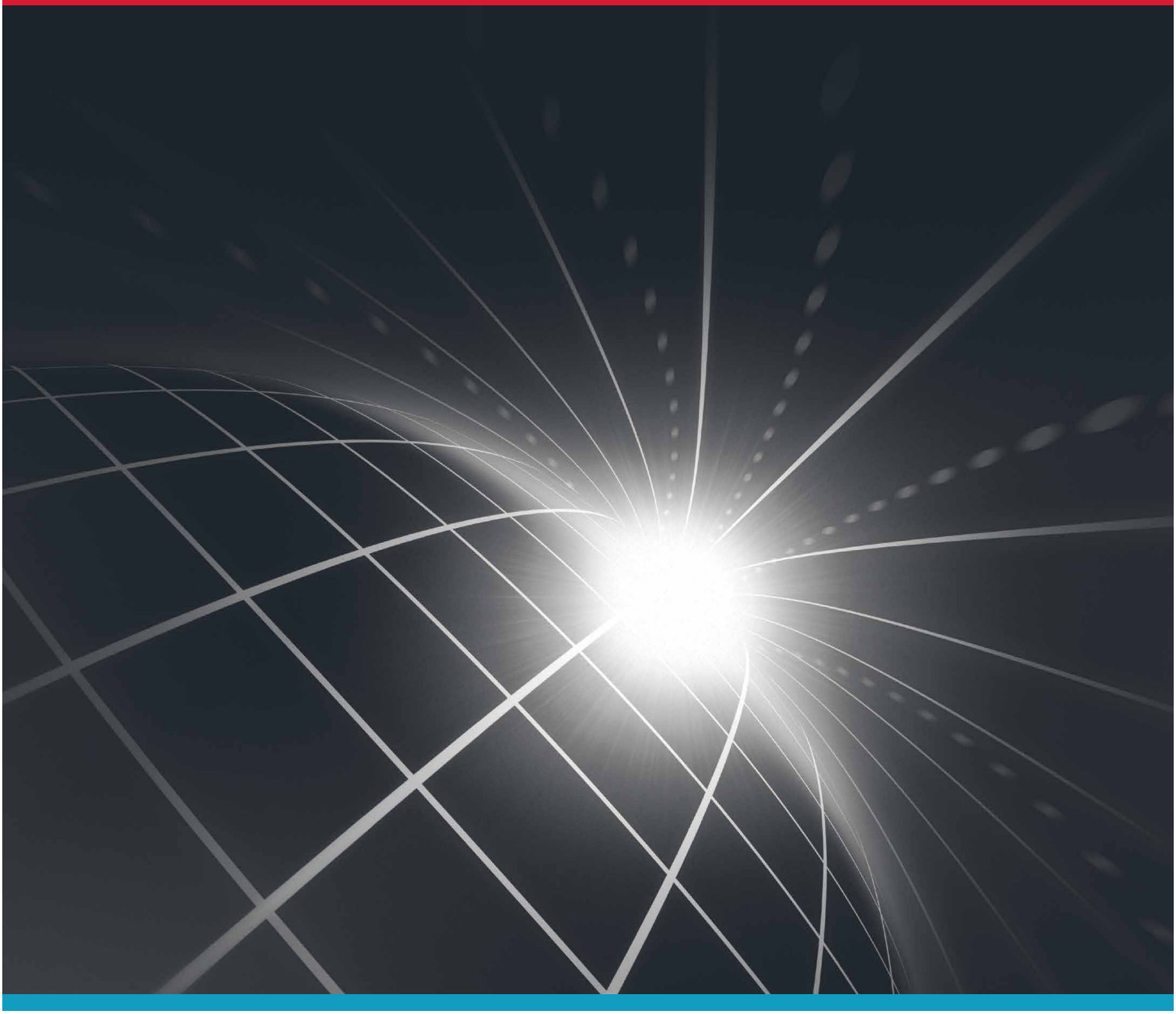
FireEye™

Pistas digitales: siete indicios para averiguar quién está detrás de los ciberataques avanzados



Índice

Resumen ejecutivo

Visto el panorama de las ciberamenazas actuales, identificar al enemigo es esencial en cualquier plan de defensa. Descubrir quiénes son los agresores, cómo trabajan y cuáles son sus objetivos es fundamental para proteger sus datos y su propiedad intelectual.

Afortunadamente, como ocurre en cualquier escena de un crimen, los malhechores dejan pistas en los sistemas informáticos que sufren el ataque. En el caso de los ciberataques avanzados, los datos del interior del código del malware, los mensajes de phishing, los servidores de comando y control (CnC) utilizados e incluso el comportamiento de los atacantes pueden servir para delatarlos. Así como el análisis de las huellas digitales, el ADN y los tejidos aportan datos clave en las investigaciones forenses criminales, la conexión de los puntos en un ciberataque avanzado puede ayudar a identificar incluso a los autores de las amenazas más sofisticadas, siempre que los investigadores sepan qué buscar.

