GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2824

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	1	1	2
MALWARE	0	0	4
NOTICIAS DE CIBERSEGURIDAD	0	0	3

VULNERABILIDADES

Vulnerabilidad Zero-Day en CISCO NX-OS CVE-2024-20399

La empresa de ciberseguridad Sygnia informó a Cisco sobre ataques vinculados con un actor de amenazas patrocinado por el estado chino, conocido como Velvet Ant. Durante una investigación forense, Sygnia detectó que Velvet Ant obtuvo credenciales de administrador para acceder a switches Cisco Nexus y desplegar malware personalizado. Este malware permitió la conexión remota a dispositivos comprometidos, la carga de archivos adicionales y la ejecución de código malicioso. Cisco identificó una vulnerabilidad, CVE-2024-20399, que permite a atacantes locales con privilegios de administrador ejecutar comandos con permisos de root en sistemas operativos de dispositivos vulnerables.

Prioridad: 1 Crítico.

Ampliar información:

https://blog.segu-info.com.ar/2024/07/vulnerabilidad-zero-day-en-cisco-nx-os.html?utm_source=SeguInfo&utm_medium=SeguInfo&utm_campaign=Segu-Info+-+Ciberseguridad+desde+el+2000&utm_content=Segu-Info+-+Ciberseguridad+desde+el+2000&lctg=205608146&m=1

Vulnerabilidad en RCE en OpenSSH CVE-2024-6387

Una nueva vulnerabilidad de ejecución remota de código (RCE) no autenticada en OpenSSH, denominada "regreSSHion," otorga privilegios de root en sistemas Linux basados en glibc. Descubierta por investigadores de Qualys en mayo de 2024, la falla recibió el identificador CVE-2024-6387. Esta vulnerabilidad se debe a una condición de carrera del controlador de señales en sshd, que permite a atacantes remotos no autenticados ejecutar código arbitrario con privilegios de root.

Prioridad: 3 Importante.

Ampliar información:

https://blog.segu-info.com.ar/2024/07/regresshion-vulnerabilidad-critca-rce.html?utm_source=SeguInfo&utm_medium=SeguInfo&utm_campaign=Segu-Info%20-%20Ciberseguridad%20desde%20el%202000&utm_content=Segu-Info%20-%20Ciberseguridad%20desde%20el%202000&lctg=205608146

Vulnerabilidad en Microsoft MSHTML CVE-2021-40444

Se ha detectado a actores de amenazas explotando una vulnerabilidad parcheada en Microsoft MSHTML para distribuir la herramienta de vigilancia MerkSpy, apuntando a usuarios en Canadá, India, Polonia y EE. UU. MerkSpy monitorea actividades de usuarios, captura información sensible y establece persistencia en sistemas comprometidos. El

ataque comienza con un documento de Microsoft Word que aparenta ser una oferta de trabajo para ingeniero de software. Esta campaña, identificada por investigadores de Fortinet FortiGuard Labs, resalta la importancia de estar atentos a documentos sospechosos y mantener los sistemas actualizados.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/07/microsoft-mshtml-flaw-exploited-to.html

---

Microsoft descubre fallas críticas en Rockwell Automation PanelView Plus CVE-2023-2071

Microsoft ha revelado dos vulnerabilidades críticas en Rockwell Automation PanelView Plus que podrían ser aprovechadas por atacantes remotos y no autenticados. La primera vulnerabilidad (CVE-2023-2071, CVSS 9.8) permite la ejecución remota de código mediante paquetes maliciosos manipulados. La segunda (CVE-2023-29464, CVSS 8.2) facilita la lectura de datos de memoria y puede provocar una denegación de servicio al enviar un paquete más grande que el búfer permitido. Estas fallas podrían resultar en la ejecución de código remoto, divulgación de información o interrupciones significativas en operaciones industriales.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/07/microsoft-uncovers-critical-flaws-in.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

Malware se propaga ampliamente a través de ataques de descarga Drive-by

El servicio de carga conocido como FakeBat se ha destacado este año como una de las familias de malware loader más extendidas, según Sekoia. Utilizando la técnica de descarga drive-by, FakeBat se especializa en descargar y ejecutar payloads de malware avanzado como IcedID, Lumma, RedLine, SmokeLoader, SectopRAT y Ursnif. Estos ataques involucran métodos como SEO poisoning, malvertising e inyecciones de código malicioso en sitios comprometidos para engañar a los usuarios y hacer que descarguen software

falso. Este enfoque subraya la persistente amenaza del phishing y la ingeniería social como vectores principales para obtener acceso inicial a sistemas comprometidos.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/07/fakebat-loader-malware-spreads-widely.html

