



INFORME DE AMENAZAS GLOBALES

2016

Avance sin miedo

Emitido por
FORCEPOINT Security Labs™

ÍNDICE

RESUMEN EJECUTIVO	02
INFORME PRINCIPAL	06
AMENAZA INTERNA	06
AMENAZAS AVANZADAS: CASOS DE ESTUDIO DEL EQUIPO DE INVESTIGACIONES ESPECIALES	10
LA WEB Y EL CORREO ELECTRÓNICO: UNA AMENAZA DOBLE	20
EL AVANCE HACIA LA NUBE	22
REFLEXIONES DE LA OFICINA DEL CSO	25
CONCLUSIÓN	29

RESUMEN EJECUTIVO



El año pasado se produjeron cambios importantes que modificaron la naturaleza de los ataques ciberneticos. Si bien, aún es común el malware de robo de datos que pasa inadvertido, el empleado moderno autónomo podría ser la mayor amenaza para los datos de su organización. Hay un nuevo grupo de audaces atacantes que utilizan ransomware y rompen con esta acción encubierta simplemente afirmando que han cifrado sus datos y piden un rescate por ellos – en una ruta mucho más rápida para obtener ganancias. Al enfrentarse con nuevas herramientas contra el malware, los atacantes reciclan métodos de ataque del pasado y vuelven a utilizar archivos de Microsoft® Office cargados de macros que terminan en los escritorios. La creciente migración a informática en la nube con controles inconsistentes está generando graves desafíos a la seguridad. Mientras tanto, en segundo plano, nuevos botnets evalúan la capacidad de la comunidad de seguridad para detectar e interceptar los objetivos tácticos de corto plazo y de los adversarios en general.

Por consiguiente, la prioridad es informar a los tomadores de decisiones sobre el contexto crucial en torno a estos ataques que proliferan en todo el mundo y dentro de sus redes, para que puedan aplicar la mayor cantidad de tiempo y recursos a las amenazas más graves. Acorde a su lema “Avance sin miedo”, el equipo de Security Labs, el equipo de Investigaciones Especiales (SI) y el equipo de la Oficina del CSO (OoCSO) de Forcepoint, continuamente sortejan los obstáculos densos y complejos de la actividad de ataques en todo el mundo e identifican las amenazas e innovaciones que más importan, ofreciendo consejos a cada paso.

El **Informe de Amenazas Globales 2016** de Forcepoint es un análisis definitivo de muchas de las amenazas a la seguridad cibernética que más impacto tienen en la actualidad, con consecuencias de gran magnitud técnica, operativa y de costos en las organizaciones afectadas. Cada sección de este informe finaliza con consejos del equipo de Forcepoint Security Labs sobre el modo de enfrentar de la mejor manera las amenazas descritas. Los capítulos incluyen:

1. AMENAZAS INTERNAS: MALICIOSAS Y ACCIDENTALES

La investigación de Forcepoint y de terceros (página 5) muestra que monitorear la actividad del personal que tiene acceso a información privilegiada y dar cuenta de las credenciales con privilegios son cuestiones de seguridad a las que las organizaciones se sienten menos preparadas para hacer frente. El 30% de la seguridad permanece concentrada en las defensas perimetrales¹, y menos del 40% de las organizaciones encuestadas tiene un presupuesto dedicado a programas de detección de amenazas internas². Aun así, muchos empleados tienen el poder de conectarse de forma remota y desde dentro y fuera de las redes tienen acceso constante a servidores (donde residen sus datos más confidenciales).

2. AMENAZAS AVANZADAS Y CASOS DE ESTUDIO DEL EQUIPO DE INVESTIGACIONES ESPECIALES: PRESENTACIÓN DE “JAKU” Y CRACKEO DE UN RANSOMWARE

Una de las mejores ventanas para conocer las amenazas avanzadas la proporciona el equipo de Investigaciones Especiales (SI) de Forcepoint, un grupo de elite integrado por investigadores de amenazas y expertos en respuestas a incidentes que se especializa en las amenazas que muestran herramientas, tácticas y procesos (TTP) únicos. El año pasado, los logros destacados del trabajo del equipo de SI incluyeron el descubrimiento de una nueva campaña de botnet llamada JAKU y el crackeo de una cepa persistente de un ransomware conocido como Locky.

3. LA WEB Y EL CORREO ELECTRÓNICO: UNA AMENAZA DOBLE

Los empleados que trabajan aún en los lugares más restringidos y seguros, típicamente no pueden ser productivos sin usar la web y el correo electrónico, lo que hace de estos medios un canal ideal para suministrar cargas maliciosas en forma de enlaces a sitios web cargados de malware y adjuntos de correo electrónico maliciosos. Casi el 92% del correo electrónico no deseado (p. ej., spam, malicioso) ahora contiene un URL, y la presencia de macros maliciosas en el correo electrónico ha aumentado un 44.7% (página 20).

4. LAS PREOCUPACIONES POR LA SEGURIDAD AÚN OBSTRUYEN EL AVANCE HACIA LA NUBE

Muchas empresas han compensado las preocupaciones de seguridad con el costo, la escalabilidad y la accesibilidad de la informática en la nube. Aun así, estas situaciones presentan dolores de cabeza para muchos usuarios potenciales de la nube preavidos de cómo los controles de seguridad inconsistentes entre los proveedores de servicios en la nube y sus propios entornos podrían afectar la protección de los datos. En cierta medida, irónicamente los CIO y CISOs que se resisten a la adopción de la nube de todos modos deben lidiar con las consecuencias de las decisiones independientes de los empleados al utilizar las aplicaciones en la nube de su preferencia para productividad y conveniencia personal. Más de los 80% de los tomadores de decisiones encuestados consideran que el “shadow” IT (hardware o software oculto) tiene graves consecuencias³.

5. REFLEXIONES DE LA OFICINA DEL CSO DE FORCEPOINT

En 2015, el equipo de la Oficina del CSO de Forcepoint vio la actividad de fusiones y adquisiciones (M&A) como uno de los mayores catalizadores de riesgo de seguridad cibernética en los sectores de la industria. Como un ejemplo del mundo real, la OoCSO saca provecho de la experiencia de sus líderes de seguridad cibernética y protección de datos para resumir el modo en que se administraron los controles de seguridad integrales durante las actividades de M&A que dieron origen a Forcepoint – la integración de las empresas Websense® y Raytheon Cyber Products (RCP), y el negocio de firewalls de próxima generación (NGFW) de Stonesoft®.

FORMACIÓN DE FORCEPOINT

Forcepoint, una compañía nueva con un enfoque moderno en seguridad cibernética, fue presentada por primera vez el 14 de enero de 2016. Forcepoint es una asociación conjunta de Raytheon Company y Vista Equity Partners, y combina tres empresas exitosas: Websense, Raytheon Cyber Products y Stonesoft, cada una con una vasta historial de innovación. Como asociación conjunta, Forcepoint cuenta con poderosas ventajas para ayudar a mantener seguros a sus clientes: el acceso constante a amplios recursos, la propiedad intelectual y la experiencia cibernética de Raytheon para solucionar los problemas más difíciles del ámbito cibernético. A lo largo de este informe, mencionaremos algunas de las maneras en que el “estar potenciados por Raytheon” proporciona a Forcepoint y a nuestros clientes una ventaja vital e inigualable en el difícil entorno actual de la información.

AMENAZAS INTERNAS

Las amenazas internas se refieren a ataques que se originan o reciben colaboración (voluntaria o involuntaria) desde adentro de una organización. Los atacantes se enfocan en empleados que tienen acceso a información privilegiada dentro de una organización, socios comerciales y proveedores a teceros, obteniendo acceso a las redes mediante la manipulación del personal para que revelen sus credenciales. Con estas credenciales robadas, los delincuentes se mueven por las redes, tienen acceso a datos confidenciales y los extraen, con frecuencia sin ser detectados hasta que es demasiado tarde. Las fugas de datos provocadas por amenazas internas continúan aumentando, y la fuente principal de los problemas son los empleados involucrados de manera accidental en una amenaza. De las firmas encuestadas por Forrester que sufrieron una fuga de datos en 2015, la causa principal fueron los incidentes internos, y más del 50% de estos incidentes se debió al mal uso involuntario o a un error de un usuario⁴, conocido como “empleado involucrado de manera accidental en una amenaza”.