Basándose en una muestra de casi 1500 campañas investigadas por FireEye®, este documento describe las siguientes facetas de los ataques de malware y lo que suelen revelar sobre los responsables:

- **Configuración del teclado.** Oculta en los ataques de phishing encontramos información sobre las preferencias del agresor en cuanto al teclado, que varían por idioma y región.
- **Metadatos de malware.** El código fuente del malware contiene detalles técnicos que pueden ser indicio del idioma, la ubicación y las conexiones del agresor con otras campañas.
- **Fuentes embebida.** Las fuentes utilizadas en los mensajes de correo electrónico de phishing señalan el origen del ataque. Esto ocurre incluso cuando las fuentes no se utilicen normalmente en el idioma materno del agresor.
- **Registro de DNS.** Los dominios que se emplean en los ataques señalan la posición del agresor. La información de registro duplicada puede asociar varios dominios al mismo agresor.
- **Lenguaje.** Los componentes lingüísticos incluidos en el malware suelen indicar el país de origen del agresor. Además, en ocasiones se puede revertir la ingeniería de los errores gramaticales comunes que aparecen en los mensajes de correo electrónico de phishing con el fin de determinar la lengua materna de la persona que los ha escrito.
- **Configuración de las herramientas de administración remota.** Las principales herramientas de creación de malware incluyen numerosas opciones de configuración. Estas opciones suelen ser elegidas exclusivamente por el agresor que utiliza la herramienta, lo que permite a los investigadores vincular ataques dispares a un mismo responsable de amenazas.
- **Comportamiento.** Los patrones de comportamiento, como métodos utilizados y objetivos del ataque, revelan información sobre las motivaciones y estrategias empleadas por el agresor.

El análisis de estos elementos permite a los profesionales de la seguridad avanzar enormemente en la identificación de los autores de las amenazas y defender mejor a sus empresas frente a futuros ciberataques.

Introducción

Aunque los ciberataques son cada vez más avanzados y tenaces, aún no han conseguido perpetrar lo que se conoce como el crimen perfecto. Cada fase de la cadena de ataque —reconocimiento, dotación de "armas", entrega, aprovechamiento, instalación, comando y control, y acciones sobre objetivos (normalmente filtración)[1]— puede dejar un rastro digital.

Esto se debe a que en cada fase se requiere un punto de contacto entre el agresor y el objetivo del ataque. A veces, este contacto es directo, como un mensaje de phishing. Otras veces, este contacto es indirecto, como durante una devolución de llamada que conecta las computadoras de las víctimas con el sistema del agresor. Ambos casos ofrecen oportunidades de conocer mejor al autor del ataque. Si se analiza correctamente, esta información puede ayudar a los profesionales de la seguridad a contener mejor los daños, reparar los sistemas que han sufrido el ataque y prever otras amenazas en el futuro.

Atención: aunque las técnicas forenses digitales descritas en este informe han resultado útiles a los investigadores de FireEye, los indicios con frecuencia llevan a error y son contradictorios. Analizar los indicios es complicado y debe realizarse con detenimiento; se requiere la combinación justa de ciencia y arte que pocas veces lleva a la prueba concluyente. Los ciberdelincuentes son especialistas en dar pistas falsas, luego no asuma que es cierto todo lo que ve. FireEye recomienda que, antes de sacar sus conclusiones sobre el origen de un ataque, contraste las pruebas de distintas fuentes y consulte a expertos en análisis forense digital.

1. Configuración del teclado

Los investigadores pueden determinar la configuración del teclado utilizado para crear una muestra concreta de malware examinando el atributo "charset" (juego de caracteres) del encabezado del mensaje de correo electrónico en el caso de phishing. En la mayoría de los intentos de phishing se utiliza la configuración de teclado estándar que no señala a ningún país en particular. Sin embargo, la detección de un teclado no estándar es un indicio importante.

Los investigadores de FireEye han descubierto que muchos aspectos de las campañas de malware tienen un distintivo que indica que han sido escritas en un teclado mandarín (GB2312), que se utiliza en China. Del mismo modo, el juego de caracteres KPS 9566 de Corea del Norte permite identificar las campañas que se han originado en dicha región.

Este método de rastrear los orígenes de un ataque no está exento de errores. En teoría, un ciudadano ruso podría emplear un teclado norcoreano, por ejemplo, para disfrazar su identidad y ocultar sus operaciones.

En marzo de 2012, el investigador de FireEye Alex Lanstein envió un mensaje de correo electrónico a un grupo de activistas tibetanos para avisarles de que eran el objetivo de un ciberataque. Los autores del ataque consiguieron una copia del mensaje de Lanstein de una de las víctimas y lo emplearon para acosar a los demás activistas. A diferencia del mensaje original, que utilizaba un teclado estándar occidental (Windows-1252), el remitente del señuelo utilizó una configuración de teclado GB2312 de China.

1 Eric M. Hutchins, Michael J. Cloppert y Rohan M. Amin (Lockheed Martin). "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains". Noviembre de 2010.

En la Figura 1 aparece el mensaje empleado como señuelo. En la Figura 2 se muestra el encabezado que revela la configuración del teclado.

