GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °3124

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

VULNERABILIDADES

CISA añade al catálogo tres vulnerabilidades explotadas conocidas

CISA ha agregado tres nuevas vulnerabilidades a su Catálogo de Vulnerabilidades Explotadas Conocidas, basándose en evidencia de su explotación activa. Estas incluyen la CVE-2024-4879, una vulnerabilidad de validación de entrada incorrecta en ServiceNow; la CVE-2024-5217, una vulnerabilidad de lista incompleta de entradas no permitidas en ServiceNow; y la CVE-2023-45249, una vulnerabilidad de contraseña predeterminada no segura en Acronis Cyber Infrastructure (ACI). Este tipo de vulnerabilidades son vectores de ataque comunes para actores cibernéticos maliciosos y representan riesgos significativos para las empresas federales.

Prioridad: 3 Importante.

Ampliar información:

https://www.cisa.gov/news-events/alerts/2024/07/29/cisa-adds-three-known-exploited-vulnerabilities-catalog

---

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

Gh0stGambit: un cuentagotas para implementar Gh0st RAT

Gh0st RAT es un antiguo troyano de acceso remoto conocido por sus capacidades de recopilación de datos y control remoto. Su código fuente, ampliamente disponible, ha permitido su uso o personalización por diversos cibercriminales y grupos de hackers. Este RAT ganó notoriedad en 2009 durante la operación GhostNet, un caso de ciberespionaje a gran escala con infraestructura de comando y control, principalmente en la República Popular China. La variante actual de Gh0st RAT ha sido mejorada con proyectos de código abierto para ampliar sus capacidades. Se ha evaluado con alta certeza que esta campaña está dirigida principalmente a usuarios de habla china, lo que se evidencia por el uso de señuelos web en chino y aplicaciones chinas para el robo de datos y la evasión de defensas por parte del malware.

Prioridad: 3 Importante.

Ampliar información:

https://www.esentire.com/blog/a-dropper-for-deploying-gh0st-rat?&web_view=true

---

Malware LummaC2, que utiliza la plataforma de juegos Steam como servidor C2

Los expertos en ciberseguridad han identificado una variante avanzada del malware LummaC2, que utiliza la popular plataforma de juegos Steam como un servidor de comando y control (C2). Esta nueva táctica representa una evolución significativa en los métodos operativos y de distribución del malware, lo que aumenta el riesgo para usuarios y organizaciones a nivel mundial. LummaC2 es un malware que roba información y se ha distribuido activamente haciéndose pasar por programas ilegales como cracks, keygens y hacks de juegos. Estos archivos maliciosos se propagan a través de varios canales,

incluidos sitios de distribución, YouTube, LinkedIn e incluso anuncios en motores de búsqueda, mediante una técnica conocida como envenenamiento SEO. Recientemente, el malware también se ha disfrazado de aplicaciones legítimas como Notion, Slack y Capcut, ampliando aún más su alcance.

Prioridad: 3 Importante.

Ampliar información:

https://gbhackers.com/lummac2-malware-using-steam/

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

Configuraciones de Proofpoint explotadas para enviar millones de correos electrónicos de phishing diariamente

Una campaña masiva de phishing llamada "EchoSpoofing" aprovechó permisos débiles (ahora corregidos) en el servicio de protección de correo electrónico de Proofpoint para enviar millones de correos electrónicos falsificados en nombre de grandes entidades como Disney, Nike, IBM y Coca-Cola, dirigidos a empresas de la lista Fortune 100. La campaña, que comenzó en enero de 2024, distribuyó un promedio de 3 millones de correos electrónicos falsificados diariamente, alcanzando un pico de 14 millones a principios de junio.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/proofpoint-settings-exploited-to-send-millions-of-phishing-emails-daily/

'Stargazer Goblin' crea 3.000 cuentas falsas de GitHub para difundir malware

Un grupo de amenazas conocido como Stargazer Goblin ha creado una red de cuentas falsas en GitHub para operar un sistema de distribución como servicio (DaaS) que propaga diversos tipos de malware que roba información, generando ganancias ilícitas de 100,000 dólares en el último año. La red, denominada "Stargazers Ghost Network" por Check Point, consta de más de 3,000 cuentas en la plataforma de alojamiento de código en la nube, con miles de repositorios utilizados para compartir enlaces maliciosos o malware. Entre las familias de malware distribuidas se encuentran Atlantida Stealer, Rhadamanthys, RisePro, Lumma Stealer y RedLine. Las cuentas falsas también interactúan con los repositorios maliciosos para simular legitimidad. Se cree que esta red ha estado activa desde agosto de 2022, aunque el anuncio de DaaS no se detectó hasta principios de julio de 2023.

Prioridad: 3 Importante.

Ampliar información:

https://www.redpacketsecurity.com/stargazer-goblin-creates-3-000-fake-github-accounts-for-malware-spread/

La omisión del arranque seguro de PKfail permite a los atacantes instalar malware UEFI

Cientos de productos UEFI de 10 proveedores están en riesgo de ser comprometidos debido a un problema crítico en la cadena de suministro de firmware conocido como PKfail, que permite a los atacantes eludir el arranque seguro e instalar malware. El equipo de investigación de Binarly descubrió que los dispositivos afectados utilizan una "clave maestra" de arranque seguro de prueba, también conocida como clave de plataforma (PK), generada por American Megatrends International (AMI), que fue etiquetada como "NO CONFIANZA". Entre los fabricantes de dispositivos UEFI que utilizaron estas claves de prueba no confiables en 813 productos se incluyen Acer, Aopen, Dell, Formelife, Fujitsu, Gigabyte, HP, Intel, Lenovo y Supermicro.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/pkfail-secure-boot-bypass-lets-attackers-install-uefi-malware/