White Paper

Ciberataques contra la energía mundial: “Night Dragon (Dragón Nocturno)”

McAfee® Foundstone® Professional Services y McAfee Labs™

10 de febrero de 2011

Índice

Resumen ejecutivo

En 2010, entramos en una nueva década en el mundo de la seguridad informática. La década anterior fue marcada por la inmadurez, por soluciones técnicas reactivas y por la falta de sofisticación de seguridad, lo que llevó a epidemias graves como la Code Red, Nimda, Blaster, Sasser, SQL Slammer, Conficker y myDoom, para mencionar apenas algunas. La comunidad de seguridad evolucionó y se tornó más inteligente acerca de la seguridad, de la informática segura y del refuerzo de sistemas, pero lo mismo ocurrió con nuestros adversarios. Esta década está pronta para ser el "trampolín" exponencial. Los adversarios están rápidamente aprovechando *kits* de herramientas de *malware* "productizados" que permiten el desarrollo de más *malwares* que en todos los años anteriores juntos, y ellos maduraron con relación a la última década, lanzando las amenazas virtuales más insidiosas y persistentes ya vistas.

Los ataques al Google ("Operación Aurora"), bautizada por McAfee y anunciada en enero de 2010, y la divulgación de documentos por WikiLeaks en 2010, destacaron el hecho de ser prácticamente imposible de evitar las amenazas externas e internas. Los bandidos continúan infiltrándose en las redes y extrayendo datos confidenciales y reservados de los cuales dependen todos los días las economías del mundo. Cuando surge un nuevo ataque, los proveedores de seguridad no pueden quedarse parados esperando y asistiendo. Somos obligados a compartir nuestros hallazgos para proteger a quien aún no fue afectado y para recuperar a quien ya lo fue. De esa forma, McAfee Foundstone Professional Services y el McAfee Labs decidieron divulgar el siguiente hallazgo.

En noviembre de 2009, ataques informáticos coordinados secretos y dirigidos comenzaron a ser dirigidos contra empresas globales de los sectores de petróleo, energía y petroquímica. Esos ataques consistían en ingeniería social, ataques de *spear-phishing*, exploración de vulnerabilidades del sistema operativo Microsoft Windows, comprometimientos del Microsoft Active Directory, y en el uso de herramientas de administración a distancia (las RAT) para atacar y recolectar operaciones reservadas confidenciales de competidores e informaciones sobre financiación de proyectos de licitaciones y operaciones en las áreas de petróleo y gas. Identificamos principalmente en la China el origen de las herramientas, técnicas y actividades de red usadas en esos ataques continuos — que bautizamos de Dragón Nocturno. Mediante el análisis coordinado de los eventos vinculados y de las herramientas usadas, McAfee definió características distintivas para auxiliar a las empresas en la detección e investigación. Aunque creemos que muchos participaron de esos ataques, conseguimos identificar a una persona que suministró la infraestructura esencial de C&C a los atacantes. *(Vea en el Apéndice B más detalles acerca de la atribución.)*

Anatomia de una invasión

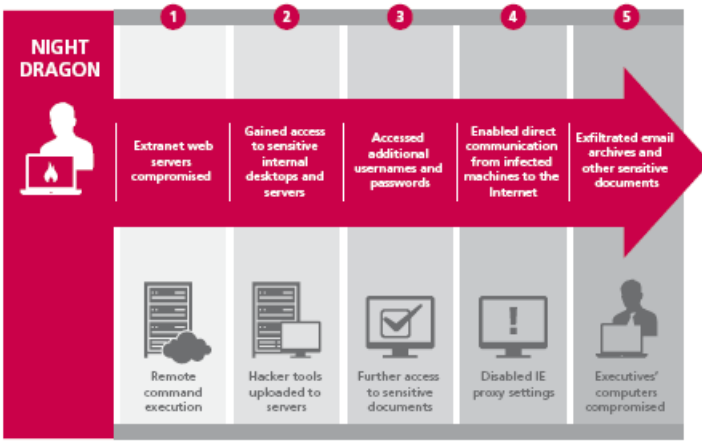


Figura 1. Anatomia de una invasión.

Los ataques del Dragón Nocturno funcionan por medio de invasiones metódicas y progresivas de la infraestructura objetivo. Las actividades básicas siguientes fueron realizadas por la operación Dragón Nocturno:

- Los servidores de Web de las extranets de las empresas fueron comprometidos mediante técnicas de inyección de SQL, lo que permite la ejecución a distancia de comandos
- Las herramientas de *hackers* normalmente disponibles son enviadas a servidores de Web comprometidos, lo que permite que los atacantes invadan la intranet de la empresa y dándoles acceso interno a *desktops* y servidores confidenciales
- Usando herramientas de apertura de contraseña y de *pass-the-hash*, los atacantes consiguen más nombres de usuario y contraseñas, lo que les permite obtener más acceso autenticado a *desktops* y servidores internos confidenciales
- Inicialmente usando los servidores Web comprometidos de la empresa como servidores de comando y control (C&C), los atacantes descubrieron que sólo precisaban desactivar las configuraciones de *proxy* del Microsoft Internet Explorer (IE) para permitir que las computadoras infectadas se comunicasen directamente con Internet
- Utilizando *malware* de RAT, pasaron a conectarse con otras máquinas (buscando ejecutivos) y extrayendo archivos de correo electrónico y otros documentos confidenciales

Detalles del ataque

Invasores en varios lugares de China aprovecharon servidores de C&C en servicios de hospedaje comprados en Estados Unidos y servidores comprometidos en Holanda para realizar ataques contra empresas mundiales de petróleo, gas y petroquímica, así como individuos y ejecutivos en Kazajistán, en Taiwán, en Grecia y en Estados Unidos, para adquirir informaciones reservadas y altamente confidenciales. La principal técnica operativa utilizada por los atacantes consistió en varias herramientas de *hackers*, incluso herramientas desarrolladas en el ámbito privado y herramientas personalizadas de RAT que proporcionaron al atacante recursos completos de administración a distancia. Las RAT ofrecen funciones semejantes al Citrix o al Microsoft Windows Terminal Services, que permiten que un individuo distante controle totalmente el sistema afectado.

Para instalar esas herramientas, los atacantes primero comprometieron los controles de seguridad perimetrales, mediante exploraciones de inyección de SQL en servidores de Web de extranets, además de ataques dirigidos de *spear-phishing* a *laptops* de empleados itinerantes, y comprometiendo cuentas corporativas de VPN para penetrar en las arquitecturas de defensa de la empresa atacada (DMZs y *firewalls*) y realizar el reconocimiento de las computadoras en red de esas empresas.

Ataques de inyección de SQL

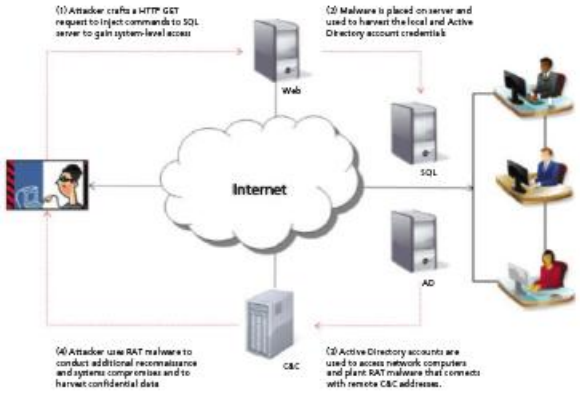


Figura 2. Ataques de inyección de SQL.

