GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4824

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABILIDADES	1	1	1
MALWARE	0	2	1
NOTICIAS DE CIBERSEGURIDAD	1	1	1

VULNERABILIDADES

Un fallo en el diseño de la VPN de Fortinet oculta ataques de fuerza bruta exitosos

Investigadores de Pentera han descubierto una vulnerabilidad en el mecanismo de registro de Fortinet VPN que permite a los atacantes ocultar intentos de inicio de sesión exitosos durante ataques de fuerza bruta. Este fallo de diseño registra únicamente los intentos fallidos en la fase de autenticación, mientras que los exitosos se registran en la fase de autorización. Al interrumpir el proceso después de la autenticación exitosa pero antes de la autorización, los atacantes pueden validar credenciales sin generar registros de éxito, creando una falsa sensación de seguridad.

Para mitigar este riesgo, se recomienda a los administradores de sistemas implementar medidas adicionales de seguridad, como limitar los intentos de inicio de sesión y configurar bloqueos temporales tras múltiples fallos.

Prioridad: Crítico

Ampliar información:

https://www.bleepingcomputer.com/news/security/fortinet-vpn-design-flaw-hides-successful-brute-force-attacks/

Apple corrige dos vulnerabilidades de día cero utilizadas en ataques a Macs con procesador Intel

Apple ha lanzado actualizaciones de seguridad de emergencia para corregir dos vulnerabilidades de día cero que estaban siendo explotadas en ataques dirigidos a sistemas Mac con procesadores Intel. Las fallas, identificadas como CVE-2024-44308 y CVE-2024-44309, se encuentran en los componentes JavaScriptCore y WebKit de macOS. La primera permite la ejecución remota de código a través de contenido web malicioso, mientras que la segunda facilita ataques de cross-site scripting (XSS).

Estas vulnerabilidades fueron descubiertas por Clément Lecigne y Benoit Sevens del Grupo de Análisis de Amenazas de Google. Apple ha abordado estos problemas en las versiones macOS Sequoia 15.1.1, iOS 17.7.2, iPadOS 17.7.2, iOS 18.1.1, iPadOS 18.1.1 y visionOS 2.1.1. Se recomienda a los usuarios actualizar sus dispositivos a las versiones más recientes para protegerse contra posibles explotaciones.

Prioridad: Urgente

Ampliar información:

https://www.bleepingcomputer.com/news/security/apple-fixes-two-zero-days-used-in-attacks-on-intel-based-macs/

Más de 2.000 firewalls de Palo Alto fueron hackeados debido a errores recientemente corregidos

Recientemente, se ha informado que más de 2,000 firewalls de Palo Alto Networks han sido comprometidos mediante la explotación de dos vulnerabilidades de día cero que fueron parcheadas hace poco. Las fallas en cuestión son CVE-2024-0012, una vulnerabilidad de omisión de autenticación en la interfaz web de gestión de PAN-OS, y CVE-2024-9474, una escalada de privilegios que permite a los atacantes ejecutar comandos con privilegios de root en el firewall. Estas vulnerabilidades han sido aprovechadas por actores maliciosos para obtener acceso no autorizado y desplegar malware en los dispositivos afectados.

Palo Alto Networks ha observado que los ataques se originan principalmente desde direcciones IP asociadas con servicios VPN anónimos, lo que indica que los atacantes están utilizando técnicas para ocultar su identidad. La empresa ha instado a sus clientes a restringir el acceso a la interfaz de gestión de los firewalls, permitiendo únicamente conexiones desde direcciones IP de confianza, y a aplicar las actualizaciones de seguridad disponibles para mitigar estas amenazas.

Prioridad: Importante

Ampliar información:

https://www.bleepingcomputer.com/news/security/over-2-000-palo-alto-firewalls-hacked-using-recently-patched-bugs/

Recomendaciones generales sobre vulnerabilidades:

Para reducir las vulnerabilidades en los sistemas, se sugieren las siguientes acciones clave:

Aplicar parches de seguridad de forma regular para solucionar fallos conocidos.

Añadir una capa adicional de seguridad, como la autenticación de dos factores (2FA), para complicar el acceso no autorizado.

