GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1824

En alianza con

TD SYNNEX FORTINET

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
VULNERABIILIDADES	0	2	3
MALWARE	0	0	6
NOTICIAS DE CIBERSEGURIDAD	0	0	3

VULNERABILIDADES

Remediación para una vulnerabilidad crítica en PAN-OS que está siendo atacada

La vulnerabilidad, identificada como CVE-2024-3400 (puntuación CVSS: 10.0), podría ser aprovechada para obtener ejecución remota de comandos de shell no autenticada en dispositivos susceptibles. Se ha abordado en varias versiones de PAN-OS 10.2.x, 11.0.x y 11.1.x.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/04/palo-alto-networks-outlines-remediation.html

CrushFTP advierte a usuarios para parchear sus servidores

CrushFTP advirtió a sus clientes en un memo privado sobre una vulnerabilidad de día cero activamente explotada, solucionada en las nuevas versiones lanzadas hoy, instándolos a parchear sus servidores de inmediato. Como también explica la compañía en un aviso de seguridad público publicado el viernes, este error de día cero permite a los atacantes no autenticados escapar del sistema de archivos virtual (VFS) del usuario y descargar archivos del sistema.

Prioridad: 2 Urgente.

Ampliar información:

https://securityaffairs.com/162067/hacking/crushftp-zero-day-exploited.html

---

Hackers patrocinados por el estado explotan dos vulnerabilidades de día cero de Cisco con fines de espionaje

Una nueva campaña de malware aprovechó dos vulnerabilidades de día cero en el equipo de red de Cisco para entregar malware personalizado y facilitar la recopilación encubierta de datos en entornos objetivo. Cisco Talos, que denominó la actividad como ArcaneDoor, la atribuyó al trabajo de un actor patrocinado por el estado, sofisticado y previamente no documentado, al que sigue bajo el nombre de UAT4356 (también conocido como Storm-1849 por Microsoft.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/04/state-sponsored-hackers-exploit-two.html

---

Vulnerabilidad de confusión de dependencias encontrada en un proyecto Apache archivado

El equipo de investigación Legit descubrió recientemente una vulnerabilidad de confusión de dependencias en un proyecto archivado de Apache. Este descubrimiento resalta la necesidad de considerar los proyectos y dependencias de terceros como posibles puntos débiles en la fábrica de desarrollo de software, especialmente los proyectos de código abierto archivados que pueden no recibir actualizaciones regulares o parches de seguridad.

Prioridad: 3 Importante.

Ampliar información:

https://www.infosecurity-magazine.com/news/dependency-confusion-flaw-found

---

Análisis de la herramienta personalizada post-compromiso de Forest Blizzard para explotar CVE-2022-38028

Microsoft Threat Intelligence está publicando los resultados de nuestra investigación de larga data sobre la actividad del actor de amenazas Forest Blizzard (STRONTIUM) con base en Rusia, utilizando una herramienta personalizada para elevar privilegios, robando credenciales en redes comprometidas. Desde al menos junio de 2020 y posiblemente desde abril de 2019, Forest Blizzard ha utilizado la herramienta, a la que nos referimos como GooseEgg, para explotar la vulnerabilidad CVE-2022-38028 en el servicio de Windows Print Spooler mediante la modificación de un archivo de restricciones de JavaScript y su ejecución con permisos de nivel del sistema.

Prioridad: 3 Importante.

Ampliar información:

https://securityaffairs.com/162154/apt/apt28-gooseegg-tool-win-bug.html

---

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y aplicaciones actualizados conforme a información directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se pueden aplicar las actualizaciones de inmediato.
- Establecer una política y un plan periódico de mitigación de vulnerabilidades.
- Utilizar soluciones de gestión de vulnerabilidades para priorizar y abordar las vulnerabilidades.
- Adquirir tecnologías para bloquear accesos maliciosos y explotaciones de vulnerabilidades conocidas y de día cero.
- Utilizar servicios de Ethical Hacking para identificar posibles superficies de ciberataque y proteger los datos sensibles.
- Implementar sistemas de detección de intrusiones, sistemas de prevención de pérdida de datos y firewalls de aplicaciones web.
- Realizar auditorías de seguridad y pruebas de penetración regularmente.
- Educar a los usuarios y al personal de TI sobre las mejores prácticas de seguridad cibernética.
- Establecer políticas de seguridad sólidas, como el uso de contraseñas seguras y la gestión adecuada de accesos y privilegios.

MALWARE

Hack de DRM de Microsoft podría permitir descarga de películas desde servicios de streaming populares

Según la empresa de investigación en ciberseguridad con sede en Polonia, AG Security Research, la tecnología de acceso y protección de contenido de Microsoft, PlayReady, se ve afectada por vulnerabilidades que podrían permitir a suscriptores malintencionados descargar ilegalmente películas pertenecientes a servicios de streaming populares.

Prioridad: 3 Importante.