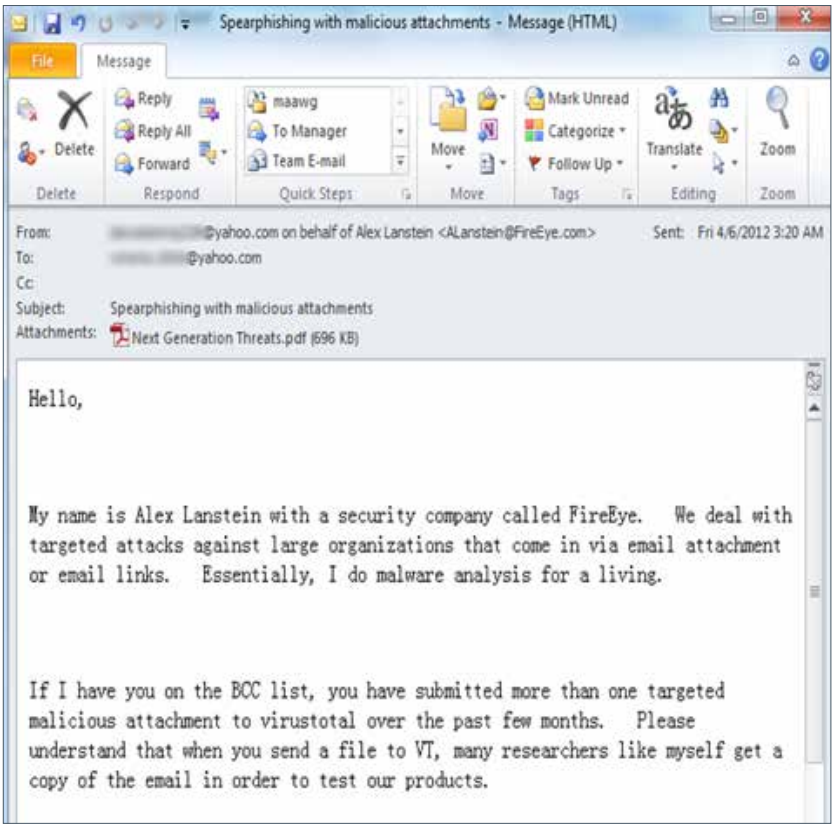


Figura 1: Mensaje de phishing enviado a activistas tibetanos.

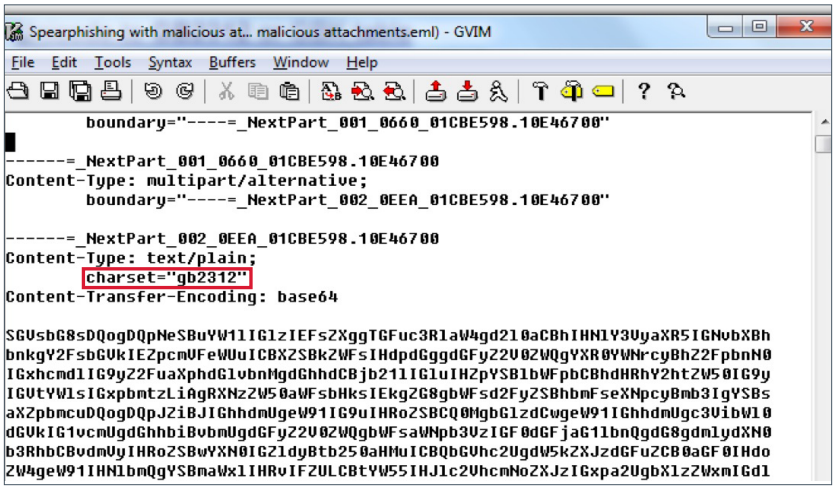


Figura 2: Codificación de juego de caracteres en mensaje de phishing (véase la Figura 1).

2. Metadatos de malware

En el código ejecutable del malware aparece el directorio de origen original que organiza el código fuente. De la misma forma, en los programas desarrollados en C++ aparece un nombre de proyecto. Este código subyacente puede revelar el idioma o país de origen del agresor, incluso cuando el código y otros aspectos del ataque se han diseñado en el idioma de la víctima.

En la Figura 3 se puede ver el código fuente de un reciente ataque de tercera fase. En este caso, el autor del ataque insulta a un desarrollador de software antivirus chino, Beijing Rising (fonéticamente "Ruixing") International Software Co., utilizando un término vulgar.

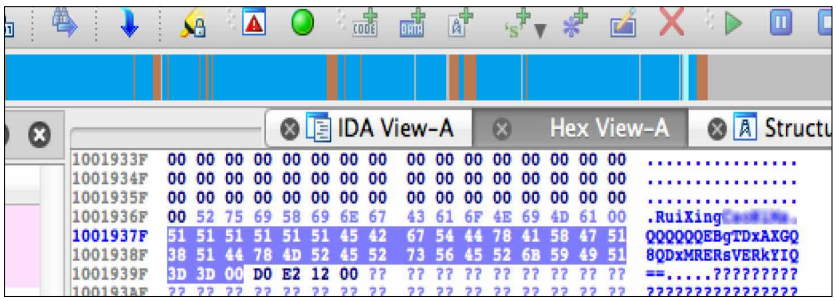


Figura 3: Código fuente de malware con insultos al desarrollador de software antivirus chino Beijing Rising (fonéticamente "Ruixing"). En la captura de pantalla hemos ocultado el insulto.

La Figura 4 muestra el código fuente de un ataque de segunda fase que no se había publicado antes, un archivo ejecutable disfrazado como archivo PNG. Se instaló en el endpoint tras el primer ataque. El código incluye una referencia al archivo de depuración de proceso (PDB) que se encuentra en la unidad de disco duro del desarrollador del malware en "E:\pjts2008\moon\Release\MoonClient2.pdb". (Los archivos PDB se crean para los programas escritos en Windows .NET Framework). El archivo "MoonClient" que se menciona es una variante del malware WEBC2 utilizado por el grupo de hackers chinos APT1, también conocido como CommentGroup.

