Publicado en Madrid el 14/02/2019

SpeakUp: el malware más buscado de enero ataca a los servidores de Linux

Los investigadores de Check Point destacan el auge de 'SpeakUp', un nuevo backdoor para servidores Linux que propaga el malware de cryptojacking XMRig, que continúa siendo el responsable del 8% de las infecciones mundiales

Check Point® Software Technologies Ltd. (NASDAQ: CHKP), proveedor líder especializado en ciberseguridad a nivel mundial, ha publicado su último Índice Global de Amenazas de enero de 2019. En esta entrega destaca la presencia de SpeakUp, un nuevo troyano que afecta a los servidores de Linux. Este nuevo malware backdoor, que utiliza mineros XMRig, es capaz de instalar y ejecutar cualquier carga en los dispositivos infectados.

En este momento, Speak Up es capaz de sortear a todos los antivirus del mercado. Ha conseguido propagarse a través de vulnerabilidades de los comandos que recibe desde el centro de control, entre los que se encuentra la octava vulnerabilidad más conocida: Command injection over HTTP (Inyección de comando sobre HTTP). Por ello, los investigadores de Check Point consideran que SpeakUp es una amenaza importante, puesto que puede utilizarse para descargar y propagar cualquier malware.

En enero, las cuatro variantes de malware predominantes fueron los criptojackers. Coinhive se mantiene en su posición de liderazgo, ya que ha afectado a un 12% de las organizaciones de todo el mundo. XMRig, por su parte, continúa en segunda posición con un impacto global del 8%, seguido de Cryptoloot con un 6% de empresas afectadas. A pesar de que en el Índice de enero se encuentran cuatro cryptojackers, la mitad de todas las variantes de malware indexadas pueden usarse para descargar otros malware en los dispositivos infectados.

"En enero se empiezan a vislumbrar nuevas formas de distribuir el malware que son una clara advertencia de los ataques de mayor impacto que están por venir", señala Maya Horowitz, responsable del Grupo de Inteligencia de Amenazas de Check Point. "El problema que presentan amenazas de backdoor como SpeakUp es que burlan los sistemas de detección para, posteriormente, propagar malware potencialmente más peligroso en los dispositivos infectados. Puesto que el uso de Linux está muy extendido en servidores corporativos, prevemos que SpeakUp es una amenaza que crecerá a lo largo de este año", añade Horowitz.

Los 3 malware más buscados en España en enero:
*Las flechas muestran el cambio de posición en el ranking en comparación con el mes anterior.

? Coinhive - Cryptojacker diseñado para minar la criptomoneda Monero, se activa cuando un usuario visita una página web. El JavaScript implantado utiliza muchos de los recursos del ordenador de la víctima para generar monedas, lo que impacta en el rendimiento del sistema. Ha atacado a un 18,98% de las empresas españolas.

? XMRig- Cryptojacker utilizado para minar ilegalmente la criptomoneda Monero. Este malware fue descubierto por primera vez en mayo de 2017. Ha atacado a un 13,53% de las empresas en España.
? DarkGate – Es una amenaza compleja que se instala de manera sigilosa. Este troyano, que ha afectado al 12,83% de las empresas españolas, provoca problemas de desempeño e incapacidad para ejecutar ciertos servicios o aplicaciones.

Top 3 del malware móvil mundial en enero:

Hiddad - Backdoor modular para Android. Este malware confiere privilegios de superusuario para descargar malware, al mismo tiempo que ayuda a integrarse en los procesos del sistema.

2. Lotoor- Herramienta de hacking que explota vulnerabilidades en el sistema operativo Android para obtener privilegios de root.

3. Triada - Backdoor modular para Android. Este malware confiere privilegios de superusuario para descargar malware, al mismo tiempo que ayuda a integrarse en los procesos del sistema. Asimismo, Triada también tiene la capacidad de falsificar URLs cargadas en el navegador.

Los investigadores de Check Point también han analizado las vulnerabilidades más explotadas en el último mes.

Top 3 de vulnerabilidades más explotadas en enero:

? Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow (CVE-2017-7269) - Al enviar una solicitud a través de una red a Microsoft Windows Server 2003 R2 desde Microsoft Internet Information Services 6.0, un ciberdelincuente podría ejecutar de forma remota un código arbitrario o causar una denegación de servicio en el servidor de destino. Esto se debe, principalmente, a una vulnerabilidad de desbordamiento del búfer como resultado de una validación incorrecta de un encabezado largo en una solicitud HTTP.
? Revelación de información del Repositorio Git a través del servidor web - Se ha descubierto una vulnerabilidad de divulgación de información en el Repositorio Git. La explotación exitosa de esta vulnerabilidad podría permitir una divulgación involuntaria de la información de la cuenta.
? Revelación de información a través de Heartbeat en OpenSSL TLS DTLS (CVE-2014-0160; CVE-2014-0346) - Existe un fallo en la divulgación de información en OpenSSL. La vulnerabilidad se debe a un error al manejar paquetes TLS/DTLS Heartbeat. Un ciberdelincuente puede aprovechar este error para robar contenidos de la memoria o del servidor de un cliente conectado.

El Índice de Impacto Global de Amenazas de Check Point y su Mapa de ThreatCloud se basan en la inteligencia ThreatCloud de Check Point, la red de colaboración más grande para combatir la ciberdelincuencia que ofrece datos de amenazas y tendencias de ataque desde una red global de

sensores de amenazas. La base de datos ThreatCloud contiene más de 250 millones de direcciones analizadas para descubrir bots, más de 11 millones de firmas de malware y más de 5.5 millones de sitios web infectados, e identifica millones de tipos de malware diariamente.

La lista completa de las 10 familias principales de malware en enero está disponible en el blog de Check Point.

Threat Prevention Resources de Check Point también está disponible aquí.

Datos de contacto:
Jorge

Nota de prensa publicada en: Madrid

Categorías: Internacional Software Ciberseguridad