La solución de Cisco brinda protección antes, durante y después de un ataque

Cisco Cloud Web Security Premium ayuda a una empresa petrolera a detectar y resolver una infección persistente de ransomware.

Desafíos

En esta época en la que el robo de información o el hecho de comprometer la seguridad de la información es generalmente el incentivo principal para un ataque, la seguridad de contenidos representa un enorme desafío. Según el informe anual de seguridad de Cisco 2014, los investigadores de Cisco determinaron que el 100% de las redes empresariales que se analizaron tenían tráfico con sitios web que alojan software malicioso.[1] La observación de esta actividad también permitió determinar que, cuando se penetraron estas redes, pudieron haber estado comprometidas durante algún tiempo sin que se detectara la infiltración primaria.[2]

Los siguientes factores están dificultando particularmente la prevención y detección de amenazas por parte de los equipos de seguridad:

- **La movilidad y la nube**, sin las medidas de seguridad adecuadas, reducen la visibilidad y aumentan la complejidad de la seguridad. Dado que cada vez más organizaciones adoptan tendencias tales como la computación en la nube, BYOD, virtualización, y trabajadores móviles y remotos, cada vez más información queda fuera del control de las empresas. La red se está volviendo más porosa, lo cual permite más vectores de ataque. Además, conforme aumente la cantidad de servicios cruciales para las empresas que se trasladen a la nube y permitan un acceso por fuera del perímetro protegido de la compañía, la superficie de ataque no hará otra cosa que expandirse.
- **Hay adversarios avanzados**, según el *Informe anual de seguridad de Cisco 2014*, que están "trabajando en forma proactiva para comprender los tipos de soluciones de seguridad que se están implementado, y están adoptando patrones de comportamiento menos visibles y detectables por contenido para que sus amenazas se oculten bien".[3] Esta estrategia deja menos "frutas al alcance de la mano" de las soluciones de seguridad y los profesionales, por lo que las organizaciones enfrentarán "más tráfico de cifrado, más enmascaramiento y más aleatorización por parte de actores maliciosos que pretenden que los comportamientos de mando y control (C&C) no puedan distinguirse del tráfico real".[4]

PERFIL DEL CLIENTE

Sector: Gas y petróleo
Empleados: aproximadamente 15 000
Operaciones: Internacional
Personal de seguridad: 12
Otras medidas de seguridad: Antivirus, firewall, Sistema de detección de intrusiones (IDS), Administración de eventos e información de seguridad (SIEM)

DESAFÍO

- Detectar amenazas avanzadas que se transmiten a través del tráfico de Internet, las cuales pueden evadir soluciones de seguridad heredadas e integrarse en la red corporativa.
- Desarrollar inteligencia práctica que ayude al equipo de seguridad a establecer un orden de prioridad de amenazas.
- Identificar una única solución que pueda implementarse en todo el entorno distribuido, integrarse con la infraestructura de seguridad existente y brindar protección constante contra todo el proceso de ataque.

SOLUCIÓN

- Cisco CWS Premium, que incluye todas las funciones de Cisco CWS Essentials.
- Cognitive Threat Analytics (CTA) y Advanced Malware Protection (AMP), para automatizar la búsqueda de amenazas de alto riesgo que se transmiten por Internet y adquirir visibilidad de ataques avanzados que operan activamente en la red de la empresa.

RESULTADOS

- Identificación y resolución de infección de malware persistente sin detección previa.
- Ahora hay protección contra amenazas a lo largo de todo el ataque.
- El equipo de seguridad del cliente ahora puede centrarse en resolver las amenazas más importantes.

[1] *Informe anual de seguridad de Cisco 2014.* http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.
[2] Ibíd.
[3] Ibíd.
[4] Ibíd.

El complejo y cambiante panorama de amenazas hace que, en un enfoque moderno de la seguridad de contenidos, la detección sea más relevante que la defensa. Las empresas actuales deben centrarse en la inspección de contenidos, la detección de anomalías de comportamiento y los análisis forenses avanzados para adquirir una mayor visibilidad de las amenazas que ya están presentes en sus redes; es decir, el "después" de un ataque.

