White Paper

Ciberataques ao setor energético mundial: “Night Dragon” (Dragão Noturno)

McAfee® Foundstone® Professional Services e McAfee Labs™

10 de fevereiro de 2011

Índice

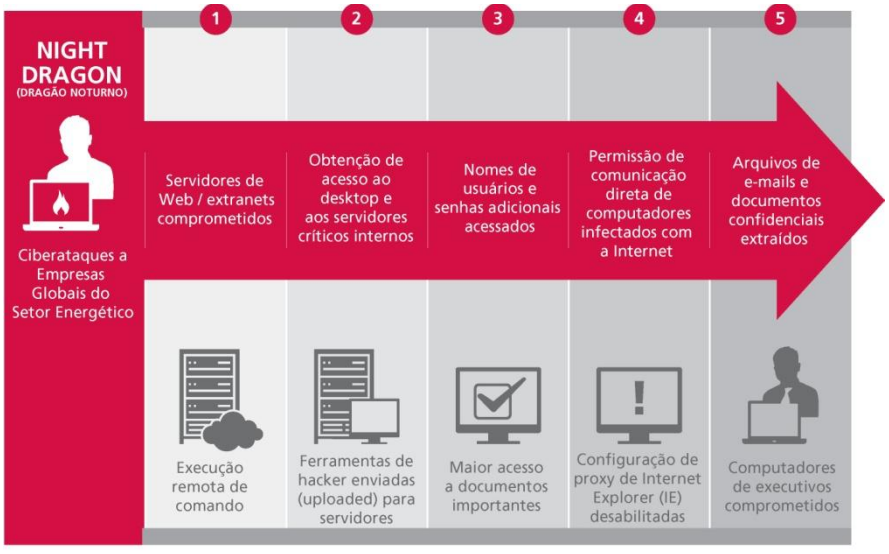
Resumo executivo

Em 2010, entramos em uma nova década no mundo da cibersegurança. A década anterior foi marcada pela imaturidade, por soluções técnicas reativas e pela falta de sofisticação na segurança, levando a epidemias graves como a Code Red, Nimda, Blaster, Sasser, SQL Slammer, Conficker e myDoom, para mencionar apenas algumas. A comunidade de segurança evoluiu e aprimorou a inteligência sobre a segurança, computação segura e reforço de sistemas, mas o mesmo ocorreu com os nossos adversários. Essa década está pronta para ser o “trampolim” exponencial. Os adversários estão rapidamente aproveitando kits de ferramentas de produção de malware que permitem o desenvolvimento de muito mais ameaças que em todos os anos anteriores juntos, e eles amadureceram em relação à última década, lançando as ameaças virtuais mais traiçoeiras e persistentes já vistas.

Os ataques ao Google (“Operação Aurora”), batizados pela McAfee e anunciados em janeiro de 2010, e a divulgação de documentos pelo WikiLeaks em 2010, destacaram o fato de ser praticamente impossível evitar as ameaças externas e internas. Os criminosos continuam se infiltrando nas redes e extraindo dados confidenciais e reservados dos quais as economias do mundo dependem todos os dias. Quando surge um novo ataque, os fornecedores de segurança não podem ficar parados, esperando e assistindo. A McAfee sente-se na obrigação de compartilhar as descobertas para proteger quem ainda não foi afetado e para auxiliar com recuperação de quem já foi. Dessa forma, a área McAfee Foundstone Professional Services e o McAfee Labs decidiram divulgar a seguinte descoberta.

Em novembro de 2009, ciberataques coordenados secretos e dirigidos começaram a ser conduzidos contra empresas globais dos setores de petróleo, energia e petroquímica. Esses ataques consistiam em engenharia social, ataques de *spear-phishing* (milhões de e-mails com link malicioso com alvo a pessoas ou empresas), exploração de vulnerabilidades do sistema operacional Microsoft Windows, comprometimentos do Microsoft Active Directory, e no uso de ferramentas de administração remota (RATs - *Remote Administration Tools*) para atacar e coletar operações reservadas confidenciais de concorrentes e informações sobre financiamento de projetos de licitações e operações nas áreas de petróleo e gás. Identificamos principalmente na China a origem das ferramentas, técnicas e atividades de rede utilizadas nesses ataques contínuos — que batizamos de Dragão Noturno. Através da análise coordenada dos eventos relacionados e das ferramentas utilizadas, a McAfee definiu características distintivas para auxiliar as empresas na detecção e investigação. Embora a McAfee acredite que muitos participaram desses ataques, foi possível identificar uma pessoa que forneceu a infraestrutura essencial de comando e controle (C&C) aos atacantes. *(Veja no Apêndice B mais detalhes sobre a atribuição.)*

Anatomia de uma invasão



Fonte: McAfee, Inc.

Figura 1. Anatomia de uma invasão.

Os ataques do Dragão Noturno funcionam através de invasões metódicas e progressivas da infraestrutura alvo da ação. As seguintes atividades básicas foram realizadas pela operação Dragão Noturno:

- Os servidores de Web das extranets das empresas foram comprometidos através de técnicas de injeção de SQL, permitindo a execução remota de comandos.
- As ferramentas de hackers, normalmente disponíveis, são enviadas a servidores de Web comprometidos, permitindo que os atacantes invadam a intranet da empresa, dando-lhes acesso interno a desktops e servidores confidenciais.
- Utilizando ferramentas de quebra de senha e de *pass-the-hash*, os atacantes ganham mais nomes de usuário e senhas, o que permite obter mais acesso autenticado a desktops e servidores internos confidenciais.
- Utilizando inicialmente os servidores de Web comprometidos da empresa como servidores de comando e controle (C&C), os atacantes descobriram que só precisavam desativar as configurações de *proxy* do Microsoft Internet Explorer (IE) para permitir que os computadores infectados se comunicassem diretamente com a Internet.
- Utilizando malware de RAT (*Remote Administration Tools*), eles passaram a se conectar com outras máquinas (buscando por executivos) e extraindo arquivos de e-mail e outros documentos confidenciais.

Detalhes do ataque

Invasores em vários locais da China aproveitaram servidores de C&C em serviços de hospedagem comprados nos Estados Unidos e servidores comprometidos na Holanda, para realizar ataques contra empresas mundiais de petróleo, gás e petroquímica, bem como indivíduos e executivos no Cazaquistão, em Taiwan, na Grécia e nos Estados Unidos, para adquirir informações reservadas e altamente confidenciais. A principal técnica operacional utilizada pelos atacantes consistiu em várias ferramentas de hackers, inclusive ferramentas desenvolvidas em âmbito privado e ferramentas personalizadas de RAT que proporcionaram ao atacante os recursos completos de administração remota. As RATs oferecem funções semelhantes ao Citrix ou ao Microsoft Windows Terminal Services, permitindo que um indivíduo remoto controle totalmente o sistema afetado.

Para instalar essas ferramentas, os atacantes comprometeram primeiramente os controles de segurança perimetrais, através de explorações de injeção de SQL em servidores de Web de extranets, além de ataques dirigidos de *spear-phishing* a laptops de funcionários (equipamentos móveis) e comprometendo contas corporativas de VPN, a fim de penetrar nas arquiteturas de defesa da empresa atacada (DMZs – DeMilitarized Zone ou zona desmilitarizada - e firewalls) e realizar o reconhecimento dos computadores em rede dessas empresas.