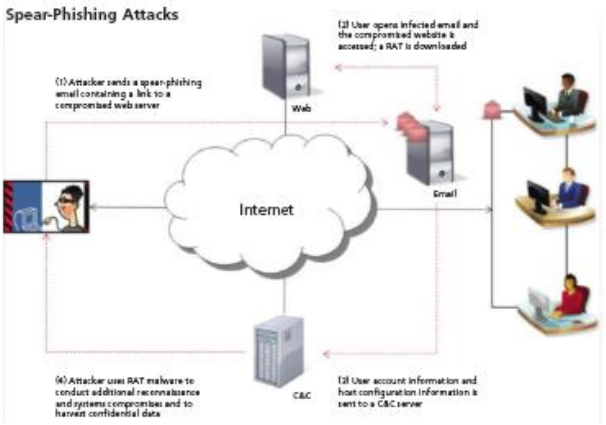


Figura 3. Ataques de spear-phishing.

Muchos sitios de *hackers* chinos ofrecen esas herramientas para descarga, incluso enlaces para reduh, WebShell, ASPXSpy y muchos otros, además de exploraciones y *malware* del ‘día cero’.

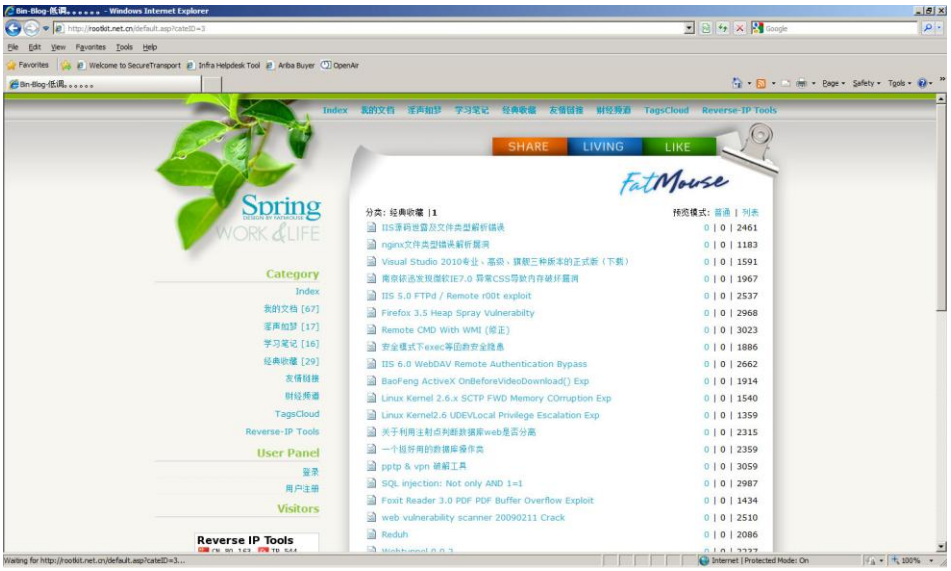


Figura 4. Rootkin.net.cn ofrece acceso a una lista interminable de herramientas y exploraciones de *hackers*.

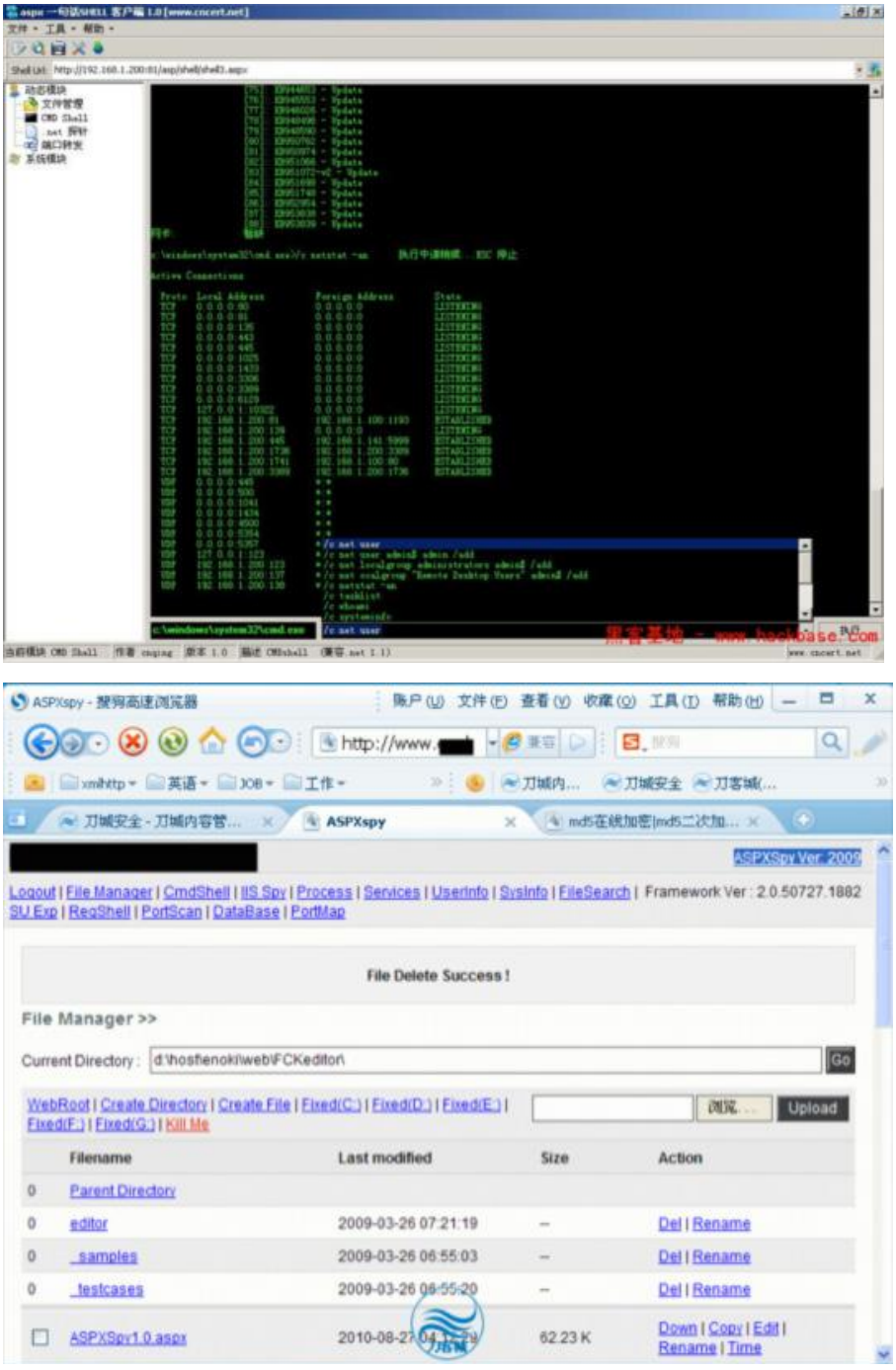


Figura 5. Las herramientas WebShell y ASPXSpy permiten que un atacante ignore muchas reglas de *firewall* para canalizar todo el control a través del servidor de Web de una empresa.

Cuando el sistema inicial fue comprometido, los atacantes comprometieron las cuentas locales de administrador y las cuentas del administrador del Active Directory (y de los usuarios y administrativos). Los atacantes usaron frecuentemente utilitarios comunes del Windows, tales como herramientas SysInternals (adquirida por Microsoft en 2006) – y otros softwares disponibles al público, entre ellos herramientas de invasión desarrolladas en China y ampliamente disponibles en sitios "subterráneos" chinos de *hackers* – para establecer "*backdoors*" por medio de *proxies* inversos, y plantaron caballos de Troya que permitieron a los atacantes ignorar las políticas y configuraciones de seguridad de red y *host*. Las herramientas antivirus y *anti-spyware* para *desktops* también fueron desactivadas en algunos casos – una técnica común de ataques dirigidos.

