APT DARKHOTEL
UNA HISTORIA DE HOSPITALIDAD INUSUAL

Versión 1.1
Noviembre de 2014

Equipo de análisis e investigación global

KASPERSKY lab

Contenidos

Resumen ejecutivo

El APT Darkhotel es un actor de amenazas que posee un conjunto de características aparentemente incoherentes y contradictorias, algunas avanzadas y otras bastante rudimentarias. Aunque ha funcionado de modo poco hospitalario desde hace casi una década, este actor de amenazas está actualmente activo. Las actividades ofensivas del actor pueden vincularse a conexiones Wi-Fi y físicas de hoteles y centros de negocios específicos. Algunas de ellas también están vinculadas a redes de uso compartido de archivos o P2P (punto a punto, del inglés "peer-to-peer"), y se sabe que también utilizan técnicas de spear phishing contra objetivos. Las herramientas de Darkhotel detectadas se conocen como "Tapaoux", "Pioneer", "Karba" y "Nemim", entre otros nombres. La siguiente lista presenta un conjunto de características del grupo:

- Competencia operativa al comprometer, usar de forma inadecuada y mantener el acceso a escala mundial de los recursos de la red comercial de confianza con precisión estratégica durante años
- Capacidades matemáticas y criptoanalíticas ofensivas avanzadas, junto con una falta de consideración al socavar la confianza atribuida a las entidades de certificación y la PKI
- Infección indiscriminada de sistemas con algún objetivo regional de recursos fiables y no fiables para construir y operar grandes botnets
- Keyloggers de bajo nivel bien desarrollados con un grupo de herramientas coherentes y eficaces
- Enfoque específico en las campañas dirigidas a categorías de víctimas específicas y etiquetado de estas

- Infraestructura mayor y dinámica de servidores web apache, registros dns dinámicos, librerías criptográficas y aplicaciones web PHP
- Acceso de día cero habitual: implementación reciente de un exploit de spear phishing de día cero de Adobe Flash integrado, e implementación no frecuente de otros recursos de día cero para mantener campañas mayores durante varios años

Introducción

Cuando los invitados ingenuos, incluidos los ejecutivos corporativos conscientes de la situación y empresarios de alta tecnología, viajan a una gran variedad de hoteles y se conectan a Internet, se infectan con un troyano APT raro que se comporta como cualquiera de los distintos lanzamientos de software principales. Estos pueden ser Google Toolbar, Adobe Flash, Windows Messenger, etc. Esta primera etapa de malware ayuda a los atacantes a identificar las víctimas más importantes, lo que conduce a la descarga selectiva de herramientas de robo más avanzadas.

En los hoteles, estas instalaciones se distribuyen de forma selectiva a personas específicas. Este grupo de atacantes parece saber de antemano cuándo llegan estas personas a sus hoteles de alta categoría y cuándo salen. Por lo tanto, los atacantes esperan a que estos viajeros lleguen y se conectan a Internet.

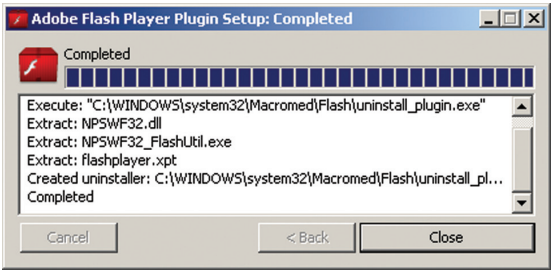
El FBI publicó avisos sobre incidentes similares en hoteles; los funcionarios del gobierno australiano emitieron comunicados parecidos de interés periodístico cuando se infectaron. Cuando en mayo de 2012 apareció un aviso del FBI relacionado con los ataques a los huéspedes de un hotel en el extranjero, muestras de Darkhotel relacionadas ya circulaban desde 2007. Los datos del registro del servidor de Darkhotel disponibles muestran conexiones que se remontan al 1 de enero de 2009. Además, la alimentación de las redes P2P con malware de amplia propagación y ataques spear phishing de día cero demuestran que el APT Darkhotel mantiene un grupo de herramientas efectivo y una operación de larga duración tras la cuestionable hospitalidad que muestra a sus huéspedes.

Análisis

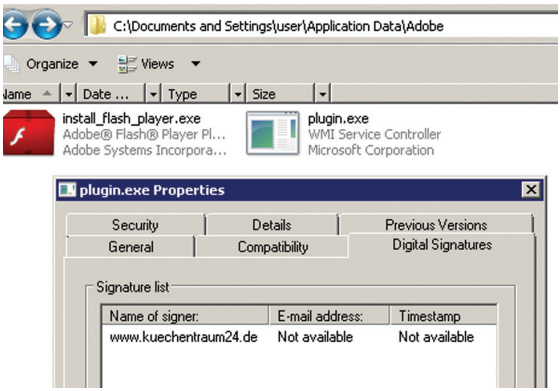
Propagación - Hoteles/centros de negocios y propagación indiscriminada

Propagación por hoteles y centros de negocios

La propagación precisa del malware del APT Darkhotel se detectó en las redes de varios hoteles, donde a los visitantes que se conectaban a la red Wi-Fi del hotel se les solicitaba que instalaran actualizaciones de software de paquetes de software populares.



Por supuesto, estos paquetes eran en realidad los instaladores de las puertas traseras del APT Darkhotel, que se suman a los instaladores legítimos de Adobe y Google. Las puertas traseras de Darkhotel firmadas digitalmente se instalaban junto con los paquetes legítimos.



El aspecto más interesante de este método de propagación es que los hoteles requieren que los huéspedes utilicen sus apellidos y el número de su habitación para iniciar sesión. Sin embargo, solo varios huéspedes recibieron el paquete de Darkhotel. Al visitar los mismos hoteles, nuestros sistemas de investigación señuelo no pudieron atraer un ataque de Darkhotel. Los datos no son concluyentes, pero todo apunta a un uso inadecuado de la información de registro.

Abuso de la infraestructura de la red

El actor Darkhotel mantiene un eficaz juego de intrusiones en las redes de los hoteles, proporcionando así un amplio acceso a puntos de ataque inesperados durante varios años. Estos puntos de ataque también proporcionan a los atacantes el acceso a la información de llegada/salida y la identidad de los visitantes de hoteles de lujo y alta categoría.