EJEMPLOS DE EMPLEADOS INVOLUCRADOS DE MANERA ACCIDENTAL EN UNA AMENAZA:

- ▶ El empleado hace clic en un enlace sospechoso en un mensaje de correo electrónico sin saber que está habilitando la descarga de código malicioso en su máquina.
- ▶ El empleado utiliza una unidad USB que “encontró” (un estudio del Laboratorio Nacional de Idaho reveló que el 20% de los empleados conectados encontraron unidades USB en computadoras del trabajo⁵).
- ▶ El empleado pierde su computadora portátil, tablet o dispositivo de almacenamiento con información de propiedad exclusiva de la empresa.
- ▶ El empleado ignora la política de seguridad relacionada con llevarse trabajo al hogar para usarlo después del horario de trabajo.

MÉTODOS DE PRUEBA INIGUALABLES.

El equipo de investigadores de seguridad de Raytheon aprovecha las últimas tecnologías para evaluar vulnerabilidades, reducir las superficies de amenazas y maximizar la eficacia de la seguridad. Esto incluye cientos de millones de pruebas por semana, análisis de software estático y dinámico, compromisos de colaboración y de no colaboración, emulación de redes de más de 100,000 puntos finales y procesos para convertir los indicadores de amenazas en acciones defensivas.

De acuerdo con la investigación del Ponemon Institute⁶ patrocinada por Forcepoint, los empleados representan la mayor amenaza para la seguridad de una compañía en gran medida debido a que el abuso por parte de empleados dentro de la misma organización puede ser difícil de detectar. Por ejemplo, las credenciales robadas de cuentas válidas de usuarios con frecuencia se utilizan para llegar a datos confidenciales a los que el usuario legítimo normalmente tendría acceso, específicamente para evitar levantar cualquier sospecha. Esto se repitió en una encuesta realizada en marzo de 2016⁷, en la que se descubrió que la detección de actividad maliciosa de empleados dentro de una organización o el secuestro de credenciales de usuarios con privilegios por parte de un hacker eran las principales áreas para las cuales los bancos se sentían menos preparados. La creciente popularidad de realizar negocios desde dispositivos personales. (Conocidos como “Trae tu propio dispositivo” (BYOD: Bring Your Own Device) se suma a la complejidad de la amenaza interna, creando más vías para que los hackers afiancen su posición sin ser detectados por los equipos de seguridad. Como resultado de esto, las organizaciones están constantemente equilibrando el acceso a los datos con el riesgo de pérdida o mal uso de los mismos.

Con frecuencia, el vínculo que lleva a la pérdida involuntaria de datos confidenciales es el usuario que maneja los datos de manera inapropiada porque no conoce las prácticas de seguridad eficaces o no tiene cuidado al emplearlas.

El error o negligencia de los empleados fueron los responsables de casi el 15% de los incidentes de fugas de datos en 2015⁸

... y es fácil ver por qué, cuando un poco menos de la mitad del personal conoce las políticas de seguridad de la empresa⁹.

A pesar del aumento del daño (cuyo resultado más común es la pérdida más frecuente de credenciales de autenticación, propiedad intelectual, datos financieros corporativos e información de identificación personal [PII]), las organizaciones continúan utilizando medidas ineficaces para educar al personal y los empleados siguen sin saber cómo llevar a cabo buenas prácticas de seguridad en el trabajo¹⁰. Siendo las amenazas internas un peligro claro y presente, ¿por qué las defensas perimetrales continúan siendo una prioridad más que los programas de detección de amenazas internas?

Un reciente estudio de Ponemon¹¹ brinda algo de información al respecto. Si bien es un problema reconocido, menos del 40% de las organizaciones encuestadas tenía un presupuesto dedicado a un programa de detección de amenazas internas. Citando la falta de información contextual junto con volúmenes de falsos positivos y visibilidad insuficiente, la mayoría confiaba en las herramientas existentes que no estaban preparadas para resolver el problema. Actualmente se está desarrollando una tecnología más sofisticada que combina la prevención de la pérdida de datos (DLP) y el análisis del comportamiento de los usuarios que se relaciona con la actividad de otros sistemas empresariales y de TI (como registros de acceso RFID y registros de IP), para determinar si una amenaza proviene de un atacante desde adentro de una organización o de un enmascarado malicioso que utiliza credenciales robadas.

Pero la amenaza interna no es solo un problema de TI; es un problema que también debe involucrar al personal. Un programa eficaz de detección de amenazas internas incorpora controles tecnológicos con planes de gestión de riesgos y capacitación de los empleados sobre mejores prácticas. Los componentes clave de un programa exitoso de detección de amenazas internas incluyen:

- ▶ **Políticas:** comunicar las políticas referentes a cómo se debe utilizar la tecnología dentro de una organización, desde los dispositivos apropiados hasta el manejo de datos y el uso de Internet.
 - ▶ **Procesos:** aplicar la segregación apropiada de tareas y otros puntos de control en los procesos.
 - ▶ **Controles tecnológicos:** limitar el acceso según los principios de menos privilegios, en función del rol asignado a cada empleado.
 - ▶ **Gestión de riesgos:** identificar y desarrollar un plan de gestión de riesgos para darles la mayor prioridad a las áreas de mayor riesgo.
 - ▶ **Auditoría y monitoreo:** verificar que cada uno de los componentes clave se implemente y cumpla con las necesidades de la organización.

CASO DE ESTUDIO DE AMENAZA INTERNA: LOS DATOS ENTRENTAN UNA REDUCCIÓN DE PERSONAL

Según una encuesta de seguridad de Forrester¹³, el 39% de las fugas de datos de los últimos 12 meses fueron el resultado de un incidente proveniente desde adentro de una organización. De estos, el 26% fue el resultado de abusos deliberados o intención maliciosa, mientras que el 56% fue resultado del mal uso involuntario de datos (el 18% fue una combinación de ambos).

El siguiente caso de estudio de Forcepoint, que se comparte por primera vez aquí, ilustra un escenario típico de una amenaza interna. Después de un proceso de fusión y adquisición, un cliente comenzó el proceso de reducción de su personal de ingeniería de software. Se les comunicó a los empleados sobre los inminentes despidos, algunos inmediatos, otros después de finalizados los proyectos en curso. Se ofreció un paquete de cesantía generoso, que incluía un año completo de pago, supeditado a que la propiedad intelectual y los bienes permanecieran en la compañía. Independientemente de esto, un sorprendente número de ingenieros regresó a sus escritorios y comenzó a intentar robar datos confidenciales. Habiéndose preparado para este escenario, la organización empleó la tecnología SureView® Insider Threat de Forcepoint para observar las conductas de los empleados de alto riesgo (comparadas con un historial de 30 días de conductas diarias típicas). Como resultado de esto, la tecnología de Forcepoint detectó operaciones atípicas: intentos de copiar y guardar archivos en dispositivos de almacenamiento USB o archivos de correo electrónico y el envío de código fuente a través de canales web para almacenarlo en la nube. SureView Insider Threat logró detener las fugas y, lo más importante, la compañía pudo proteger su propiedad intelectual más valiosa a través de la identificación de los empleados que violaron el acuerdo de cesantía al intentar robar los datos. Si bien este caso particular ilustra al empleado malicioso, un empleado involucrado de manera accidental en una amenaza (cuyas credenciales fueron robadas o cuya computadora fue secuestrada) podría fácilmente activar las mismas alertas a través de movimiento inusual en la red, acceso después del horario de trabajo o transferencias de datos.