Figura 1. Nuevo modelo de seguridad: seguridad continua después del ataque

Cisco® Cloud Web Security (CWS) Premium ayuda a las organizaciones a superar el desafío de mantener una seguridad continua en toda la red extendida. Cisco CWS, una versión de Cisco Web Security basada en la nube, es una plataforma que extiende la seguridad web a los dispositivos móviles y los entornos distribuidos. Protege a todos los usuarios mediante la inteligencia global de amenazas, las capacidades de defensa de amenazas avanzadas y la protección de usuarios itinerantes de Cisco. Incluye todas las funciones de Cisco CWS Essentials, además de combinar dos innovadores sistemas de detección de software malicioso para automatizar la búsqueda de amenazas de alto riesgo en el tráfico de Internet:

- **Cognitive Threat Analytics (CTA)** es un sistema de análisis del comportamiento de la red casi en tiempo real que utiliza aprendizaje automático y estadísticas avanzadas para detectar actividad inusual en una red: indicadores de compromiso (IOC). CTA detecta anomalías y luego orienta a los analistas de seguridad hacia problemas potenciales, lo cual ayuda a reducir el volumen de trabajo y permite abordar las amenazas siguiendo un orden de prioridades.
- **Advanced Malware Protection (AMP)** emplea una combinación de reputación, sandboxing y análisis retrospectivo de archivos para identificar y detener amenazas en todo el ataque.

La combinación de estas soluciones le permite a CWS Premium identificar nuevos canales de mando y control no detectados anteriormente por el sector de seguridad.

Este caso de estudio muestra cómo CWS Premium ayudó a una empresa petrolera internacional a lograr lo siguiente:

- Incrementar la visibilidad de un gran volumen de tráfico de Internet (más de 35 millones de solicitudes HTTP por día).
- Generar inteligencia práctica contra amenazas que simplifica la asignación de prioridades por parte del equipo de respuesta a amenazas.
- Implementar una única solución que se integra fácilmente con la infraestructura de seguridad existente, y brinda protección constante contra todo el ataque: antes, durante y después.

Solución

Cisco le recomendó al cliente la actualización a CWS Premium, que incluye CTA y AMP, a fin de adquirir una mayor visibilidad de su red y ayudar al equipo de respuesta a amenazas a establecer un orden de prioridades de amenazas.

Es posible que el análisis retrospectivo de AMP revele que los archivos que se consideraban “limpios” al atravesar las defensas perimetrales en realidad eran un avanzado software malicioso con un buen disfraz. AMP alerta de inmediato al administrador de seguridad y permite detectar a los usuarios de la red que podrían haberse infectado y en qué momento.

CTA, por su parte, detecta amenazas incluso más furtivas que han penetrado las defensas y están operando activamente en la red corporativa. Es un innovador sistema de detección de software malicioso que emplea análisis de comportamiento y detección de anomalías para identificar dispositivos comprometidos. CTA emplea un avanzado sistema de modelado de estadísticas y aprendizaje automático para identificar nuevas amenazas de manera independiente, aprendiendo de lo que ve y adaptándose con el tiempo, sin necesidad de ajustes o configuración.

CTA identificó evidencia de actividad de software malicioso en la red del cliente y lo informó. El software malicioso constaba de un conjunto de módulos controlados por una única entidad de software malicioso. En este caso, la carga útil fue Cryptolocker, un tipo de software malicioso denominado ransomware que encripta archivos en el equipo de la víctima y “bloquea” el dispositivo hasta que la víctima paga un rescate.[5]

Tal como se muestra en la Figura 2, el adversario operó una infraestructura de mando y control para realizar el ataque. El ataque se realizó en 4 etapas:

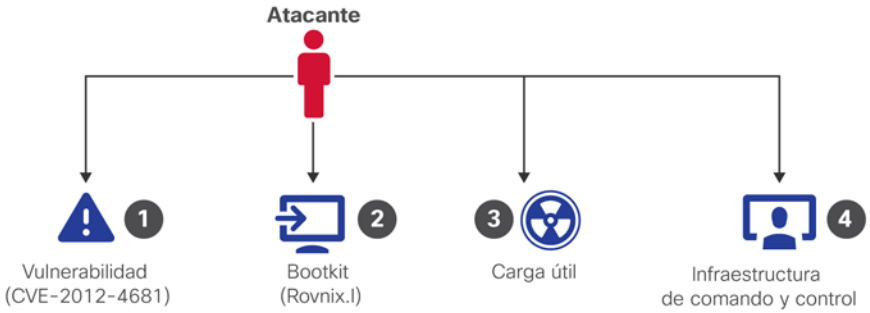
Paso 1. El atacante aprovechó una vulnerabilidad en el componente JRE (Java Runtime Environment) de Java SE 7, actualización 6, de Oracle para atacar (CVE-2012-4681); esto le permitió ejecutar un código en forma remota y eludir al administrador de seguridad.