Uso de herramientas de administración a distancia

Herramientas de administración a distancia (las RAT) son normalmente utilizadas como herramientas administrativas que permiten a los *hackers* (y administradores) administrar las computadoras de las víctimas (o sistemas administrados) y controlar completamente su utilización y su funcionamiento. Una RAT normalmente usada en la comunidad *hacker* es el Gh0st y sus diversas variantes. Los recursos de la RAT generalmente son el espionaje de pantalla y *webcam*, grabación de la digitación, control del ratón, archivo/registro y administración de procesos, y, naturalmente, el recurso de *shell* de comando remoto.

McAfee identificó varias RAT que fueron usadas para establecer un canal de infiltración persistente para las empresas comprometidas. Una RAT más predominante es la zwShell, que McAfee ha visto en estado salvaje desde marzo/abril de 2010 (compilado el 17-03-2010 08:47:00). Escrita en el lenguaje Delphi, la zwShell fue usada por atacantes para crear variantes personalizadas del caballo de Troya que instalaron en decenas de máquinas dentro de cada empresa víctima, así como para controlar las máquinas comprometidas que iniciarían conexiones de "guía" con él en un protocolo personalizado.

Los atacantes usaron ampliamente la zwShell para generar decenas de variantes exclusivas del caballo de Troya y controlar las máquinas infectadas y extraer datos confidenciales directamente a través de ellas. (Consulte en el Apéndice A los pormenores de la zwShell).

Así que los atacantes asumieron el control completo del sistema interno atacado, ellos introdujeron *hashes* de cuenta con el gsecdump y utilizaron la herramienta Caín & Abel para abrir los *hashes* a fin de usarlos en el ataque a infraestructuras cada vez más delicadas.

Los archivos de interés se concentraban en sistemas operativos de producción de campos de petróleo y gas y en documentos financieros relacionados con la exploración y licitación de campos, que fueron después copiados de los *hosts* comprometidos o por medio de servidores de extranet. En algunos casos, los archivos fueron copiados para los servidores de Web de la empresa por los atacantes y descargados a partir de ellos. En algunos casos, los atacantes recolectaron datos de los sistemas SCADA.

Detección

Los métodos y las herramientas utilizados en esos ataques son relativamente simples, pues simplemente parecen ser técnicas comunes de administración de *host*, utilizando credenciales administrativas comunes. Esto se debe principalmente al hecho de que ellos son capaces de evitar la detección por medio de softwares de seguridad y políticas de red comunes. Sin embargo, desde los primeros comprometimientos, los proveedores de seguridad (incluso McAfee) identificaron muchas firmas individuales originales del caballo de Troya y de las respectivas herramientas; pero fue apenas por medio de análisis recientes y del hallazgo de artefactos comunes y de la correlación de evidencias que conseguimos determinar que una iniciativa dedicada estaba en marcha hacía por lo menos dos años, y probablemente hasta cuatro años. Ahora, podemos asociar las diversas firmas a esos eventos.

Los siguientes artefactos pueden ayudar a determinar si una empresa fue comprometida:

- Archivos de *host* y/o claves de Registro
- Alertas de antivírus
- Comunicaciones de red

Archivos de *host* y claves de registro

Utilitario	Descripción
Aplicación de comando y control	Shell.exe 093640a69c8eafbc60343bf9cd1d3ad3 zwShell.exe 18801e3e7083bc2928a275e212a5590e zwShell.exe 85df6b3e2c1a4c6ce20fc8080e0b53e9
Instalador (*dropper*) de caballo de Troya	Un ejecutable embalado personalizado para cada víctima, que incluye el archivo DLL y parámetros de configuración para instalar el *backdoor* en el sistema remoto. El *dropper* puede ser ejecutado desde cualquier directorio y normalmente es ejecutado con el PSEXEC o una sesión de RDP. Así, los respectivos logs de Eventos de Seguridad del Windows proveen informaciones útiles referentes a las cuentas comprometidas del Active Directory. Esos logs pueden ser analizados con el Windows Event Log Manager o programas, tales como el "Event Log Explorer" o p EnCase, que tienen recursos de búsqueda. Cuando es ejecutado, el *dropper* crea un archivo temporal que se refleja en los logs de actualización del Windows (archivos KB*.log en la carpeta C:\Windows). Eso sucede porque el Registro del Windows es modificado por el *dropper*, que crea una clave "netsvcs". Así, es posible saber la fecha de instalación del *backdoor* con una búsqueda en los archivos de log KB. Ese archivo temporal también es identificado en la propia DLL del *backdoor*. El archivo temporal es, generalmente, una combinación alfanumérica que incluye "gzg" (por ejemplo, xgt0gzg), aunque también ha sido visto con nombres genéricos (por ejemplo, server.exe). El *dropper* es excluido cuando el *backdoor* es instalado, y el archivo temporal es retirado cuando la computadora es reiniciada. Si un *backdoor* ya fue configurado en el sistema, la instalación del *dropper* fallará a menos que él use una configuración diferente.
***Backdoor* caballo de Troya**	Bibliotecas de vínculo dinámico (las DLL), que también aparecen con otros diversos nombres. Esos archivos tienen una clave de Registro del Windows correlacionada que es determinada por el *dropper* cuando el *backdoor* es instalado. El *dropper* se repite por medio de las claves netsvcs del Registro del Windows y usa la primera clave disponible, indicando el camino y el nombre del *backdoor* en un registro ServiceDLL. El *backdoor* funciona como un servicio mediante una configuración de registro “svchost.exe netsvcs –k”. La clave del servicio puede ser encontrada en: HKLM\system\<controlset>\services\ La DLL es un archivo oculto o de sistema, con tamaño de 19 KB a 23 KB, e incluye una sección de datos con codificación XOR que es definida por la aplicación de C&C cuando el *dropper* es creado. Él incluye el identificador de servicio de red, la clave de servicio del registro, la descripción del servicio, el nombre del mutex, la dirección del servidor de C&C, la puerta y el nombre del archivo temporal del *dropper*. El *backdoor* puede funcionar a partir de cualquier puerta TCP configurada. Esa DLL es especificada en la clave ServiceDLL en el respectivo ítem de registro netsvcs del Windows. La DLL es generalmente encontrada en la carpeta %System%\System32 ó %System%\SysWow64.
Backdoor* caballo de Troya 2	startup.dll A6CBA73405C77FEDEAF4722AD7D35D60 Inicialmente configurado con lo siguiente: connect.dll 6E31CCA77255F9CDE228A2DB9E2A3855 La connect.dll crea el archivo temporal "HostID.DAT", que es enviado al servidor de C&C. En seguida, ella descarga y configura las respectivas DLL: PluginFile.dll PluginScreen.dll PluginCmd.dll PluginKeyboard.dll PluginProcess.dll PluginService.dll PluginRegedit.dll A partir de allí, la "Startup.dll" opera el servicio en una clave del Registro del Windows. Todas las comunicaciones vistas hasta ahora con esta versión estuvieron en las puertas 25 y 80 a través de TCP, pero pueden operar en cualquier puerta determinada. La clave de servicio es identificada en la DLL (que no incluye datos cifrados) como: HKLM\Software\RAT Esa DLL es generalmente encontrada en el directorio %System%\System32, pero también ya fue encontrada en otros lugares. El camino para la DLL de *backdoor* es indicado en la clave ServiceDLL del Registro del Windows.

* Esta DLL usa una aplicación de C&C diferente que puede ser una versión anterior del zwShell. Los análisis prosiguen.