Como parte de una investigación en curso, nuestro análisis nos llevó a iframes integrados en las redes de los hoteles que redirigen los navegadores web de los usuarios a instaladores falsos. Los atacantes fueron muy cuidadosos con la colocación de estos iframes y ejecutables en recursos fiables: los propios portales de inicio de sesión de la red de los hoteles. Los atacantes fueron también muy cuidadosos a la hora de eliminar inmediatamente todas las huellas de sus herramientas en cuanto el ataque se llevó a cabo correctamente. Los portales ahora se están examinando y limpiando, y se están sometiendo a un proceso más profundo de revisión y refuerzo. Hemos observado las huellas de un par de estos incidentes de finales de 2013 y comienzos de 2014 en la red de uno de los hoteles víctima. Los agresores prepararon el entorno y atacaron a sus objetivos individuales con precisión. En cuanto finalizó la estancia de su objetivo y el marco del ataque se cerró, los atacantes eliminaron la colocación de sus iframes y los ejecutables de puerta trasera de la red del hotel. Eliminaron correctamente las huellas de su trabajo de ataques anteriores en otro hotel, pero sus técnicas ofensivas eran las mismas. Informes externos de la misma actividad en otros hoteles proporcionan datos suficientes para confirmar las mismas cuidadosas operaciones aquí.

La técnica de ataque difumina la línea entre un par de tácticas de APT comunes; "ataques de abrevadero" o "compromisos web estratégicos" bastante inexactos y técnicas spear phishing más precisas. En este caso, los atacantes de Darkhotel esperan a que su víctima se conecte a Internet a través de la red Wi-Fi del hotel o el cable en su habitación. Hay una gran probabilidad de que los objetivos se conecten a través de estos recursos, y los atacantes confían en esta

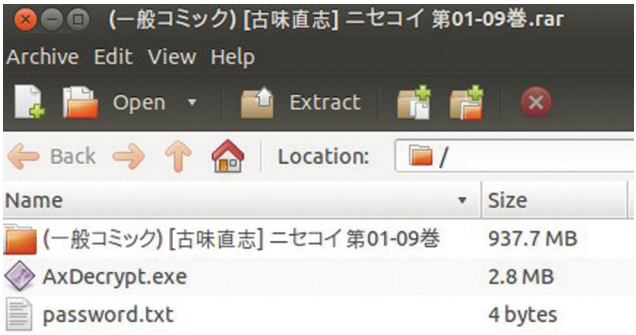
probabilidad, como en un abrevadero. Pero los atacantes también mantienen información realmente precisa relacionada con la visita de la víctima; por ejemplo, saben la dirección de correo electrónico y los intereses del contenido de la víctima en un ataque de spear phishing. Al configurar el ataque, los atacantes de Darkhotel sabían los horarios de llegada y salida previstos, el número de habitación y el nombre completo del objetivo, entre otros datos. Esta información permite a los atacantes presentar el iframe malicioso específicamente a ese objetivo específico. Por lo tanto, aquí tenemos otra característica única de este atacante: emplea un enfoque ofensivo más o menos general, pero a la vez muy preciso.

Propagación indiscriminada

Un ejemplo de la propagación de malware indiscriminada del APT Darkhotel se demuestra por la manera en que alimentan los sitios de uso compartido P2P japoneses, donde el malware se propaga como parte de un archivo rar grande (aproximadamente 900 mb). El archivo también se propaga por bittorrent, como se detalla a continuación. Darkhotel utiliza este método para distribuir su troyano Karba. Estos archivos japoneses, traducidos para los visitantes que hablan chino, parecen ser de naturaleza sexual, parte de la escena de un cómic anime erótico/militar, exponiendo los intereses probables de los objetivos potenciales.

Este paquete Darkhotel se descargó más de 30 000 veces en menos de seis meses. El enlace de Darkhotel de bittorrent P2P aparece aquí, publicado el 22.11.2013. Se propagó durante 2014.

（一般コミック）［古味直志］ニセコイ 第01−09巻.rar



Este torrent descarga un archivo de unos 900 MB. El archivo rar se descomprime en un directorio lleno de archivos zip cifrados, el descifrador asociado y un archivo de contraseña para descifrar los archivos zip. Pero lo que parece el descifrador AxDecrypt.exe está vinculado tanto al verdadero descifrador como al instalador del troyano Karba Catch.exe de Darkhotel. Cuando un usuario descarga el torrent y descifra los archivos zip, el troyano se instala de manera oculta y se ejecuta en el sistema de la víctima.

Catch.exe, detectado como Backdoor.Win32.Agent.dgrn, se comunica con los siguientes servidores de mando y control de Darkhotel:

microdelta.crabdance.com microyours.ignorelist.com micronames.jumpingcrab.com microchisk.mooo.com microalba.serveftp.com

Otros ejemplos de este vínculo de la puerta trasera de Darkhotel con un torrent compartido incluyen anime japonés con contenido para adultos y mucho más. Hay decenas de miles de descargas de estos torrents individuales.

“torrent\[hgd资源组][漫画]comic1☆7漫画合集③+④+⑤+特典[5.08g][绅士向][总第四十三弹]（七夕节快乐！）\汉化\(comic1☆7）［莉零（小鹿りな，古代兵器)］凌 -shinogi-（闪乱カグラ）［中文］ “

y

“動漫\[hgd资源组][漫画]comic1☆7漫画合集③+④+⑤+特典[5.08g][绅士向][总第四十三弹]（七夕节快乐！）\汉化”）

La puerta trasera de Darkhotel asociada estaba alojada en bittorrent, emule, etc., con una gran variedad de nombres de cómics. Los ejemplos incluyen ofertas de cómics y anime. Los dominios del servidor de mando y control de Darkhotel relacionados incluyen:

microblo5.mooo.com
microyours.ignorelist.com
micronames.jumpingcrab.com
microchisk.mooo.com
microalba.serveftp.com

Campañas de spear phishing de Darkhotel

Las campañas de Darkhotel con implantes típicos de Tapaoux de spear phishing aparecieron públicamente en bits y partes varias veces en los últimos cinco años. Estos esfuerzos del subproyecto se centraron en la base industrial de defensa (DIB), el gobierno y las organizaciones no gubernamentales. Se utilizó como señuelo el contenido de los mensajes de correo electrónico sobre temas como la energía nuclear y las capacidades de las armas. Se publicaron las primeras cuentas en contagio describiendo los ataques contra organizaciones no gubernamentales y responsables políticos del gobierno. Estas actividades de spear phishing continúan en 2014. Los ataques siguen el típico proceso de spear phishing y en los últimos dos meses, los sistemas vulnerados recuperaron archivos ejecutables de programas de descarga de servidores web como hxxp://office-revision.com/update/files22/update.exe o hxxp://trade-inf.com/mt/duspr.exe.

