Boletín de Ciberseguridad

Fecha de Publicación
04/07/2022- N.º 37

Mes de Julio
20/06/2022 - 04/07/2022

Datasec

Índice

Introducción

Por medio de este boletín informativo estaremos destacando de forma quincenal, las noticias más relevantes en el ámbito de la ciberseguridad a nivel regional e internacional.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes activos, amenazas por medios informáticos nuevos, así como recomendaciones específicas de prevención. La publicación de dichas noticias dependerá de la importancia y calidad informativa de las mismas.

A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

En esta primera quincena del mes de julio se destacan 5 noticias de relevancia: 3 sobre vulnerabilidades tecnológicas y 2 sobre prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Amazon parchea la vulnerabilidad en la aplicación Fotos de Android

Amazon, en diciembre de 2021, corrige una vulnerabilidad de alta gravedad que afectaba a su aplicación Fotos para Android y que podría haberse aprovechado para robar los tokens de acceso de un usuario.

CISA advierte sobre la explotación activa de la vulnerabilidad de Linux 'PwnKit'

La CISA agregó esta semana una vulnerabilidad de Linux denominada PwnKit a su Catálogo de Vulnerabilidades Explotadas Conocidas, citando evidencia de explotación activa.

Se lanzó un descifrador gratuito para el ransomware Hive

Se lanzó un ejecutable junto con un manual de usuario que proporciona instrucciones paso a paso para recuperar datos cifrados de forma gratuita.

Microsoft	**Campaña de malware de criptominería dirigida a servidores Linux**	CRÍTICO

Descripción

Un grupo de actores de amenazas en la nube rastreado como 8220 ha actualizado su conjunto de herramientas de malware para violar los servidores Linux con el objetivo de instalar criptomineros como parte de una campaña de larga duración.

Estado

8220, activo desde principios de 2017, es un actor de amenazas de minería Monero de habla china llamado así por su preferencia para comunicarse con servidores de comando y control (C2) a través del puerto 8220. También es el desarrollador de una herramienta llamada whatMiner.

En julio de 2019, el equipo de seguridad en la nube de Alibaba descubrió un cambio adicional en las tácticas del adversario y señaló el uso de rootkits para ocultar el programa de minería. Dos años más tarde, la pandilla resurgió con variantes de botnet Tsunami IRC y un minero personalizado "PwnRig".

Ahora, según Microsoft, se ha observado que la campaña más reciente que afecta a los sistemas Linux i686 y x86_64 convierte en armas los exploits de ejecución remota de código para el Atlassian Confluence Server (CVE-2022-26134) y Oracle WebLogic (CVE-2019-2725) recientemente revelados para el acceso inicial.

Remediación / Referencias

Microsoft recomienda encarecidamente que los clientes instalen las actualizaciones para estar completamente protegidos contra la vulnerabilidad.

Por mayor información acceder a:
https://thecybersecurity.news/general-cyber-security-news/microsoft-warns-of-cryptomining-malware-campaign-targeting-linux-servers-19918/

amazon	Amazon parchea la vulnerabilidad en la aplicación Fotos de Android	CRÍTICO

Descripción

Amazon, en diciembre de 2021, corrige una vulnerabilidad de alta gravedad que afectaba a su aplicación Fotos para Android y que podría haberse aprovechado para robar los tokens de acceso de un usuario.

Estado

La fuga es el resultado de una configuración incorrecta en uno de los componentes de la aplicación llamado "com.amazon.gallery.thor.app.activity.ThorViewActivity" que está definido en el archivo AndroidManifest.xml y que, cuando se inicia, inicia una solicitud HTTP con un encabezado que contiene el token de acceso.

En pocas palabras, significa que una aplicación externa podría enviar una petición, un “request HTTP” es un mensaje para facilitar la comunicación entre aplicaciones, esta inicia la actividad y para la petición vulnerable en cuestión, esta redirige la solicitud HTTP a un servidor controlado por el atacante y extraer el token de acceso.

Este error está calificado como de pérdida de autenticación, que podría haber permitido que las aplicaciones maliciosas instaladas en el dispositivo obtuvieran los tokens de acceso, otorgando al atacante permisos para hacer uso de las API para actividades de seguimiento.

Esto podría variar desde eliminar archivos y carpetas en Amazon Drive hasta incluso explotar el acceso para organizar un ataque de ransomware leyendo, encriptando y reescribiendo los archivos de la víctima mientras borra su historial.

Remediación / Referencias

Amazon declaró que los problemas estaban "resueltos" y dijo que se había "implementado en producción" una solución.