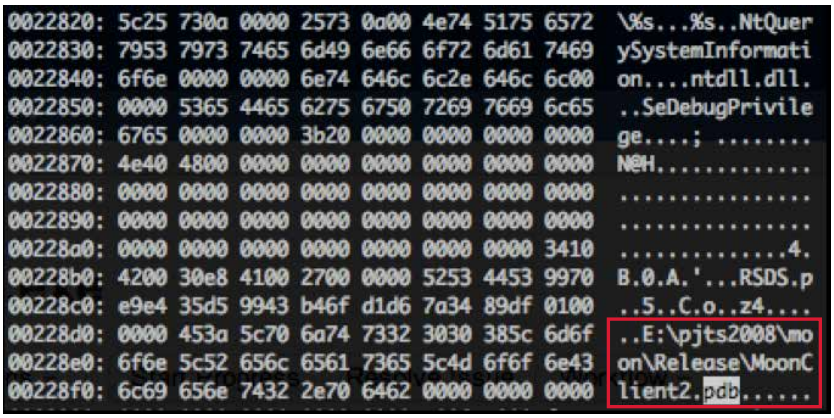
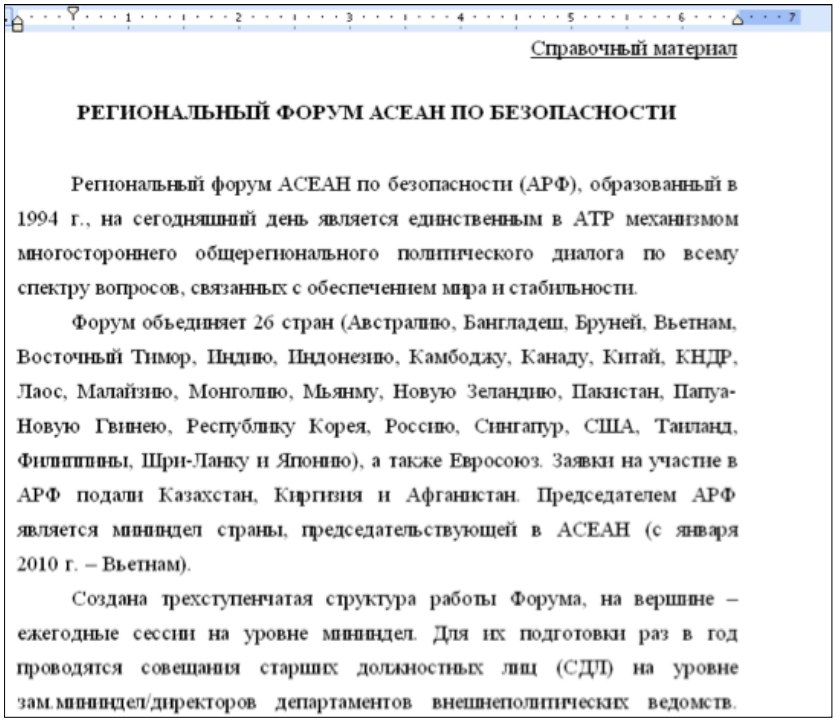


Figura 4: Archivo ejecutable descodificado (referencia a PDB resaltada).

3. Fuentes embebidas

Al igual que el atributo del juego de caracteres que se describe en la sección "Configuración del teclado", la fuente empleada en los mensajes de phishing y en otros documentos maliciosos puede resultar de utilidad para averiguar el origen de un ataque APT.

Analicemos el ejemplo de la amenaza avanzada persistente (APT) Sanny descubierta por los investigadores de FireEye recientemente. En la Figura 5 se muestra el documento utilizado como señuelo para atraer a las víctimas.



Справочный материал

РЕГИОНАЛЬНЫЙ ФОРУМ АСЕАН ПО БЕЗОПАСНОСТИ

Региональный форум АСЕАН по безопасности (АРФ), образованный в 1994 г., на сегодняшний день является единственным в АТР механизмом многостороннего общерегионального политического диалога по всему спектру вопросов, связанных с обеспечением мира и стабильности.

Форум объединяет 26 стран (Австралию, Бангладеш, Бруней, Вьетнам, Восточный Тимор, Индию, Индонезию, Камбоджу, Канаду, Китай, КНДР, Лаос, Малайзию, Монголию, Мьянму, Новую Зеландию, Пакистан, Папуа-Новую Гвинею, Республику Корея, Россию, Сингапур, США, Таиланд, Филиппины, Шри-Ланку и Японию), а также Евросоюз. Заявки на участие в АРФ подали Казахстан, Киргизия и Афганистан. Председателем АРФ является министр страны, председательствующей в АСЕАН (с января 2010 г. – Вьетнам).

Создана трехступенчатая структура работы Форума, на вершине – ежегодные сессии на уровне министров. Для их подготовки раз в год проводятся совещания старших должностных лиц (СДЛ) на уровне зам.министров/директоров департаментов внешнеполитических ведомств.

Figura 5: Documento utilizado como señuelo escrito en caracteres rusos, pero con una fuente coreana.

Aunque dicho documento se escribió en ruso para dirigir el ataque contra intereses rusos, utilizaba las fuentes coreanas Batang y KPCheongPong. El hecho de que se eligieran estas fuentes confirma las pruebas de otras fuentes que apuntaban a Corea del Norte, como el nombre del autor y los servidores CnC utilizados en el ataque. Combinadas, las pruebas demostraban los orígenes del agresor.