En los últimos años, el grupo ha enviado por correo electrónico los enlaces que redirigen a los navegadores de los objetivos a exploits de día cero de Internet Explorer. A veces, el propio archivo adjunto incluye un exploit de día cero de Adobe.

Implementación de día cero reciente

Este grupo implementa ocasionalmente exploits de día cero, pero los inhabilita si es necesario. En los últimos años, han implementado ataques de spear phishing de día cero a productos de Adobe y Microsoft Internet Explorer, incluido cve-2010-0188. A comienzos de 2014, nuestros investigadores expusieron su uso de cve-2014-0497, una actividad de día cero de Flash descrita en Securelist a principios de febrero.

El grupo lanzó un ataque de spear phishing a un conjunto de sistemas objetivo conectados a Internet a través de ISP chinos y desarrollaron capacidades en exploits de día cero para gestionar sistemas Windows 8.1 reforzados. Es interesante el hecho de que los objetos Flash estaban integrados en documentos coreanos titulados "Lista de los últimos AV wind japoneses y cómo utilizar torrents. docx" (traducción libre del inglés). El programa de descarga instalado (d8137 ded710d83e2339a97ee78494c34) propagaba código dañino, similar al de la funcionalidad del componente "Ladrón de información" que se resume a continuación y se describe de forma detallada en el Apéndice D.

Certificados digitales y deslegitimización de la fiabilidad de la entidad de certificación

Normalmente, los actores Darkhotel firman sus puertas traseras con certificados digitales de uno u otro tipo. No obstante, los certificados inicialmente escogidos por este grupo son muy interesantes por sus claves no seguras y probable abuso por parte de los atacantes. A continuación aparece el listado de los certificados que se utilizaron habitualmente para firmar el código dañino de Darkhotel, que requieren capacidades matemáticas avanzadas para factorizar las claves en el momento. No son los únicos certificados que el grupo utilizó. La actividad más reciente sugiere que el grupo ha robado certificados para firmar su código.

Entidad de certificación (CA) raíz	CA subordinada/ emisor	Propietario	Estado	Válido desde	Válido hasta
GTE CyberTrust	Digisign Server ID (Enrich)	flexicorp.jaring.my sha1/ RSA (512 bits)	Caducado	17/12/2008	17/12/2010
GTE CyberTrust	Cybertrust SureServer CA	inpack.syniverse.my sha1/RSA (512 bits)	Revocado	13/02/2009	13/02/2011
GTE CyberTrust	Cybertrust SureServer CA	inpack.syniverse.com sha1/RSA (512bits)	Revocado	13/02/2009	13/02/2011
GTE CyberTrust	Anthem Inc Certificate Auth	ahi.anthem.com sha1/ RSA (512 bits)	Firma no válida	13/01/2010	13/01/2011
GlobalSign	Deutsche Telekom CA 5	www.kuechentraum2 4.de sha1/RSA (512 bits)	Revocado	20/10/2008	25/10/2009
GTE CyberTrust	Digisign Server ID (Enrich)	payments.bnm.gov.m y sha1/RSA (512 bits)	Firma no válida	07/12/2009	07/12/2010
GTE CyberTrust	TaiCA Secure CA	esupplychain.com.tw sha1/RSA (512 bits)	Caducado	02/07/2010	17/07/2011
GTE CyberTrust	Digisign Server ID (Enrich)	mcrs2.digicert.com. my sha1/RSA (512 bits)	Firma no válida	28/03/2010	28/03/2012
GTE CyberTrust	Cybertrust SureServer CA	agreement.syniverse. com sha1/RSA (512 bits)	Firma no válida	13/02/2009	13/02/2011
GTE CyberTrust	Cybertrust SureServer CA	ambermms.syniverse. com sha1/RSA (512 bits)	Firma no válida	16/02/2009	16/02/2011

Entidad de certificación (CA) raíz	CA subordinada/ emisor	Propietario	Estado	Válido desde	Válido hasta
Equifax Secure eBusiness CA-1	Equifax Secure eBusiness CA-1	secure.hotelreykjavik.i s md5/RSA (512 bits)	Firma no válida	27/02/2005	30/03/2007
GTE CyberTrust	Cybertrust Educational CA	stfmail.ccn.ac.uk sha1/ RSA (512 bits)	Firma no válida	12/11/2008	12/11/2011
GTE CyberTrust	Digisign Server ID (Enrich)	webmail.jaring.my sha1/ RSA (512 bits)	Firma no válida	01/06/2009	01/06/2011
GTE CyberTrust	Cybertrust Educational CA	skillsforge.londonmet. ac.uk sha1/RSA (512 bits)	Firma no válida	16/01/2009	16/01/2012
GTE CyberTrust	Digisign Server ID (Enrich)	anjungnet.mardi.gov. my sha1/RSA (512 bits)	Firma no válida	29/09/2009	29/09/2011
GTE CyberTrust	Anthem Inc Certificate Authority	dl-ait-middleware@an them.com sha1/RSA (512 bits)	Firma no válida	22/04/2009	22/04/2010
GTE CyberTrust	Cybertrust Educational CA	ad-idmapp.cityofbrist ol.ac.uk sha1/RSA (512 bits)	Firma no válida	11/09/2008	11/09/2011
Verisign	Verisign Class 3 Secure OFX CA G3	secure2.eecu.com sha1/ RSA (512 bits)	Firma no válida	25/10/2009	26/10/2010
Agencia raíz	Agencia raíz	Microsoft md5/RSA (1024 bits)	Firma no válida	09/06/2009	31/12/2039
GTE Cybertrust	CyberTrust SureServer CA	trainingforms.syniverse. com sha1/RSA (512 bits)	Firma no válida	17/02/2009	17/02/2011

Todos los casos relacionados con casos de malware de Darkhotel firmado comparten la misma entidad de certificación raíz y entidad de certificación intermedia que expedían certificados con claves md5 no seguras (RSA 512 bits). Estamos seguros de que nuestro actor de amenazas Darkhotel duplicó fraudulentamente estos certificados para firmar su malware. Estas claves no fueron robadas. Muchos de los certificados se incluyeron en una publicación de Fox-IT de 2011, "Certificados RSA-512 usados de forma fraudulenta".