Ataques de injeção de SQL

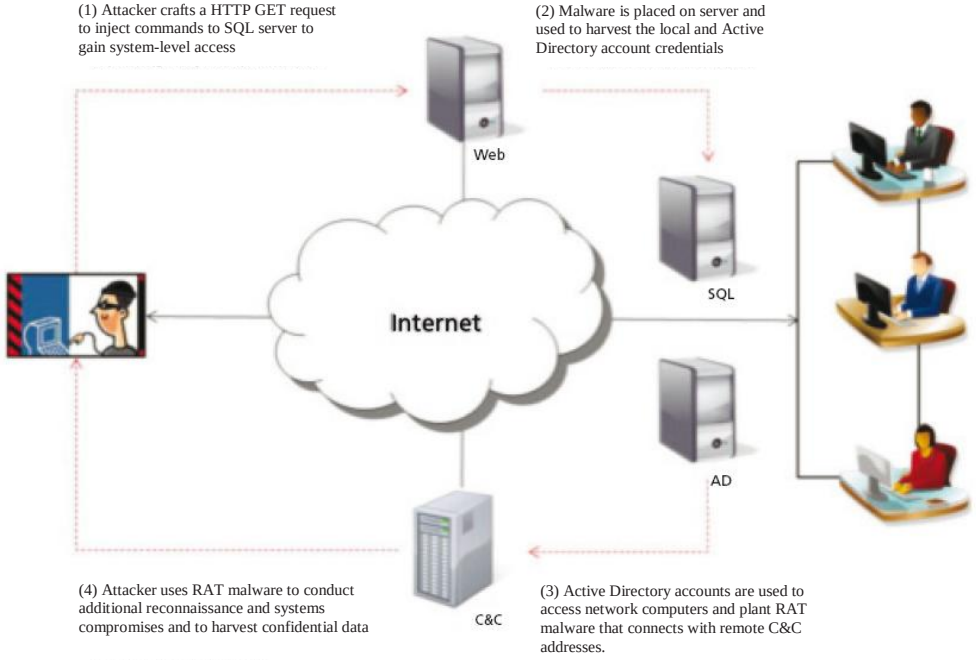


Figura 2. Ataques de injeção de SQL.

Ataques de Spear-Phishing

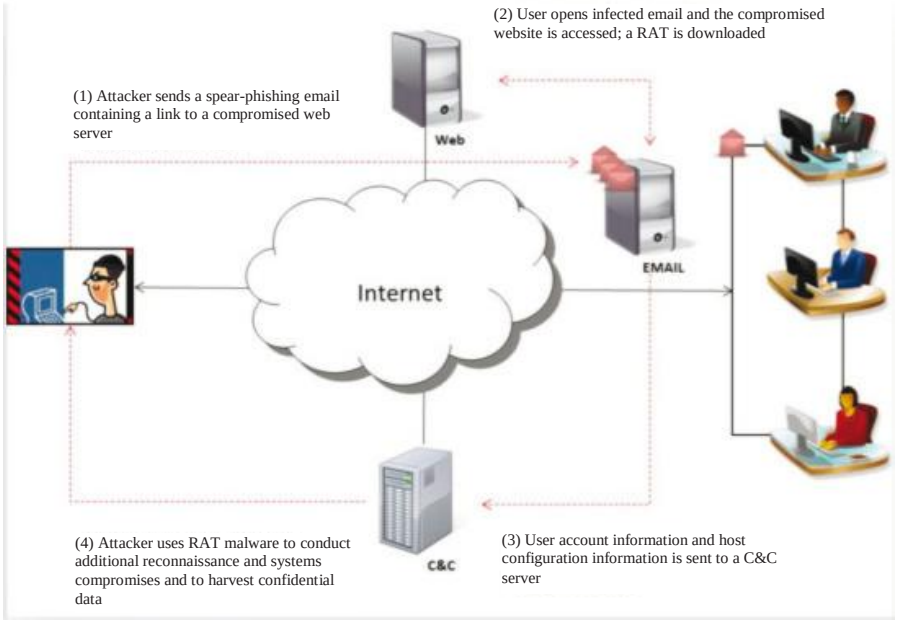


Figura 3. Ataques de *spear-phishing*.

Muitos sites de hackers chineses oferecem essas ferramentas para download, inclusive links para *reduh*, WebShell, ASPXSpy e muitos outros, além de explorações e malware do dia-zero.

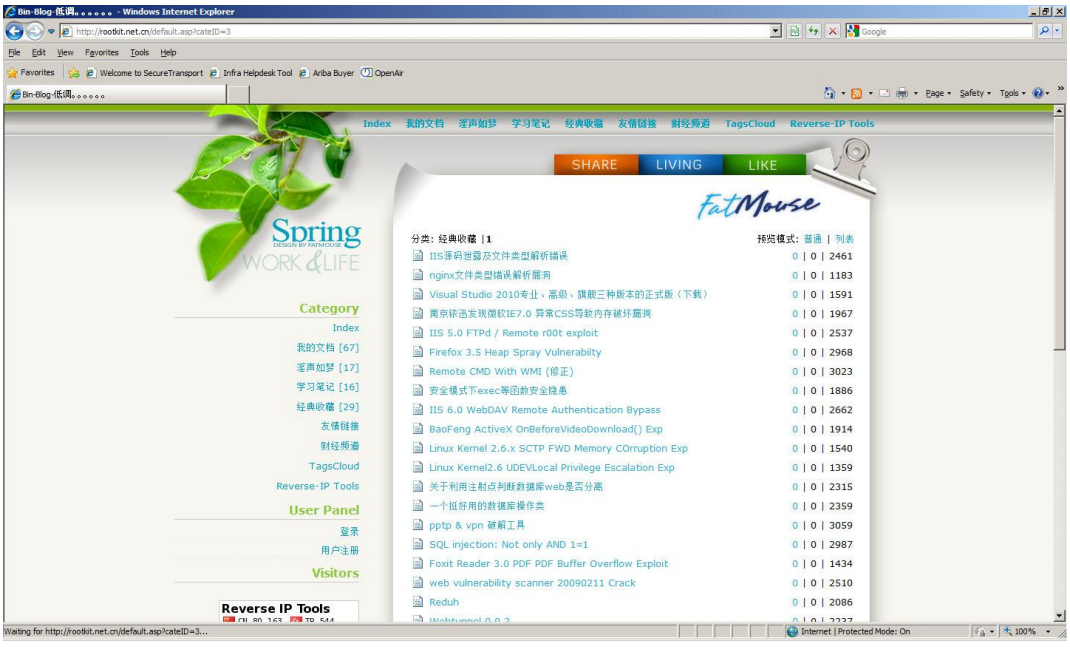


Figura 4. Rootkin.net.cn oferece acesso a uma lista interminável de ferramentas e explorações de hackers.