4. Registro de DNS

En algunos casos, los autores de las amenazas pagan para registrar dominios con el fin de eludir la detección de defensas de malware estándar, como listas negras de dominios. Con frecuencia estos registros de DNS son un claro indicio del país de origen del agresor.

Incluso los registros de DNS que emplean nombres y direcciones falsos pueden servir para señalar al culpable. En algunos casos, los agresores reutilizan datos de contacto falsos en varios dominios. Esta circunstancia permite a los investigadores relacionar distintos ataques con un solo autor de amenazas y recomponer las piezas de información recogidas de cada ataque.

Ejemplo: el conocido como caso "Sin Digoo". Entre 2004 y 2011, alguien, utilizando una dirección de correo electrónico Hotmail, registró varios dominios con los mismos nombres. Esta persona incluyó una dirección física como apartado de correos en la ciudad de "Sin Digoo, Californa", según parece un error ortográfico de "San Diego". Gracias a la información de registro duplicada, los investigadores pudieron conectar los ataques de malware individuales con un patrón de amenazas persistentes avanzadas de mayor alcance[2].

De esta forma utilizó también el investigador de malware Nart Villeneuve la información de registro de DNS para vincular a la Universidad de Zhejiang de China a un ataque de 2010 dirigido contra Amnistía Internacional en Hong Kong, periodistas y activistas pro derechos humanos.[3]

FireEye hizo uso hace poco tiempo de datos de registro de DNS para establecer la relación entre varias muestras de malware cargadas al sitio web de comprobación de virus VirusTotal (véase la Figura 6). Parece que el agresor cargó las muestras para probar si la comunidad antivirus las detectaba.

Figura 6: Ejemplo de carga de muestra de malware.

Si bien el agresor ocultó la primera fase (es decir, el intento de comando y control), la segunda, que solo se revela al ejecutar el malware en una infraestructura real, utiliza el dominio secureplanning.net (Figura 7), registrado por alguien con una dirección en Nueva Delhi supuestamente falsa.

```
POST /download/ad.php HTTP/1.0
Accept: text/plain, text/html
Content-Type: multipart/form-data; boundary=--------------------------
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV2)
Host: secureplanning.net
Content-Length: 4565
Pragma: no-cache
```

Figura 7: Información de carga de malware en VirusTotal.

2 Joe Stewart (Dell SecureWorks). *The Sin Digoo Affair.* Febrero de 2012.

3 Villeneuve, Nart. *Nobel Peace Prize, Amnesty HK and Malware*. Noviembre de 2010.

La información de registro no es un indicador perfecto; un agresor lo suficientemente sofisticado puede generar datos de contacto falsos para alejar a los investigadores de la pista. Pero en este caso, los investigadores de FireEye observaron que se habían cargado en VirusTotal distintas versiones del malware con ligeras modificaciones más de 15 veces. Todas las muestras intentaban conectarse a dominios registrados con la misma dirección en Nueva Delhi, lo que establecía un claro patrón.

5. Lenguaje

A menudo hay muchos indicadores de que el lenguaje utilizado en una campaña de malware no es el de un hablante nativo. A veces dichos indicadores pueden incluso servir para revelar el origen del agresor.

Los errores de tecleo y faltas de ortografía evidentes son señales claras. En otros casos, tras un análisis más detallado se descubre que el agresor ha utilizado un sitio de traducción automática. Los investigadores, que saben cómo traducen los sitios de traducción más populares determinadas palabras y frases, pueden determinar el idioma original de los mensajes de correo electrónico de phishing utilizados en un ataque.

Examinemos, por ejemplo, el ataque contra RSA que dio tanto que hablar en 2011. Dos grupos que se creía trabajaban para el gobierno consiguieron acceso a la red de la empresa para extraer datos sobre los productos SecurID de RSA. El ataque aprovechó una vulnerabilidad desconocida de Flash, lo que reveló un alto grado de sofisticación técnica. Pero, como muestra la Figura 8, la redacción del mensaje de phishing en inglés no era muy fluida e incluía una petición bastante tosca para que se abriera el adjunto, que sin embargo, funcionó. Estas características sugieren que el agresor no es angloparlante nativo.

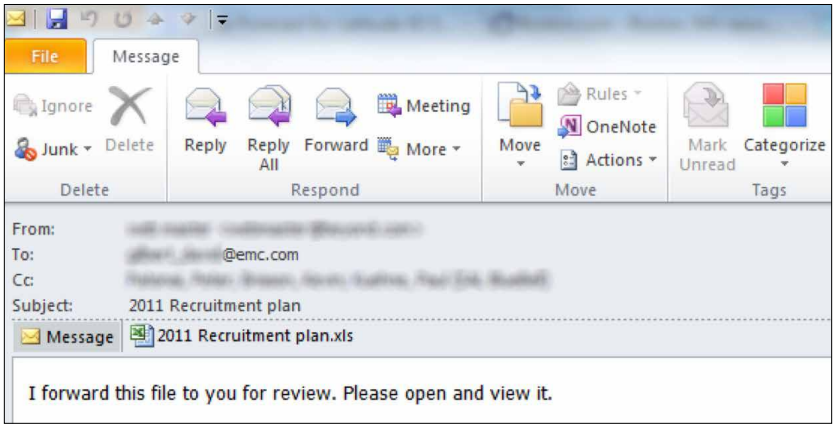


Figura 8: Mensaje de correo electrónico de phishing utilizado en un ataque de 2011 contra RSA.