AMENAZAS AVANZADAS

CASOS DE ESTUDIO DEL EQUIPO DE INVESTIGACIONES ESPECIALES

Un dramático aumento en el tamaño y la complejidad de TI está transformando rápidamente en obsoleta la visión convencional de una “amenaza avanzada”. Ahora las organizaciones se enfrentan con “amenazas combinadas” que han expandido su capacidad a medida que los perímetros tradicionales fueron desapareciendo y los datos ahora se transmiten en dispositivos finales, redes, usuarios móviles y la nube. Estas nuevas complejidades requieren de enfoques novedosos y plantean la importancia de implementar soluciones integradas que puedan compartir la inteligencia sobre amenazas y reducir el tiempo de permanencia de una amenaza¹⁴.

El tiempo de permanencia de una amenaza comienza cuando un atacante ingresa a una red y finaliza cuando éste la abandona o es obligado a hacerlo. Minimizar el tiempo de permanencia reduce la oportunidad de que un atacante logre un movimiento lateral y extraiga datos confidenciales.

Estos nuevos ataques avanzados son el foco de atención del equipo de Investigaciones Especiales (SI) de Forcepoint, que se pone en acción cuando una explotación muestra herramientas, tácticas y procesos (TTP) fuera de lo que se considera normal. Las habilidades y el conocimiento del equipo de SI cubre ingeniería inversa, análisis de ataques avanzados y neutralización de malware evasivo; y a esto se le agrega la aplicación de la ley.

El equipo de SI también toma puntos de referencia de datos de ataques conocidos y se sumerge en varios niveles de profundidad para crear técnicas de comprensión y mitigación de nuevos TTP. Este enfoque se utilizó para analizar JAKU – una campaña de botnet mundial recientemente identificada que se describe aquí por primera vez.

PRESENTACIÓN DE JAKU

JAKU es una campaña de botnet mundial en desarrollo. Demuestra la reutilización de infraestructura y TTP, la cual exhibe una doble personalidad. JAKU ataca a víctimas en masa y realiza ataques altamente dirigidos a individuos específicos a través de la ejecución de campañas operativas concurrentes. El resultado es la fuga de datos de información de máquinas, perfiles de usuarios finales e incorporación a conjuntos de datos de ataque más extenso.

Gracias a una investigación de seis meses de duración, Forcepoint Security Labs ha logrado trazar con precisión las ubicaciones de los servidores de comando y control y las víctimas en todo el mundo. A través del análisis estático y conductual, el equipo de Security Labs ha logrado comprender los componentes del ataque y el mecanismo de rastreo utilizado por este botnet. A lo largo de la investigación, coordinaron tareas con diversas agencias de aplicación de la ley y ahora se encuentran en un punto donde pueden compartir públicamente la información obtenida. Los clientes de Forcepoint han estado protegidos contra las amenazas presentadas por JAKU desde antes del comienzo de esta investigación en octubre de 2015.

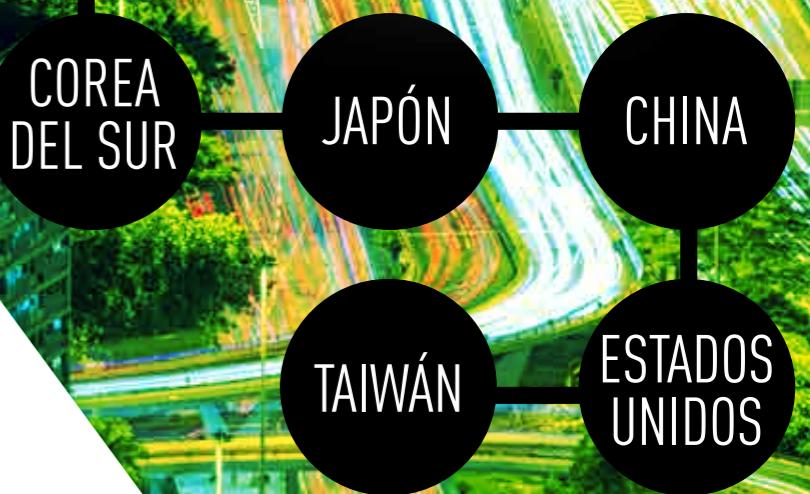
“Lo que es, en cierta medida, un cambio es la ejecución de una cantidad de operaciones concurrentes dentro de una campaña utilizando TTP casi idénticos para atacar a miles de víctimas y, al mismo tiempo, ejecutar una operación dirigida”.

– Dr. Richard Ford, Director Científico de Forcepoint, sobre JAKU

LAS CINCO PRINCIPALES VÍCTIMAS DE JAKU POR PAÍS

TIEMPO DE PERMANENCIA PROMEDIO
93 DÍAS

TIEMPO MÁXIMO DE PERMANENCIA: 348 DÍAS



JAKU HECHOS Y CIFRAS

DURACIÓN DE LA INVESTIGACIÓN HASTA LA FECHA:

6 MESES

UBICACIÓN DE LAS VÍCTIMAS:

MUNDIAL

(AGRUPAMIENTO IMPORTANTE EN JAPÓN, COREA DEL SUR Y CHINA)

LAS CARGAS SON DISTRIBUIDAS VÍA:

**EXPOSICIÓN A SITIOS DE BITTORRENTS COMPROMETIDOS,
USO DE SOFTWARE NO AUTORIZADO Y DESCARGA DE SOFTWARE WAREZ**

TÉCNICAS DE EVASIÓN USADAS:

**CRPTOGRAFÍA, ESTEGANOGRAFÍA,
TIPOS DE ARCHIVOS FALSOS,
INYECCIÓN FURTIVA, DETECCIÓN DE MOTORES ANTIVIRUS (Y OTRAS)**



PREGUNTAS FRECUENTES SOBRE JAKU

¿Cuándo se pondrá a disposición al público un análisis técnico completo de JAKU?

El 4 de mayo de 2016 estará disponible en el [blog](#) de Security Labs un informe técnico completo en el que se comparten todos los Indicadores de compromiso (IOC) conocidos.

¿Qué otros miembros de la comunidad de seguridad estuvieron involucrados en la investigación?

Forcepoint desea reconocer el extenso trabajo realizado por Kaspersky en su análisis de la campaña Dark Hotel y también a la Agencia Nacional contra el Crimen (National Crime Agency, NCA) del Reino Unido, a CERT-UK, a Europol y a la Interpol por su ayuda y colaboración en esta investigación. Únicamente a través de un enfoque de colaboración para la recolección, el cotejo y el análisis de la información Internet se convertirá en un lugar más seguro para que las personas puedan hacer negocios y vivir sus vidas modernas.

1. Construya procesos dentro de su organización para reducir el tiempo potencial de permanencia de una amenaza¹⁵.
2. Limite o evite el contacto con sitios de Torrents y software ilegal.
3. Monitoree en busca de actividad inusual, como tráfico enviado a servidores de comando y control, conocida por los sistemas de inteligencia sobre amenazas.

CONSEJOS DE FORCEPOINT

UNA FUERZA PARA TENER EN CUENTA

“DeepRed”, un equipo de ingenieros de Raytheon y expertos informáticos de Forcepoint, está creando un programa informático para encontrar fallas de seguridad en software y repararlas casi al instante como parte del Gran Desafío Cibernético de la Agencia de Proyectos de Investigación Avanzados de Defensa (ARPA). DeepRed competirá en la convención de hackers, DEF CON, en Las Vegas en agosto de 2016 por un premio de \$2 millones.

CONTRAATAQUE AL RANSOMWARE: ANÁLISIS DE LOCKY

Ransomware es el nombre dado al malware que cifra sus archivos y luego le ofrece venderle la clave de cifrado para recuperarlos. El ransomware se traduce en destrucción de datos si el propietario de los datos no logra recuperar sus archivos.

Durante el último año, el ransomware apareció con mucha frecuencia en las noticias. Durante muchos años, Forcepoint Security Labs ha realizado el seguimiento del desarrollo de las técnicas de ransomware, con frecuencia diseminadas a través de archivos adjuntos maliciosos de correo electrónico o malvertising.

Después de conocerse la noticia de que un hospital¹⁶ pagó un rescate por un ataque que inhabilitó el servicio, el equipo de SI investigó cómo prevenir el cifrado de archivos y compartir ese conocimiento con toda la comunidad.

