Boletín de Ciberseguridad N°76

Fecha de publicación: 11/03/2024

Mes de Marzo

26/02/2023 – 11/03/2024

Datasec

BOLETÍN DE CIBERSEGURIDAD

Indice

Introducción

Por medio de este boletín informativo estaremos destacando de forma quincenal, las noticias más relevantes en el ámbito de la ciberseguridad a nivel regional e internacional.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes activos, amenazas por medios informáticos nuevos, así como recomendaciones específicas de prevención. La publicación de dichas noticias dependerá de la importancia y calidad informativa de las mismas.

A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

En esta primera quincena del mes de marzo se destacan 6 noticias de relevancia, siendo estas sobre vulnerabilidades tecnológicas.

Aquellas noticias a tener especial recaudo son las siguientes:

Microsoft: actores malintencionados roban código fuente

Microsoft confirma que piratas informáticos rusos robaron el código fuente y algunos secretos de sus clientes.

Cisco: parchea error de secuestro de VPN

Cisco publica un parche para un error de secuestro de VPN de alta gravedad en Secure Client.

Ladrón de información basado en Python se difunde a través de mensajes de Facebook

Nuevo ladrón de información basado en Python que se difunde a través de mensajes de Facebook.

Vulnerabilidad Crítica

Microsoft	Microsoft: actores malintencionados roban código fuente	CRÍTICO

Descripción

Microsoft confirma que piratas informáticos rusos robaron el código fuente y algunos secretos de sus clientes.

Estado

Microsoft reveló que el actor de amenazas respaldado por el Kremlin conocido como Midnight Blizzard (también conocido como APT29 o Cozy Bear) logró obtener acceso a algunos de sus repositorios de código fuente y sistemas internos luego de un hack que salió a la luz en enero de 2024.

"En las últimas semanas, hemos visto evidencia de que Midnight Blizzard está utilizando información inicialmente extraída de nuestros sistemas de correo electrónico corporativo para obtener, o intentar obtener, acceso no autorizado", informó Microsoft.

Esto ha incluido el acceso a algunos de los repositorios de código fuente y sistemas internos de la compañía. Hasta la fecha no se ha encontrado evidencia de que los sistemas de cara al cliente alojados en Microsoft hayan sido comprometidos.

Investigadores, continúan investigando el alcance del ataque, asimismo informaron que el actor de amenazas patrocinado por el estado ruso está intentando aprovechar los diferentes tipos de secretos que encontró, incluidos aquellos que se compartieron entre los clientes y Microsoft por correo electrónico. Sin embargo, aún no se han revelado cuáles son estos secretos ni la escala del compromiso, asimismo, aún no está claro a qué código fuente se accedió.

Al afirmar que ha aumentado sus inversiones en seguridad, Microsoft señaló además que el adversario incrementó sus ataques de pulverización de contraseñas hasta 10 veces en febrero, en comparación con el "volumen ya grande" observado en enero.

"El ataque en curso de Midnight Blizzard se caracteriza por un compromiso sostenido y significativo de los recursos, la coordinación y el enfoque del actor de la amenaza", dijo.

"Puede estar utilizando la información que ha obtenido para acumular una imagen de las áreas que atacar y mejorar su capacidad para hacerlo. Esto refleja lo que se ha convertido en un panorama de amenazas globales sin precedentes, especialmente en términos de ataques sofisticados a Estados-nación".

Se dice que la infracción de Microsoft tuvo lugar en noviembre de 2023, y Midnight Blizzard empleó un ataque de pulverización de contraseñas para infiltrarse con éxito en una cuenta de inquilino de prueba heredada que no era de producción y que no tenía habilitada la autenticación multifactor (MFA).

El gigante tecnológico, a finales de enero, reveló que APT29 se había dirigido a otras organizaciones aprovechando un conjunto diverso de métodos de acceso inicial que iban desde credenciales robadas hasta ataques a la cadena de suministro.

Midnight Blizzard se considera parte del Servicio de Inteligencia Exterior de Rusia (SVR). Activo desde al menos 2008, el actor de amenazas es uno de los grupos de piratería más prolíficos y sofisticados, comprometiendo objetivos de alto perfil como SolarWinds.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2024/01/microsofts-top-execs-emails-breached-in.html
https://thehackernews.com/2024/03/microsoft-confirms-russian-hackers.html

CISCO	Cisco: parchea error de secuestro de VPN	CRÍTICO

Descripción

Cisco publica un parche para un error de secuestro de VPN de alta gravedad en Secure Client

Estado

Cisco ha lanzado parches para abordar una falla de seguridad de alta gravedad que afecta su software Secure Client y que podría ser explotada por un actor de amenazas para abrir una sesión VPN con la de un usuario objetivo.

La compañía de equipos de red describió la vulnerabilidad con un puntaje CVSS de 8.2, que permite a un atacante remoto no autenticado realizar un ataque de inyección de avance de línea de retorno de carro (CRLF) contra un usuario.

Como resultado de una validación insuficiente de la información proporcionada por el usuario, un actor de amenazas podría aprovechar la falla para engañar a un usuario para que haga clic en un enlace especialmente diseñado mientras establece una sesión VPN.

"Un exploit exitoso podría permitir al atacante ejecutar código de script arbitrario en el navegador o acceder a información confidencial basada en el navegador, incluido un token SAML válido", informó la compañía en un aviso oficial.