En otras ocasiones, el lenguaje utilizado en el interior del malware puede ayudar a determinar la identidad de los agresores. En la Figura 9, un fragmento de código del malware Backdoor.LV utiliza nombres y palabras en árabe para "señalar" los objetivos.

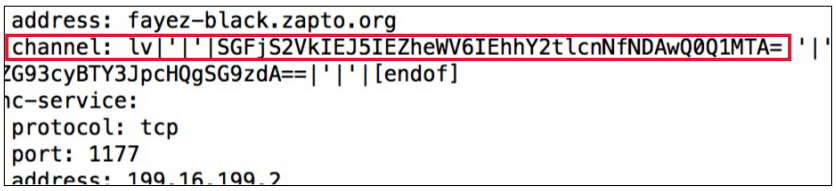


Figura 9: Fragmento del malware Backdoor.LV. Al descodificar la parte resaltada se obtiene la cadena que muestra la Figura 10.

Al descodificar la cadena de caracteres se obtiene "HacKed By Fayez Hacker_400CD510", como muestra la Figura 10.

Figura 10: Backdoor.LV descodificado

Parece que el código que se muestra en la Figura 11 es del mismo autor. La cadena de caracteres, al descodificarse, muestra el identificador "400CD510" (véase la Figura 12), esta vez en árabe.

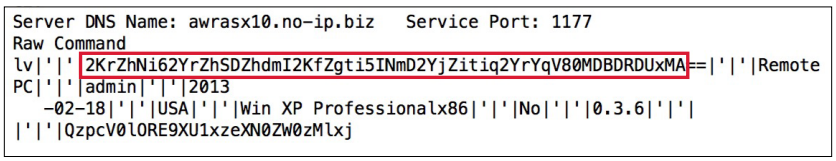


Figura 11: Otro fragmento de malware vinculado a Fayez. Al descodificar la parte resaltada se obtiene la cadena que muestra la Figura 12.

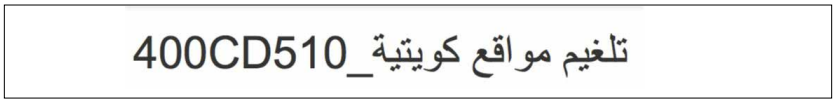


Figura 12: La referencia 400CD510, con caracteres en árabe

6. Configuración de las herramientas de administración remota

Las herramientas de administración remota (RAT, en sus siglas en inglés) son un tipo de malware que concede a los agresores control en tiempo real de la computadora de una víctima. Las herramientas admiten diversas funciones, como registro de pulsaciones, capturas de pantalla, capturas de video, transferencias de archivos, administración de sistemas y acceso al shell de comandos. Disponibles para su venta al público o incluso gratis, las herramientas RAT son muy atractivas para los agresores, ya que normalmente ya han sido probadas y ofrecen multitud de funciones.

Estas herramientas pueden dificultar la atribución de la autoría, ya que las puede utilizar cualquiera y muchos grupos diferentes usan las mismas herramientas. Sin embargo, sus numerosas opciones de personalización crean una combinación de parámetros que es particular de cada agresor. Si en varios ataques se utiliza una herramienta RAT configurada de la misma forma, todo apunta a que se trata del mismo agresor.

Un ejemplo es la RAT Poison Ivy, que tiene ocho años. Entre las opciones de configuración más reveladores están el ID, grupo, contraseña y mutex.

En la Figura 13 se muestran los campos de ID y contraseña de la ventana de configuración de conexión de Poison Ivy.
La Figura 14 muestra el campo mutex en la ventana de configuración avanzada.

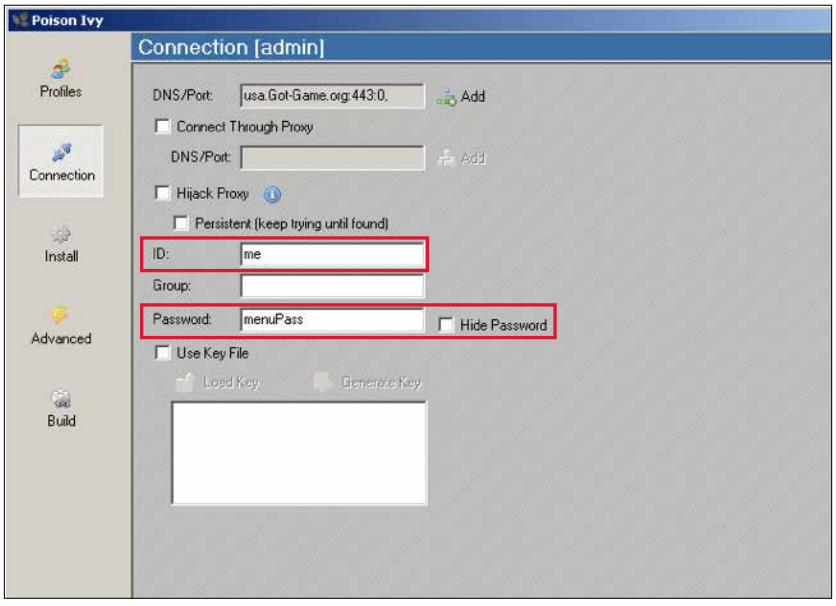


Figura 13: Ventanas de configuración de conexión de Poison Ivy (con los campos de ID y contraseña resaltados).