Los componentes del caballo de Troya son copiados o entregados manualmente a los sistemas remotos mediante utilitarios administrativos. Ellos no tienen ningún recurso de gusano o de autoduplicación, ni el caballo de Troya es capaz de "infectar" a otras computadoras. Retirar los componentes del caballo de Troya es simplemente una cuestión de borrar los archivos y las respectivas configuraciones de registro.

El *backdoor* caballo de Troya se comunica con el servidor de C&C en la dirección codificada de manera fija en cada DLL. El servidor de C&C no puede modificar el *backdoor* después que haya sido instalado; el archivo de caballo de Troya debe ser retirado de los respectivos sistemas para que una nueva DLL de *backdoor* pueda ser instalada en el sistema. Así, si la dirección del servidor de C&C fuese alterada, los servidores que tengan la DLL con direcciones antiguas deben ser administradas a distancia por el atacante.

Alertas de antivirus

Los patrones de antivirus son definidos de acuerdo con las muestras enviadas por los clientes o analistas a medida que son descubiertos. Algunos caballos de Troya exhiben características de otros tipos de *malware*, como gusanos o virus, que tienen la capacidad de infectar a otros sistemas. Las RAT no suelen contener esos recursos y, como son definidas con configuraciones exclusivas para fines específicos, generalmente cambian más rápido de lo que las muestras originales pueden ser identificadas.

Solamente cuando un *kit* de herramientas de RAT completo es encontrado podemos definir un patrón de antivirus suficientemente genérico para detectar la RAT, independientemente de los cambios de configuración. El paquete contiene necesariamente un servidor de aplicaciones de C&C, el utilitario generador para la creación de *droppers*, los respectivos *droppers* y *backdoor*s – y un número suficiente de cada uno para correlacionar el *kit* de herramientas.

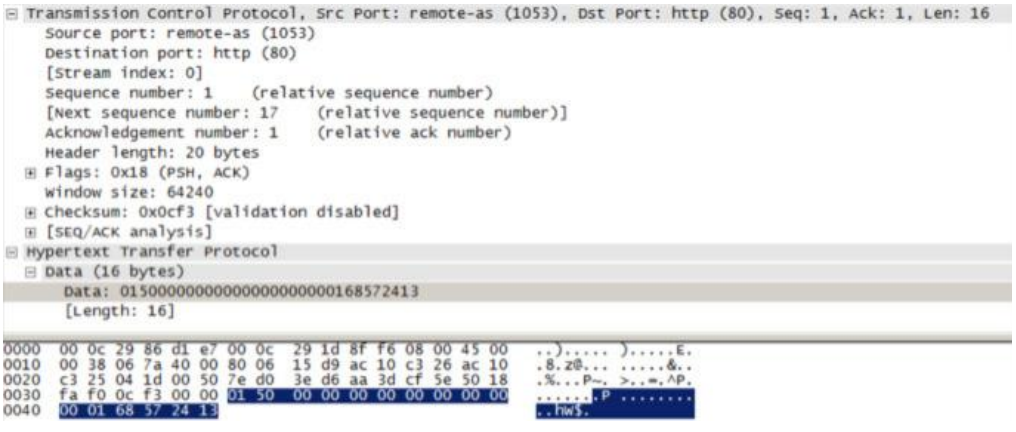
Como mencionamos anteriormente, varios patrones exclusivos fueron desarrollados a partir de muestras enviadas a McAfee y a otros proveedores de antivirus.

> McAfee recomienda que las empresas examinen en el software McAfee ePolicy Orchestrator® (McAfee ePO™) y en los registros del antivirus las detecciones de la firma del "Dragón Nocturno" para identificar alertas relacionados desde 2007 y, en seguida, recuperen y reenvíen esas muestras para investigar los incidentes relacionados. McAfee puede auxiliar en el análisis o proveer instrucciones y herramientas para análisis interno.

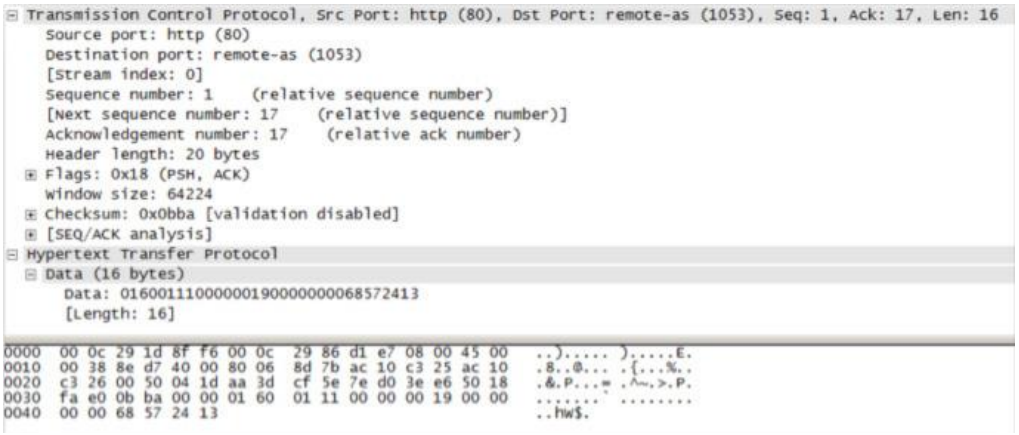
Comunicaciones de red

Las comunicaciones de red son relativamente fáciles de detectar porque el *malware* usa una guía de *host* exclusivo y un protocolo exclusivo de respuesta al servidor. Cada paquete de comunicación entre el *host* comprometido y el servidor de C&C es firmado con una firma de texto sin formatación "HW$". (o "\x68\x57\x24\x13") en el *offset* de byte 0x42 dentro del paquete TCP.

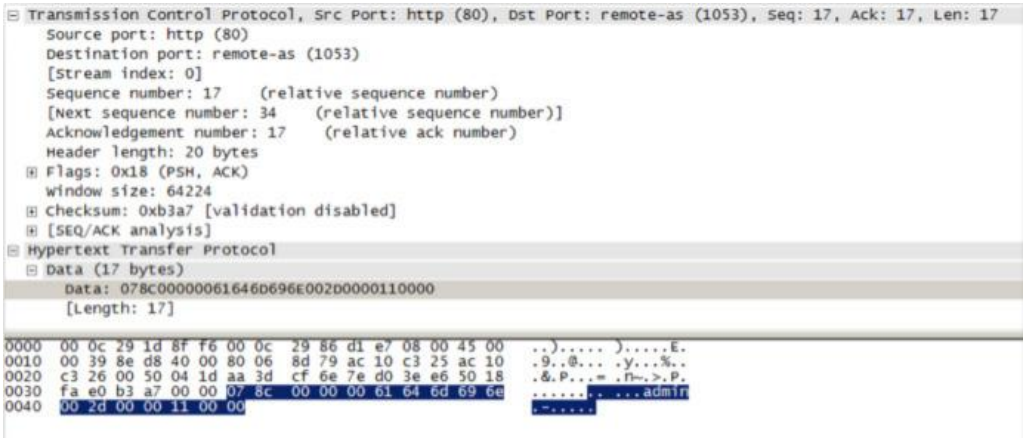
El *backdoor* acciona su guía a intervalos de aproximadamente cinco segundos con un paquete inicial que puede ser detectado con el patrón: "\x01\x50[\x00-\xff]+\x68\x57\x24\x13."