FORCEPOINT DESENMASCARA A LOCKY: INGENIERÍA INVERSA DEL ALGORITMO DE GENERACIÓN DE DOMINIO

Forcepoint ofreció protección a los clientes contra el señuelo utilizado para disseminar la carga de Locky (un mensaje de correo electrónico malicioso que contenía un documento de Microsoft Office que incluía una macro maliciosa) y Forcepoint Security Labs también descubrió que podía inhabilitar el proceso de cifrado de archivos.

Locky utiliza cifrado AES de 128 bits y es capaz de cifrar bases de datos SQL, código fuente, billeteras BitCoin, etc. [Análisis de la carga](#) en nuestro módulo Threat Protection Cloud (comportamiento de archivos sandbox) identificó una llamada obvia a servidores conocidos de comando y control.

Lamentablemente, Locky emplea un algoritmo de generación de dominio que genera un conjunto diferente de URL basados en una marca de tiempo y un valor de semilla. De este modo, existe la posibilidad de que no se conozcan todos los URL sin una mayor investigación. El primer análisis de Labs mostró que Locky se comunicaba con un máximo de seis URL por día.

Forcepoint Security Labs realizó la ingeniería inversa del algoritmo de generación de dominio (DGA) del ransomware Locky y lo reveló al público; y de este modo, les dio a los defensores la oportunidad de contraatacar y bloquear el acceso a los dominios con los que se estaba comunicando el ransomware¹⁷. Al impedir que el ransomware tenga acceso a URL conocidos y obtenga las claves de cifrado requeridas utilizadas en un determinado día, los archivos permanecen intactos.

Cinco días después, los autores del malware cambiaron su DGA y actualizaron los valores de semilla. Así, el ransomware logró llegar a 14 dominios en un día determinado. Nuevamente, Forcepoint descubrió el algoritmo y brindó la lista de los dominios con los que se comunicaría durante los siguientes 30 días calendario¹⁸. Tras un monitoreo constante, Forcepoint descubrió que los autores cambiaron sus tácticas otra vez 23 días calendarios más tarde¹⁹.

Si bien pagar un rescate no garantiza la recuperación de los archivos, algunas empresas han decidido pagar lo requerido, con frecuencia con un costo de varios miles de dólares²⁰.

**LOS EXPERTOS HAN ESTIMADO QUE
EL MONTO TOTAL PAGADO A
AUTORES DE RANSOMWARE
PODRÍA ASCENDER A**

**325
MILLONES
DE DÓLARES**

**PARA ALGUNAS VARIANTES
DE RANSOMWARE²¹.**

Algunas variantes de ransomware, como CTB-Locker, no necesitan comunicarse con un servidor de comando y control para tener acceso a la clave requerida para cifrar archivos, lo que les da a los defensores una oportunidad menos de desbaratar el incidente de destrucción de datos. Esta es la razón por la que Forcepoint concentra sus esfuerzos para interceptar el malware en las primeras etapas del ciclo de vida de una amenaza, en particular en la etapa de "señuelo" (cuando los delincuentes cibernéticos crean un mensaje de correo electrónico en apariencia inocente u otro señuelo para engañar a los usuarios para que hagan clic en enlaces a sitios comprometidos²²).

El ransomware ahora también se está ajustando al idioma local de sus objetivos²³ o, contrariamente, está evitando deliberadamente infectar a los usuarios en territorios particulares²⁴. Los autores de malware pueden hacer esto para evitar llamar la atención de las agencias de aplicación de la ley en los lugares donde operan o para atacar a países y economías donde es más probable que se pague un rescate elevado.

PREGUNTAS FRECUENTES SOBRE EL RANSOMWARE

¿Con qué rapidez el ransomware cifra sus archivos después de la infección?

De *inmediato*, tan pronto como pueda conectarse con su servidor de comando y control.

Un ransomware comenzará el cifrado tan pronto como haya enumerado todos los controladores y buscado los tipos de archivo objetivo (por extensión).

Vale la pena mencionar que algunos ransomware no necesitan una conexión con el servidor de comando y control para comenzar el cifrado, ya que pueden generar las claves ellos mismos y una vez finalizado el proceso de cifrado la información sobre la clave se envía al servidor de comando y control. Un ejemplo de esto es CTB-Locker.

¿Qué probabilidad hay de recuperar los archivos después de pagarle a un ransomware?

Los autores de malware tienen la motivación de liberar los archivos para alentar a futuras víctimas a pagar. Sin embargo, si el servidor de comando y control que almacena la información sobre las claves que han sido desmontadas, no habrá manera de decodificar los archivos, incluso después de pagar el rescate.

¿Qué algoritmos de cifrado utiliza el ransomware?

Algunas variantes de ransomware utilizan algoritmos simétricos como AES-256 (TeslaCrypt); otros usan RSA-2048 de clave pública (CryptoLocker, CryptoWall). En ocasiones, el ransomware utiliza un algoritmo de cifrado personalizado.

CONSEJOS DE FORCEPOINT

1. Haga una copia de seguridad de sus datos en una unidad o servicio externo. No hay necesidad de pagar un rescate cuando puede recuperar los documentos de este modo.
2. Eduque a los usuarios para que no abran adjuntos inesperados o extraños que reciban en mensajes de correo electrónico ni hagan clic en hipervínculos desconocidos.
3. Determine si hay puntos débiles en su infraestructura o procesos que puedan ser aprovechados por tácticas de ransomware.
4. Considere la posibilidad de que el monto de rescate para recuperar datos sería mejor utilizado en la inversión de medidas de protección más efectivas para evitar incidentes similares en el futuro (como educación para usuarios y entorno seguro para URL y adjuntos de archivos).

DEJANDO EN EVIDENCIA LA EVASIÓN

Los firewalls de próxima generación (NGFW) se utilizan para controlar usuarios y aplicaciones y, al mismo tiempo, proporcionan identificación y mitigación de ataques con alta efectividad. Se diferencian de los firewalls tradicionales en que están atentos a las aplicaciones y pueden realizar un seguimiento del estado del flujo del tráfico en la red en forma granular, entre otras características. Los NGFW también son estupendas herramientas que proporcionan visibilidad de la red.

Las técnicas de evasión se utilizan para eludir los controles de seguridad de las soluciones (los atacantes pueden combinar técnicas para crear un enfoque de intrusión más difícil de detectar). Estas tácticas son una respuesta directa de los autores de malware a la visibilidad otorgada a los administradores de seguridad por las mejores soluciones de seguridad de su clase actuales (que incluyen los NGFW).

FORCEPOINT SECURITY LABS HA OBSERVADO TÉCNICAS DE EVASIÓN EMPLEADAS EN LAS SIGUIENTES ETAPAS DEL CICLO DE VIDA DE UNA AMENAZA:

- ETAPA 4
KIT DE EXPLOTACIONES
- ETAPA 5
ARCHIVO "DROPPER"
- ETAPA 6
"LLAMADA A CASA"
- ETAPA 7
ROBO DE DATOS

Forcepoint Security Labs agrupa los escenarios en los que se emplea evasión en tres categorías: el canal entrante (un ataque que utiliza evasión para atravesar las defensas de una red), el canal saliente (una carga de ataque que utiliza evasión para "llamar a casa") o la evasión para acceder a recursos denegados (por ejemplo, utilizando TOR). Estas técnicas de evasión avanzadas constituyen una importante amenaza para la seguridad de los datos de cualquier organización.

EVASIÓN POR TODAS PARTES

Las técnicas de evasión avanzadas combinan múltiples métodos de evasión existentes para crear nuevos métodos de evasión desconocidos; métodos que son más exitosos. Se ha observado que los autores de malware y de explotaciones utilizan un repertorio de métodos de evasión para manipular el caudal de nivel de protocolo y evadir la detección.

► Fragmentación de IP

La fragmentación de IP es el proceso de descomponer un datagrama de protocolo de Internet (IP) en múltiples paquetes de menor tamaño, y se especifica en RFC 791²⁵.