Paso 2. Luego, se instaló el bootkit Rovnix.l para asegurar la persistencia en la máquina.

Paso 3. A continuación, se entregó la carga útil, que volvió al software malicioso totalmente operativo. (En este caso, la carga fue el ransomware Cryptolocker).

Paso 4. El ataque estableció canales de mando y control para mantener la operación activa.

Figura 2. Cuatro pasos clave en el ataque

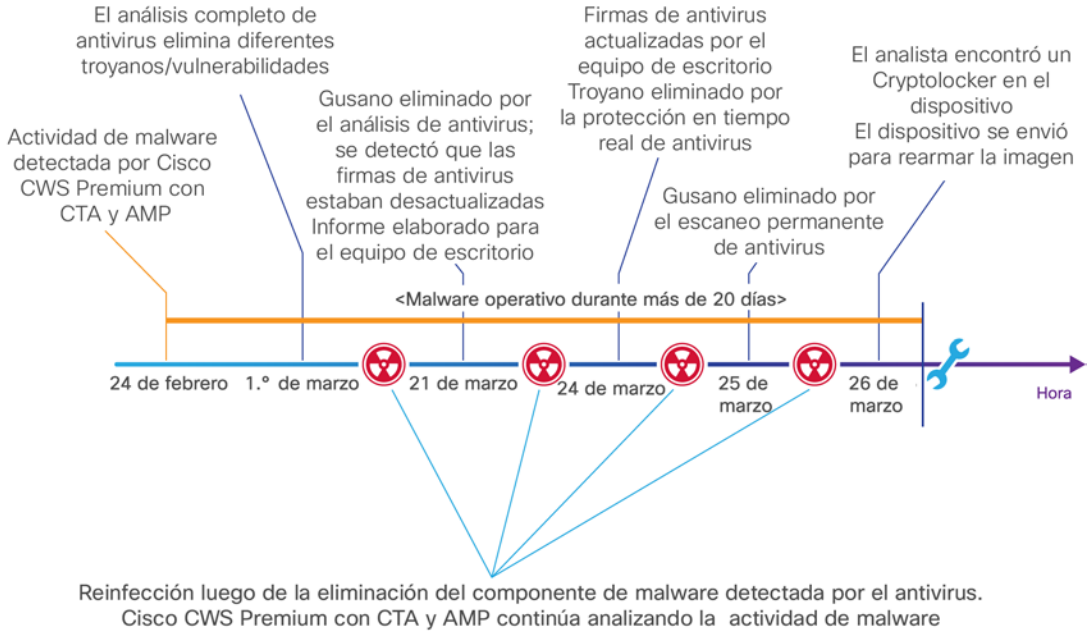


[5] La publicidad malintencionada, anuncios en línea utilizados para diseminar software malicioso, jugó un papel importante en la distribución de Cryptolocker, que se ha neutralizado desde entonces. Sin embargo, la publicidad malintencionada y el ransomware siguen siendo amenazas frecuentes utilizadas por adversarios para lanzar campañas altamente focalizadas a través de la red. Para obtener más detalles, consulte el Informe semestral de seguridad de Cisco 2014: http://www.cisco.com/web/offer/grs/190720/SecurityReport_Cisco_v4.pdf.

El equipo de seguridad del cliente intentó resolver la amenaza con herramientas antivirus. Sin embargo, como se trataba de una infección de rootkit, el software malicioso estaba profundamente integrado en el sistema infectado. La solución antivirus solo pudo eliminar algunos componentes del software malicioso. Hasta que la infección se resolvió por completo, CTA continuó alertando al equipo de seguridad de la presencia de actividad maliciosa persistente.

La Figura 3 muestra la cronología completa, desde la detección de la actividad del software malicioso hasta la resolución de la amenaza.

Figura 3. Cronología de actividad del software malicioso: de la detección a la resolución



La situación que experimentó el cliente demuestra el valor de tener CWS Premium en funcionamiento en la etapa posterior a un ataque. También recalca la dificultad de mitigar ataques avanzados con productos antivirus. El sistema CTA proporcionó evidencia de los canales de mando y control actualmente activos. Además, identificó varios dominios más que se utilizaron en la extracción no autorizada de datos. Tales infecciones representan violaciones de largo plazo enterradas en la infraestructura del cliente.

Resultados

En el mundo actual, donde los equipos de seguridad deben administrar un gran volumen de incidentes por día, no hay tiempo para buscar “una aguja en un pajar”. Los equipos de seguridad necesitan ayuda para centrarse en los ataques más avanzados, y el sistema CTA está diseñado para detectar y categorizar tales ataques.