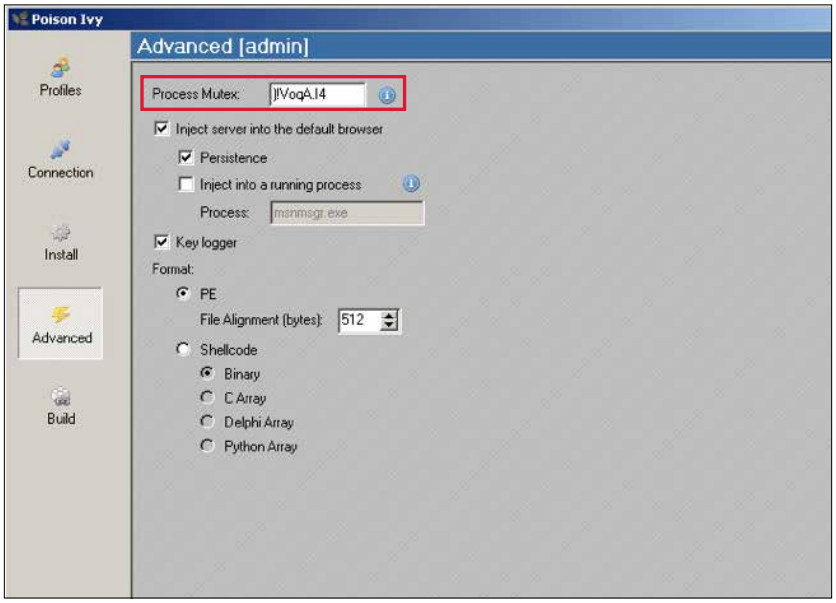


Figura 14: Ventana de configuración avanzada de Poison Ivy (campo de mutex del proceso resaltado).

Estas opciones de configuración pueden extraerse de las RAT compiladas utilizando Volatility, una infraestructura de análisis forense de memoria de archivos de código abierto que funciona con volcados de memoria.

En Poison Ivy, el agresor define los campos de ID y grupo para identificar y organizar a los grupos de víctimas. Cuando aparece el mismo ID o grupo en varios ataques, los investigadores pueden deducir que existe un vínculo entre ellos.

El campo de contraseña se emplea como una clave para cifrar las comunicaciones de Poison Ivy. De manera predeterminada, es "admin" y suele permanecer sin modificar. Pero, cuando se definen de forma activa, las contraseñas pueden servir como una especie de huellas digitales. Suelen ser exclusivas y los agresores las reutilizan con frecuencia en campañas de ataques selectivos.

En software, un mutex (o exclusión mutua) es un objeto de programa que permite garantizar que varios subprocesos de un programa no van a intentar utilizar los mismos recursos al mismo tiempo. En Poison Ivy, el mutex sirve como marcador para determinar si la herramienta ya está en ejecución en un sistema infectado, de forma que no se ejecute más de una instancia. Poison Ivy emplea el valor predeterminado de mutex)!VoqA.I4. Como las contraseñas definidas en Poison Ivy, cualquier valor distinto del predeterminado suele ser exclusivo y se convierte en un útil identificador.

7. Comportamiento

El ser humano es un animal de costumbres. Como todo el mundo, los autores de las amenazas muestran con frecuencia patrones fijos de comportamiento a lo largo del tiempo. Se centran en los mismos objetivos, utilizan los mismos servidores CnC y dirigen su atención a los mismos sectores. La repetición de estas tácticas puede revelar estrategias, objetivos y movimientos de los agresores. Y es aquí donde la identificación del perfil del autor de la amenaza puede servir de ayuda. Al igual que la determinación de los perfiles delictivos ayuda a los detectives a cerrar el cerco sobre los posibles sospechosos, los profesionales de la seguridad pueden observar a los agresores a lo largo del tiempo y registrar sus patrones de comportamiento. Utilizando esta información, los investigadores pueden identificar la propensión de un grupo concreto a determinados estilos y procedimientos.

De la misma forma, las herramientas y tácticas empleados por un agresor en sus ataques pueden ayudar a identificarle. En la Figura 15 se muestran cuatro ataques diferentes que utilizan distintos exploits, métodos de engaño y medios de implantación de malware durante la primera fase del ataque. Sin embargo, todos van dirigidos contra activistas religiosos. Y, como revela la información del encabezado (véase la Figura 16), todos se enviaron desde el mismo servidor; algunos desde el servicio de correo electrónico Yahoo! Messenger y otros a través de una secuencia de comandos. Esta prueba lleva a varios autores del mismo equipo y que utilizan la misma infraestructura.