Las explotaciones de fragmentación de IP utilizan el protocolo de fragmentación dentro de IP como vector de ataque a través de la diseminación de la carga en múltiples marcos.

► Segmentación y avería de TCP

El Protocolo de control de transmisión (TCP) se define en RFC 793²⁶. Se utilizan números de secuencia para ordenar correctamente segmentos que pueden ser recibidos con avería.

Los ataques de segmentación y avería de TCP buscan disfrazar los ataques utilizando esta característica de TCP.

► Apuntador urgente de TCP

El campo apuntador urgente de TCP (URG) también se especifica en RFC 793. Este apuntador especifica la presencia de datos urgentes, o fuera de banda, que si se incluyen durante el análisis de carga pueden provocar que el código de explotación malicioso eluda la detección.

5 PRINCIPALES USOS PREVISTOS DE EVASIÓN EN 2016

1. ELUDIR EL CONTROL DE ACCESO

para tener acceso a una red de otro modo no autorizado

2. ATACAR POZOS DE AGUA

comunicarse con un pozo de agua de manera imposible de rastrear sin activar las alarmas usuales y la respuesta esperada de un equipo de seguridad de redes

3. COMANDO Y CONTROL DE BOTNET

disfrazar el tráfico desde y hacia el servidor de comando y control mejora la resistencia y mantiene el tiempo productivo del botnet

4. EXPLORACIONES (ENTREGA Y EJECUCIÓN)

la ejecución de código se puede obtener utilizando explotaciones que de otro modo serían fáciles de detectar

5. EXFILTRAR DATOS

el tráfico que no puede ser detectado por el firewall se puede usar para ocultar la transferencia de datos robados

CONSEJOS DE FORCEPOINT

1. Asegúrese de implementar tecnologías apropiadas que identifiquen y mitiguen el uso de la evasión.
2. Confirme la comprensión y el conocimiento de las técnicas de evasión en toda la cadena de ataque. El principio del vínculo más débil se aplica si se reduce la visibilidad en cualquiera de las etapas del ciclo de vida de un ataque o si esta visibilidad es insuficiente.

WEB Y CORREO ELECTRÓNICO UNA AMENAZA DOBLE

La web y el correo electrónico son los principales canales de comunicación y siguen siendo los principales vectores de ataque para los delincuentes cibernéticos. Ampliamente reconocido como el punto de entrada inicial a una organización de los ataques dirigidos, en 2015 el vector de ataque al correo electrónico envío cargas maliciosas a organizaciones, con un enfoque en documentos de Office y archivos comprimidos. Forcepoint Security Labs descubrió que el contenido malicioso en el correo electrónico aumentó un 250% en comparación con 2014. Dridex²⁷ (una cepa de malware bancario) y diversas campañas de ransomware²⁸ fueron en gran medida responsables de este aumento. El malware o los enlaces web maliciosos dentro de un mensaje de correo electrónico pueden aprovecharse de vulnerabilidades para poner en peligro las máquinas – y eventualmente redes completas – a través de Internet. Los vectores de ataque al correo electrónico y la web tuvieron una convergencia significativa en 2015, con nueve de diez mensajes de correo electrónico no deseado que contenían un URL. Según el informe sobre fuga de datos 2015 del Centro de Recursos sobre Robo de Identidad²⁹, la exposición accidental al correo electrónico/Internet fue la tercera causa más común de datos comprometidos en 2015, lo que destaca la importancia del análisis de amenazas en ambos vectores de ataque.

- ▶ El **91.7%** del correo electrónico no deseado contiene un URL.
- ▶ El **2.34%** del correo electrónico no deseado contiene un adjunto.
- ▶ Aumento del **44.7%** en marcos maliciosas en adjuntos de correo electrónico; las marcos se utilizan para entregar una carga hospedada en la web.
- ▶ El **68.4%** del correo electrónico es spam (una disminución en relación con el 88.5% en 2014).

Los datos de Forcepoint muestran que las macros maliciosas incorporadas en tipos de archivos de Microsoft Office fueron un mecanismo prominente de ataque-entrega en 2015. El Informe de amenazas del año pasado³⁰ reveló tres millones de macros maliciosas observadas en un período de treinta días al final de 2014. Al realizar un período de obtención de muestras similar al final de 2015, Forcepoint encontró más de cuatro millones de macros, un aumento del 44.7% con respecto a 2014.



LOS 5 PRINCIPALES

LOS 10 PAÍSES

QUE HOSPEDAN MÁS CONTENIDO MALICIOSO

LOS 8 PRINCIPALES PAÍSES

QUE HOSPEDAN MAYORES SITIOS WEB DE PHISHING

- | País | País | País | País |
|-----------------|-----------|-------------|----------|
| ESTADOS UNIDOS* | HONG KONG | REINO UNIDO | ALEMANIA |
| BELICE | BÉLGICA | CHILE | SUECIA |

*Estados Unidos hospedó más sitios web de phishing que los demás países de esta categoría combinados.

CONSEJOS DE FORCEPOINT

TIPOS DE ARCHIVOS MALICIOSOS QUE SE ENVÍAN COMO ADJUNTOS DE CORREO ELECTRÓNICO

1. ARCHIVO ZIP
2. PROGRAMA SDOS/WINDOWS
3. BASADO EN ARCHIVO DE TEXTO
4. MICROSOFT WORD 97
5. FORMATO MHT

- | País | País | País | País |
|----------------|-----------|--------|--------------|
| ESTADOS UNIDOS | IRLANDA | ITALIA | REINO UNIDO |
| ALEMANIA | FRANCIA | RUSIA | PAÍSES BAJOS |
| TURQUÍA | INDONESIA | | |

1. Examine las soluciones de seguridad provistas de análisis de vectores de ataque a la web y el correo electrónico, lo que proporcionará una mayor eficacia a cada producto.
2. Implemente un programa de educación/capacitación de usuarios que recuerde periódicamente a los usuarios las maneras típicas de identificar un mensaje de correo electrónico malicioso con adjuntos o URL que probablemente activen una conexión con la web para el envío de cargas adicionales.
3. Considere la posibilidad de activar la tecnología de entorno seguro de URL y adjuntos en archivos para evitar que los usuarios tomen malas decisiones o no reconozcan el correo electrónico malicioso.

EL AVANCE HACIA LA NUBE

Cada vez más empresas adoptan tecnologías basadas en la nube para obtener ahorros de costos y colaboración. Si bien la nube es un mercado que todavía está en crecimiento, los beneficios que aporta la informática en la nube relativos a la reducción de la necesidad de hardware y de soporte y a la oferta de flexibilidad a los empleados y velocidad para completar tareas críticas de la empresa han provocado un cambio gradual, aunque constante hacia la nube. En una encuesta global realizada por Harvard Business Review Analytic Services³¹, el 85% de los encuestados dijo que en los próximos tres años sus organizaciones estarán utilizando herramientas en la nube de forma moderada a extensa.

A pesar de las muchas ventajas que brinda TI en la nube a las misiones empresariales, algunas organizaciones han demorado más en adoptar esta tecnología debido a preocupaciones por la posibilidad de que las aplicaciones basadas en la nube tengan una protección ineficaz o puedan contraponerse a los requisitos de cumplimiento. Más del 60% de las organizaciones indica "preocupaciones sobre seguridad" como el motivo más importante por el que han postergado la adopción de la nube³². De acuerdo con una investigación de Ponemon³³, la preocupación aumenta ante la dificultad para implementar métodos de seguridad eficaces en aplicaciones y productos en la nube, junto con la incertidumbre de si los usuarios finales o los proveedores de servicios en la nube son responsables de la seguridad de los datos.

Sin embargo, puede suceder que la resistencia a la adopción de la nube no postergue su uso. Empleados, grupos o incluso divisiones completas con frecuencia migran a la nube aunque su empresa no lo haga, y evaden esfuerzos de aprobación o de integración formal cuando las soluciones externas satisfacen mejor los requisitos de productividad. Esto crea la posibilidad de que la tecnología no autorizada afecte la postura de seguridad y de cumplimiento de una organización, y la exponga a riesgos no deseados y no planeados.