En el caso de las infecciones de Cryptolocker del cliente, CWS Premium detectó actividad de software malicioso y aplicó la inteligencia de seguridad existente para bloquear algunos de los canales de mando y control que intentó establecer el dispositivo infectado. Sin embargo, el atacante luego utilizó una dirección IP adicional con reputación desconocida; este nuevo canal funcionó durante toda la infección. Este ejemplo destaca las virtudes (bloqueo automático) y los defectos (los nuevos canales no se bloquean) de confiar únicamente en la detección basada en firmas y reputación en Internet, y muestra por qué se requiere protección continua después de un ataque.

El siguiente es un análisis de los canales de mando y control identificados por el sistema CTA en CWS Premium, junto con modelos de solicitudes de tráfico web y estadísticas:

Tabla 1. Infraestructura de ataque

Pedido	Servidor remoto	IP de destino	País de destino	Cantidad de solicitudes	Estado de actividad
1	Servidor de C&C N.° 1	109.XXX.XXX.XXX	Países Bajos	17 (intentos)	BLOQUEADO por reputación web
2	**Servidor de C&C N.° 2**	**94.XXX.XXX.XXX**	**Luxemburgo**	**75**	**CANAL ACTIVO**
3	Servidor de C&C N.° 3	fistristy.com	Luxemburgo	175 (intentos)	BLOQUEADO por reputación web
4	Servidor de C&C N.° 4	ffeed5.com	Rusia	7 (intentos)	BLOQUEADO por reputación web

Tabla 2. Amenazas identificadas por CTA que se eliminaron posteriormente del dispositivo

Nombre de la amenaza	Eliminada
Gusano Cridex	19 de marzo
Gusano Cridex.E	19 de marzo
Troyano Tesch.B	19 de marzo
Vulnerabilidad de Java/CVE-2012-4681	19 de marzo
Descargador de troyanos Win32/Upatre	19 de marzo
Gusano Cridex	21 de marzo
Troyano Win32/Viknok.C	24 de marzo
Gusano Cridex	24 de marzo
Crypto Defense	26 de marzo

Comunicación con servidor de C&C n.° 1 (109.XXX.XXX.XXX)

Características de la comunicación:

- La cantidad total de intentos de solicitudes al servidor fue de 17; todas las comunicaciones fueron de C&C y se bloquearon por reputación.
- CTA detectó las solicitudes como intentos de utilizar la cadena de la URL como canal de comunicación (C&C). La URL (se muestra a continuación en “Ejemplo de solicitud HTTP") representa un mensaje codificado. Varias URL utilizadas en este ataque compartieron una estructura similar a la de la cadena de la URL (dirección IP/m/IbQ. *). El hecho de que el sistema de reputación haya bloqueado la comunicación agrega aún más evidencia contextual.
- Para garantizar la continuación operativa del software malicioso, el atacante también estableció un segundo canal de C&C en un servidor que aún no aparecía en los listados de reputación. La URL propiamente dicha es un mensaje codificado.

Ejemplo de solicitud HTTP (anonimizada y truncada)

http://109.XXX.XX.XXX/m/IbQXXXVjjpcE6+54HXXXdmmGcNZxtMZdvqyB5EkJAUmL/1sOXXXvq5zzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXX.g+fq4XXXOTYke6uhGHDOEeqje76v7z7i+wgqXXXFBuMz5k08yocxOH63bwQ9JMfwy8uNRM…

Comunicación con servidor de C&C n.° 2 (94.XXX.XXX.XXX)

Características de la comunicación:

- La cantidad total de solicitudes a este servidor fue de 75; todas fueron solicitudes de C&C.
- CTA detectó dos intentos de C&C como **tráfico HTTP a dirección IP (sin especificación de dominio)**. Esta categoría de comportamiento detecta solicitudes anómalas que representan comunicaciones fuera de secuencia a una dirección IP pura. Este tipo de actividades puede ser producto de un software malicioso a modo de “señal de mantenimiento” para asegurarse de que el software malicioso siga activo, o simplemente para extraer datos y recibir instrucciones adicionales de su infraestructura maliciosa (C&C). La navegación normal por Internet no produce este tipo de tráfico.
- Las 75 solicitudes de C&C pasaron inadvertidas por tecnologías basadas en firmas y reputación.