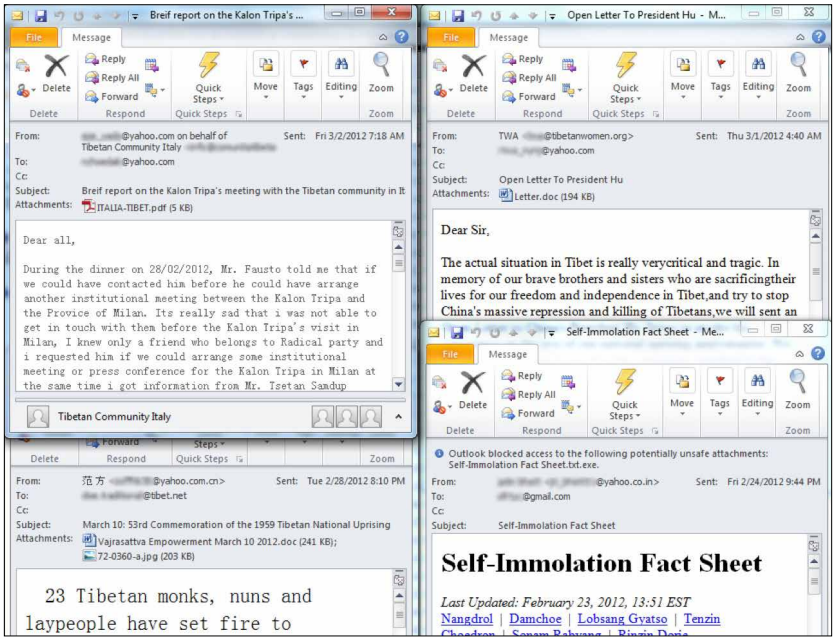


Figura 15: Cuatro mensajes de phishing.

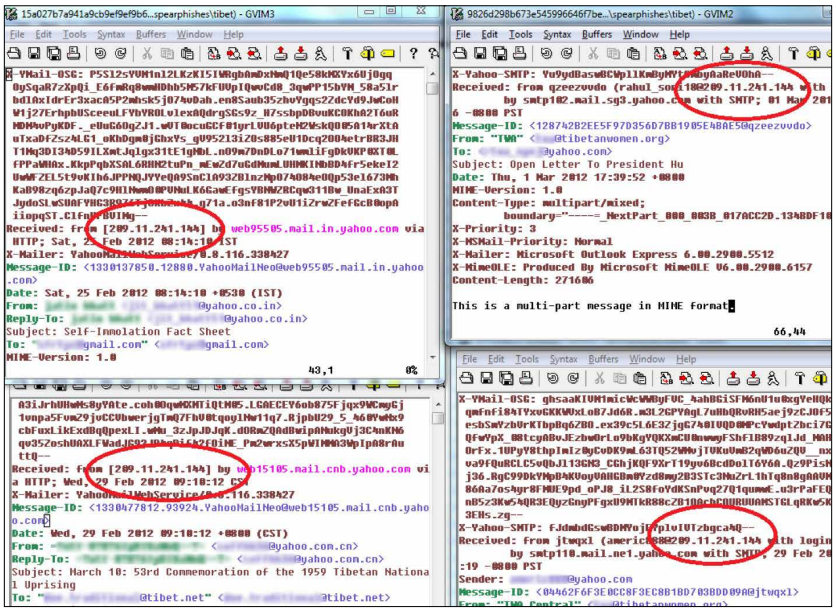


Figura 16: Información de encabezado de mensaje de phishing (direcciones IP resaltadas).

Conclusión

Por sí solos, ninguno de estos elementos constituye una prueba absoluta. Sin embargo, cuando varios indicios señalan al mismo agresor, los investigadores pueden concluir con un alto nivel de probabilidad quién está detrás de una campaña concreta. Esa información puede ayudar a prever métodos de ataque y motivaciones, lo que permite a los profesionales de la seguridad anticiparse a futuros ataques y proteger los sistemas y datos a los que se dirigen.

Cuando lo que urge es contener un ataque y reparar los daños, determinar el origen puede parecer secundario. Pero no lo es. Cuando una organización que ha sido víctima de un ataque conoce los métodos y el objetivo del autor, puede usar esa información para:

- Dedicar recursos inmediatamente a la protección de los datos vulnerables
- Conseguir ayuda adicional, ya sea de recursos internos o de las fuerzas de seguridad
- Examinar más detenidamente otros vectores, que posiblemente se habían pasado por alto, utilizados por los agresores en otras campañas

Conocer el origen de un ataque puede resultar especialmente útil cuando se combina con la información obtenida de ataques anteriores del mismo autor, ocurridos en otros lugares. Soluciones como la nube FireEye® Dynamic Threat Intelligence™, que comparte información de amenazas de manera anónima con la creciente base de clientes de FireEye, proporcionan información sobre tácticas, protocolos, puertos y canales de devolución de llamada utilizados por los agresores.

Para obtener más información sobre cómo puede ayudarle la plataforma de protección contra amenazas de FireEye a defenderse mejor contra los ciberataques, visite FireEye en http://www.FireEye.com.

Acerca de FireEye

FireEye® ha inventado una plataforma de seguridad basada en una máquina virtual, con un fin concreto, que proporciona protección contra amenazas en tiempo real a empresas y Administraciones en todo el mundo contra la próxima generación de ciberataques. Estos sofisticadísimos ciberataques sortean con facilidad las defensas basadas en firmas, como los firewalls de próxima generación, sistemas de prevención de intrusiones, antivirus y puertas de enlace. La plataforma de FireEye ofrece seguridad contra amenazas dinámicas en tiempo real sin el uso de firmas para proteger a la organización contra los vectores de amenazas principales, como la Web, el correo electrónico y los archivos, en las distintas fases del ciclo de vida de un ataque. El alma de la plataforma de FireEye es un motor de ejecución virtual, complementado por información dinámica sobre amenazas, para identificar y bloquear ciberataques en tiempo real. FireEye tiene más de 1000 clientes en más de 40 países, incluidas un tercio de las empresas del índice Fortune 100.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408.321.6300 | LATAM@FireEye.com | www.FireEye.com