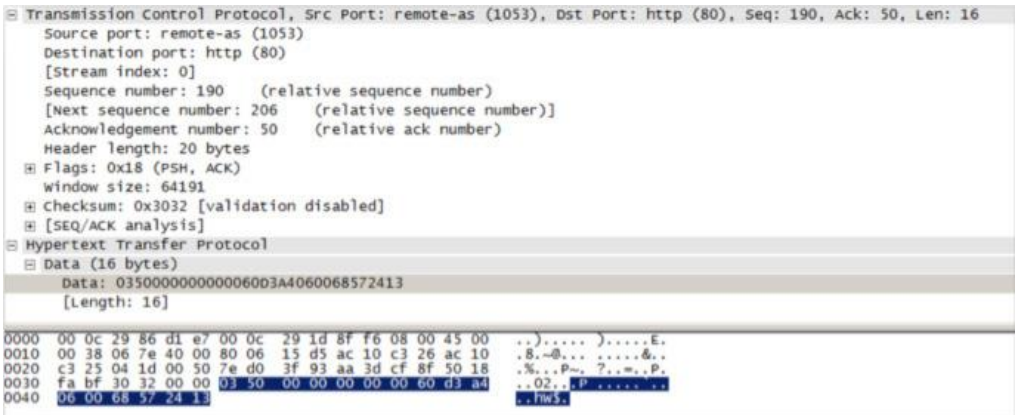
El servidor reconoce la guía con una respuesta inicial de “\x01\x60[\x00-\xff]+\x68\x57\x24\x13.”



El *backdoor* envía la contraseña al servidor en texto simple después que el servidor reconoce la conexión.



Mientras que el *backdoor* y el servidor mantengan una conexión activa, el *backdoor* envía mensajes de “keep-alive” que pueden ser detectados por: “\x03\x50[\x00-\xff]+\x68\x57\x24\x13.”



Los atacantes usan cuentas de servicios de nombre de Internet con “DNS dinámico” para retransmitir las comunicaciones de C&C o vincular temporalmente direcciones DNS a servidores remotos. Los dominios más utilizados para el tráfico de C&C han sido (todos han sido utilizados con frecuencia por otros tipos de *malware*):

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

Servidores de extranet de empresas también han sido utilizados como servidores exclusivos o secundarios/redundantes de C&C. En algunos casos, los atacantes usan (probablemente por equívoco) *droppers* configurados para comprometer las computadoras de una empresa – en computadoras de otra empresa.

McAfee recomienda que las empresas configuren reglas en el sistema de detección de intrusiones (IDS) para detectar las firmas indicadas (o que utilicen la firma definida por el usuario [UDS] “BACKDOOR: NightDragon Communication Detected” en la McAfee Network Security Platform) y monitoreen en el DNS las comunicaciones de salida con direcciones dinámicas de DNS convertidas o devueltas como subasignadas para servidores en China, en las cuales el nombre da empresa o formas comunes de abreviatura forman la primera parte de la dirección. Eso puede ser difícil. No obstante, si fuesen encontradas muestras de las DLL de *backdoor*, el monitoreo del DNS puede ayudar a identificar otros *hosts* comprometidos en la red de la empresa. McAfee también recomienda que las empresas *web* procuren hallar en sus logs de Web o de IDS transferencias de archivos para direcciones registradas en China. McAfee puede auxiliar en el análisis o proveer instrucciones y herramientas para análisis interno.

Otras técnicas de detección

El *backdoor* intercambia señales con su respectivo servidor de C&C siempre que la respectiva dirección esté activa. Si la dirección fuese abandonada o quedase inaccesible, el *backdoor* para de emitir señales tras un intervalo indeterminado. Sin embargo, cuando una computadora infectada es reiniciada, la señalización recomienza porque él está registrado como un servicio en el Registro del Windows. Los antivirus pueden o no detectar al caballo de Troya, a menos que él esté emitiendo señales o que sea realizado un barrido completo del sistema de archivos.

Detección anticipada de McAfee

Los clientes pueden instalar una serie de productos de McAfee para ayudarles a proteger sus sistemas de información contra el ataque Dragón Nocturno:

- *McAfee Vulnerability Manager:* Usando el hallazgo sin agente y verificaciones de vulnerabilidades para evaluar los sistemas en su red, el McAfee Vulnerability Manager es un sistema de gran porte para administración de vulnerabilidades que detecta sistemas infectados con el Dragón Nocturno y las fallas de seguridad en los sistemas que fueron comprometidos. El guión “wham-apt-nightdragon-detected-v7.fasl3” detecta esa amenaza remotamente en los sistemas.
- *McAfee Policy Auditor:* Utilizando verificaciones de auditoría de configuración para determinar la configuración más segura de un sistema, el software McAfee Policy Auditor detecta las fallas de seguridad en los sistemas que hayan sido comprometidos.
- *McAfee Risk Advisory (MRA):* Debidamente instalado, el McAfee Risk Advisor habría permitido que los administradores viesen los errores de configuración y las fallas en la cobertura de seguridad que facilitaron la exploración Dragón Nocturno.

Detección de McAfee

El Dragón Nocturno también presenta un patrón de actividades correlacionadas con una variedad de otras herramientas de software que McAfee puede ayudar a las empresas a identificar.

- *McAfee VirusScan Enterprise:* Actualice los DAT de su antivirus al menos en la versión 6232 y verifique si los barridos por encomienda están funcionando correctamente, y ejecute un barrido completo de virus en el sistema de archivos. Busque en los alertas del software McAfee ePO o de antivirus y en los logs de red las detecciones de firma "NightDragon" para identificar los sistemas infectados. Envíe todas las muestras relacionadas para virus_research@mcafee.com o por la Web, en la dirección https://www.webimmune.net/default.asp.
- *McAfee Network Threat Response:* La tecnología McAfee Network Threat Response tendría detectado el tráfico malintencionado de C&C y alertado con antecedencia a los administradores acerca del ataque, dándoles tiempo para reaccionar y evitar más daños

Los administradores también pueden descargar las siguientes herramientas gratuitas de McAfee:

- McAfee "Night Dragon Vulnerability Scanner", que utiliza la tecnología McAfee Vulnerability Manager para realizar en sus redes un barrido de la presencia de *malware*
- McAfee Labs Stinger

Prevención de McAfee

Para evitar de manera completa ese y la mayoría de los otros ataques que involucran amenazas avanzadas persistentes (las APT), los clientes pueden crear listas blancas de aplicaciones y sww de control de alteraciones/configuraciones en sus servidores más importantes. Esas tecnologías impiden completamente la ejecución no autorizada de DLL/EXE, además de la alteración de las claves de registro, de servicios y de otros elementos presentes en todos los ataques de APT y de 'día cero' de hoy.

- *McAfee Application Control:* El software McAfee Application Control bloquea al Dragón Nocturno, impidiendo la ejecución de los archivos *dropper* (hasta como administrador en el Windows), evitando, así, que sea descargado más *malware* y que sean instalados canales de C&C para permitir el control por las RAT y robar archivos confidenciales
- *McAfee Configuration Control:* El software McAfee Configuration Control permite que usted prohiba cualquier alteración en la configuración de sus sistemas, protegiéndolos contra modificaciones sin permisión explícita (aun con acceso administrativo)
- *McAfee Network Security Manager:* Con el conjunto correcto de firmas de UDS instalado, los *appliances* McAfee Network Security Platform protegen contra ataques basados en la red, como el Dragón Nocturno, detectando tráficos malintencionados en la red y alertando a los administradores para que ellos tengan tiempo de reaccionar y prevenir futuros ataques
- *McAfee Enterprise Firewall:* Correctamente instalado y configurado en el perímetro y dentro de su organización, el McAfee Firewall habría impedido que la operación Dragón Nocturno penetrase tan profundamente en las organizaciones afectadas y habría bloqueado la comunicación de C&C de la RAT
- *McAfee Web Gateway:* Instalado y configurado correctamente, el McAfee Web Gateway habría impedido que la operación Dragón Nocturno utilizase sus RAT, obligándola a hacer que sus RAT reconocieran *proxies* o usar otras RAT compatibles con *proxies*
- *McAfee Endpoint Encryption:* Instalado y configurado correctamente, el software McAfee Endpoint Encryption reduce el impacto del ataque Dragón Nocturno, restringiendo el acceso a los recursos principales atacados
- *McAfee Data Loss Protection:* Instalado y configurado correctamente, el McAfee Network DLP y/o las soluciones McAfee Host DLP permiten que usted impida y detecte la extracción de informaciones sensibles desde fuera de la empresa