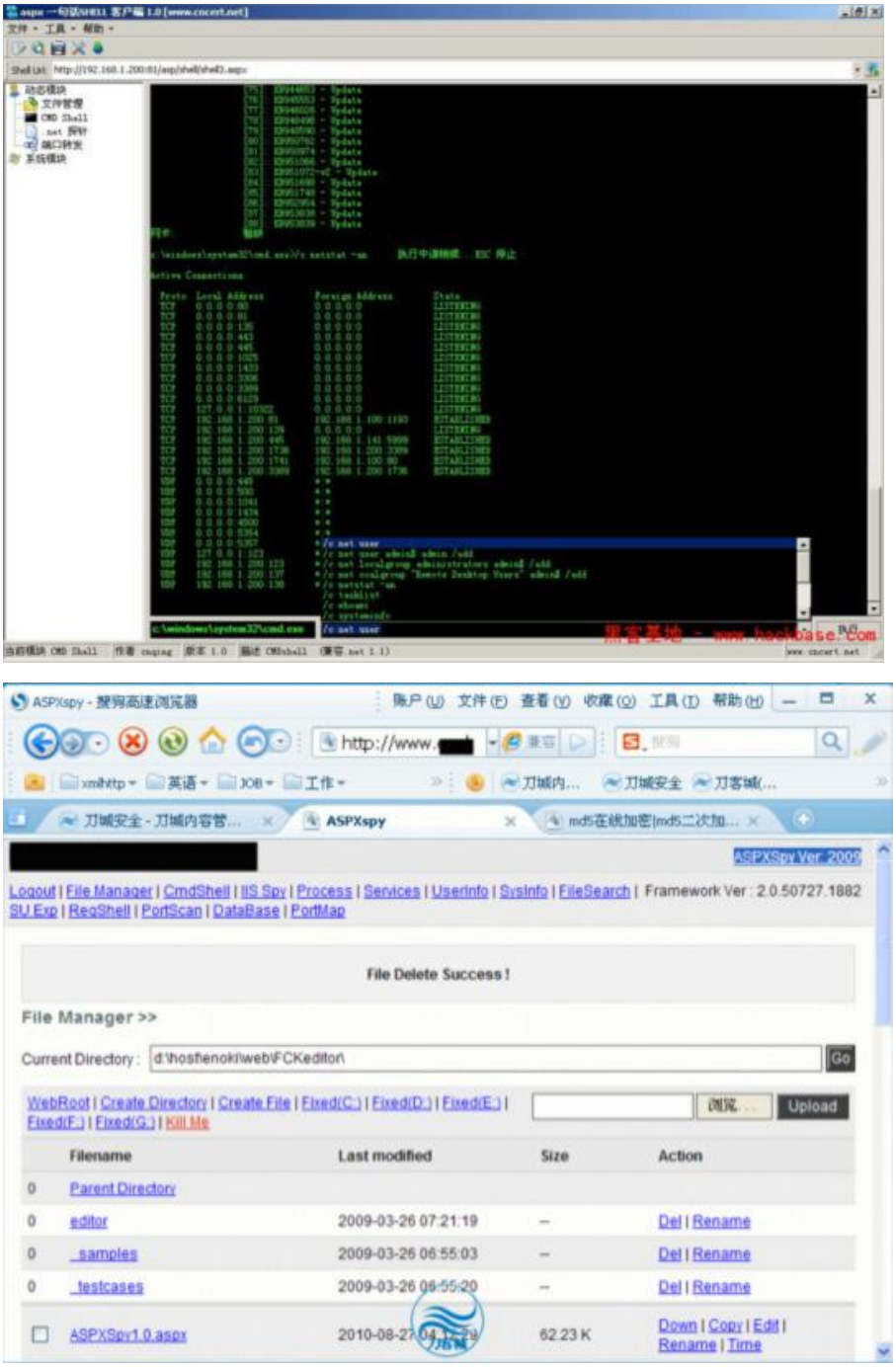


Figura 5. As ferramentas WebShell e ASPXSpy permitem que um atacante ignore muitas regras de firewall para canalizar todo o controle através do servidor de Web de uma empresa.

Quando o sistema inicial foi comprometido, os atacantes danificaram as contas locais de administrador e as contas do administrador do Active Directory (e dos usuários e administrativos). Os atacantes usaram frequentemente utilitários comuns do Windows, tais como ferramentas SysInternals (adquirida pela Microsoft em 2006) – e outros softwares disponíveis ao público, entre eles ferramentas de invasão desenvolvidas na China e amplamente disponíveis em sites secretos chineses de hackers – para estabelecer “*backdoor*s” através de *proxies* reversos, e “plantaram” cavalos de Troia que permitiram aos atacantes ignorar as políticas e configurações de segurança de rede e host. As ferramentas antivírus e antispyware para desktops também foram desativadas em alguns casos – uma técnica comum de ataques dirigidos.

Uso de ferramentas de administração remota

Ferramentas de administração remota (RATs) são normalmente utilizadas como ferramentas administrativas que permitem aos hackers (e administradores) gerenciar os computadores das vítimas (ou sistemas gerenciados) e controlar completamente sua utilização e seu funcionamento. Uma RAT normalmente utilizada na comunidade hacker é o Gh0st e suas diversas variantes. Os recursos de RAT geralmente são espionagem de tela e webcam, gravação de digitação, controle do mouse, arquivo/registro e gerenciamento de processos e, naturalmente, o recurso de *shell* de comando remoto.

A McAfee identificou várias RATs que foram usadas para estabelecer um canal de infiltração persistente para as empresas comprometidas. A RATs mais predominante é o zwShell, que a McAfee tem visto agir ativamente desde março/abril de 2010 (compilado em 2010-03-17 08:47:00). Escrita na linguagem Delphi, o zwShell foi utilizado por atacantes para criar variantes personalizadas do cavalo de Troia que eles instalaram em dezenas de máquinas dentro de cada empresa vítima, bem como para controlar as máquinas comprometidas que iniciariam conexões guiadas a ele em um protocolo personalizado.

Os atacantes utilizaram amplamente o zwShell para gerar dezenas de variantes exclusivas do cavalo de Troia e controlar as máquinas infectadas e extrair dados confidenciais diretamente através delas. (Consulte no Apêndice A um detalhamento do zwShell).

Assim que os atacantes assumiram o controle completo do sistema interno atacado, eles despejaram *hashes* (sequência de bits geradas por um algoritmo de dispersão) de conta com o *gsecdump* e utilizaram a ferramenta *Cain & Abel* para quebrar os *hashes* a fim de usá-los no ataque a infraestruturas cada vez mais frágeis.

Os arquivos de interesse se concentravam em sistemas operacionais de produção de campos de petróleo e gás e em documentos financeiros relacionados à exploração e licitação de campos, que foram depois copiados dos *hosts* comprometidos ou através de servidores de extranet. Em alguns casos, os arquivos foram copiados para os servidores de Web da empresa pelos atacantes e baixados a partir deles. Em alguns casos, os atacantes coletaram dados dos sistemas SCADA.

Detecção

Os métodos e as ferramentas utilizados nesses ataques não são sofisticados, pois simplesmente parecem ser técnicas comuns de administração de *host*, utilizando credenciais administrativas comuns. Isto se deve principalmente ao fato de serem capazes de evitar a detecção por meio de softwares de segurança e políticas de rede comuns. No entanto, desde os primeiros comprometimentos, os fornecedores de segurança (inclusive a McAfee) identificaram muitas assinaturas individuais originais do cavalo de Troia e das respectivas ferramentas; mas, foi apenas através das análises recentes e da descoberta de recursos comuns, além da correlação de evidências, que foi possível determinar que uma iniciativa dedicada estivesse em andamento havia pelo menos dois anos e, provavelmente, até quatro anos. Agora, podemos associar as diversas assinaturas a esses eventos.

Os seguintes recursos podem ajudar a determinar se uma empresa foi comprometida:

- Arquivos de *host* e/ou chaves de Registro
- Alertas de antivírus
- Comunicações de rede