Por mayor información acceder a:
https://dearce.com.uy/amazon-corrige-una-vulnerabilidad-de-alta-gravedad-en-la-aplicacion-amazon-photos-para-android/

	CISA advierte sobre la explotación activa de la vulnerabilidad de Linux 'PwnKit'	CRÍTICO

Descripción

La CISA agregó esta semana una vulnerabilidad de Linux denominada PwnKit a su Catálogo de Vulnerabilidades Explotadas Conocidas, citando evidencia de explotación activa.

Estado

El problema, rastreado como CVE-2021-4034 (puntuación CVSS: 7,8), salió a la luz en enero de 2022 y se refiere a un caso de escalada de privilegios locales en la utilidad pkexec de polkit, que permite a un usuario autorizado ejecutar comandos como otro usuario.

Polkit es un conjunto de herramientas para controlar los privilegios de todo el sistema en sistemas operativos similares a Unix y proporciona un mecanismo para que los procesos sin privilegios se comuniquen con los procesos privilegiados.

La explotación exitosa de la falla podría inducir a pkexec a ejecutar código arbitrario, otorgando a un atacante sin privilegios derechos administrativos en la máquina de destino. No está claro de inmediato cómo se está armando la vulnerabilidad, ni hay información sobre la identidad del actor de amenazas que puede estar explotándola.

También se incluye en el catálogo CVE-2021-30533, una deficiencia de seguridad en los navegadores web basados en Chromium que fue aprovechada por un actor de amenazas de publicidad maliciosa con nombre en código Yosec para entregar cargas útiles peligrosas el año pasado.

Remediación / Referencias

Se recomienda que las organizaciones den prioridad a la corrección oportuna de los problemas. Sin embargo, las Agencias del Poder Ejecutivo Federal Civil están obligadas a reparar las fallas antes del 18 de julio de 2022.

Para saber más invitamos a visitar el siguiente sitio:
https://nvd.nist.gov/vuln/detail/CVE-2021-4034

	Se lanzó un descifrador gratuito para el ransomware Hive	PREVENCIÓN

Descripción

Se publicó un ejecutable junto con un manual de usuario que proporciona instrucciones paso a paso para recuperar datos cifrados de forma gratuita.

Estado

La operación de ransomware Hive ha estado activa desde junio de 2021, proporciona Ransomware-as-a-Service Hive y adopta un modelo de doble extorsión que amenaza con publicar datos robados a las víctimas en su sitio de fuga (HiveLeaks).
En abril de 2021, la Oficina Federal de Investigaciones (FBI) publicó una alerta rápida sobre los ataques de ransomware Hive que incluye detalles técnicos e indicadores de compromiso asociados con las operaciones de la pandilla. Según un informe, el ransomware Hive es una de las 10 principales cepas de ransomware por ingresos en 2021. El grupo usó una variedad de métodos de ataque, incluidas campañas de malspam, servidores RDP vulnerables y credenciales de VPN comprometidas.

En febrero, se descubrió una falla en el algoritmo de cifrado utilizado por el ransomware Hive que les permitía descifrar datos sin conocer la clave privada utilizada por la pandilla para cifrar archivos.

Hive ransomware utiliza un esquema de cifrado híbrido, pero utiliza su propio cifrado simétrico para cifrar archivos. Se pudo recuperar la clave maestra para generar la clave de cifrado de archivos sin la clave privada del atacante, mediante el uso de una vulnerabilidad criptográfica identificada a través del análisis. Como resultado de diversos experimentos, los archivos cifrados se descifraron con éxito utilizando la clave maestra recuperada. Hasta donde se sabe, este es el primer intento exitoso de descifrar el ransomware Hive.

Los expertos detallaron el proceso utilizado por el ransomware Hive para generar y almacenar la clave maestra para los archivos de las víctimas. El ransomware genera 10MB de datos aleatorios y los utiliza como clave maestra. El malware se extrae de un desplazamiento específico de la clave maestra de 1 MB y 1 KB de datos para cada archivo que se va a cifrar y usar como flujo de claves. El desplazamiento se almacena en el nombre de archivo cifrado de cada archivo. Esto significa que los expertos pudieron determinar el desplazamiento del flujo de claves almacenado en el nombre del archivo y descifrar el archivo.

Remediación / Referencias

Los hallazgos de los investigadores probablemente fueron el punto de partida para el trabajo de la agencia KISA que finalmente desarrolló un descifrador.

Por mayor información acceder a:
https://www.welivesecurity.com/la-es/2022/07/01/publican-descifrador-gratis-ransomware-hive/

kaspersky	**La guía de Kaspersky para los TTP de los grupos de ransomware modernos**	PREVENCIÓN

Descripción

El análisis de ransomware recibe mucha cobertura en informes comerciales y públicos, y los proveedores publican docenas de publicaciones relacionadas con ransomware cada año. Estos informes brindan análisis sobre familias de malware específicas o nuevas muestras, describen las actividades de un grupo de ransomware en particular, brindan consejos generales sobre cómo evitar que funcione el ransomware, etc.