Ejemplo de solicitud HTTP (anonimizada y truncada)

http://94.XXX.XXX.XXX/m/IbQXXXVjj7iA+O54XXXodmmGcNZxtMZdvqyB5EkJAUmLb3pvGIRvqizzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXXog+fq4XXXaE0qfJf1FwalZJKnDc7U0H30+XkiXXXIApkslTo5yvM0TkHrZncwIvumxLCQ+fq4XXXOT…

Comunicación con servidor de C&C n.° 3 (fistristy.com)

Características de la comunicación:

- La cantidad total de solicitudes al dominio fistristy.com fue de 175; todas fueron comunicaciones de C&C.
- Las tecnologías basadas en firmas y reputación bloquearon todas las solicitudes.

Ejemplo de solicitud HTTP

hXXp://fistristy.com/aa/

Comunicación con servidor de C&C n.° 4 (ffeed5.com)

Características de la comunicación:

- La cantidad total de solicitudes a ffeed5.com fue de 7; todas fueron comunicaciones de C&C bloqueadas por CWS Premium.
- CTA han detectado 6 solicitudes que se ajustan a la categoría **Tráfico HTTP anómalo**. Esta categoría de comportamiento incluye comportamiento de software malicioso que no suele ajustarse a la línea de base de comportamiento que establece el análisis continuo de CTA. El término “línea de base” denota el estado de los modelos estadísticos creados por el sistema CTA, que "aprende" las tendencias y características del tráfico web analizado. CTA ajusta la línea de base automáticamente conforme cambia la red (por ejemplo, de noche y de día) para ofrecer los mejores resultados de detección.
- CTA emplea un modelado del comportamiento de la red a largo plazo para establecer una correlación entre actividades aparentemente dispares. Luego, compara esos datos con los comportamientos de los usuarios individuales en toda la red del cliente para mejorar las capacidades de detección de amenazas furtivas y persistentes.

Ejemplo de solicitud HTTP

hXXp://ffeed5.com/cmd?version=1.5&aid=555&id=24c6b407-5010-4d8d-a266-ffdac7d6f901&os=6.1.7601_1.0_64

Conclusión

El equipo de seguridad del cliente necesitaba una forma más fácil de monitorear la actividad y manejar los eventos de seguridad según un orden de prioridades en una red que tiene más de 15 000 usuarios y genera, en promedio, más de 35 millones de transacciones web por día. El cliente también necesitaba una solución que no solo bloqueara amenazas, sino que también identificara rápidamente aquellas que inevitablemente superaban otras defensas. El cliente requería una tecnología diseñada para alertar al personal de seguridad de la presencia de actividad sospechosa persistente hasta que la amenaza se resolviera por completo.

Al implementar CTA como parte de Cisco CWS Premium, el cliente tiene ahora un sistema de análisis del comportamiento de la red casi en tiempo real, que utiliza un aprendizaje automático y estadísticas avanzadas para detectar IOC en la red. En el ejemplo de infección con el ransomware Cryptolocker, CTA siguió enviando alertas de actividad maliciosa hasta que el equipo de seguridad eliminó la infección por completo. Además, la perspectiva de comportamiento de software malicioso que brinda CTA le permite al equipo de seguridad del cliente centrar su atención únicamente en la resolución de las amenazas más importantes, antes, durante y después de un ataque.

Más información

Cisco CWS Premium, que incluye CTA y AMP, se alinea con la estrategia de Cisco de ayudar a las organizaciones a superar desafíos de seguridad conocidos y emergentes, al contribuir con la detección, comprensión y erradicación de amenazas mediante análisis continuos e inteligencia de seguridad en tiempo real provista desde la nube y compartida en todas las soluciones de seguridad para mejorar la eficacia. La combinación de estas tres soluciones le permite a CWS Premium identificar nuevos canales de mando y control hasta entonces no detectados por el sector de seguridad, y ayudar a las organizaciones a superar desafíos de seguridad durante todo el ataque.

Para obtener más información sobre CWS Premium, ingrese en: http://www.cisco.com/go/cws.

Para obtener más información sobre CTA, consulte http://www.cisco.com/go/cognitive.

Para obtener más información sobre AMP, visite http://www.cisco.com/go/amp.

Sede central en América
Cisco Systems, Inc.
San José CA

Sede Central en Asia-Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede Central en Europa
Cisco Systems International BV Amsterdam.
Holanda

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y los números de fax están disponibles en el sitio web de Cisco en **www.cisco.com/go/offices**.

Impreso en EE. UU. C36-733153-00 10/14