- *McAfee Host Intrusion Prevention 8.0:* El software McAfee Host Intrusion Prevention 8.0 introdujo un nuevo recurso de detección de APT, el "TrustedSource", que permite a las empresas a correlacionar actividades de ejecutables en terminales con comunicaciones de C&C en la red, a fin de detectar e impedir la comunicación de las RAT y actividades de extracción de datos
- *McAfee VirusScan® Enterprise:* Además de detectar los *malwares* y las RAT asociadas en los terminales, los clientes también pueden aprovechar los recursos de protección de acceso del McAfee VirusScan Enterprise para evitar (y alertar) la creación de archivos y estructuras de carpetas vinculados con el Dragón Nocturno. Otros recursos internos, tales como rastreo de infecciones y el McAfee Global Threat Intelligence™ pueden ayudar en la identificación y en la puesta en cuarentena o supresión de *malwares* y RAT asociados nuevos y aún desconocidos.

Si usted descubrió la presencia del Dragón Nocturno en su ambiente y quisiera contar con asistencia pericial o de reacción a incidentes para reaccionar al problema y solucionarlo, entre en contacto con Foundstone Professional Services por el *email* incidentresponse@foundstone.com o envíe todas las muestras respectivas a la dirección Virus_Research@avertlabs.com o, por la Web, McAfee Labs WebImmune.

Conclusión

El número de ataques dirigidos y bien coordinados, tales como el Dragón Nocturno, engendrados por un grupo creciente de atacantes malintencionados comprometidos con sus metas, está aumentando rápidamente. Esos objetivos ya no son apenas las computadoras de la base industrial de defensa, del gobierno y de las Fuerzas Armadas. Ahora, ellos también están en grandes empresas privadas globales. Aunque los ataques del Dragón Nocturno se hayan concentrado específicamente en el sector de energía, las herramientas y técnicas de ese tipo pueden ser altamente exitosas cuando fuesen dirigidas contra cualquier sector de actividad. Nuestra experiencia muestra que otros muchos sectores están vulnerables y bajo ataques de ciberespionaje continuos y persistentes de ese tipo. Cada vez más, esos ataques no se concentran en usar y abusar de máquinas en las organizaciones comprometidas, y sí en el robo de datos específicos y de propiedad intelectual. Es esencial que las organizaciones tomen la iniciativa de proteger el corazón de su valor: la propiedad intelectual. Las empresas precisan tomar medidas para descubrir esos recursos en sus ambientes, evaluar si hay vulnerabilidades en sus configuraciones, y protegerlos contra el uso indebido y los ataques.

Para conocer más estudios y obtener más información, lea *Hacking Exposed: Network Secret and Solutions — 6ª Edición* (Osborne McGraw-Hill). También puede visitar http://www.hackingexposed.com para obtener informaciones sobre técnicas avanzadas de *hackers* e inscribirse en los seminarios virtuales "Hacking Exposed" realizados mensualmente.

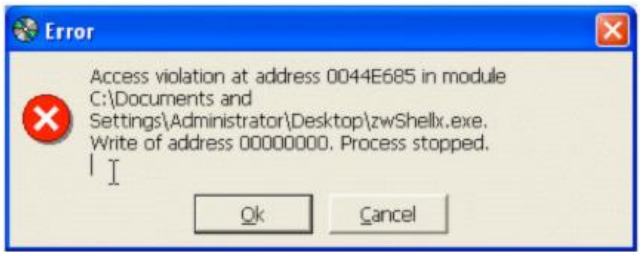
Créditos y agradecimientos

Este *white paper* ha sido un trabajo de colaboración entre varias personas y organizaciones, entre ellas los consultores de McAfee Foundstone Professional Services, McAfee Labs, empleados de McAfee, ejecutivos e investigadores, HBGary y la Alianza Nacional de Pericia Informática y Entrenamiento (NCFTA). Entre los principales colaboradores están Shane Shook, Dmitri Alperovitch, Stuart McClure, Georg Wicherski, Greg Hoglund, Shawn Bracken, Ryan Permeh, Vitaly Zaytsev, Mark Gilbert, Mike Spohn y George Kurtz.

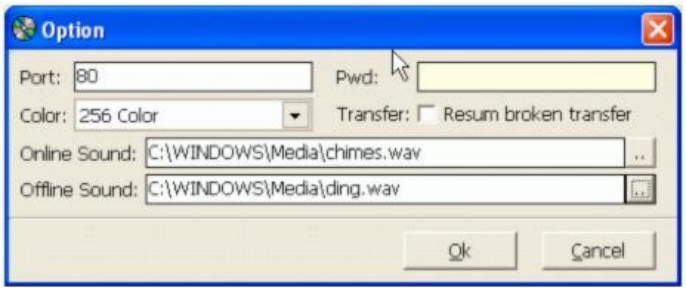
Apéndice A: zwShell — la RAT

Vea a continuación una explicación de los recursos del zwShell y una demostración de cómo los atacantes usaron el zwShell como un servidor de comando y control para extraer datos de dentro de las empresas atacadas.

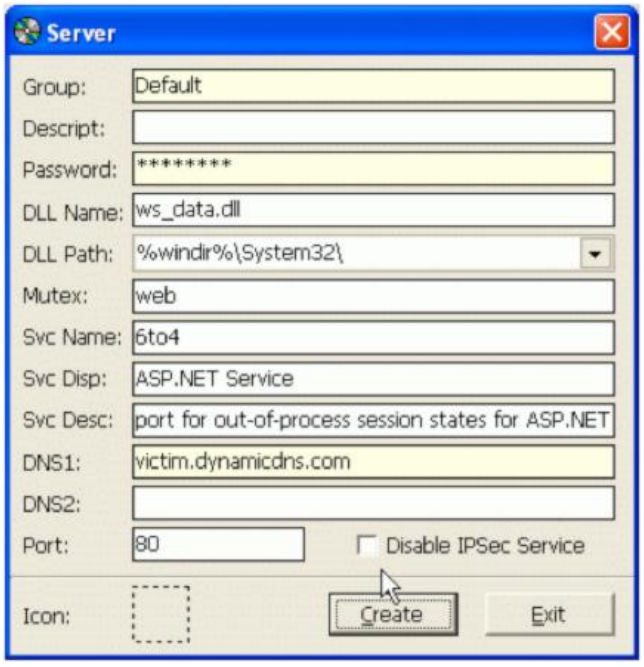
1. Cuando el zwShell es iniciado, presenta al usuario un falso error de trabamiento y contiene un campo oculto de inserción de texto abajo de la línea “Write of address 00000000. Process stopped”. La caja de diálogo oculta arriba del botón "Ok" exige la digitación de la contraseña especial, "zw.china" para iniciar la aplicación. Sin la contraseña, la herramienta no será iniciada. Este método de ofuscación es probablemente usado para confundir a los investigadores sobre el verdadero propósito de este ejecutable.