Arquivos de host e chaves de registro

Utilitário	Descrição
Aplicativo de comando e controle	Shell.exe 093640a69c8eafbc60343bf9cd1d3ad3 zwShell.exe 18801e3e7083bc2928a275e212a5590e zwShell.exe 85df6b3e2c1a4c6ce20fc8080e0b53e9
Instalador (*dropper*) de cavalo de Troia	Um pacote executável, personalizado a cada vítima, que inclui o arquivo DLL e os parâmetros de configuração para instalar o *backdoor* no sistema remoto. O *dropper* pode ser executado de qualquer diretório e normalmente é executado com o PSEXEC ou uma sessão de RDP. Assim, os respectivos logs de Eventos de Segurança do Windows fornecem informações úteis referentes às contas comprometidas do Active Directory. Esses logs podem ser analisados com o Windows Event Log Manager ou programas, tais como o "Event Log Explorer" ou p EnCase, que têm recursos de pesquisa. Quando é executado, o *dropper* cria um arquivo temporário que se reflete nos logs de atualização do Windows (arquivos KB*.log na pasta C:\Windows). Isso ocorre porque o Registro do Windows é modificado pelo *dropper*, que cria uma chave "netsvcs". Assim, é possível saber a data de instalação do *backdoor* com uma pesquisa nos arquivos de log KB. Esse arquivo temporário também é identificado na própria DLL do *backdoor*. O arquivo temporário é, geralmente, uma combinação alfanumérica que inclui "gzg" (por exemplo, xgt0gzg), mas ele também tem sido visto com nomes genéricos (por exemplo, server.exe). O *dropper* é excluído quando o *backdoor* é instalado, e o arquivo temporário é removido quando o computador é reiniciado. Se um *backdoor* já foi configurado no sistema, a instalação do *dropper* falhará, a menos que ele use uma configuração diferente.
Backdoor cavalo de Troia	Bibliotecas de vínculo dinâmico (DLLs - Dynamic Link Libraries), que também aparecem com vários outros nomes. Esses arquivos têm uma chave de Registro do Windows correlacionada que é determinada pelo *dropper* quando o *backdoor* é instalado. O *dropper* se repete através das chaves netsvcs do Registro do Windows e usa a primeira chave disponível, indicando o caminho e o nome do *backdoor* num registro ServiceDLL. O *backdoor* funciona como um serviço através de uma configuração de registro “svchost.exe netsvcs –k”. A chave do serviço pode ser encontrada em: HKLM\system\<controlset>\services\ A DLL é um arquivo oculto ou de sistema, com tamanho de 19 KB a 23 KB, e inclui uma seção de dados com codificação XOR que é definida pelo aplicativo de C&C quando o *dropper* é criado. Ele inclui o identificador de serviço de rede, a chave de serviço do registro, a descrição do serviço, o nome do mutex, o endereço do servidor de C&C , a porta e o nome do arquivo temporário do *dropper*. O *backdoor* pode funcionar a partir de qualquer porta TCP configurada. Essa DLL é especificada na chave ServiceDLL no respectivo item de registro netsvcs do Windows. A DLL é geralmente encontrada na pasta %System%\System32 ou %System%\SysWow64.
Backdoor* cavalo de Troia 2	startup.dll A6CBA73405C77FEDEAF4722AD7D35D60 Inicialmente configurado com o seguinte: connect.dll 6E31CCA77255F9CDE228A2DB9E2A3855 A connect.dll cria o arquivo temporário "HostID.DAT", que é enviado ao servidor de C&C. Em seguida, ela baixa e configura as respectivas DLLs: PluginFile.dll PluginScreen.dll PluginCmd.dll PluginKeyboard.dll PluginProcess.dll PluginService.dll PluginRegedit.dll Daí em diante, a "Startup.dll" opera o serviço em uma chave do Registro do Windows. Todas as comunicações vistas até agora com esta versão estiveram nas portas 25 e 80 através de TCP, mas podem operar em qualquer porta determinada. A chave de serviço é identificada na DLL (que não inclui dados criptografados) como: HKLM\Software\RAT Essa DLL é geralmente encontrada no diretório %System%\System32, mas também já foi encontrada em outros locais. O caminho para a DLL de *backdoor* é indicado na chave ServiceDLL do Registro do Windows.

* Esta DLL usa um aplicativo de C&C diferente que pode ser uma versão anterior do zwShell. As análises prosseguem.

Os componentes do cavalo de Troia são copiados ou entregues manualmente aos sistemas remotos através de utilitários administrativos. Eles não têm nenhum recurso de worm ou de autoduplicação, nem o cavalo de Troia é capaz de “infectar” outros computadores. Remover os componentes do cavalo de Troia é simplesmente uma questão de apagar os arquivos e as respectivas configurações de registro.

O *backdoor* cavalo de Troia se comunica com o servidor de C&C no endereço codificado de maneira fixa em cada DLL. O servidor de C&C não pode modificar o *backdoor* depois que ele for instalado; o arquivo de cavalo de Troia deve ser removido dos respectivos sistemas para que uma nova DLL de *backdoor* possa ser instalada no sistema. Assim, se o endereço do servidor de C&C for alterado, os servidores que tiverem a DLL com endereços antigos devem ser administrados remotamente pelo atacante.

Alertas de antivírus

Os padrões de antivírus são definidos de acordo com as amostras enviadas pelos clientes ou analistas à medida que são descobertos. Alguns cavalos de Tróia exibem características de outros tipos de malware, como worms ou vírus, que têm a capacidade de infectar outros sistemas. As RATs não costumam conter esses recursos e, como são definidas com configurações exclusivas para fins específicos, geralmente mudam mais rapidamente do que as amostras originais podem ser identificadas.

Somente quando um kit de ferramentas de RAT completo é encontrado podemos definir um padrão de antivírus suficientemente genérico para detectar a RAT, independentemente das mudanças de configuração. O pacote contém necessariamente um servidor de aplicativos de C&C, o utilitário gerador para a criação de *droppers*, os respectivos *droppers* e *backdoor*s – e um número suficiente de cada um para correlacionar o kit de ferramentas.

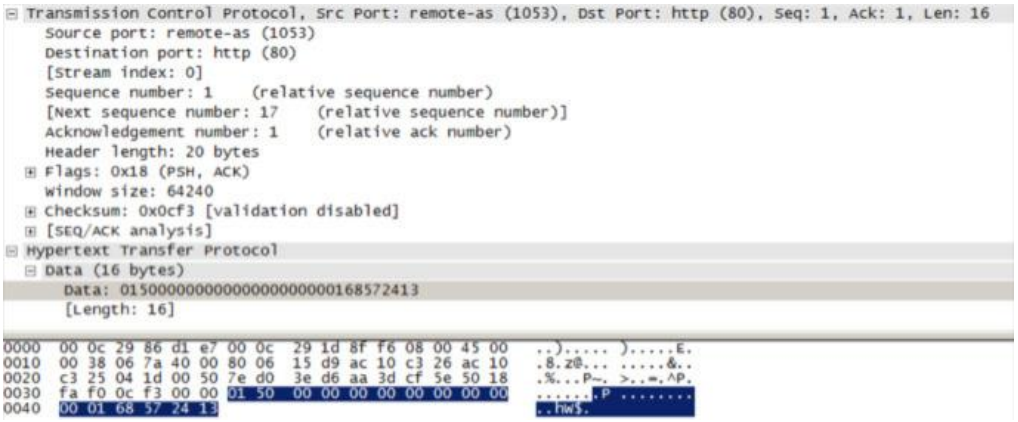
Como mencionamos anteriormente, vários padrões exclusivos foram desenvolvidos a partir de amostras enviadas à McAfee e a outros fornecedores de antivírus.

> A McAfee recomenda que as empresas examinem no sistema de gerenciamento McAfee ePolicy Orchestrator® (McAfee ePO™) e nos registros do antivírus as detecções da assinatura do “Night Dragon”(Dragão Noturno) para identificar alertas relacionados desde 2007 e, em seguida, recuperem e reenviem essas amostras para investigar os incidentes relacionados. A McAfee pode auxiliar na análise ou fornecer instruções e ferramentas para análise interna.

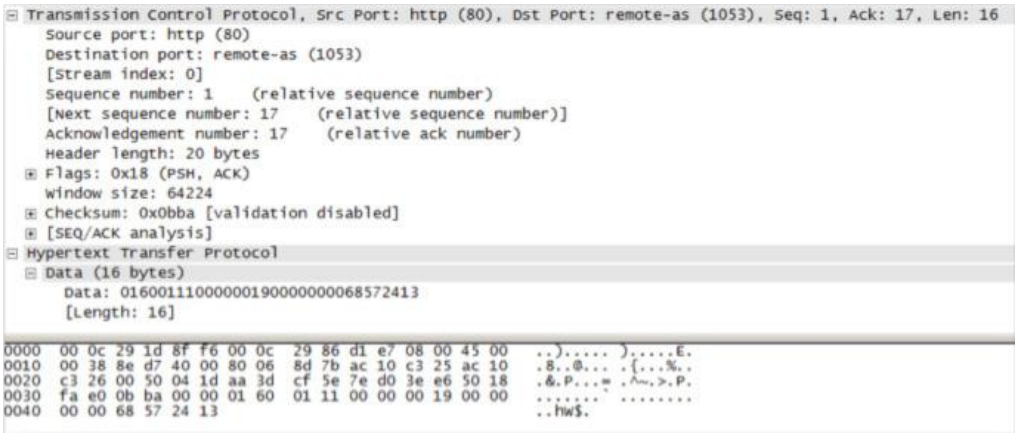
Comunicações de rede

As comunicações de rede são relativamente fáceis de detectar porque o malware usa um guia de host exclusivo e um protocolo exclusivo de resposta ao servidor. Cada pacote de comunicação entre o host comprometido e o servidor de C&C é assinado com uma assinatura de texto sem formatação “HW$”. (ou “\x68\x57\x24\x13”) no offset de byte 0x42 dentro do pacote TCP.