Para apoyar esta especulación, lea el aviso de Microsoft Security no específico que aparece a continuación, el aviso de Mozilla que ofreció información sobre el problema en su momento, y las respuestas de Entrust.

Extracto del aviso de seguridad de Microsoft del jueves 10 de noviembre de 2011:

"Microsoft tiene constancia de que DigiCert Sdn. Bhd, una entidad de certificación (CA) subordinada de Malasia en Entrust y GTE CyberTrust, ha emitido 22 certificados con claves de 512 bits poco seguras. Estas claves poco seguras, cuando se atacan, podrían permitir a un atacante usar los certificados de forma fraudulenta para suplantar el contenido, llevar a cabo ataques de suplantación de identidad (phishing) o realizar ataques del tipo 'Man in the middle' contra todos los usuarios de explorador web, incluidos los usuarios de Internet Explorer. Aunque no se trata de una vulnerabilidad de un producto de Microsoft, este problema afecta a todas las versiones compatibles de Microsoft Windows.

No existe ninguna indicación de que los certificados se hayan emitido de forma fraudulenta. En su lugar, las claves con poca seguridad criptográfica han permitido que algunos certificados se dupliquen y usen de forma fraudulenta.

Microsoft proporciona una actualización para todas las versiones compatibles de Microsoft Windows que revoca la confianza en DigiCert Sdn. Bhd. La actualización revoca la confianza de los dos certificados de CA intermedios siguientes: Digisign Server ID – (Enrich), emitido por la entidad de certificado Entrust.net (2048) **Digisign Server ID (Enrich)**, emitido por **GTE CyberTrust Global Root**".

Extracto de la respuesta de Mozilla de 2011:

"Si bien **no existe ninguna indicación de que se hayan emitido de forma fraudulenta, las claves poco seguras han permitido que los certificados sean vulnerables.** Por otra parte, los certificados de esta CA contienen varios problemas técnicos. Carecen de una extensión EKU que especifique la intención de su uso y se han emitido sin información de revocación".

Extracto de la respuesta de Entrust:

"No hay pruebas de que las entidades de certificación Digicert de Malasia hayan visto su seguridad afectada".

Pirateo de las claves

A continuación se ofrece información sobre los costes y requisitos técnicos relacionados con el ataque a estos certificados.

La potencia informática necesaria para piratear y factorizar una clave de 512 bits RSA fue de alrededor de 4250 euros y el periodo de tiempo requerido era de aproximadamente 2 semanas. (Consulte http://lukenotricks.blogspot.co.at/2010/03/rsa-512-factoring-service-two-weeks.html).

En octubre de 2012, Tom Ritter indicó que costaría aproximadamente de 100 a 130 euros, quizás incluso menos de 65.

Si nos remontamos aún más, se ha debatido mucho sobre los métodos técnicos del pirateo de estas claves: El documento de 2001 de DJ Bernstein sobre la creación de un equipo que reduzca el coste de la factorización de enteros con técnicas de criba del cuerpo de números, pirateando las claves RSA de 1024 bits.

Reacción de RSA y declaración de 2002 sobre si las claves RSA de 1024 bits se piratean o no: "NIST ofreció una tabla de tamaños de clave recomendados para su estudio en su taller de gestión de claves en noviembre de 2001 [7]. Para los datos que se deben proteger a más tardar en el año 2015, la tabla indica que el tamaño de la clave RSA debe ser de al menos 1024 bits. Para los datos que se deben proteger durante más tiempo, el tamaño de la clave debe ser de al menos 2048 bits."

Otros certificados de Tapaoux

Los ataques y puertas traseras recientes de Tapaoux incluyen malware firmado con certificados SHA1/RSA de 2048 bits seguros, lo que sugiere el robo de certificados.

Entidad de certificación (CA) raíz	CA subordinada/ emisor	Propietario	Estado	Válido desde	Válido hasta
thawte	thawte Primary Root CA	Xuchang Hongguang Technology Co.,Ltd. sha1/RSA (2048 bits)	Revocado	18/07/2013	16/07014
thawte	thawte Primary Root CA	Ningbo Gaoxinqu zhidian Electric Power Technology Co., Ltd. sha1/RSA (2048 bits)	Revocado	05/11/2013	05/11/2014

Keyloggers mejorados y desarrollo

Uno de los componentes más interesantes que descubrimos como parte de esta campaña fue el uso de un keylogger avanzado firmado digitalmente. Se trata de código malicioso limpio, bien escrito y a nivel del kernel. Los idiomas de estas cadenas son una mezcla de inglés y coreano. Está firmado con el certificado digital familiar "belinda.jablonski@syniverse.com".

Este keylogger se instala mediante código que se ejecuta dentro de svchost.exe en WinXP SP3, que contiene una interesante cadena de depuración: d:\KerKey\KerKey(일반)\KerKey\release\KerKey.pdb

Tenga en cuenta que 일반 significa "General" en coreano.

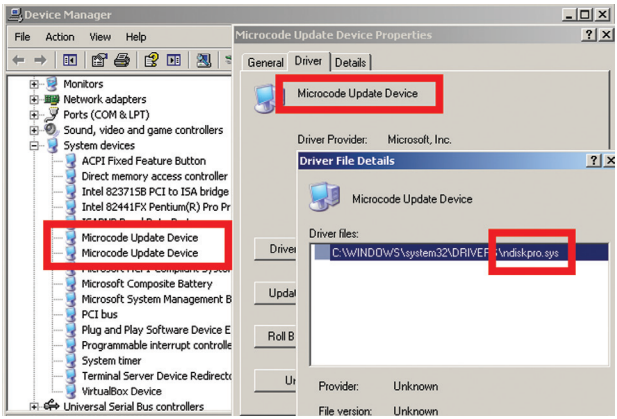
Probablemente se desarrolló como parte de un proyecto de mediados o finales de 2009:
e:\project\2009\x\total_source\32bit\ndiskpro\src\ioman.c