Restringir los permisos de usuarios y aplicaciones, limitando el acceso solo a lo necesario para reducir riesgos.

Utilizar herramientas de detección de intrusiones para monitorizar y detectar comportamientos sospechosos.

Estas medidas son esenciales para contribuir a fortalecer la seguridad de los sistemas.

MALWARE

APT-K-47 utiliza señuelos con temática de Hajj para distribuir malware avanzado Asyncshell

El grupo de amenazas conocido como APT-K-47, también denominado Mysterious Elephant, ha sido vinculado a una campaña de ciberataques que emplea señuelos temáticos relacionados con el Hajj para distribuir una versión avanzada del malware Asyncshell. Según el equipo de Knownsec 404, los atacantes utilizan archivos CHM (Microsoft Compiled HTML Help) que aparentan contener información sobre la política del Hajj 2024. Al abrir estos archivos, se muestra un documento señuelo mientras, en segundo plano, se ejecuta un archivo malicioso que establece una conexión de comando y control con servidores remotos.

Esta variante de Asyncshell permite a los atacantes ejecutar comandos cmd y PowerShell en los sistemas comprometidos. Se han identificado cuatro versiones diferentes de Asyncshell, que han evolucionado en sus métodos de comunicación y técnicas de persistencia. Inicialmente, el malware utilizaba TCP para las comunicaciones C2, pero las versiones más recientes han adoptado HTTPS para mejorar la evasión de detección. Además, se ha observado el uso de scripts de Visual Basic y tareas programadas para mantener la persistencia en los sistemas afectados

Prioridad: Urgente

Ampliar información:

https://thehackernews.com/2024/11/apt-k-47-uses-hajj-themed-lures-to.html

---

TAG-112, grupo vinculado a China, lanza campaña de espionaje con Cobalt Strike

El grupo de ciberamenazas TAG-112, vinculado a China, ha comprometido sitios web de la comunidad tibetana, como Tibet Post y la Universidad Tántrica Gyudmed, para distribuir el malware Cobalt Strike. Según el Insikt Group de Recorded Future, los atacantes inyectaron JavaScript malicioso en estos sitios, presentando alertas falsas de certificados TLS para engañar a los visitantes y hacerles descargar un archivo ejecutable disfrazado de certificado de seguridad.

Este archivo, al ejecutarse, carga una versión de Cobalt Strike Beacon, permitiendo a los atacantes realizar actividades de espionaje. La campaña muestra similitudes con las tácticas de TAG-102, también conocido como Evasive Panda, aunque TAG-112 emplea técnicas menos sofisticadas, como la falta de ofuscación en su JavaScript y el uso de herramientas estándar en lugar de malware personalizado.

Prioridad: Urgente

Ampliar información:

https://thehackernews.com/2024/11/china-linked-tag-112-targets-tibetan.html

---

Hackers rusos distribuyen el malware HATVIBE y CHERRYSPY en Europa y Asia

Investigadores de Recorded Future han identificado una campaña de ciberespionaje atribuida al grupo TAG-110, vinculado a actores estatales rusos, que afecta a organizaciones gubernamentales, grupos de derechos humanos e instituciones educativas en Asia Central, Asia Oriental y Europa. Este grupo emplea las herramientas maliciosas HATVIBE y CHERRYSPY; la primera actúa como cargador para desplegar CHERRYSPY, un backdoor escrito en Python diseñado para la exfiltración de datos y espionaje. Las

infecciones iniciales se logran mediante la explotación de vulnerabilidades en aplicaciones web públicas y correos electrónicos de phishing.

Para mitigar estos riesgos, se recomienda a las organizaciones revisar y fortalecer las configuraciones de seguridad de sus servidores, implementar soluciones avanzadas de detección de intrusiones y monitorear de forma continua la actividad de la red en busca de comportamientos anómalos. Estas medidas son clave para proteger las redes corporativas de ataques potenciales.