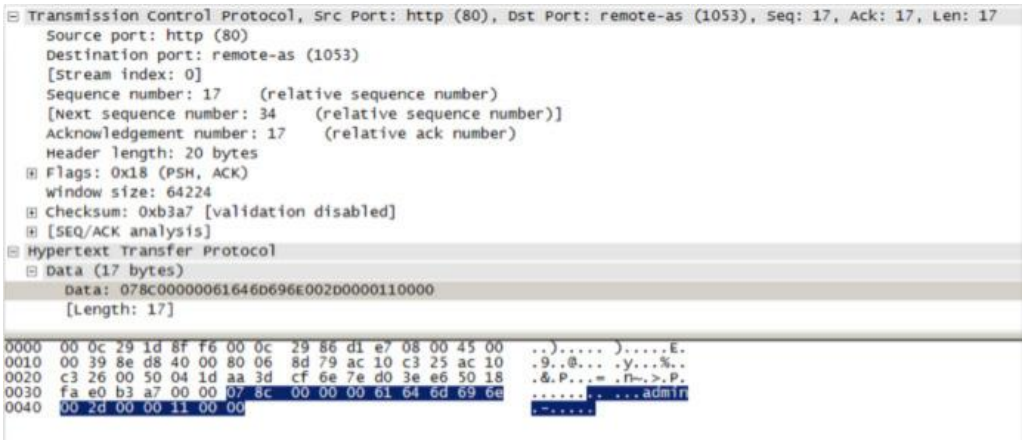
O *backdoor* aciona seu guia a intervalos de aproximadamente cinco segundos com um pacote inicial que pode ser detectado com o padrão: “\x01\x50[\x00-\xff]+\x68\x57\x24\x13.”



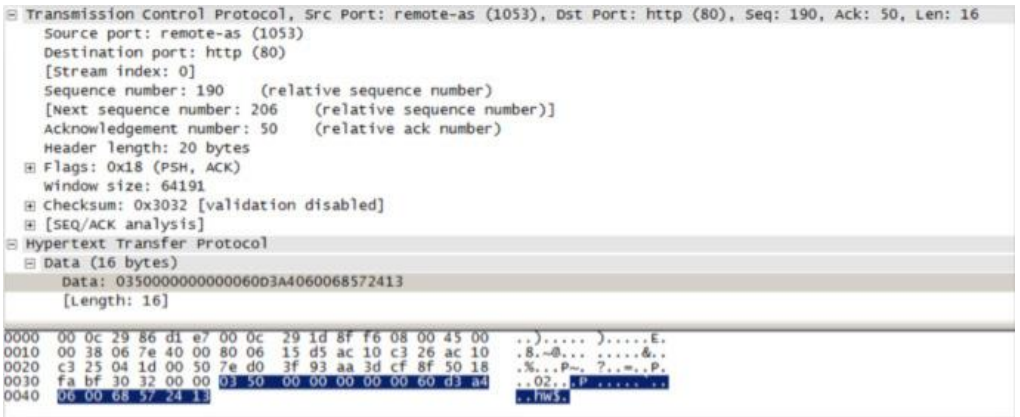
O servidor reconhece o guia com uma resposta inicial de “\x01\x60[\x00-\xff]+\x68\x57\x24\x13.”



O *backdoor* envia a senha ao servidor em texto simples depois que o servidor reconhece a conexão.



Enquanto o *backdoor* e o servidor tiverem uma conexão ativa, o *backdoor* envia mensagens de “keep-alive” que podem ser detectadas por: “\x03\x50[\x00-\xff]+\x68\x57\x24\x13.”



Os atacantes utilizam contas de serviços de nome de Internet com “DNS dinâmico” para retransmitir as comunicações de C&C ou associar temporariamente endereços DNS a servidores remotos. Os domínios mais utilizados para o tráfego de C&C têm sido (todos têm sido utilizados com frequência por outros tipos de malware):

- is-a-chef.com
- thruhere.net
- office-on-the.net
- selfip.com

Servidores de extranet de empresas também têm sido utilizados como servidores exclusivos ou secundários/redundantes de C&C. Em alguns casos, os atacantes utilizam (provavelmente por engano) *droppers* configurados para comprometer os computadores de uma empresa – em computadores de outra empresa.

A McAfee recomenda que as empresas configurem regras no sistema de detecção de intrusões (IDS) para detectar as assinaturas indicadas (ou que utilizem a assinatura definida pelo usuário [UDS] “BACKDOOR: NightDragon Communication Detected” na McAfee Network Security Platform) e monitorem no DNS as comunicações de saída com endereços dinâmicos de DNS convertidos ou devolvidos como sublocados para servidores na China, em que o nome da empresa ou formas comuns de abreviação formam a primeira parte do endereço. Isso pode ser difícil. No entanto, se forem encontradas amostras das DLLs de *backdoor*, o monitoramento do DNS pode ajudar a identificar outros hosts comprometidos na rede da empresa. A McAfee também recomenda que as empresas procurem em seus *logs* de Web ou de IDS transferências de arquivos para endereços registrados na China. A McAfee pode auxiliar na análise ou fornecer instruções e ferramentas para análise interna.

Outras técnicas de detecção

O *backdoor* troca sinais com seu respectivo servidor de C&C, enquanto o endereço relacionado estiver ativo. Se o endereço for abandonado ou ficar inacessível, o *backdoor* para de emitir sinais após um intervalo indeterminado. Entretanto, quando um computador infectado é reiniciado, a sinalização recomeça porque ele está registrado como um serviço no Registro do Windows. Os antivírus podem ou não detectar o cavalo de Troia, a menos que ele esteja emitindo sinais ou que uma varredura completa do sistema de arquivos seja realizada.

Detecção antecipada da McAfee

Os clientes podem instalar uma série de produtos da McAfee para ajudar a proteger os sistemas de informação contra o ataque Dragão Noturno:

- *McAfee Vulnerability Manager:* Utilizando a descoberta sem agente e verificações de vulnerabilidades para avaliar os sistemas na rede, o McAfee Vulnerability Manager é um sistema de grande porte para gerenciamento de vulnerabilidades que detecta sistemas infectados com o Dragão Noturno e as falhas de segurança nos sistemas que foram comprometidos. O script “wham-apt-nightdragon-detected-v7.fasl3” detecta essa ameaça remotamente nos sistemas.
- *McAfee Policy Auditor:* Utilizando verificações de auditoria de configuração para determinar a configuração mais segura de um sistema, o software McAfee Policy Auditor detecta as falhas de segurança nos sistemas que tenham sido comprometidos.
- *McAfee Risk Advisory (MRA):* Devidamente instalado, o McAfee Risk Advisor teria permitido que os administradores vissem os erros de configuração e as falhas na cobertura de segurança que facilitaram a exploração Dragão Noturno.

Detecção da McAfee

O Dragão Noturno também apresenta um padrão de atividades correlatas com uma variedade de outras ferramentas de software que a McAfee pode ajudar as empresas a identificar.

- *McAfee VirusScan Enterprise:* Atualize os DATs do seu antivírus ao menos na versão 6232 e verifique se as varreduras sob demanda estão funcionando corretamente, e execute uma varredura completa de vírus no sistema de arquivos. Procure nos alertas do software McAfee ePO ou de antivírus e nos *logs* de rede as detecções de assinatura “NightDragon” para identificar os sistemas infectados. Envie todas as amostras relacionadas para virus_research@mcafee.com ou pela Web, no endereço https://www.webimmune.net/default.asp.
- *McAfee Network Threat Response:* A tecnologia McAfee Network Threat Response teria detectado o tráfego mal-intencionado de C&C e alertado com antecedência os administradores sobre o ataque, dando a eles o tempo para reagir e evitar mais danos.

Os administradores também podem baixar as seguintes ferramentas grátis da McAfee:

- O McAfee “Night Dragon Vulnerability Scanner”, que utiliza a tecnologia McAfee Vulnerability Manager para realizar em suas redes uma varredura da presença de malware.
- McAfee Labs Stinger.