Código del keylogger

Este paquete de controlador está diseñado para parecerse a un dispositivo de un sistema Microsoft de bajo nivel legítimo. Se instala como un servicio "Ndiskpro" del controlador de kernel del sistema, descrito como un "Dispositivo de actualización de microcódigo". Es un poco sorprendente que no haya ninguna funcionalidad rootkit que oculte este servicio:

```
SERVICE_NAME: Ndiskpro
DISPLAY_NAME: Ndiskpro
        TYPE               : 1  KERNEL_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms
```

Cuando se carga, el controlador NDISKPRO.SYS enlaza INT 0x01 e INT 0xff, y recupera datos de pulsaciones de teclas directamente del puerto 0x60, el propio controlador del teclado de la placa base. Se carga y luego comunica los datos del usuario registrado al componente de modo usuario en ejecución. A continuación, este componente cifra y escribe los valores recuperados ondisk a un archivo .tmp con un nombre aleatorio, como ffffz07131101.tmp. Este archivo se encuentra en el mismo directorio que el instalador original, que mantiene la persistencia durante los reinicios con una simple adición a la clave de ejecución HKCU.



Este módulo keylogger cifra y almacena los datos recopilados en un archivo de registro, como se ha mencionado anteriormente. El algoritmo de cifrado es similar a RC4. La parte más interesante es que el módulo genera aleatoriamente la clave y la almacena en un lugar inesperado: en medio del nombre del archivo de registro. Por lo tanto, la parte numérica del nombre de archivo se utiliza como semilla para el generador de números pseudoaleatorios. La función rand se vincula estáticamente a fin de garantizar los mismos resultados en diferentes ordenadores.

Componentes de malware interesantes

El grupo de herramientas de Darkhotel consta de varios componentes que se han ido modificando levemente con el tiempo. Estas herramientas se incorporan mediante instaladores de hoteles suplantando instaladores de software legítimos, vinculados a paquetes de torrent o mediante exploits o hipertexto vinculados a correos electrónicos de spear phishing.

Las herramientas más avanzadas, como el keylogger descrito anteriormente, se descargan más adelante en el sistema de la víctima mediante uno de estos implantes. En un caso reciente, documentos de word integrados con archivos swf flash de día cero instalaban estas puertas traseras, o bien descargaban y ejecutaban puertas traseras desde servidores web remotos. Estas herramientas instalan el keylogger, roban información del sistema o descargan otras herramientas.

- Programa de descarga pequeño
- Ladrón de información
- Troyano
- Instalador e inyector automático
- Virus selectivo

Entre los comportamientos más interesantes de estos componentes se incluyen los siguientes:

- Demora en las comunicaciones de comando y control de 180 días condicional muy inusual
- Rutinas de autodestrucción cuando el código de página predeterminado del sistema se establece en coreano
- Gestión mejorada del robo de la autenticación IntelliForm de Microsoft
- Módulo infostealer compatible con Internet Explorer, Firefox y Chrome
- Mantenimiento de campaña o ID de fase
- Sensibilidad de ejecución de la máquina virtual
- Rutinas de infección viral selectiva para centrar la propagación de malware dentro de las empresas
- Código malicioso firmado (descrito anteriormente)

Programa de descarga pequeño

Este módulo es bastante pequeño (27 Kb) y forma parte de un archivo SFX WinRar que instala e inicia el módulo desde %APPDATA%\Microsoft\Crypto\DES64v7\msieckc.exe. Este módulo está diseñado para actualizar los componentes maliciosos mediante comprobaciones periódicas en el servidor de mando y control o C&C (por sus siglas en inglés). También puede eliminar algunos componentes anteriores, los nombres de los cuales están codificados de forma rígida en el cuerpo del malware. El módulo añade opciones de registro de ejecución automática para activar un inicio automático durante el arranque del sistema.

Una de las funciones más interesantes de este ejecutable es su demora y persistencia inusuales. Si existe un archivo especial en el sistema, el módulo no comenzará a devolver la llamada al servidor de C&C hasta que el archivo especial tenga 180 días de antigüedad. Por lo tanto, si algún otro componente malicioso crítico se eliminó durante este periodo, el módulo actual realiza una copia de seguridad y restaura el acceso al sistema en un periodo de 6 meses.

El componente recopila información del sistema y la envía a los servidores de mando y control de Darkhotel, como se describe en el Apéndice D.

Ladrón de información

Este módulo es relativamente grande (455 Kb) y forma parte de un archivo SFX WinRar que instala e inicia el módulo desde %APPDATA%\Microsoft\Display\DmaUp3.exe. El objetivo principal de este módulo es recopilar diversos secretos almacenados en un sistema local y cargarlos en los servidores de mando y control de Darkhotel:

- Contraseñas guardadas en la memoria caché de Internet Explorer 6/7/8/9 (Windows Protected Storage)
- Secretos almacenados en Mozilla Firefox (< 12.0)
- Secretos almacenados en Chrome
- Credenciales de Gmail Notifier
- Datos y credenciales gestionados por Intelliform:
  - Twitter
  - Facebook
  - Yandex
  - Qip
  - Nifty

- Mail.ru
- Correo electrónico 126.com
- Zapak
- Lavabit (servicio de correo electrónico cifrado ahora desactivado)
- Bigstring
- Gmx
- Sohu
- Zoho
- Sina
- Care2
- Mail.com
- Fastmail
- Inbox
- Gawab (servicio de correo electrónico de Oriente Medio)
- 163.com
- Lycos
- Correo electrónico de Lycos
- Inicio de sesión en AOL
- Inicios de sesión en Yahoo!
- Inicios de sesión en Yahoo! de Japón
- Inicios de sesión en Microsoft Live
- Credenciales de inicio de sesión en Google

Este módulo está diseñado para autodestruirse en Windows cuando el código de página predeterminado del sistema se establece en coreano.

Trojan.Win32.Karba.e

Este malware tiene un tamaño de 220 Kb. Fue creado como aplicación de marco de trabajo de MFC con muchas llamadas adicionales que deberían haber complicado el análisis de la muestra. Imita una aplicación de escritorio de la interfaz gráfica de usuario, pero no crea ninguna ventana o cuadro de diálogo visible para interactuar con los usuarios locales. El Troyano recopila datos sobre el sistema y el software antimalware instalado en este, y carga los datos en los servidores de mando y control de Darkhotel. En el Apéndice D se incluyen más detalles técnicos.

