ACME FINANCIAL SERVICES

Powered by GLESEC

CYBERSECURITY NEWS CUSTOM REPORT

Generated on 03/26/2020 by Sergio Heker

Operación Panda-19

03/19/2020 18:20

Cadena masiva de infección de malware impulsada por hackers chinos utilizando temática sobre el Coronavirus

El objetivo final de esta cadena del COVID-19 es el de acceder a los sistemas informáticos de manera remota y robar información sensible.

Check Point Research, ha detectado un **ciberataque organizado por un grupo APT chino** de contra el Ministerio de Asuntos Exteriores de Mongolia. La compañía ha desvelado que este grupo, aprovechando el flujo de noticias y alerta general en torno a la expansión del Coronavirus, **suplantó la identidad del Ministerio de Relaciones Exteriores de Mongolia y envío documentos adjuntos maliciosos** a través de correos electrónicos a los funcionarios del país. El objetivo era persuadirles, utilizando mensajes centrados en la situación actual con respecto a este virus, para que dieran a los cibercriminales de este grupo acceso remoto a la red y dejaran una **puerta abierta para el robo de información confidencial.**

Asimismo, los expertos de la compañía señalan que uno de los dos documentos relacionados con COVID-19, se titulaba **"Sobre la propagación de nuevas infecciones de Coronavirus»** e incluso citaba al Comité Nacional de Salud de China. Check Point pudo **rastrear el ciberataque y detectar la autoría** gracias a la extracción de las **huellas dactilares que dejaron los crackers en el propio código del malware** almacenado en sus servidores, que estuvieron al descubierto durante unos segundos en Internet. Gracias a esos datos, los investigadores pudieron descubrir el origen de la cadena, concluyendo que el grupo chino APT estuvo **operando desde 2016** y tiene como objetivo habitual diversas **entidades públicas y empresas de telecomunicaciones de distintos lugares del mundo**: Rusia, Ucrania, Bielorrusia y ahora Mongolia.

¿Cómo han llevado a cabo esta campaña masiva de infección de malware?

Este grupo de cibercriminales **infectaba los archivos adjuntos con un virus conocido como RoyalRoad**, que descarga un archivo en la carpeta de inicio de Word para llevar a cabo una "técnica de persistencia", que consiste en que cada vez que inicia esta aplicación, se inicia una **cadena de infección en todos los archivos con extensión WLL**. De esta forma, independientemente del archivo que se abra con Word, se produce la descarga de malware que infecta el equipo del usuario y permite **acceder y robar grandes cantidades de información sensible**

Por otra parte, el cibercriminal que se encuentra detrás de este ciberataque **operaba el servidor C&C dentro de una ventana diaria limitada**, poniéndose en línea sólo unas pocas horas cada

día, lo que hace más difícil analizar y acceder a las partes avanzadas de la cadena de infección. Este hecho, pone de manifiesto cómo **los cibercriminales aprovechan temáticas variadas para lanzar campañas masivas de ciberataques**. Sin ir más lejos, la compañía señala que ha registrado más de 4.000 dominios relacionados con el Coronavirus en todo el mundo, y que estos dominios son un 50% más maliciosos que la media.

*«El COVID-19 no sólo representa una amenaza física, sino también una **ciberamenaza**. En este sentido, nuestra investigación pone de manifiesto que un grupo chino de APT aprovechó el interés público sobre todo lo relacionado con el Coronavirus para su propio beneficio, por lo cual decidieron utilizarlo como una novedosa **cadena de infecciones informáticas**«*, señala Lotem Finkelsteen, jefe de Inteligencia de Amenazas de Check Point. *«Además, hemos descubierto que este grupo no sólo ha estado atacando a Mongolia, sino también a otros países del mundo. Por tanto, desde Check Point señalamos que todas las empresas públicas y de telecomunicaciones a nivel mundial deberían **proteger sus documentos y sitios web relacionados con el Coronavirus»***, añade Finkelsteen.

Claves para estar protegidos frente a este tipo de ciberamenazas

Aunque el objetivo de este grupo de cibercriminales eran funcionarios de instituciones públicas, desde Check Point advierten de que cualquier persona o empresa puede convertirse en una nueva víctima de este tipo de ataque informático. Por este motivo, desde la compañía señalan que *"la **prevención** es la mejor medida de seguridad **para combatir este tipo de ciberamenazas. Desconfiar** de aquellos mensajes que provengan de **remitentes desconocidos**, así como no descargar archivos adjuntos ni pinchar en enlaces dentro del correo ayudará a proteger nuestros equipos e información y reducirá en gran medida la posibilidad de convertirse en una nueva víctima de estos grupos de cibercriminales".*

Por otra parte, los expertos de Check Point aconsejan **implementar herramientas de ciberseguridad** en los dispositivos, ya que la prevención es la mejor manera de evitar riesgos. La compañía cuenta con SandBlast Mobile, una **solución contra amenazas móviles avanzadas** con infraestructura On-device Network Protection. Al revisar y controlar todo el tráfico de red del dispositivo, SandBlast Mobile evita los ataques de robo de información en todas las aplicaciones, correo electrónico, SMS, iMessage y aplicaciones de mensajería instantánea. Esta solución, además, **evita tanto el acceso a sitios web maliciosos** como el **acceso y comunicación del dispositivo con botnets**, para lo cual valida el tráfico en el propio dispositivo sin enrutar los datos a través de un gateway corporativo.