Ampliar información:

https://security-explorations.com/microsoft-playready.html

Abuso de los comentarios de GitHub para enviar malware a través de direcciones URL de repositorio de Microsoft

Una falla en GitHub, o posiblemente una decisión de diseño, está siendo aprovechada por actores de amenazas para distribuir malware utilizando URL asociadas con un repositorio de Microsoft, lo que hace que los archivos parezcan confiables. Aunque la mayoría de la actividad de malware se ha centrado en las URL de GitHub de Microsoft, esta "falla" podría ser aprovechada con cualquier repositorio público en GitHub, permitiendo a los actores de amenazas crear señuelos muy convincentes.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/github-comments-abused-to-push-malware-via-microsoft-repo-urls

---

Doble caída del ransomware Revictimización

La ciberextorsión (Cy-X) o ransomware, como se le conoce más comúnmente, es un tema que ha atraído mucha atención en los últimos tres o cuatro años. Orange Cyberdefense ha cubierto ampliamente esta amenaza desde 2020. En el último informe anual de seguridad, Security Navigator 2024 (SN24), la investigación mostró un aumento del 46% entre 2022 y 2023 (período del cuarto trimestre de 2022 al tercer trimestre de 2023).

Prioridad: 3 importante.

Ampliar información:

https://thehackernews.com/2024/04/ransomware-double-dip-re-victimization.html

---

CoralRaider continúa expandiendo su victimología utilizando tres programas de robo de información

Cisco Talos descubrió una nueva campaña en curso desde al menos febrero de 2024, operada por un actor de amenazas que distribuye tres conocidos malwares de robo de información, incluidos Cryptbot, LummaC2 y Rhadamanthys. Talos también descubrió un nuevo argumento de línea de comandos de PowerShell incrustado en el archivo LNK para evadir los productos antivirus y descargar la carga útil final en el host de las víctimas.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/coralraider-attacks-use-cdn-cache-to-push-info-stealer-malware

---

Distribución de un infostealer creado con Electron

El Centro de Inteligencia de Seguridad de AhnLab (ASEC) ha descubierto una variante de Infostealer creada con Electron. Electron es un marco que permite desarrollar aplicaciones utilizando JavaScript, HTML y CSS. Discord y Microsoft VSCode son ejemplos importantes de aplicaciones creadas con Electron. Las aplicaciones desarrolladas con Electron se empaquetan y suelen distribuirse en formato de instalador Nullsoft Scriptable Install System (NSIS).

Prioridad: 3 Importante.

Ampliar información:

https://asec.ahnlab.com/en/64445/

Anuncio de Google para Facebook redirige a estafa

Es ampliamente conocido que los estafadores de soporte técnico atraen a nuevas víctimas comprando anuncios para ciertas palabras clave relacionadas con su audiencia. Lo que quizás sea menos conocido es cómo es posible suplantar a las principales marcas y salir impune.

Prioridad: 3 Importante.

Ampliar información:

https://www.malwarebytes.com/blog/scams/2024/04/google-ad-for-facebook-redirects-to-scam

---

Recomendaciones generales sobre Malware:

- Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
- Utilizar soluciones de seguridad confiables, como antivirus y firewalls, y mantenerlos actualizados.
- Implementar autenticación multifactor en cuentas y sistemas para agregar una capa adicional de seguridad.
- Educar a los usuarios sobre la importancia de no hacer clic en enlaces o adjuntos sospechosos en correos electrónicos o mensajes.
- Realizar copias de seguridad regulares de los datos importantes y guardarlas en un lugar seguro y fuera de línea.
- Evitar descargar software de fuentes no confiables y solo utilizar tiendas oficiales para obtener aplicaciones.
- Establecer políticas de contraseñas sólidas y cambiarlas regularmente.
- Limitar los privilegios de acceso para los usuarios y las cuentas, y solo otorgar los permisos necesarios.
- Monitorear de cerca la actividad de red y utilizar herramientas de detección de intrusiones.

NOTICIAS DE CIBERSEGURIDAD

Piratas informáticos amenazan con filtrar World-Check

Un grupo de hackers criminales con motivación financiera afirma haber robado una base de datos confidencial que contiene millones de registros que las empresas utilizan para la evaluación de posibles clientes en busca de vínculos con sanciones y delitos financieros.

Prioridad: 3 Importante.

Ampliar información:

https://www.theregister.com/2024/04/19/cybercriminals_threaten_to_leak_all/

La ciberseguridad en la era de la inteligencia artificial ofensiva

A medida que las herramientas de inteligencia artificial (IA) abiertas se vuelven más accesibles, la barrera de entrada a los ciberataques se ha reducido, lo que hace crucial que las empresas reconozcan cómo la tecnología puede ser aprovechada tanto para fines ofensivos como defensivos.

Prioridad: 3 Importante.

Ampliar información:

https://www.infosecurity-magazine.com/news/security-leaders-ai-driven-attacks/

---

5 tendencias de ataque que deben ser monitoreadas por las organizaciones

Está claro que las organizaciones continúan experimentando más ataques que nunca y las cadenas de ataques se están volviendo más complejas. Los tiempos de permanencia se han acortado y las tácticas, técnicas y procedimientos (TTP) han evolucionado para volverse más ágiles y de naturaleza más evasiva. Para ello se hace necesario estar actualizados en las tendencias de ataques que van perfeccionando los ciberdelincuentes.

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/threat-intelligence/5-attack-trends-organizations-of-all-sizes-should-be-monitoring

---