GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4224

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	2	1	0
MALWARE	0	1	1
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Ransomware Akira y Fog aprovechan fallo crítico en Veeam

Los grupos de ransomware Akira y Fog están explotando una vulnerabilidad crítica de ejecución remota de código (CVE-2024-40711) en los servidores Veeam Backup & Replication (VBR). Esta vulnerabilidad es causada por una deserialización insegura de datos, lo que permite que atacantes sin autenticación ejecuten código malicioso en los sistemas afectados. La vulnerabilidad fue descubierta por el investigador Florian Hauser y corregida por Veeam en septiembre de 2024, pero los atacantes han aprovechado este fallo para infiltrarse en sistemas vulnerables, en muchos casos a través de gateways VPN mal configurados o sin autenticación multifactor.

Para mitigar estos riesgos, se recomienda a los administradores de sistemas actualizar inmediatamente sus servidores Veeam con los parches disponibles. También es crucial implementar medidas de seguridad adicionales, como el uso de autenticación multifactor

y la deshabilitación de versiones de software no compatibles. En varios ataques, los actores han utilizado credenciales previamente comprometidas y herramientas como rclone para exfiltrar datos. Este tipo de vulnerabilidades pone en riesgo a empresas que utilizan soluciones de respaldo y recuperación de datos, haciéndolas blancos atractivos para el ransomware.

Prioridad: 1 Crítico.

Ampliar información:

https://www.bleepingcomputer.com/news/security/akira-and-fog-ransomware-now-exploiting-critical-veeam-rce-flaw/

Hackers rusos APT29 atacan servidores Zimbra y TeamCity

Los gobiernos de EE. UU. y el Reino Unido han emitido una advertencia conjunta sobre ataques dirigidos por el grupo de ciberespionaje ruso APT29, también conocido como Cozy Bear. Estos ataques están explotando vulnerabilidades críticas en los servidores Zimbra y JetBrains TeamCity, específicamente CVE-2022-27924 y CVE-2023-42793, que permiten la ejecución remota de código y el robo de credenciales. APT29 ha estado atacando masivamente estos servidores desactualizados en organizaciones gubernamentales y privadas en todo el mundo desde al menos 2022, buscando obtener acceso inicial y comprometer la infraestructura de TI.

Las agencias de ciberseguridad recomiendan actualizar inmediatamente los servidores vulnerables y aplicar parches de seguridad para mitigar los riesgos de estos ataques. Además, sugieren implementar medidas adicionales de seguridad como la autenticación multifactor (MFA) y realizar revisiones periódicas de las configuraciones de seguridad. El grupo APT29 ha estado detrás de varios ciberataques importantes, incluido el famoso ataque a la cadena de suministro de SolarWinds, lo que subraya la sofisticación y la amenaza continua que representa este grupo.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/us-uk-warn-of-russian-apt29-hackers-targeting-zimbra-teamcity-servers/

Hackers estatales explotan vulnerabilidad de WinRAR

Grupos de hackers respaldados por los gobiernos de Rusia y China, como Sandworm y APT28, están explotando activamente la vulnerabilidad CVE-2023-38831 en WinRAR. Esta vulnerabilidad permite a los atacantes ejecutar código malicioso cuando los usuarios abren archivos ZIP que contienen archivos aparentemente inofensivos, como imágenes o PDFs. A pesar de que el parche fue lanzado en agosto de 2023, muchos usuarios aún no han actualizado su software, lo que permite que los atacantes continúen explotando esta falla. Los ataques se han centrado en sectores estratégicos, como la infraestructura energética ucraniana y usuarios en Papúa Nueva Guinea.

Se recomienda a los usuarios de WinRAR que actualicen a la versión 6.23 para protegerse contra esta vulnerabilidad. Además, es crucial evitar abrir archivos ZIP de fuentes desconocidas y utilizar herramientas de seguridad avanzadas para escanear archivos. Las organizaciones deben reforzar la autenticación multifactor (MFA) y establecer políticas de seguridad adicionales para mitigar el riesgo de estas amenazas, ya que los atacantes siguen explotando estas vulnerabilidades para lanzar campañas de espionaje y robo de información.

Prioridad: 1 Critico.

Ampliar información:

https://www.securityweek.com/three-months-after-patch-gov-backed-actors-exploiting-winrar-flaw/

Recomendaciones generales sobre vulnerabilidades:

Para mitigar las vulnerabilidades en los sistemas, se recomiendan las siguientes medidas claves

1. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.

2. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.

3. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.

4. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.

5. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

Hackers usan ChatGPT para desarrollar malware

OpenAI confirmó que actores estatales, como los grupos SweetSpecter de China y CyberAv3ngers de Irán, han utilizado ChatGPT para desarrollar malware, realizar ataques de phishing y mejorar la eficiencia de sus operaciones cibernéticas. Los hackers han empleado ChatGPT para escribir código malicioso, realizar análisis de vulnerabilidades y crear herramientas para evadir la detección. Un ejemplo es el uso de ChatGPT para crear scripts que distribuyen malware a través de correos electrónicos de phishing, afectando a objetivos gubernamentales e industriales.

Los actores maliciosos también han aprovechado esta herramienta para ofuscar código y encontrar credenciales por defecto en sistemas críticos, lo que facilita la propagación del malware. Aunque OpenAI ha bloqueado las cuentas asociadas con estas actividades, se recomienda que las organizaciones implementen medidas de seguridad como autenticación multifactor y capacitación en phishing para mitigar el riesgo de futuros ataques.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/openai-confirms-threat-actors-use-chatgpt-to-write-malware/

Nueva Ola de ataques de phishing abusa de GitHub, Bots de Telegram y códigos QR

Una campaña reciente de malware dirigida a los sectores de finanzas y seguros utiliza enlaces a repositorios de GitHub en correos de phishing para distribuir el troyano de acceso remoto Remcos RAT. Los atacantes abusan de repositorios confiables para alojar archivos maliciosos, lo que permite que los correos pasen por filtros de seguridad sin ser detectados. También se emplean bots de Telegram y códigos QR basados en ASCII para evadir la detección y mejorar la distribución del malware. Esta técnica fue detectada por investigadores de Cofense y OALABS, quienes informaron que este método está ganando tracción entre los actores de amenazas.

El malware Remcos RAT permite a los atacantes controlar remotamente los dispositivos comprometidos, robar credenciales, capturar pulsaciones de teclas y realizar otras actividades maliciosas. Para mitigar el riesgo, se recomienda implementar autenticación multifactor, endurecer las políticas de filtrado de correos electrónicos y capacitar a los

empleados para reconocer enlaces sospechosos, incluidos aquellos que aparentan ser confiables como los de GitHub.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/10/github-telegram-bots-and-qr-codes.html

---

Recomendaciones generales sobre malware:

Para protegerse contra malware, es esencial:

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.

2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.

3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.

4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.

5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.

6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

Operador de Malware Ucraniano se Declara Culpable en EE.UU.

Mark Sokolovsky, un ciudadano ucraniano de 28 años, se declaró culpable en un tribunal de EE.UU. por operar el malware Raccoon Infostealer, el cual funcionaba bajo un modelo de malware-as-a-service (MaaS). Este malware permitía a los delincuentes alquilarlo por $200 al mes para robar credenciales de inicio de sesión, información financiera y criptomonedas de dispositivos infectados. Sokolovsky fue arrestado en los Países Bajos en marzo de 2022 y extraditado a EE.UU. en 2024. El Departamento de Justicia también desmanteló la infraestructura del malware, aunque este fue relanzado posteriormente.

El FBI identificó a Sokolovsky como uno de los principales administradores del malware, responsable de su operación a gran escala. Como parte de su acuerdo de culpabilidad, deberá pagar más de $900,000 en restitución y perderá cerca de $24,000 en bienes. Las autoridades recomiendan a los usuarios verificar si sus datos fueron robados usando un portal creado por el FBI y reforzar medidas de seguridad como el uso de autenticación multifactor para prevenir futuros robos de información.

Prioridad: 3 Importante.

Ampliar información:

https://www.securityweek.com/ukrainian-malware-operator-pleads-guilty-in-us-court/

Microsoft rediseña acceso al kernel tras el error de CrowdStrike

En julio de 2024, una actualización defectuosa del sensor Falcon de CrowdStrike causó un fallo que provocó pantallas azules en sistemas Windows a nivel mundial. Aunque Microsoft no fue directamente responsable, el incidente destacó la vulnerabilidad de permitir que controladores de terceros operen en el kernel del sistema operativo. David Weston, vicepresidente de seguridad de Microsoft, señaló que el fallo ocurrió debido a un error de lectura de memoria causado por datos malinterpretados de un archivo IPC, un área que Microsoft no podía prever ni controlar directamente.

Para prevenir futuros incidentes, Microsoft está rediseñando la interacción entre los proveedores de seguridad y el kernel de Windows, proponiendo que más soluciones operen en modo usuario en lugar de en el kernel. Además, Microsoft promueve el uso de prácticas de despliegue seguro (SDP), que incluyen despliegues graduales de actualizaciones y la capacidad de pausar o revertir cambios si es necesario. Estas medidas buscan mejorar la resiliencia y minimizar el impacto de futuros errores.

Prioridad: 3 Importante.

Ampliar información:

https://www.securityweek.com/microsofts-take-on-kernel-access-and-safe-deployment-practices-following-crowdstrike-incident/