Cómo implementar un sistema de teletrabajo seguro de emergencia

03/24/2020 18:20

La implementación de un sistema de teletrabajo requiere que las empresas tomen una serie de precauciones

A tenor de los últimos acontecimientos derivados de la crisis sanitaria provocada por el brote de enfermedad por coronavirus (COVID–19), y ante el aumento de prácticas de teletrabajo, Stormshield, muestra cómo **implementar un sistema seguro de teletrabajo de emergencia.**

"El teletrabajo es una opción valorada por el personal y puesta en práctica por un número cada vez mayor de empresas, teniendo aún más sentido durante una crisis de salud como la que estamos afrontando. Sin embargo, incluso en una emergencia, la ***implementación de un sistema de teletrabajo*** *requiere que las empresas tomen una serie de* ***precauciones para evitar sorpresas desagradables,*** *especialmente en términos de* ***protección de datos***", asegura Borja Pérez, Country Manager de Stormshield Iberia.

Teletrabajo; los datos también están en riesgo

En España, el **artículo 13 del Estatuto de los Trabajadores** recoge que *"tendrá la consideración de trabajo a distancia aquel en que la prestación de la actividad laboral se realice de manera preponderante en el domicilio del trabajador o en el lugar libremente elegido por este, de modo alternativo a su desarrollo presencial en el centro de trabajo de la empresa".*

Por tanto, dicha práctica, además de un desarrollo de la actividad a distancia conlleva también el acceso remoto **a los recursos y a la información de la empresa,** información, que, por otra parte, puede contender **datos sensibles** o incluso críticos, por lo que es necesario **evitar cualquier riesgo de contaminación, fuga o pérdida de datos en el sistema de información** de la empresa. Incluso, en caso de emergencia, es necesario tomar algunas medidas antes de poner en marcha el teletrabajo, como **comprobar que los ordenadores se encuentren actualizados y el software antivirus funcionando y actualizado, proteger el acceso WiFi con una contraseña fuerte o eliminar cualquier información contenida en el nombre de la red WiFi personal** (SSID). Otro paso importante es bloquear la sesión cuando no se esté trabajando, a fin de evitar accidentes domésticos causados por una negligencia propia o de terceros.

Cuando se trate de ordenadores portátiles, y aunque lo ideal sería que se habilitara la **encriptación de todo el disco duro** del portátil para evitar ser descubierto, si esta práctica no es posible, los propietarios deben **extremar precauciones**, no perdiendo de vista sus ordenadores en ningún momento.

Por otro lado, y aunque las empresas que ya cuenten con un sistema de protección de la red para proporcionar acceso remoto seguro a su fuerza de trabajo móvil, en circunstancias especiales como estas, en las que el número de trabajadores se verá incrementado, es el momento d**e instalar clientes SSL VPN** en los ordenadores de los usuarios que los necesitarán para teletrabajar de

forma improvisada.

Mantener el contacto con lo teletrabajadores...

A pesar de las recomendaciones y procedimientos urgentes que desde la empresa se aconseja enviar a los trabajadores para explicarles la nueva forma de trabajar, especialmente a los que tienen **menos experiencia técnica,** los responsables deberán ofrecer a estos empleados puntos de contacto claramente identificados a los que recurrir. Por tanto, los **responsables de informática** deberán estar disponibles para atender a estos trabajadores, una tarea que, es posible, les reste mucho tiempo. Los equipos informáticos tendrán que estar disponibles, estén disponibles; dedicarán mucho tiempo al **soporte de los usuarios** durante este período, lo que afectará negativamente a su otro trabajo.

... y entre los trabajadores

Para facilitar la comunicación a distancia, varios proveedores de soluciones de videoconferencia están ofreciendo sus **servicios de videoconferencia de forma gratuita** en estos tiempos difíciles. No solo son útiles para las reuniones, sino también para compartir pantallas y facilitar el **apoyo técnico a distancia** sin tener que instalar otras herramientas. Sin embargo, haga una rápida comprobación para asegurarse de que sus **condiciones de servicio cumplen con sus limitaciones reglamentarias**, incluida GDPR.

Una vez las cosas vuelvan a la normalidad, será un buen momento para hacer una **recapitulación de las lecciones aprendidas**: ¿qué hay que hacer de manera diferente, y qué podría ser utilizado de nuevo en el futuro? ¿Podrían mejorarse y reutilizarse algunos procedimientos elaborados durante la anterior etapa? ¿Dónde están los principales fallos?

Por supuesto, todo esto supone que, con o sin emergencia, **todas las acciones tomadas y los problemas a los que se enfrenta la empresa han sido rastreados**, ya sea en correos electrónicos o a través de un sistema de gestión de entradas. Y tal vez haya una oportunidad de introducir el teletrabajo de forma más regular... pero esta vez con los preparativos adecuados y la **mejora de la seguridad**...