EL “SHADOW” IT (HARDWARE O SOFTWARE OCULTO) ESTA NO ES LA NUBE QUE USTED ESTÁ BUSCANDO

- ▶ **SOLAMENTE EL 8%** de las compañías conoce el alcance el “shadow” IT (hardware o software oculto) en sus organizaciones.
- ▶ **EL 71%** está en cierta medida muy preocupado por el “shadow” IT (hardware o software oculto)*

“CLOUD ADOPTION PRACTICES & PRIORITIES SURVEY REPORT,”
enero de 2015, Cloud Security Alliance

Más del 80% de los encargados de la toma de decisiones de TI consideran que el “shadow” IT (Hardware o software oculto) constituye un riesgo para la seguridad de TI, un tercio lo considera un riesgo muy importante y un 16% lo clasifica como el riesgo más importante³⁴. Sin embargo, solamente el 34% de los que utilizan el “shadow” IT (Hardware o software oculto) cree que presenta un riesgo de seguridad, y más de la mitad menciona que su uso permite a los departamentos comerciales ser más productivos³⁵. Lamentablemente cuando TI no puede ver los datos, tampoco puede protegerlos adecuadamente, y esto genera el entorno perfecto para la pérdida o el robo de datos.

Una encuesta de IDG Enterprise³⁶ descubrió que los CIOs creen que 2016 será el primer año en que habrá más servicios de TI en la nube que en las instalaciones. Las soluciones de privacidad y seguridad centradas en datos que cubren todas las plataformas y sistemas informáticos son esenciales para el cumplimiento de regulaciones de privacidad y seguridad. Además de las defensas atentas a los datos, evaluaciones hechas por terceros independientes, como la Certificación CSA STAR³⁷, pueden ayudar a determinar la seguridad de los proveedores de servicios en la nube.

CONSEJOS DE FORCEPOINT

- 
 - 1. Las soluciones de prevención contra la pérdida de datos (DLP) y los firewalls de próxima generación (NGFW) pueden ayudar a las organizaciones a darse cuenta del alcance de su “shadow” IT (Hardware o software oculto).
 - 2. Una vez que se conocen los servicios y las entidades de TI con los que los usuarios se conectan, las organizaciones pueden aplicar pautas de datos y uso, capacitar a los usuarios o deshabilitar TI en función de sus políticas.
 - 3. Los empleados con frecuencia utilizan el “shadow” IT (Hardware o software oculto) para adoptar nuevas perspectivas en sus ideas y su trabajo. Demasiado control puede dar como resultado usuarios frustrados e intentos de evadir las restricciones. Considere la posibilidad de trabajar con el personal para ayudarlo a ser más productivo en lugar de bloquear rotundamente sus intentos de innovar.

LA NECESIDAD DE TALENTO CIBERNÉTICO

A medida que los datos continúan alejándose de las defensas perimetrales, es primordial promover una fuerza de trabajo de seguridad cibernética capaz de proteger la información de las amenazas cibernéticas. Estudio anual de Raytheon “Securing Our Future: Closing the Cyber Talent Gap”³⁸, en colaboración con la Alianza Nacional de Seguridad Cibernética (*National Cyber Security Alliance*), trabaja para identificar las causas de la falta de talento cibernético como parte de un compromiso compartido a largo plazo de construir una sólida cartera de talento.



La actividad de fusiones y adquisiciones de nuevas empresas está aumentando, pero la fusión de empresas aumenta la complejidad de la protección de los datos confidenciales de una organización. Dado que el 84% del valor total del índice S&P 500 ahora consiste en propiedad intelectual y otros valores intangibles³⁹, es esencial poner los datos a disposición de las partes apropiadas y, al mismo tiempo, protegerlos de la pérdida, el robo y el mal uso. La tecnología y los procesos empresariales necesarios para proteger los datos confidenciales y mantener una ventaja competitiva son una parte inherente de las fusiones, adquisiciones y otras proposiciones empresariales. La pérdida de propiedad intelectual o de otros datos tiene un efecto inmediato en la reputación, puede derivar en una medida legal o reguladora, y afectar de manera adversa la posición competitiva, el precio de las acciones y el valor de los accionistas. Es indispensable crear un plan para la consolidación y la gestión seguras de los datos confidenciales, a fin de lograr la integración exitosa de organizaciones otra vez independientes.

CREACIÓN DE FORCEPOINT: CÓMO UNA ORGANIZACIÓN DE SEGURIDAD CIBERNÉTICA SE INTEGRA DE MANERA SEGURA

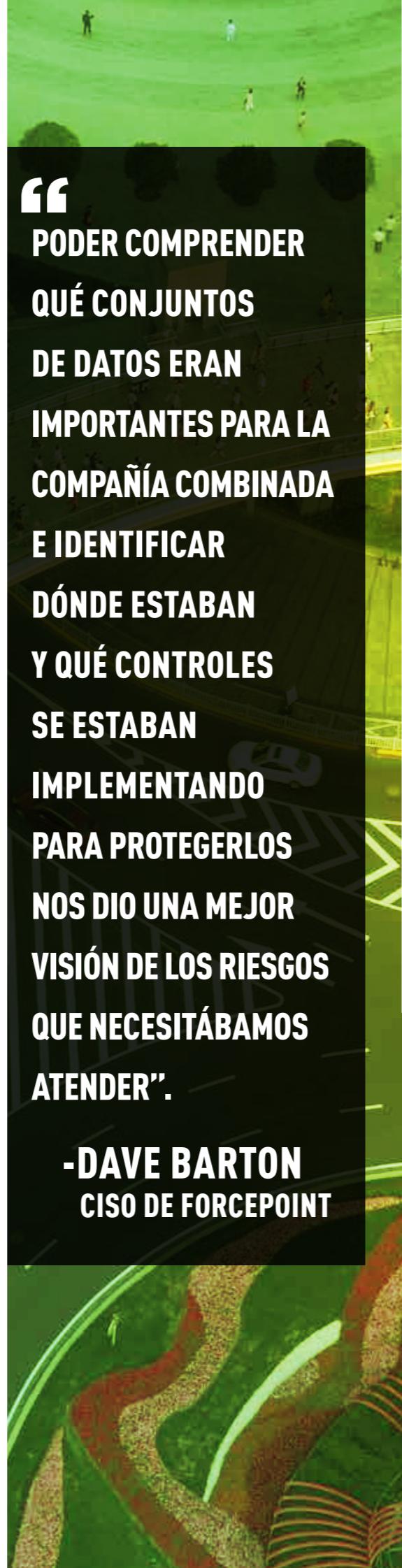
El 14 de enero de 2016, se anunció la creación de una nueva asociación conjunta con la integración de Websense, Raytheon Cyber Products y el negocio de firewalls de última generación (NGFW) de Stonesoft. Conocida como Forcepoint, esta nueva compañía fue la culminación de casi un año de integración de sistemas empresariales.

EVALUACIÓN

Antes de comenzar con la integración de datos, sistemas o procesos de Websense, RCP y Stonesoft, fue necesario realizar una evaluación de la postura de seguridad interna y externa de cada compañía. Una compañía independiente realizó una prueba de penetración y examinó en profundidad la web en busca de alguna vulnerabilidad o hackeo en desarrollo de los cuales las compañías no estuvieran en conocimiento. Se pidió a los integrantes del personal de seguridad que detallaran sus programas de seguridad que incluían educación de usuarios, gestión de la vulnerabilidad, clasificación de datos y flujos, y administración de controles de acceso. Esta debida diligencia de seguridad confirmó que las políticas implementadas estaban ciertamente en ejecución y resaltó las potenciales disparidades; por ejemplo, donde una organización tenía requerimientos de seguridad más estrictos se debió alinear a las otras organizaciones en esos aspectos.

VALORACIÓN

Después de finalizar nuestra propia evaluación de seguridad, comenzó una evaluación de las redes de las entidades que pronto se combinarían en busca de amenazas. En este sentido, se utilizó una herramienta personalizada para detectar y denunciar actividad sospechosa y evaluar la salud de la red, para luego desarrollar consejos. Con frecuencia estos consejos eran tan simples como emparchar un servidor o actualizar certificados.