Instalador e inyector de troyanos (archivos legítimos infectados)

Este malware tiene un tamaño de 63 kb. Está vinculado a una gran variedad de paquetes de software con diferentes nombres, pero el paquete host siempre se detecta de forma coherente como “Virus.Win32.Pioneer.dx”. Instala el componente "virus selectivo" igfxext.exe en el disco y lo ejecuta.

Virus selectivo

Este componente es un **virus** y se utiliza para infiltrarse de forma selectiva en otros ordenadores a través de USB o recursos compartidos de red.

En primer lugar, el virus recupera todos los discos disponibles y, desde el disco número 4 (D:\) al disco número 20 (Z:\), busca archivos ejecutables y los infecta. El código simplemente fuerza la lista de unidades extraíbles asignadas.

Durante la rutina de infección, el virus cambia el punto de entrada de archivos ejecutables, crea una sección .rdat e inserta un cargador pequeño en la sección; a continuación, coloca su carga principal en la superposición. Cada archivo infectado tiene una funcionalidad que se describe en la sección Instalador e inyector de troyanos, de tal manera que puede recopilar información acerca del ordenador, enviarla al servidor de C&C y descargar otros componentes de Darkhotel como se ha solicitado. Los componentes descargados estudiados están firmados con certificado familiar caducado de www.esupplychain.com.tw, emitido por Cybertrust SureServer CA.

Una vez más, en el Apéndice D se incluyen más detalles técnicos.

Códigos de campaña

Casi cada puerta trasera en este grupo mantiene un código o ID de campaña interno, que se utiliza en las comunicaciones del servidor de C&C iniciales, como se ha descrito anteriormente. Algunos ID parecen estar relacionados con intereses geográficos, otros no parecen tan evidentes. A continuación aparece una lista de los ID de campaña de Darkhotel que hemos recopilado. Los ID internos y los recursos del servidor de C&C se superponen en estos componentes, no existe un patrón de distribución en función de recursos connectback. El ID más común es "DEXT87":

DEXT87	NKstep2-auto
step2-auto	PANA(AMB)-auto
dome1-auto	PANA#MERA
step2-down	SOYA#2-auto
Java5.22	step2-down-u
C@RNUL-auto	(ULT)Q5SS@E.S-down
dome-down	VER1.5.1
M1Q84K3H	VICTORY
NKEX#V1.Q-auto	WINM#V1.Q

Infraestructura y víctimas

Este equipo de infraestructura parece emplear un conjunto inferior de habilidades en comparación con las sofisticadas campañas, manteniendo configuraciones de servidor poco seguras con escasa vigilancia y reacciones defensivas, así como cometiendo algunos simples errores. No obstante, son eficaces en mantener una infraestructura totalmente disponible para apoyar las infecciones nuevas y las existentes.

En general, se encontraron víctimas de todo el mundo en nuestros registros de Sinkhole y en los datos KSN, la mayoría de Japón, Taiwán, China, Rusia, Corea y Hong Kong.

Dominios en Sinkhole

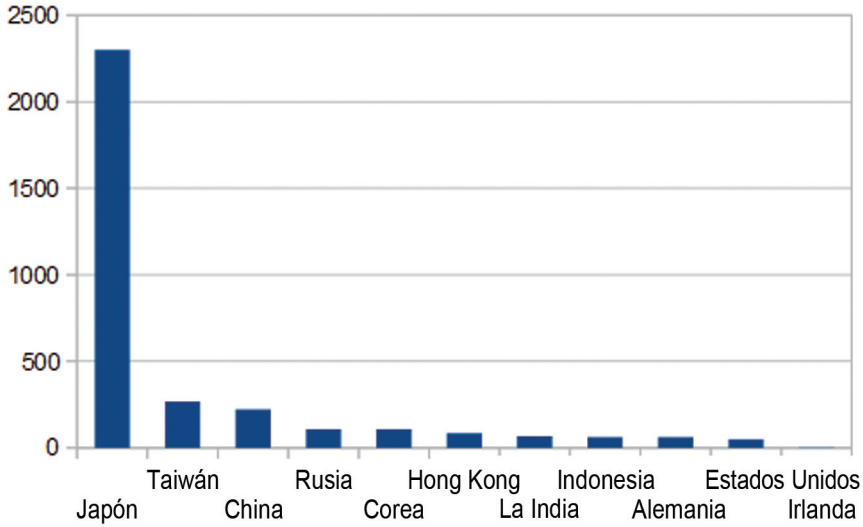
Los siguientes dominios de C&C se han añadido a nuestro Sinkhole y se han redirigido al servidor Sinkhole de Kaspersky:

42world.net
academyhouse.us
adobeplugs.net
amanity50.biz
autocashhh.hostmefree.org
autochecker.myftp.biz
autoshop.hostmefree.org
autoupdatfreeee.coolwwweb.com
checkingvirusscan.com
dailyissue.net
dailypatch-rnr2008.net
fenraw.northgeremy.info
generalemountina.com
goathoney.biz
jpnspts.biz
jpqueen.biz
mechanicalcomfort.net
micromacs.org
ncnbroadcasting.reportinside.net
neao.biz
private.neao.biz
reportinside.net
self-makeups.com
self-makingups.com
sourcecodecenter.org
support-forum.org
updatewifis.dyndns-wiki.com

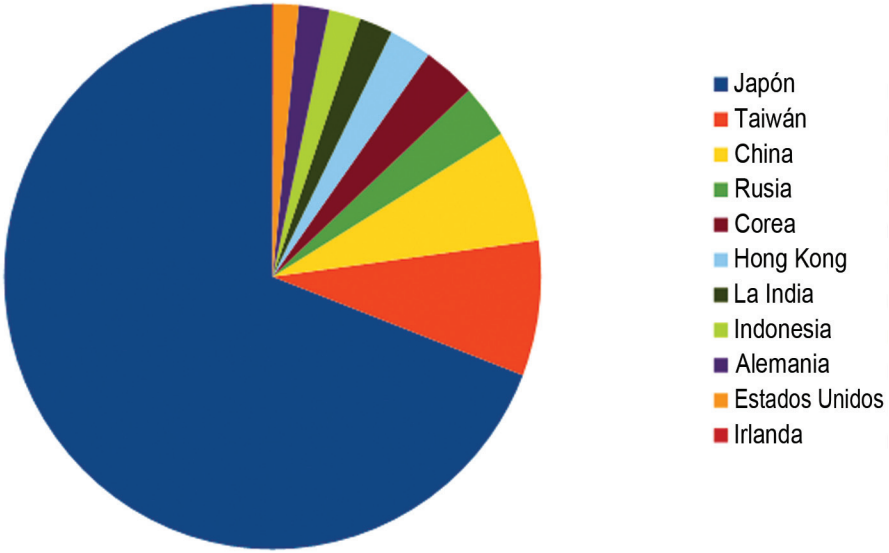
Ubicaciones de las víctimas - Datos de KSN y Sinkhole