Prevenção da McAfee

Para evitar, de maneira completa, esse e a maioria dos outros ataques que envolvem ameaças avançadas persistentes (APTs - Advanced Persistent Threats), os clientes podem criar *whitelists* de aplicativos e software de controle de alterações/configurações em seus servidores mais importantes. Essas tecnologias impedem completamente a execução não autorizada de DLLs/EXEs, além da alteração das chaves de registro, de serviços e de outros elementos presentes em todos os ataques de APT e do dia-zero atuais.

- *McAfee Application Control:* O software McAfee Application Control bloqueia o Dragão Noturno, impedindo a execução dos arquivos *dropper* (até mesmo como administrador no Windows), evitando, assim, que mais malware seja baixado e que canais de C&C sejam instalados para permitir o controle por RATs e roubar arquivos confidenciais.
- *McAfee Configuration Control:* O software McAfee Configuration Control permite que o usuário proíba qualquer alteração na configuração dos seus sistemas, protegendo-os contra modificações sem permissão explícita (mesmo com acesso administrativo).
- *McAfee Network Security Manager:* Com o conjunto correto de assinaturas de UDS instalado, os appliances McAfee Network Security Platform protegem contra ataques baseados na rede, como o Dragão Noturno, detectando tráfegos mal-intencionados na rede e alertando os administradores para que eles tenham tempo de reagir e prevenir futuros ataques.
- *McAfee Firewall Enterprise:* Corretamente instalado e configurado no perímetro e dentro da sua organização, o McAfee Firewall teria impedido que a operação Dragão Noturno penetrasse tão profundamente nas organizações afetadas e teria bloqueado a comunicação de C&C da RAT.
- *McAfee Web Gateway:* Instalado e configurado corretamente, o McAfee Web Gateway teria impedido que a operação Dragão Noturno utilizasse suas RATs, obrigando-a a fazer com que as RATs reconhecessem *proxies* ou utilizar outras RATs compatíveis com *proxies*.
- *McAfee Endpoint Encryption:* Instalado e configurado corretamente, o software McAfee Endpoint Encryption reduz o impacto do ataque Dragão Noturno, restringindo o acesso aos recursos principais atacados.
- *McAfee Data Loss Protection:* Instalado e configurado corretamente, o McAfee Network DLP e/ou as soluções McAfee Host DLP permitem que o usuário impeça e detecte a extração de informações sensíveis de fora da empresa.

- *McAfee Host Intrusion Prevention 8.0:* O software McAfee Host Intrusion Prevention 8.0 introduziu um novo recurso de detecção de APTs, o “TrustedSource”, que permite às empresas correlacionar atividades de executáveis em terminais com comunicações de C&C na rede, a fim de detectar e impedir a comunicação de RATs e atividades de extração de dados.
- *McAfee VirusScan® Enterprise:* Além de detectar os malwares e as RATs associados nos terminais, os clientes também podem aproveitar os recursos de proteção de acesso do McAfee VirusScan Enterprise para evitar (e alertar) a criação de arquivos e estruturas de pastas relacionados ao Dragão Noturno. Outros recursos internos, tais como rastreamento de infecções e o McAfee Global Threat Intelligence™ (GTI) podem ajudar na identificação e na quarentena ou remoção de malwares e RATs novos e ainda desconhecidos associados.

Se o usuário descobriu a presença do Dragão Noturno no seu ambiente e quiser contar com assistência pericial ou de reação a incidentes para reagir ao problema e solucioná-lo, poderá entrar em contato com a Foundstone Professional Services pelo e-mail incidentresponse@foundstone.com ou enviar todas as respectivas amostras ao endereço Virus_Research@avertlabs.com ou, pela Web, McAfee Labs WebImmune.

Conclusão

O número de ataques direcionados e bem coordenados, tais como o Dragão Noturno, orquestrados por um grupo crescente de atacantes mal-intencionados comprometidos com suas metas, está aumentando rapidamente. Esses alvos já não são apenas os computadores da base industrial de defesa, do governo e das Forças Armadas. Agora, eles também estão em grandes empresas privadas globais. Embora os ataques do Dragão Noturno tenham se concentrado especificamente no setor energético, as ferramentas e técnicas desse tipo podem ser altamente bem-sucedidas quando direcionadas a qualquer setor de atividade. Nossa experiência mostra que muitos outros setores estão vulneráveis e sob ataques de ciberespionagem contínuos e persistentes desse tipo. Cada vez mais, esses ataques não se concentram em usar e abusar de máquinas nas organizações comprometidas, e sim no roubo de dados específicos e de propriedade intelectual. É essencial que as organizações tomem a iniciativa de proteger seu bem maior e de grande valor: a propriedade intelectual. As empresas precisam tomar medidas para descobrir esses recursos em seus ambientes, avaliar se há vulnerabilidades em suas configurações e protegê-los contra uso indevido e ataques.

Para conhecer mais pesquisas e obter mais informações, leia o livro *Hacking Exposed: Network Secret and Solutions — 6ª Edição* (Osborne McGraw-Hill). Também é possível acessar http://www.hackingexposed.com para obter informações sobre técnicas avançadas de hackers e inscrever-se nos seminários virtuais “Hacking Exposed” realizados mensalmente (em inglês).

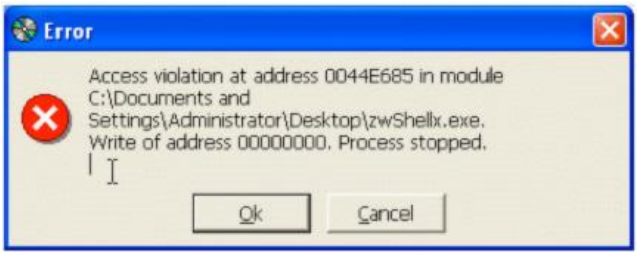
Créditos e agradecimentos

Este *white paper* foi um trabalho de colaboração entre várias pessoas e organizações, entre elas os consultores da área McAfee Foundstone Professional Services, do McAfee Labs, funcionários da McAfee, executivos e pesquisadores, a HBGary e a Aliança Nacional de Perícia Informática e Treinamento (NCFTA) dos Estados Unidos. Entre os principais colaboradores estão Shane Shook, Dmitri Alperovitch, Stuart McClure, Georg Wicherski, Greg Hoglund, Shawn Bracken, Ryan Permeh, Vitaly Zaytsev, Mark Gilbert, Mike Spohn e George Kurtz.

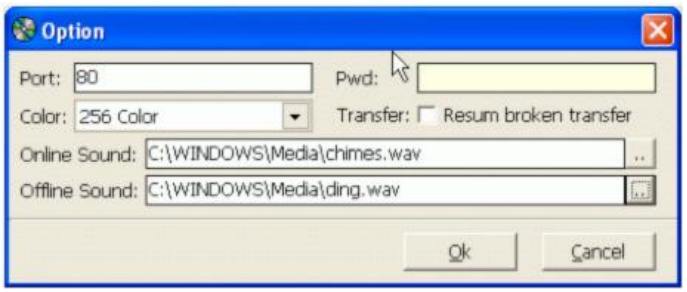
Apêndice A: zwShell — a RAT

Veja a seguir uma explicação dos recursos do zwShell e uma demonstração de como os atacantes usaram o zwShell como um servidor de comando e controle para extrair dados de dentro das empresas atacadas.

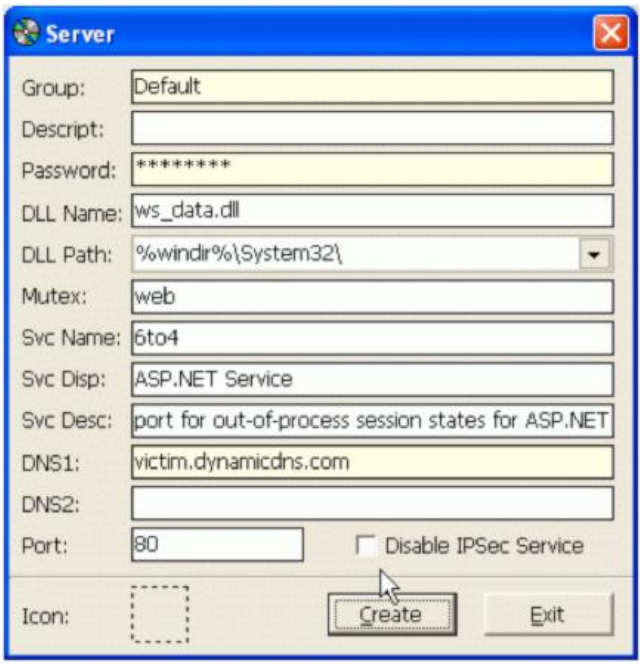
1. Quando o zwShell é iniciado, ele apresenta ao usuário um erro falso de travamento e contém um campo oculto de inserção de texto abaixo da linha “Write of address 00000000. Process stopped”. A caixa de diálogo oculta acima do botão "ok" exige a digitação da senha especial, "zw.china" para iniciar o aplicativo. Sem a senha, a ferramenta não será iniciada. Este método de ofuscação é provavelmente utilizado para confundir os investigadores sobre o verdadeiro propósito deste executável.