Al mismo tiempo, se identificaron “los tesoros más valiosos” de RCP y de Websense (propiedad intelectual, datos financieros, etc.) y se desarrollaron comunicaciones apropiadas para combatir las amenazas dirigidas y la actividad maliciosa (p. ej., ataques de spam y de phishing), que son comunes cuando se consolidan compañías. Forcepoint recibió lo que parecían ser (pero no eran) mensajes de correo electrónico legítimos de Raytheon solicitando datos confidenciales e información financiera, y gracias a las medidas proactivas que ya se habían implementado no fuimos víctima de estos intentos de intrusiones maliciosas.

ACCIÓN

Antes del día del anuncio, se realizó una prueba estática y dinámica en todo el código fuente de las entidades recientemente combinadas. Esto se hizo para determinar las vulnerabilidades de código que posiblemente se desconocían o no se habían divulgado.

DÍA DEL ANUNCIO

Aunque las redes no estaban conectadas ni comunicadas directamente entre sí, aún había medidas que tomar para garantizar que los meses de integración por venir transcurrieran sin problemas. En primer lugar se comunicaron a todos los empleados las políticas de acceso a los datos, especialmente en torno al manejo de datos esenciales o confidenciales durante toda la transición. También era necesario que los empleados comprendieran que los modelos de fijación de precios de propiedad exclusiva de la compañía no se podían compartir hasta que la adquisición estuviera formalmente terminada. Esta comunicación proactiva con los usuarios finales fue clave para proteger los bienes y la información durante el proceso de fusión y adquisición.

UN NUEVO NIVEL DE PRUEBAS DE RESISTENCIA

El Centro de Desarrollo y Evaluación de Operaciones Cibernéticas (*Cyber Operations, Development and Evaluation, CODE*) de Raytheon es un rango cibernético de última generación que se utiliza para evaluar sistemas críticos actuales y futuros contra ataques cibernéticos.

El Centro CODE forma parte de la red de centros de innovación y demostración cibernéticas de Raytheon en todo el mundo que ayuda a los clientes a detectar soluciones con rapidez para sus desafíos cibernéticos más difíciles y complejos.

En segundo lugar, se aumentó el monitoreo de las redes de la compañía utilizando herramientas de protección contra el robo de datos con un enfoque en el uso de cuentas de administradores y los intentos de transferencias de datos confidenciales por correo electrónico o internet. Cuando llegaban las alertas, los equipos de TI, de Seguridad y de Desarrollo comenzaron la remediación de las amenazas y vulnerabilidades identificadas. De este modo, lograron resolverse los problemas o las brechas restantes y las diferencias en políticas de seguridad antes de la conexión de las redes.

La integración de Forcepoint fue más compleja que la mayoría de las integraciones. Al mismo tiempo que se completaba la asociación conjunta con Websense y RCP, adquirimos Stonesoft y tuvimos que volver a realizar muchos de los mismos pasos realizados para garantizar una integración segura y sin problemas. Además, el cambio a una nueva identidad de marca exigió que TI tuviera que trasladar empleados, estaciones de trabajo y datos a un nuevo dominio: Forcepoint.com. Todo esto sucedió mientras trabajábamos para evitar que nuestra marca y nuestro nombre se filtraran antes del anuncio formal. Esto se logró mediante la implementación de nuestras propias herramientas que restringieron la capacidad para compartir datos que contenían el nuevo nombre y otra información de la marca fuera de la red interna. Incluso con estos escollos potenciales, la planificación y el trabajo que los precedió hicieron posible la rápida continuación de la integración y la mitigación de desafíos menores antes del cierre de la fusión.

En cualquier actividad de fusión y adquisición, la seguridad es primordial. Existen demasiados riesgos potenciales durante las fusiones que no se descubrirán sin la participación importante de los expertos en seguridad.



CONCLUSIÓN

El Informe de Amenazas Globales 2016 de Forcepoint confirma un notable cambio en la naturaleza de los ataques este pasado año. La seguridad cibernetica – a menudo un área de debates técnicos, alertas y problemas de TI – actualmente es, en última instancia, un riesgo dominante y un problema de consecuencia para ejecutivos corporativos, funcionarios electos, autoridades gubernamentales y líderes en todas partes.

Las acciones de una pandilla oportunista que distribuye ransomware, un empleado descuidado o un mecanismo de ataque avanzado bien concebido pueden generar un cambio y un terrible impacto – en algunos casos, amenazando la estabilidad misma de las finanzas, la capacidad de misión y las marcas invaluables de una organización. Aun así, no todos los ataques son una amenaza existencial; estamos en una era en la que cualquier oficina u objeto conectado a internet puede ser bombardeado con ataques en cualquier momento.

Creemos que se necesita un nuevo enfoque holístico que proporcione a las empresas una visión de 360° con análisis en tiempo real y alertas significativas que anticipen y comuniquen el panorama de amenazas y sus implicancias para que los clientes puedan actuar rápidamente y derrotar hasta a los adversarios más decididos. El equipo de Security Labs, el equipo de Investigaciones Especiales y el equipo de la Oficina del CSO de Forcepoint continúan aplicando su experiencia en la identificación de amenazas mundiales y actividad de ataques. Con asesoramiento a lo largo del camino, juntos podremos ***Avanzar sin Miedo.***