Datos de KSN

Kaspersky Security Network detectó infecciones de Darkhotel en miles de equipos, la mayoría relacionadas con las campañas P2P de Darkhotel. Es probable que estas estimaciones de ubicaciones geográficas proporcionen el panorama más preciso de los lugares donde se realizan actividades de Darkhotel.

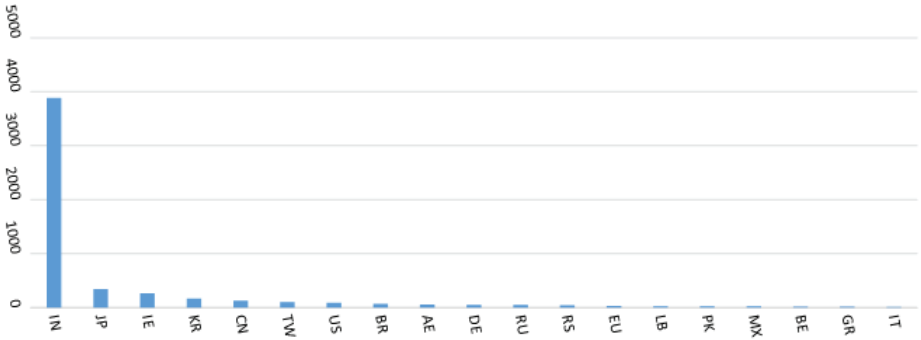


A continuación aparece un gráfico circular que permite visualizar mejor las proporciones de las actividades de ataque en todo el mundo. Como se puede ver, más del 90 % se produce en los cinco países que aparecen en la parte superior: Japón, seguido de Taiwán, China, Rusia y Corea.



Datos de Sinkhole

Como los operadores crean nuevos servidores de mando y control de forma muy activa, es difícil añadir suficientes dominios a nuestro sinkhole para obtener una visión global precisa de las ubicaciones de los sistemas de la víctima en función de estos datos. Además, muchos sistemas de investigación están conectados a los dominios añadidos al Sinkhole. No obstante, este gráfico de devoluciones de llamada de Sinkhole presenta una distribución poco fiable de las ubicaciones geográficas de las víctimas, con la India, Japón, Irlanda, Corea, China y Taiwán en los primeros puestos. Si ignoramos la India e Irlanda, el conjunto coincide de forma más precisa con nuestros datos de KSN.



Datos de las víctimas de ddrlog disponibles

Muchos de estos servidores de C&C mantienen una ruta de directorios común que sirve a un ddrlog. Los ddrlog parecen mantener datos de devolución de llamada que los atacantes desean reservar en registros de error. Muchas de las URL de devolución de llamada tienen errores, muchos de ellos se deben a rangos de IP no deseados y otros son claramente devoluciones de llamadas de sistema sandbox de investigación no deseadas.

Una descripción detallada de los valores de URL connectback y su esquema de codificación xor/base64 se incluye en las notas técnicas de la sección "Malware interesante: Trojan.Win32.Karba.e", en el Apéndice D.

El servidor de C&C de Darkhotel mantiene estas estructuras de directorios para almacenar y servir contenido ddrlog:

- /bin/error/ddrlog
- /patch/error/ddrlog

Las siguientes estructuras parecen ser comunes a todos los servidores, pero no producen ddrlog y no mantienen un directorio /error/:

- /u2/
- /u3/
- /patch2/
- /major/
- inor/
- /asp/
- /update3/

Dos archivos ddrlog registran entradas a partir del 1 de enero de 2009 a las 9:16.

- autozone.000space.com
- genuinsman.phpnet.us

Todos los registros mantienen un número elevado de entradas, casi 50 000, con un simple sello "B" o "L". Estos registros tienen el siguiente formato:

```
2009.01.01 09:16:00 150.70.xxx.xx --> B
2009.01.01 09:16:33 150.70.xxx.xx --> B
2009.01.01 09:14:52 220.108.x.xxx --> L
2009.01.01 09:16:04 112.70.xx.xx --> L
```

Solo 120 direcciones IP realizan el registro "B" y el 90 % de estos son del rango 150.70.97.x. Todo este rango completo es propiedad de Trend Micro en Tokio, Japón.

Varias de las direcciones restantes, como 222.150.70.228, parecen provenir de otros rangos de Trend Micro en Japón. Un valor atípico proviene de un ISP de El Salvador, y la otra está conectada a un ISP japonés. Aproximadamente 20 000 direcciones IP realizan el registro "L".

Otros ddrlog pueden incluir también etiquetas "A".

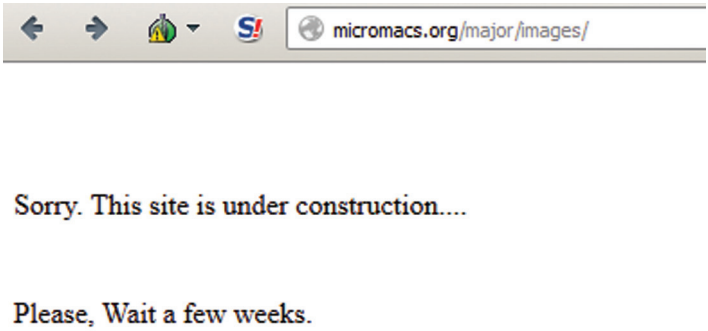
La etiqueta "A" indica registros no deseados de ubicaciones no localizadas, como Hungría e Italia. La etiqueta "B" indica registros no deseados de rangos de IP de Trend Micro.

La etiqueta "L" indica registros no deseados de una amplia variedad de rangos, pero incluye una IP extraña como dirección de bucle invertido, 127.0.0.1, claramente un error.