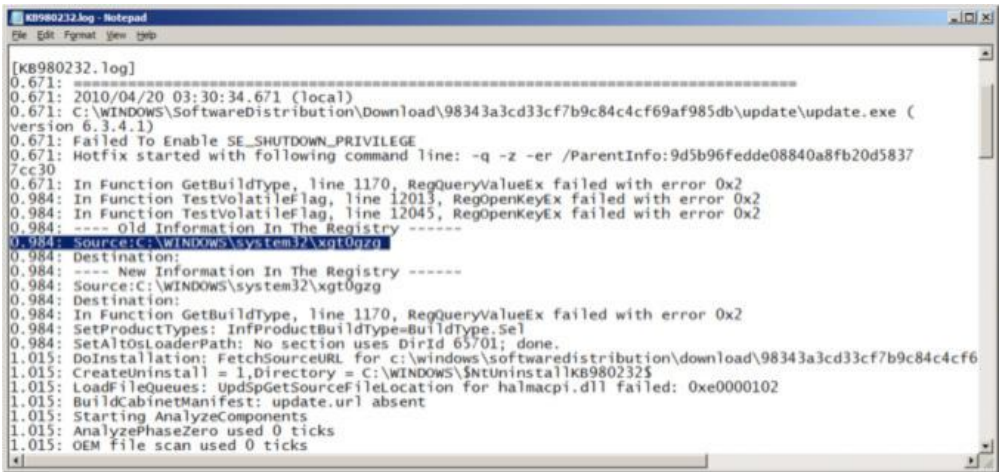
2. Cuando el error haya sido ignorado y el zwShell sea iniciado, éste permite que el invasor cree un caballo de Troya personalizado, seleccionando el menú Server, o iniciar el servidor de C&C, haciendo clic en Iniciar y entrando en la puerta para “escuchar” el tráfico con la contraseña usada por las DLL de *backdoor*. Una vez iniciada, la aplicación comenzará a escuchar las conexiones recibidas por el cliente infectado y a exhibirlas dentro de la matriz. El atacante puede iniciar cuantas instancias de la aplicación zwShell quiera, siempre y cuando que cada una escuche una puerta o contraseña diferente. De esa manera, varias “redes” de computadoras infectadas pueden ser monitoreadas.
3. El atacante también puede hacer clic en el menú Opciones para configurar los parámetros del servidor de C&C. Esas configuraciones incluyen la selección de la puerta de escucha, la contraseña que cifrará el tráfico de C&C (que debe coincidir con la contraseña escogida en el momento de la generación del caballo de Troya), la capacidad de especificar notificaciones sonoras personalizadas cuando las máquinas infectadas se conecten y desconecten del servidor de C&C, y la capacidad de aumentar la profundidad de colores usada en el acceso remoto a la máquina, así como un recurso opcional para permitir la continuación, a partir de la máquina cliente, de transferencias de archivos interrumpidas. El atacante puede parar al “espía” e iniciarlo con nuevas opciones para monitorear o conectarse con otras computadoras infectadas.



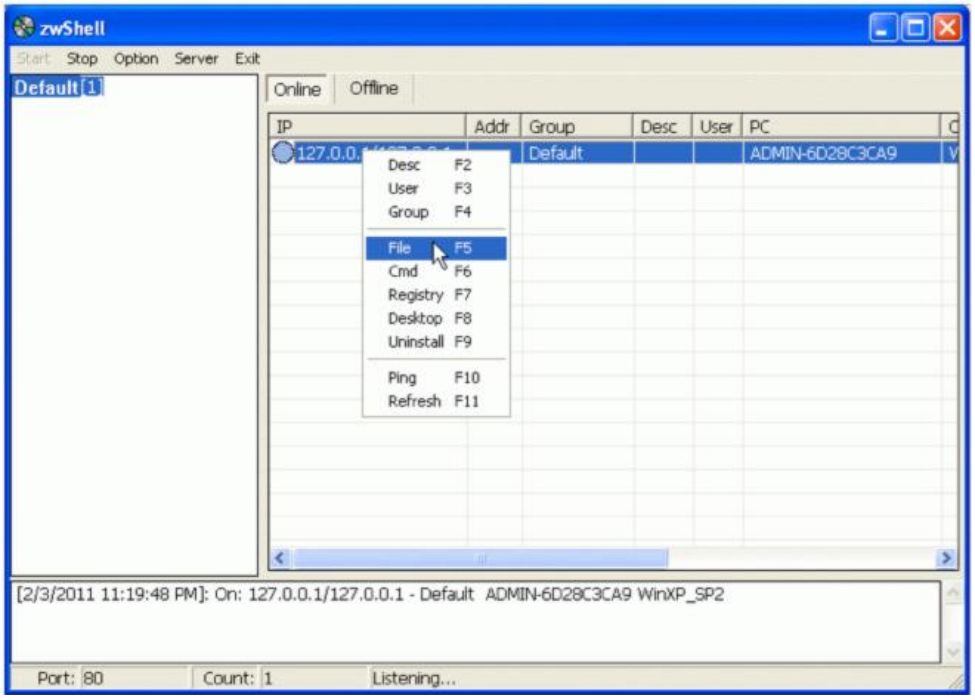
4. El atacante puede especificar la contraseña (que debe coincidir con la contraseña creada para el servidor en la Etapa 3), el nombre y el camino de la DLL de la RAT que será inyectada en el proceso de servicios svchost.exe del Windows, los nombres de servicio y *mutex*, y el nombre y la descripción exhibidos del servicio. El atacante también puede especificar hasta dos *hostnames* de C&C o la dirección IP, la dirección de puerta y el icono del proceso EXE del *dropper*. Cuando el botón “Create” sea pulsado, el zwShell generará un proceso *dropper* EXE personalizado que, cuando sea ejecutado, excluirá a sí mismo y extraerá una DLL de RAT que será iniciada como un servicio persistente del Windows. Entonces, la RAT enviará inmediatamente en la puerta configurada una guía para el servidor de C&C designado y aguardará instrucciones.



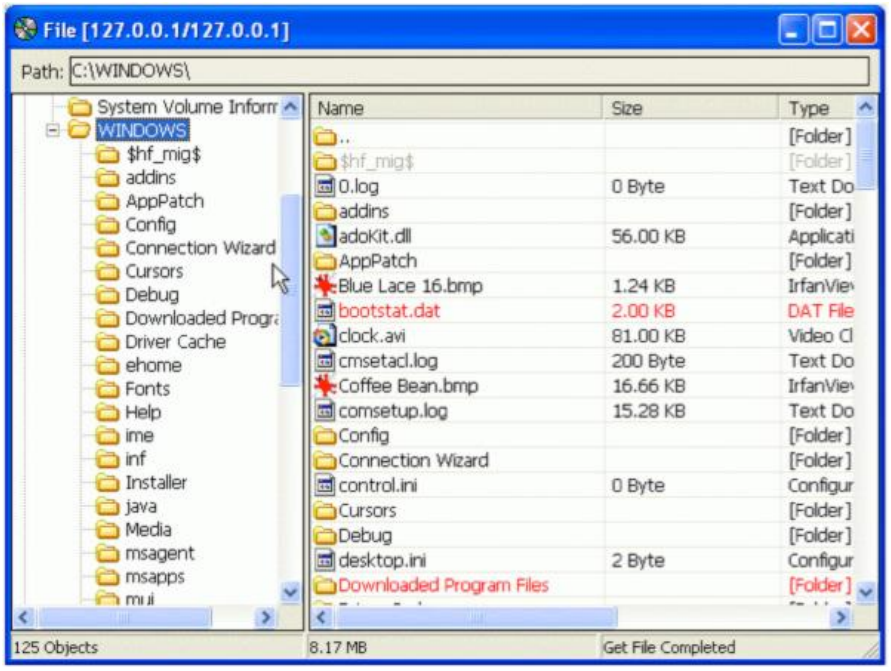
5. El *dropper* será copiado a través de comparticiones de red en la computadora comprometida y será ejecutado remotamente con el psexec o por medio de los Servicios de Terminal del Windows Terminal (RDP). En algunos casos, un ítem “AT.job” o “Schtasks” será usado para ejecutar el *driopper* por la red en la computadora comprometida. Cuando sea ejecutado, el *dropper* creará un archivo temporal y extraerá una DLL de RAT, que será iniciada como un servicio persistente del Windows. Entonce, la RAT enviará inmediatamente en la puerta configurada una guía para el servidor de C&C designado y aguardará instrucciones. El *dropper* excluirá automáticamente a si mismo después que el servicio de *backdoor* haya sido creado, y el archivo temporal será borrado cuando el sistema sea reiniciado. Un ítem será creado en los logs del Windows Update (KB****.log) en la carpeta C:\Windows con la fecha y la hora y el camino+nombre del archivo temporal.