BIBLIOGRAFÍA

1. Ponemon Institute LLC. "2015 Cost of Cyber Crime Study: Global". Octubre de 2015. <https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf>
2. Ponemon Institute LLC. "Privileged User Abuse & The Insider Threat." Mayo de 2014. http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf
3. Anderson, Ed; Nag, Sid y Gartner, Inc. "Forecast Overview: Public Cloud Services, Worldwide, 2016 Update". 17 de febrero de 2016. <https://www.gartner.com/doc/3214717?ref=SiteSearch&sthkw=security%20concerns%20cloud%20adoption&fnl=search&srclid=1-347892254>
4. Shey, Heidi. "Understand The State Of Data Security And Privacy: 2015 To 2016". Forrester Research, Inc., 8 de enero de 2016. <https://www.forrester.com/report/Understand+The+State+Of+Data+Security+And+Privacy+2015+To+2016/-/E-RES117447>
5. Mearian, Lucas. "Government Tests Show Security's People Problem". Computerworld. 6 de julio de 2011. <http://www.computerworld.com/article/2510014/security0/government-tests-show-security-s-people-problem.html>
6. Ponemon Institute LLC. "Ponemon Study: The Unintentional Insider Risk in United States and German Organizations". 30 de julio de 2015. <http://www.raytheoncyber.com/spotlight/ponemon/index.html>
7. Bank Director. "Bank Director's 2016 Risk Practices Survey". 21 de marzo de 2016. http://www.bankdirector.com/download_file/view_inline/4996
8. Centro de Recursos sobre el Robo de Identidad (Identity Theft Resource Center). "2015 Data Breaches | ITRC Surveys & Studies | ID Theft Blog". 25 de enero de 2016. <http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html>
9. Forrester Research, Inc. "Global Business Technographics® Security Survey, 2015". Julio de 2015. https://www.forrester.com/Global_Business_Technographics_Security_Survey_2015/-/E-sus2957
10. Forrester Research, Inc. "Global Business Technographics® Devices And Security Workforce Survey, 2015". Agosto de 2015. <https://www.forrester.com/Global+Business+Technographics+Devices+And+Security+Workforce+Survey+2015/-/E-sus2971>
11. Ponemon Institute LLC. "Privileged User Abuse & The Insider Threat." Mayo de 2014. http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf
12. Litan, Avivah y Gartner, Inc. "Best Practices and Success Stories for User Behavior Analytics". 4 de marzo de 2015. <https://www.gartner.com/doc/2998124/best-practices-success-stories-user>
13. Forrester Research, Inc. "Global Business Technographics® Security Survey, 2015". Julio de 2015. https://www.forrester.com/Global_Business_Technographics_Security_Survey_2015/-/E-sus2957
14. Forcepoint LLC. "Cyber Dwell Time and Lateral Movement THE NEW CYBERSECURITY BLUEPRINT". <https://www.forcepoint.com/resources/whitepapers/cyber-dwell-time-and-lateral-movement>
15. Forcepoint LLC. "Cyber Dwell Time and Lateral Movement THE NEW CYBERSECURITY BLUEPRINT". <https://www.forcepoint.com/resources/whitepapers/cyber-dwell-time-and-lateral-movement>
16. Vanian, Jonathan. "Hollywood Hospital Pays Off Hackers To Restore Computer System". 18 de febrero de 2016. <http://fortune.com/2016/02/18/hollywood-hospital-hackers-computer-system/>
17. Forcepoint Security Labs y Forcepoint LLC. "Locky Ransomware - Encrypts Documents, Databases, Code, BitCoin Wallets and More..." 19 de febrero de 2016. <https://blogs.forcepoint.com/security-labs/locky-ransomware-encrypts-documents-databases-code-bitcoin-wallets-and-more>
18. Forcepoint Security Labs y Forcepoint LLC. "Locky's New DGA - Seeding the New Domains [ACTUALIZACIÓN DE RUSIA: 26/FEB/16]". 25 de febrero de 2016. <https://blogs.forcepoint.com/security-labs/lockys-new-dga-seeding-new-domains>
19. @Forcepointsec Twitter handle. 22 de marzo de 2016. Tweet, <https://twitter.com/Forcepointsec/status/712316915687948289>
20. Winton, Richard. "Hollywood Hospital Pays \$17,000 in Bitcoin to Hackers; FBI Investigating". Los Angeles Times. 18 de febrero de 2016. <http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html>
21. Vijayan, Jai. "With \$325 Million In Extorted Payments CryptoWall 3 Highlights Ransomware Threat". Dark Reading. 29 de octubre de 2015. [http://www.darkreading.com/endpoint/with-\\$325-million-in-extorted-payments-cryptowall-3-highlights-ransomware-threat/d/d-id/1322899](http://www.darkreading.com/endpoint/with-$325-million-in-extorted-payments-cryptowall-3-highlights-ransomware-threat/d/d-id/1322899)
22. Forcepoint LLC (anteriormente Websense). "The Seven Stages of Advanced Threats". <https://www.websense.com/assets/pdf/understanding-the-cyber-attack-infographic.pdf>
23. Forcepoint Security Labs y Forcepoint LLC. "TorrentLocker is Back and Targets Sweden & Italy". 15 de marzo de 2016. <https://blogs.forcepoint.com/security-labs/torrentlocker-back-and-targets-sweden-italy>
24. Forcepoint Security Labs y Forcepoint LLC. "Locky's New DGA - Seeding the New Domains [ACTUALIZACIÓN DE RUSIA: 26/FEB/16]". 25 de febrero de 2016. <https://blogs.forcepoint.com/security-labs/lockys-new-dga-seeding-new-domains>
25. Instituto de Ciencias de la Información (Information Sciences Institute); University of Southern California. "DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION". INTERNET PROTOCOL, Septiembre de 1981. <https://tools.ietf.org/html/rfc791>
26. Instituto de Ciencias de la Información (Information Sciences Institute); University of Southern California. "DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION". TRANSMISSION CONTROL PROTOCOL, Septiembre de 1981. <https://tools.ietf.org/html/rfc793>
27. Forcepoint Security Labs y Forcepoint LLC. "Dridex Down Under". 5 de noviembre de 2015. <https://blogs.forcepoint.com/security-labs/dridex-down-under>
28. Forcepoint Security Labs y Forcepoint LLC. "Accounts Payable in the Czech Republic Targeted by Dridex". 4 de agosto de 2015. <https://blogs.forcepoint.com/security-labs/accounts-payable-czech-republic-targeted-dridex>
29. Centro de Recursos sobre el Robo de Identidad (Identity Theft Resource Center). "2015 Data Breaches | ITRC Surveys & Studies | ID Theft Blog". 25 de enero de 2016. <http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html>
30. Forcepoint LLC. "Websense 2015 Threat Report". 8 de abril de 2015. <https://www.websense.com/content/websense-2015-threat-report.aspx>
31. Harvard Business Review. "How the Cloud Looks from the Top: Achieving Competitive Advantage In the Age of Cloud Computing". 2011. https://hbr.org/resources/pdfs/tools/16700_HBR_Microsoft%20Report_LONG_webview.pdf
32. Anderson, Ed; Nag, Sid y Gartner, Inc. "Forecast Overview: Public Cloud Services, Worldwide, 2016 Update". 17 de febrero de 2016. <https://www.gartner.com/doc/3214717?ref=SiteSearch&sthkw=security%20concerns%20cloud%20adoption&fnl=search&srclid=1-347892254>
33. Ponemon Institute LLC. "The Challenges of Cloud Information Governance: A Global Data Security Study". Octubre de 2014. <http://www2.gemalto.com/cloud-security-research/SafeNet-Cloud-Governance.pdf>
34. VansonBourne. "Shadow IT ITDMs Data Summary", p. 34. 11 de julio de 2014. http://www.vansonbourne.com/files/1914/1225/3447/VB-Shadow_IT-ITDMs-Data-Summary.pdf
35. VansonBourne. "Shadow IT BDM Data Summary", p. 24. 22 de julio de 2014. http://www.vansonbourne.com/files/7614/1225/3401/VB-Shadow_IT-BDM-Data-Summary.pdf
36. IDG Enterprise. "2015 IDG enterprise cloud computing survey". 17 de noviembre de 2015. <http://www.idgenterprise.com/resource/research/2015-cloud-computing-study/>
37. CAS Cloud Security Alliance. <https://cloudsecurityalliance.org/star/certification/>
38. Raytheon Company, "Securing Our Future: Closing the Cyber Talent Gap". 19 de octubre de 2015. <http://raytheon.mediaroom.com/2015-10-26-Many-more-men-than-women-are-drawn-to-cybersecurity-careers-and-the-gap-is-widening-dramatically-new-survey-says>
39. Ocean Tomo LLC. "Intangible Asset Market Value Study". 4 de marzo de 2015. <http://www.oceansomo.com/2015/03/04/2015-intangible-asset-market-value-study/>

¿QUIÉN ES FORCEPOINT?

Forcepoint existe para ayudar a las organizaciones a avanzar en sus negocios. Nuestro objetivo es satisfacer la necesidad de nuestros clientes de adoptar tecnologías empresariales transformadoras de manera segura en un mundo donde los servicios en la nube, las arquitecturas híbridas y las fuerzas de trabajo móviles son la norma. El modelo de seguridad perimetral ha quedado obsoleto; y ahora las organizaciones necesitan soluciones que ubiquen a la seguridad cerca de los datos dondequiera que estén y que vayan, en múltiples entornos y dispositivos, desde redes hasta dispositivos finales y desde dispositivos móviles a la nube. Independientemente de la región, el mercado o el tamaño de las empresas, las amenazas que enfrentan nuestros clientes son cada vez más desafiantes, y los equipos de seguridad dependientes de recursos se esfuerzan por mantenerse a la par. La plataforma Forcepoint permite a las organizaciones automatizar las partes rutinarias de seguridad, eliminar la diversidad de productos de punto y descubrir información verdadera y confiable, como la incluida en nuestro informe anual de amenazas.

THREATSEEKER® INTELLIGENCE CLOUD

Threatseeker Intelligence Cloud fue desarrollada para dar a Forcepoint visibilidad sobre las amenazas de reciente aparición. Threatseeker procesa hasta cinco mil millones de puntos de datos recolectados de múltiples entradas en 155 países, y nos ayuda a proteger a nuestros clientes trabajando detrás de escena las 24 horas del día, los 7 días de la semana, los 365 días del año para que puedan hacer negocios de manera segura. Los expertos de Forcepoint interactúan a diario con Threatseeker y recolectan la inteligencia sobre amenazas precisa y en tiempo real y la información presentada en nuestros informes anuales detallados sobre amenazas y predicciones de la industria.

