo apoio e reconhecimento

À equipe de investigação e suas chefias, pela eficiência e diálogo

Referências

[1] Wireshark, http://www.wireshark.org, visitado em 11/07/2009
[2] *Socat*, http://www.dest-unreach.org/socat, visitado em 11/07/2009
[3] Cryptcat, http://sourceforge.net/projects/cryptcat, visitado em 11/07/2009
[4] Python, http://www.python.org, visitado em 11/07/2009

[5] Sun Secure Global Desktop, http://www.oracle.com/us/products/servers-storage/desktop-workstations/030738.htm, visitado em 11/07/2009

[6] *Tar* for windows, http://gnuwin32.sourceforge.net/packages/gtar.htm, visitado em 11/07/2009

[7] *7zip*, http://www.7-zip.org, visitado em 11/07/2009

Daniel Araújo Miranda Perito Criminal Federal, Departamento de Polícia Federal, miranda.dam@dpf.gov.br, *Brasília-DF, Brasil*

Rodrigo Alves Carvalho *Perito Criminal Federal, Departamento de Polícia Federal, carvalho.rac@dpf.gov.b, Porto Alegre-RS, Brasil*