Prioridad: Importante

Ampliar información:

https://thehackernews.com/2024/11/russian-hackers-deploy-hatvibe-and.html

---

Recomendaciones generales sobre malware:

Para protegerse del malware, es fundamental:

- Mantener el software y los sistemas operativos actualizados de manera regular, ya que los atacantes suelen aprovechar vulnerabilidades en versiones obsoletas.
- Utilizar programas antivirus y antimalware confiables, asegurándose de que siempre estén actualizados.
- Activar la autenticación multifactor (MFA) para asegurar cuentas sensibles y dificultar el acceso no autorizado.
- Ser cauteloso con correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de infección por malware.
- Hacer copias de seguridad periódicas de los archivos importantes, para evitar pérdidas en caso de ataques como el ransomware.

- Restringir los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

Hackers vulneran el wifi de una empresa estadounidense desde Rusia en un "ataque al vecino más cercano"

El grupo de hackers rusos APT28, también conocido como Fancy Bear, ha llevado a cabo una intrusión cibernética en una empresa estadounidense mediante una técnica innovadora denominada "ataque al vecino más cercano". Según un informe de BleepingComputer, los atacantes comprometieron inicialmente una organización ubicada en un edificio adyacente al objetivo principal, dentro del alcance de su red Wi-Fi. Desde esta posición, lograron acceder a la red Wi-Fi de la empresa estadounidense, a pesar de estar físicamente en Rusia.

Este método permitió a APT28 eludir las medidas de seguridad tradicionales que dependen de la proximidad física para la autenticación de redes inalámbricas. La técnica destaca la capacidad de los atacantes para explotar vulnerabilidades en redes Wi-Fi corporativas desde ubicaciones remotas y la necesidad de implementar medidas de seguridad más robustas en las comunicaciones inalámbricas empresariales.

Prioridad: Crítico

Ampliar información:

https://www.bleepingcomputer.com/news/security/hackers-breach-us-firm-over-wi-fi-from-russia-in-nearest-neighbor-attack/

Google expone GLASSBRIDGE: una red de sitios de noticias falsas con influencia pro-China

Google ha revelado la existencia de GLASSBRIDGE, una operación de influencia pro-China que utiliza una red de sitios de noticias falsos y servicios de distribución de prensa para difundir narrativas alineadas con los intereses del gobierno chino. Según el equipo de Análisis de Amenazas de Google (TAG), desde 2022 se han bloqueado más de mil sitios web operados por GLASSBRIDGE en productos como Google News y Google Discover.

Estos sitios, gestionados por empresas de relaciones públicas digitales como Shanghai Haixun Technology y Shenzhen Haimai Yunxiang Media, se presentan como medios independientes que republican contenido de medios estatales chinos y comunicados de prensa. Además, se ha identificado a DURINBRIDGE como una firma comercial que distribuye contenido para Haixun y DRAGONBRIDGE, otro actor conocido por sus operaciones de influencia pro-China.

Prioridad: Urgente

Ampliar información:

https://thehackernews.com/2024/11/google-exposes-glassbridge-pro-china.html

---

Hackers norcoreanos roban 10 millones de dólares con estafas basadas en inteligencia artificial y malware en LinkedIn

El grupo de amenazas cibernéticas conocido como Sapphire Sleet, vinculado a Corea del Norte, ha llevado a cabo campañas de ingeniería social que resultaron en el robo de más de $10 millones en criptomonedas en un período de seis meses. Según Microsoft, estos actores maliciosos crearon perfiles falsos en LinkedIn, haciéndose pasar por reclutadores y solicitantes de empleo, para atraer a sus víctimas.

Una de las tácticas empleadas por Sapphire Sleet consistía en hacerse pasar por capitalistas de riesgo interesados en las empresas de las víctimas, organizando reuniones en línea. Durante estas interacciones, se inducía a las víctimas a descargar archivos maliciosos, como scripts de AppleScript o Visual Basic, que instalaban malware en sus sistemas. Este software permitía a los atacantes obtener credenciales y acceder a billeteras de criptomonedas. Además, se observó el uso de herramientas de inteligencia artificial, como Faceswap, para crear imágenes falsas y suplantar identidades en plataformas como GitHub y LinkedIn, facilitando la obtención de empleos remotos y el acceso a información sensible.

Prioridad: Importante

Ampliar información:

https://thehackernews.com/2024/11/north-korean-hackers-steal-10m-with-ai.html