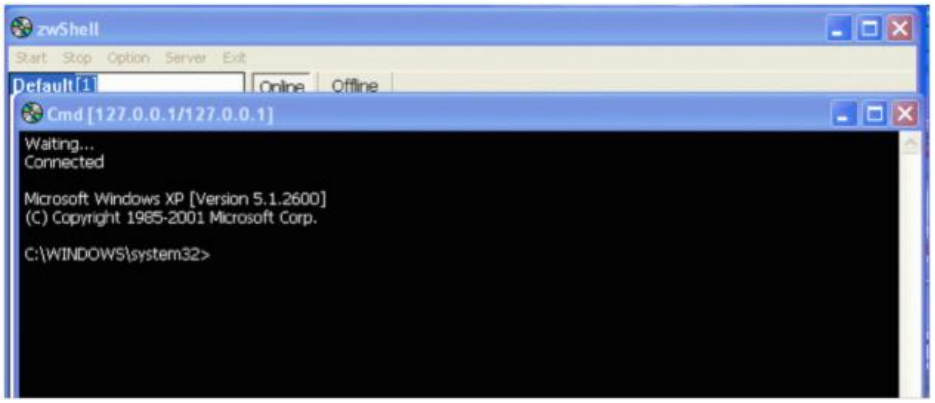
6. Cuando un cliente es ejecutado, éste se conecta con la interfaz zwShell del atacante, junto con su dirección IP, nombre de la PC, nombre del usuario conectado, e informaciones sobre el sistema operativo (SO), la versión de la máquina, incluso los niveles de *patch* principales.
7. El atacante encargado del servidor de C&C puede establecer el control remoto total de la máquina conectada y puede buscar en el sistema de archivos, iniciar *shells* de línea de comando, manipular el registro, visualizar el área de trabajo remota, y desinstalar el caballo de Troya del cliente.



8. La navegación por el sistema de archivos del cliente es un proceso totalmente interactivo y presenta una interfaz de usuario familiar semejante a la del Windows Explorer. Es posible excluir, redenominar, copiar, descargar y enviar a la máquina remota cada archivo y carpeta.



9. Un *shell* de línea de comando remoto puede ser iniciado para ejecutar comandos directamente en la máquina remota. Cuando el atacante utiliza esa función, una copia del CMD.EXE es copiada en el sistema infectado en un directorio Windows %Temp% con el nombre svchost.exe. Esa copia es una versión original del ejecutable del *shell* de comando del Microsoft Windows.



10. El Registro también pueden ser visualizado y editado en una interfaz semejante a la del editor de Registro del Windows.

Apéndice B: Atribución

IMPORTANTE: McAfee no tiene ninguna evidencia directa para nombrar a los autores de eses ataques, empero presentó pruebas circunstanciales.

Aunque creemos que muchos han participado de esos ataques, conseguimos identificar a una persona que proveyó la infraestructura esencial de C&C a los atacantes – esa persona se encuentra en la ciudad de Heze, provincia de Shandong, en China. Aunque no creemos que esa persona sea el mentor de esos ataques, es probable que ella tenga conocimiento o que tenga informaciones que puedan ayudar a identificar por lo menos algunos de los individuos, grupos u organizaciones responsables de esas invasiones.

Figura 6. Provincia de Shandong, China

La persona dirige una empresa que, según los propios anuncios de la empresa, provee “Servidores Hospedados en EE.UU. sin mantener registros” a partir de 68 RMB (USD 10) por año para un espacio de 100 MB. Los servidores alquilados por la empresa, ubicados en EE.UU., fueron usados para hospedar la aplicación de C&C zwShell que controló las máquinas de todas las empresas víctimas.

Además de la conexión con la operación de reventa de los servicios de hospedaje, existen otras evidencias que indican que los atacantes eran de origen china. Además del uso curioso de la contraseña “zw.china” que destraba el funcionamiento del caballo de Troya de C&C zwShell, McAfee descubrió que todas las actividades identificadas de extracción de datos ocurrieron a partir de direcciones IP ubicadas en Pekín y operadas dentro de las empresas atacadas en días útiles, de las 9 h a las 17 h (hora de Pekín), lo que también indica que las personas involucradas eran “empleados de la empresa” con empleos formales, y no *hackers* autónomos o no profesionales. Además de eso, los atacantes emplearon herramientas de *hacking* de origen china y predominantes en foros chinos de *hacking* subterráneo. Entre esas herramientas estaban la Hookmsgina y la WinlogonHack, que interceptan solicitaciones de *logon* del Windows y secuestran nombres de usuario y contraseñas.

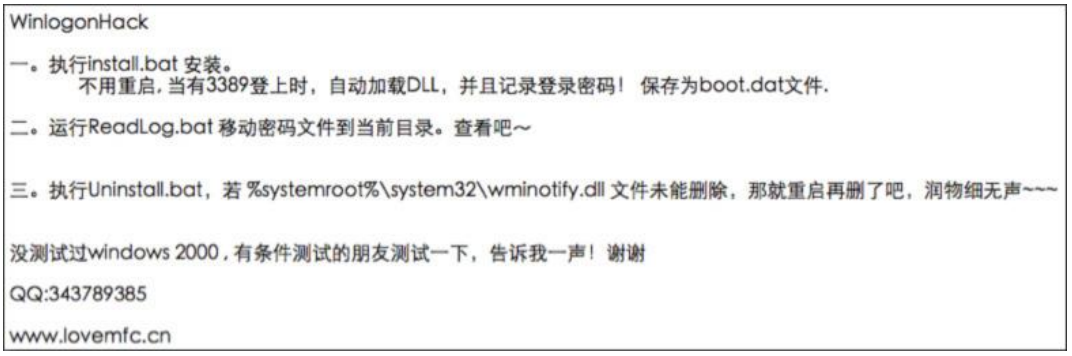


Figura 7. Instrucciones de uso de la herramienta WinlogonHack por sus desarrolladores chinos.

En el servidor Web comprometido, ellos también instalaron la ASPXSpy, una herramienta de administración remota por la Web, también de origen china.

Figura 8. Partes del código de la ASPXSpy, atribuido al desarrollador chino.

Nada indica que los desarrolladores de esas herramientas tengan cualquier vinculación directa con esas invasiones, pues las herramientas están ampliamente disponibles en foros de Internet chinos y tienden a ser ampliamente utilizadas por grupos de *hackers* chinos. Aunque sea posible que todos estos indicios sean una elaborada operación de pistas falsas para atribuir la culpa por los ataques a *hackers* chinos, creemos que eso sea bastante improbable. Además, no está claro quién tendría la motivación de esforzarse tanto para colocar en otra persona la culpa por los ataques. Tenemos evidencias sólidas que indican que los atacantes se localizaban en China.

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

21401wp_night-dragon_0211