Estado

Los analistas de malware y los profesionales de la seguridad pueden aprender mucho de estos informes, pero no gran parte del contenido tiene un uso inmediato o práctico.

Con el lanzamiento del informe TTP del ransomware moderno, los expertos de Kaspersky han adoptado un enfoque diferente. Se quiere familiarizar al lector con las diferentes etapas de la implementación del ransomware, cómo los ciberdelincuentes usan RAT y otras herramientas en las distintas etapas y qué pretenden lograr.

El informe también proporciona una guía visual para defenderse contra ataques de ransomware dirigidos, utilizando los grupos más prolíficos como ejemplos, y presenta al lector las reglas de detección SIGMA.

Para el informe, se seleccionaron los ocho grupos de ransomware más comunes:

- Conti/Ryuk
- Pysa
- Clop (TA505)
- Hive
- Lockbit2.0
- RagnarLocker
- BlackByte
- BlackCat

Se analizó en detalle los ataques perpetrados por estos grupos y se emplearon técnicas y tácticas para identificar una gran cantidad de TTP (Técnicas tácticas y comportamientos) compartidos. Al rastrear a todos los grupos y detectar sus ataques, se observó que las técnicas centrales siguen siendo las mismas a lo largo de la cadena de ataques cibernéticos.

Los patrones de ataque revelados no son accidentales porque esta clase de ataque requiere que los “piratas informáticos” pasen por ciertas etapas, como penetrar en la red corporativa o en la computadora de la víctima, entregar malware, descubrimiento adicional, secuestro de cuentas, eliminación de instantáneas, eliminación de copias de seguridad y, finalmente, logrando sus objetivos.

Para resaltar los componentes comunes y los TTP compartidos por los grupos de ransomware en diferentes patrones de ataque, se ha creado un diagrama de cadena de eliminación cibernética común. Proporciona una representación visual de las técnicas y tácticas utilizadas por diferentes operadores de ransomware.

Remediación / Referencias

Este informe está escrito para analistas de SOC, equipos de búsqueda de amenazas, analistas de inteligencia de amenazas cibernéticas, especialistas en análisis forense digital y especialistas

en seguridad cibernética que están involucrados en el proceso de respuesta a incidentes y/o desean proteger el entorno del que son responsables de ataques de ransomware dirigidos

Para saber más invitamos a visitar el siguiente sitio:
https://blog.segu-info.com.ar/2022/06/kill-chain-para-8-familias-de.html

Conclusiones

Vemos en las últimas noticias que se realizan avances importantes en cuanto a reducir la destrucción de información, la extorsión y demás riesgos y amenazas.
Esto es gracias a grupos de personas que trabajamos en la defensa de los activos de información más relevantes.
Los grupos de inteligencia coordinadas, están basados en investigadores que diariamente observan comportamientos y escudriñan con ingeniería inversa los softwares que otras personas con intenciones delictivas crearon.

Existen múltiples equipos multidisciplinarios que realizan estas actividades. Las operaciones de monitoreo de ciberseguridad son parte fundamental, para que los activos digitales estén garantizadamente protegidos.

Los centros de operaciones de un SOC, son los especialistas en detectar y reconocer la información y comportamientos legítimos de los no legítimos y prohibidos por las políticas de seguridad.
Estos equipos de trabajo son los que garantizan y hacen cumplir esta política que muchas veces queda solamente escrita y nadie la implementa. Es entonces así que la ciberseguridad de las organizaciones se empieza a efectivizar.
Esto sucede porque en muchas organizaciones pensaron que con un CISO (Gerente de Seguridad de la Información) y este con un equipo de Infraestructura y Operaciones tecnológicas podría hacer casi todo su trabajo, lo cual claramente no era cierto.
Los equipos de ciberseguridad tienen una basta interrelación con otros equipos de trabajo en una organización y además contar con sus propios roles y funciones operativas, de esta forma los arquitectos de seguridad se interrelacionan con administradores de firewalls, gestores de accesos personales, entre otros.

El CISO moderno se apoya de equipos que trabajan solamente en actualizaciones de software por parches de seguridad, un rol específico para reducir los riesgos que provienen por falta de mantenimiento del ciclo de vida de los programas y sistemas, que suele ser un gran riesgo en la mayoría de organizaciones.
El CISO tendrá una mirada global y podrá decidir en cuanto a las directrices y prioridades del negocio, pero sin un equipo de trabajo que lo acompañe de forma completa y dedicada, su trabajo suele dar pocos frutos.
Desde Datasec acompañamos a organizaciones y CISOs para que cuenten con especialistas dedicados a la mejora en la efectividad de controles de seguridad de la información y ciberseguridad.

¡Hasta la próxima quincena de noticias!