---

Nuevo botnet Zergeca basado en Golang

Investigadores de ciberseguridad han descubierto un nuevo botnet llamado Zergeca capaz de realizar ataques de denegación de servicio distribuido (DDoS). Escrito en Golang, el botnet recibe su nombre por la referencia a la cadena "ootheca" presente en los servidores de comando y control (C2) ("ootheca[.]pw" y "ootheca[.]top"). Según el equipo QiAnXin XLab, Zergeca va más allá de ser solo un botnet típico de DDoS; además de admitir seis métodos de ataque diferentes, tiene capacidades de proxy, escaneo, autoactualización, persistencia, transferencia de archivos, acceso a shell inversa y recolección de información sensible de dispositivos. Esta versatilidad lo convierte en una amenaza significativa en el panorama de la ciberseguridad.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/07/new-golang-based-zergeca-botnet-capable.html

---

El malware GootLoader sigue activo, lanzando nuevas versiones para mejorar sus ataques

El malware GootLoader sigue siendo activamente utilizado por actores de amenazas para desplegar cargas adicionales en sistemas comprometidos. Cybereason ha identificado

múltiples versiones de GootLoader, destacando la versión 3 como la más reciente en uso. Aunque ha habido actualizaciones en sus payloads, las estrategias de infección y funcionalidades básicas han permanecido consistentes desde su resurgimiento en 2020. GootLoader, parte del troyano bancario Gootkit, es distribuido por el grupo de amenazas Hive0127 (UNC2565) a través de tácticas de envenenamiento de SEO, aprovechando JavaScript para descargar herramientas de post-explotación.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/07/gootloader-malware-delivers-new.html

---

Ransomware como servicio "Eldorado"

Un nuevo servicio de ransomware llamado "Eldorado", operado como un servicio (RaaS), ha surgido con variantes diseñadas para cifrar archivos en sistemas Windows y Linux. Descubierto por Group-IB el 16 de marzo de 2024, a través de un anuncio en el foro RAMP, este ransomware utiliza Golang para ser compatible con múltiples plataformas y emplea Chacha20 para el cifrado de archivos y RSA-OAEP para el cifrado de claves. Eldorado puede cifrar archivos en redes compartidas a través del protocolo Server Message Block (SMB), y su representante es conocido por su fluidez en ruso, diferenciándose de cepas previamente filtradas como LockBit o Babuk.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/07/new-ransomware-as-service-eldorado.html

---

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

Apple elimina aplicaciones VPN de la App Store rusa ante presión del gobierno

Apple retiró varias aplicaciones de redes privadas virtuales (VPN) de su App Store en Rusia el 4 de julio de 2024, en respuesta a una solicitud de Roskomnadzor, el regulador de comunicaciones estatal ruso. Esta medida afectó a aplicaciones de 25 proveedores de VPN, incluyendo ProtonVPN, Red Shield VPN, NordVPN y Le VPN, según reportes de MediaZona. NordVPN había cerrado previamente todos sus servidores en Rusia en marzo de 2019. Red Shield VPN criticó la acción de Apple, acusándola de apoyar activamente un régimen autoritario al retener ingresos del mercado ruso, calificando la acción como perjudicial para la sociedad civil.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/07/apple-removes-vpn-apps-from-russian-app.html

---

Ataque a Polyfill[.]io afecta a más de 380,000 hosts, incluyendo grandes empresas

Un ataque de cadena de suministro dirigido a la biblioteca JavaScript ampliamente utilizada Polyfill[.]io ha afectado a más de 380,000 hosts según nuevos hallazgos de Censys. El ataque involucra la inserción de un script polyfill vinculado a dominios maliciosos como "https://cdn.polyfill[.]io" o "https://cdn.polyfill[.]com" en las respuestas HTTP de estos hosts. En particular, aproximadamente 237,700 de estos hosts están ubicados en la red de Hetzner en Alemania (AS24940), una popular plataforma de alojamiento web. Este incidente destaca la vulnerabilidad de las cadenas de suministro digitales y la necesidad de medidas robustas de seguridad cibernética para proteger contra tales ataques.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/07/polyfillio-attack-impacts-over-380000.html

---

El Nuevo Ransomware detrás del ataque al centro de datos en Indonesia

La nueva operación de ransomware Brain Cipher ha comenzado a atacar organizaciones en todo el mundo, ganando atención mediática por un reciente ataque al Centro Nacional de Datos temporal de Indonesia. Indonesia está construyendo Centros Nacionales de Datos para almacenar de forma segura servidores utilizados por el gobierno para servicios en línea y alojamiento de datos. El 20 de junio, uno de estos centros sufrió un ciberataque que encriptó los servidores del gobierno y afectó servicios de inmigración, control de

pasaportes, emisión de permisos para eventos y otros servicios en línea. El gobierno confirmó que la operación de ransomware Brain Cipher fue la responsable, afectando a más de 200 agencias gubernamentales.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/meet-brain-cipher-the-new-ransomware-behind-indonesia-data-center-attack