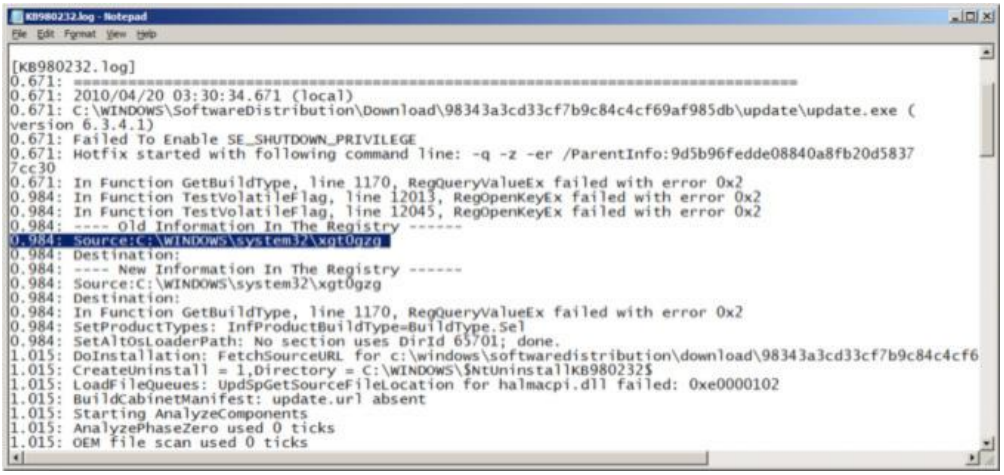
2. Quando o erro for ignorado e o zwShell for iniciado, ele permite que o invasor crie um cavalo de Troia personalizado, selecionando o menu Server, ou iniciar o servidor de C&C, clicando em Iniciar e entrando na porta para “escutar” o tráfego com a senha usada pelas DLLs de *backdoor*. Uma vez iniciado, o aplicativo começará a escutar as conexões recebidas pelo cliente infectado e exibi-las dentro da grade. O atacante pode iniciar quantas instâncias do aplicativo zwShell ele quiser, desde que cada uma possibilite “escutar” uma porta ou senha diferente. Dessa forma, várias “redes” de computadores infectados podem ser monitoradas.
3. O atacante também pode clicar no menu Opções para configurar os parâmetros do servidor de C&C. Essas configurações incluem a seleção da porta de escuta, a senha que criptografará o tráfego de C&C (que deve coincidir com a senha escolhida no momento da geração do cavalo de Troia), a capacidade de especificar notificações sonoras personalizadas quando as máquinas infectadas se conectarem e desconectarem do servidor de C&C, e a capacidade de aumentar a profundidade de cores usada no acesso remoto à máquina, bem como um recurso opcional para permitir a continuação, a partir da máquina cliente, de transferências de arquivos interrompidas. O atacante pode parar o “espião” e iniciá-lo com novas opções para monitorar ou conectar-se com outros computadores infectados.



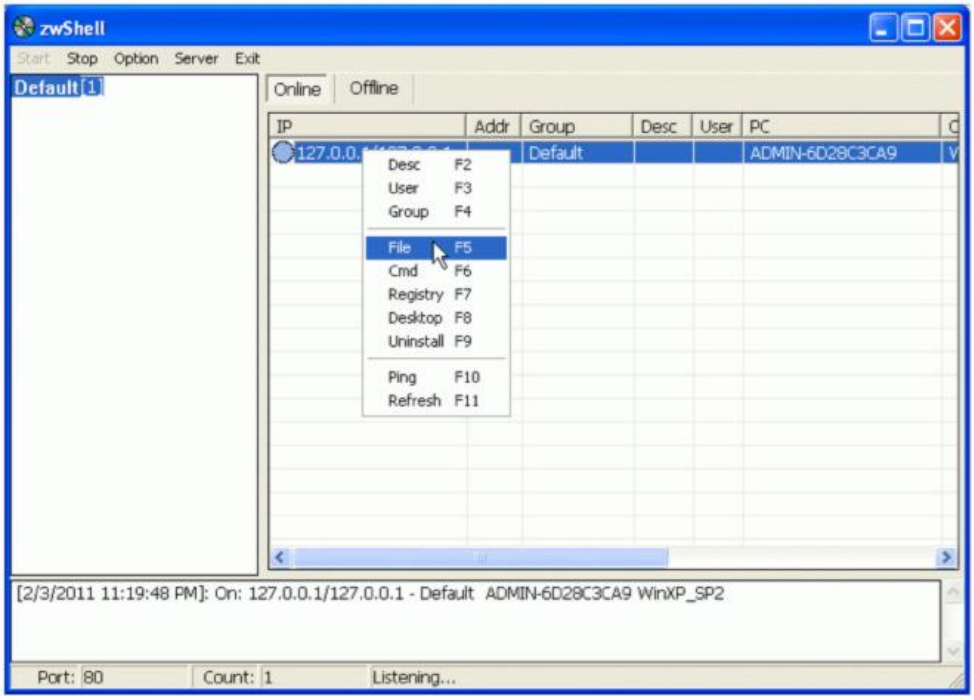
4. O atacante pode especificar a senha (que deve coincidir com a senha criada para o servidor na Etapa 3), o nome e o caminho da DLL da RAT que será injetada no processo de serviços svchost.exe do Windows, os nomes de serviço e *mutex*, e o nome e a descrição exibidos do serviço. O atacante também pode especificar até dois *hostnames* de C&C ou o endereço IP, o endereço de porta e o ícone do processo EXE do *dropper*. Quando o botão “Create” for clicado, o zwShell gerará um processo *dropper* EXE personalizado que, quando executado, excluirá a si mesmo e extrairá uma DLL de RAT que será iniciada como um serviço persistente do Windows. Então, a RAT enviará imediatamente na porta configurada um guia para o servidor de C&C designado e aguardará instruções.