Las entradas de estos registros incluyen URL de devolución de llamada que tienen espacios y caracteres inusuales que no se ajustan al diccionario de caracteres base64 necesario.

Comunicaciones y estructura del servidor de C&C

Página principal típica:



Para begatrendstone.com, tenemos la siguiente estructura de directorios:

/bin
    -read_i.php (script de C&C principal)
    -login.php (desconocido, responde "Wrong ID()")
/bin/error (aquí se almacenan los registros de errores)
    -ddrlog
/bin/tmp
 /bin/SElhxxwiN3pxxiAPxxc9
    -all.gif
    /i
    - contenido robado cifrado del sistema de la víctima
    /L
    /f

Para auto2116.phpnet.us, tenemos la siguiente estructura de directorios:

/patch
    -chkupdate.php (comando principal y script de control)
/patch/error
    -ddrlog

El grupo cifra los datos de las víctimas en sus servidores con combinaciones de un solo usuario/clave de paso a través de varias víctimas. Cuando un usuario

no autorizado intenta acceder a una interfaz web de Darkhotel para la gestión de la víctima sin la clave de paso correcta, la página html y el diseño de tabla se representan correctamente, pero todos los valores de datos de la página se devuelven como texto cifrado confuso.

Gestión de la víctima

Parece que los nuevos sistemas de la víctima se investigan sistemáticamente. Los atacantes mantienen una interfaz web para investigar los sistemas nuevos de las víctimas. En primer lugar y sobre todo, los atacantes registran y clasifican los sistemas de la víctima en función de sus últimos registros del servidor de C&C. Los datos recopilados se presentan probablemente en orden de importancia:

1. Nombre de inicio de sesión del usuario
2. CPU y SO del sistema
3. "Segundos de ping", o la distancia a la que se encuentra el sistema del servidor de C&C
4. "En", o el proceso que el código dll de los atacantes ejecuta
5. Vac: identificador del producto antivirus
6. IP de LAN del sistema
7. IP de WAN de la red

A continuación aparece un ejemplo de una de estas páginas web:

Last connection	Information
0d 0h 2m 17s	Sys@User : [redacted](0411) C P U : Intel(R) Pentium(R) M processor 1600MHz System OS: Microsoft Windows XP (Service Pack 3) Ping sec : [redacted]ms -> average [redacted]ms In : C:₩WINDOWS₩system32₩alg.exe Vac : Net card : [redacted] ([redacted]) Inter IP : [redacted]
0d 3h 10m 49s	Sys@User : [redacted](0411) C P U : Intel(R) Core(TM) i7-2600K CPU @ 3.40GHz System OS: Windows 7 Professional () Ping sec : [redacted]ms -> average [redacted]ms In : c:₩program files (x86)₩uTorrent₩uTorrent.exe Vac : TR, Net card : [redacted] ([redacted]) Inter IP : [redacted]

Actividad de investigación

Está claro que alguna actividad de análisis automático relacionada con las herramientas sandbox de los investigadores aparece en estos registros. Desde junio de 2013 a abril de 2014 (un periodo aproximado de 11 meses), solo en 15 archivos ddrlog detectamos casi 7000 conexiones de sistemas sandbox de investigación. Las conexiones de red proporcionan valores de a1= a a3= que identifican un sandbox basado en QEMU, todos procedentes de solo 485 direcciones IP WAN. Se han registrado menos de 30 IP de LAN, todas en el mismo rango 172.16.2.14-126. Estos sistemas utilizan una cuenta de usuario "Dave" y un nombre de sistema Windows "HOME-OFF-D5F0AC".

Estas características se corresponden con la actividad de red generada por las herramientas "CWsandbox" del software GFI, ahora propiedad de "ThreatTrack Security".

Conclusiones

En los últimos siete años, un potente actor de amenazas llamado Darkhotel, también conocido como Tapaoux, ha llevado a cabo con éxito una serie de ataques contra una amplia gama de víctimas de todo el mundo. Emplea métodos y técnicas que van mucho más allá de los típicos comportamientos cibercriminales.

El conjunto de habilidades del grupo Darkhotel le permite lanzar ataques criptográficos interesantes, por ejemplo, la factorización de claves RSA de 512 bits. El uso de ataques de día cero es otro indicador de un potente actor de amenazas.

La selección de los altos ejecutivos de varias grandes empresas de todo el mundo durante su estancia en determinados "hoteles oscuros" es uno de los aspectos más interesantes de esta operación. El método exacto de selección aún se desconoce; por ejemplo, ¿por qué se seleccionan algunas personas y otras no? El hecho de que, en la mayoría de las ocasiones, las víctimas sean altos ejecutivos, indica que los atacantes tienen conocimiento del paradero de sus víctimas, incluidos el nombre y lugar de estancia. Esto dibuja una red oscura y peligrosa en la que los viajeros confiados pueden caer fácilmente. Aunque se desconoce el motivo exacto por el que algunos hoteles funcionan como un vector de ataque, existen ciertas sospechas que indican posiblemente un compromiso mucho mayor. Aún estamos investigando este aspecto de la operación y en el futuro publicaremos más información.

Otra interesante característica es la implementación de varios tipos de campañas, tanto con un objetivo como con un botnet. Esta característica es cada vez más común en el panorama de APT, donde se utilizan los ataques con un objetivo para comprometer víctimas importantes y operaciones de estilo botnet para vigilancia extrema o realizar otras tareas, tales como el lanzamiento de ataques de DDoS a partes hostiles o simplemente actualizar a las víctimas a herramientas de espionaje más sofisticadas.

Prevemos que el grupo Darkhotel continúe con sus actividades contra DIB, el gobierno y los sectores no gubernamentales. El apéndice publicado con este documento proporciona indicadores técnicos de compromiso que deberían ayudar a las víctimas a identificar el tráfico malicioso y permitir que los objetivos puedan protegerse mejor contra el ataque.

Kaspersky Lab Iberia

Kaspersky Lab España C/ Virgilio, nº 25, 1º B,
28223, Pozuelo de Alarcón
Madrid, España

Más detalles de contacto

Tel.: +34 91 398 3752
Fax: +34 91 518 8792

Correo electrónico: ventas@kaspersky.es
Sitio web: www.kaspersky.es