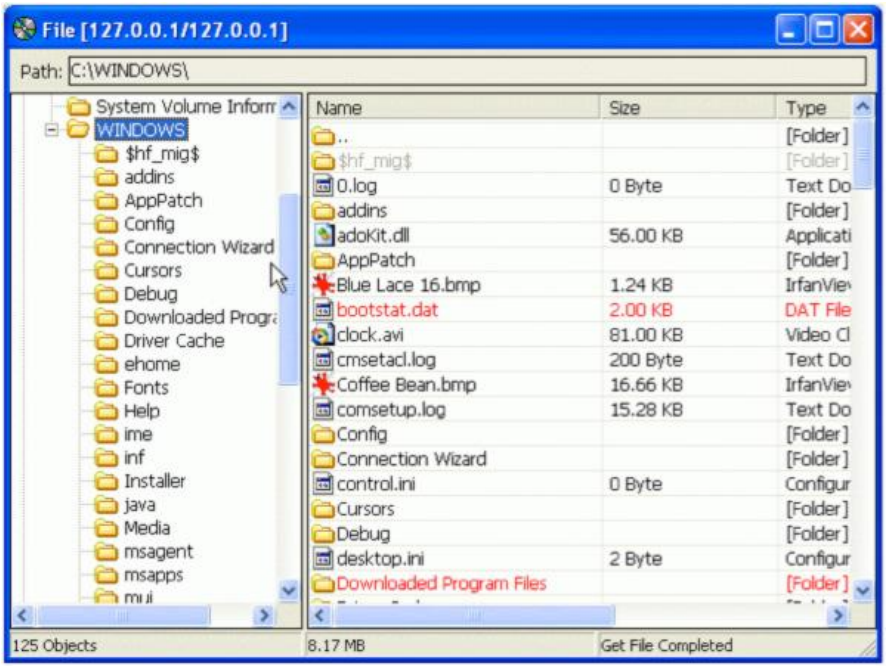
5. O *dropper* será copiado através de compartilhamentos de rede no computador comprometido e será executado remotamente com o psexec ou através dos Serviços de Terminal do Windows Terminal (RDP). Em alguns casos, um item “AT.job” ou “Schtasks” será usado para executar o *dropper* pela rede no computador comprometido. Quando executado, o *dropper* criará um arquivo temporário e extrairá uma DLL de RAT, que será iniciada como um serviço persistente do Windows. Então, a RAT enviará imediatamente na porta configurada um guia para o servidor de C&C designado e aguardará instruções. O *dropper* excluirá automaticamente a si mesmo depois que o serviço de *backdoor* for criado, e o arquivo temporário será apagado quando o sistema for reiniciado. Um item será criado nos *logs* do Windows Update (KB****.log) na pasta C:\Windows com a data e a hora e o caminho+nome do arquivo temporário.



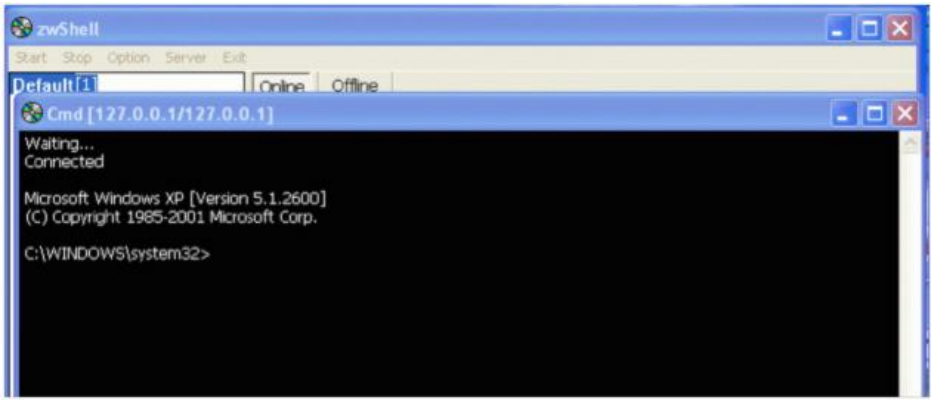
6. Quando um cliente é executado, ele se conecta à interface zwShell do atacante, com seu endereço IP, nome do PC, nome do usuário conectado e informações sobre o sistema operacional da versão da máquina, inclusive os níveis de *patch* principais.
7. O atacante encarregado do servidor de C&C pode estabelecer o controle remoto total da máquina conectada e pode pesquisar o sistema de arquivos, iniciar *shells* de linha de comando, manipular o registro, ver a área de trabalho remota e desinstalar o cavalo de Troia do cliente.



8. A navegação pelo sistema de arquivos do cliente é um processo totalmente interativo e apresenta uma interface de usuário familiar semelhante à do Windows Explorer. É possível excluir, renomear, copiar, baixar e enviar à máquina remota cada arquivo e pasta.



9. Um *shell* de linha de comando remoto pode ser iniciado para executar comandos diretamente na máquina remota. Quando o atacante utiliza essa função, uma cópia do CMD.EXE é reproduzida no sistema infectado em um diretório Windows %Temp% com o nome svchost.exe. Essa cópia é uma versão original do executável do *shell* de comando do Microsoft Windows.



10. O Registro também pode ser visualizado e editado em uma interface semelhante à do editor de Registro do Windows.

Apêndice B: Atribuição

IMPORTANTE: A McAfee não tem nenhuma evidência direta para nomear os autores desses ataques, mas apresentou provas circunstanciais.

Embora acreditemos que muitos participaram desses ataques, conseguimos identificar uma pessoa que forneceu a infraestrutura essencial de C&C aos atacantes – essa pessoa se encontra na cidade de Heze, província de Shandong, na China. Embora nós não acreditemos que essa pessoa seja o mentor desses ataques, é provável que ela tenha conhecimento ou que tenha informações que possam ajudar a identificar pelo menos alguns dos indivíduos, grupos ou organizações responsáveis por essas invasões.

Figura 6. Província de Shandong, China

A pessoa dirige uma empresa que, segundo os anúncios da própria empresa, fornece “Servidores Hospedados nos EUA sem manter registros” a partir de 68 RMB (US$10) por ano para um espaço de 100 MB. Os servidores alugados pela empresa, localizados nos EUA, foram usados para hospedar o aplicativo de C&C zwShell que controlou as máquinas de todas as empresas vítimas.

Além da conexão com a operação de revenda dos serviços de hospedagem, existem outras evidências que indicam que os atacantes eram de origem chinesa. Além do uso curioso da senha “zw.china” que destrava o funcionamento do cavalo de Troia de C&C zwShell, a McAfee descobriu que todas as atividades identificadas de extração de dados ocorreram a partir de endereços IP localizados em Pequim e operados dentro das empresas atacadas em dias úteis, das 9h00 às 17h00 (hora de Pequim), o que também indica que as pessoas envolvidas eram “funcionários da empresa” com empregos formais, e não hackers autônomos ou não-profissionais. Além disso, os atacantes empregaram ferramentas de *hacking* de origem chinesa e predominantes em fóruns chineses de *hacking* secretos. Entre essas ferramentas estavam a Hookmsgina e a WinlogonHack, que interceptam solicitações de *logon* do Windows e sequestram nomes de usuário e senhas.

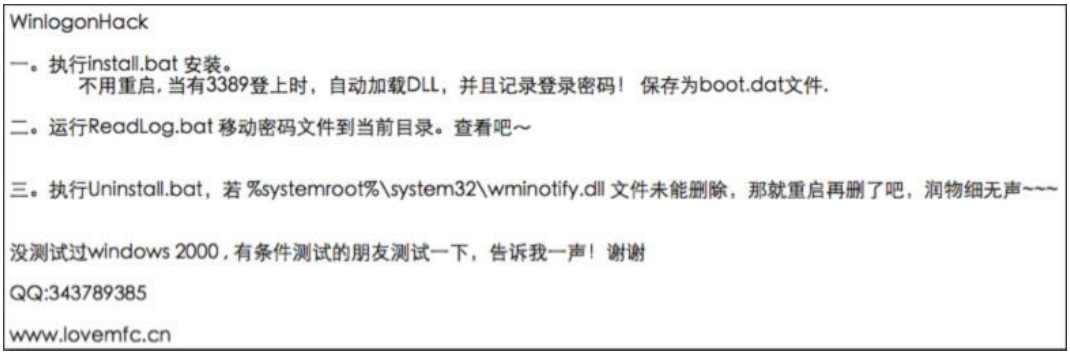


Figura 7. Instruções de uso da ferramenta WinlogonHack por seus desenvolvedores chineses.

No servidor Web comprometido, eles também instalaram a ASPXSpy, uma ferramenta de administração remota pela Web, também de origem chinesa.

Figura 8. Partes do código da ASPXSpy, atribuído ao desenvolvedor chinês.

Nada indica que os desenvolvedores dessas ferramentas tinham qualquer ligação direta com essas invasões, pois as ferramentas estão amplamente disponíveis em fóruns de Internet chineses e tendem a ser amplamente utilizadas por grupos de hackers chineses. Embora seja possível que todos estes indícios sejam uma elaborada operação de pistas falsas para atribuir a culpa pelos ataques a hackers chineses, acreditamos que isso seja altamente improvável. Além disso, não está claro quem teria a motivação de se esforçar tanto para colocar em outra pessoa a culpa pelos ataques. Temos evidências sólidas que indicam que os atacantes se localizavam na China.

McAfee, Inc.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com