"El atacante podría luego usar el token para establecer una sesión VPN de acceso remoto con los privilegios del usuario afectado. Los hosts y servicios individuales detrás de la cabecera VPN aún necesitarían credenciales adicionales para un acceso exitoso".

La vulnerabilidad afecta a Secure Client para Windows, Linux y macOS y se ha solucionado en las siguientes versiones:

- Anterior a 4.10.04065 (no vulnerable)
- 4.10.04065 y posteriores (corregido en 4.10.08025)
- 5.0 (migrar a una versión fija)
- 5.1 (corregido en 5.1.2.42)

Cisco también ha publicado correcciones para una segunda vulnerabilidad con una puntuación CVSS de 7.3, otra falla de alta gravedad en Secure Client para Linux que podría permitir a un atacante local autenticado elevar los privilegios en un dispositivo afectado. Se ha resuelto en la versión 5.1.2.42.

"Un atacante podría explotar esta vulnerabilidad copiando un archivo de biblioteca malicioso a un directorio específico en el sistema de archivos y persuadiendo a un administrador para que reinicie un proceso específico", informó. "Un exploit exitoso podría permitir al atacante ejecutar código arbitrario en un dispositivo afectado con privilegios de root".

Remediación / Referencias

Por mayor información acceder a:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-client-crlf-W43V4G7

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-privesc-sYxQO6ds

https://thehackernews.com/2024/03/cisco-issues-patch-for-high-severity.html

facebook	Ladrón de información basado en Python se difunde a través de mensajes de Facebook	CRÍTICO

Descripción

Nuevo ladrón de información basado en Python que se difunde a través de mensajes de Facebook.

Estado

Los actores de amenazas están utilizando los mensajes de Facebook para distribuir un ladrón de información basado en Python llamado Snake que está diseñado para capturar credenciales y otros datos confidenciales.

"Las credenciales obtenidas de usuarios desprevenidos se transmiten a diferentes plataformas como Discord, GitHub y Telegram", dijeron en un informe técnicos investigadores en seguridad informática.

Los detalles sobre la campaña surgieron por primera vez en la plataforma de redes sociales X en agosto de 2023. Los ataques implican enviar a los posibles usuarios archivos RAR o ZIP aparentemente inofensivos que, al abrirlos, activan la secuencia de infección.

Las etapas intermedias involucran dos descargadores (un script por lotes y un script cmd), siendo este último responsable de descargar y ejecutar el ladrón de información desde un repositorio GitLab controlado por el actor.

Los investigadores detectaron tres variantes diferentes del ladrón, siendo la tercera un ejecutable ensamblado por PyInstaller. El malware, por su parte, está diseñado para recopilar datos de diferentes navegadores web, incluido Cốc Cốc, lo que sugiere un enfoque vietnamita.

La información recopilada, que incluye credenciales y cookies, luego se extrae en forma de archivo ZIP a través de la API de Telegram Bot. El ladrón también está diseñado para volcar información de cookies específica de Facebook, una indicación de que el actor de la amenaza probablemente esté buscando secuestrar las cuentas para sus propios fines.

La conexión vietnamita se ve reforzada aún más por la convención de nomenclatura de los repositorios GitHub y GitLab y el hecho de que el código fuente contiene referencias al idioma vietnamita.

"Todas las variantes son compatibles con el navegador Cốc Cốc, que es un navegador vietnamita muy conocido y utilizado ampliamente por la comunidad vietnamita", informaron.

Durante el año pasado, aparecieron múltiples ladrones de información dirigidos a las cookies de Facebook, entre ellos S1deload Stealer, MrTonyScam, NodeStealer y VietCredCare.

El desarrollo se produce cuando Meta ha sido criticada en los EE. UU. por no ayudar a las víctimas cuyas cuentas han sido pirateadas, y ha pedido a la compañía que tome medidas inmediatas para abordar un "aumento dramático y persistente" en los incidentes de apropiación de cuentas.

También sigue al descubrimiento de que los actores de amenazas están "utilizando un sitio web de trampas de juegos clonado, envenenamiento de SEO y un error en GitHub para engañar a los posibles hackers de juegos para que ejecuten malware Lua".

Específicamente, los operadores de malware están aprovechando una vulnerabilidad de GitHub que permite que un archivo cargado asociado con un problema en un repositorio persista incluso en escenarios donde el problema nunca se guarda.

"Esto significa que cualquiera puede cargar un archivo en cualquier repositorio git en GitHub y no dejar ningún rastro de que el archivo existe excepto el enlace directo", dijeron

los investigadores, y agregaron que el malware viene equipado con capacidades de comando y control (C2) comunicaciones.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2024/03/new-python-based-snake-info-stealer.html

Sitios falsificados de Zoom, Skype y Google Meet que entregan malware

CRÍTICO

Descripción

Los actores de amenazas han estado aprovechando sitios web falsos que anuncian software de videoconferencia popular como Google Meet, Skype y Zoom para entregar una variedad de malware dirigido a usuarios de Android y Windows desde diciembre de 2023.

Estado

El actor de amenazas está distribuyendo troyanos de acceso remoto (RAT), incluido SpyNote RAT para plataformas Android y NjRAT y DCRat para sistemas Windows.

Los sitios falsificados están en ruso y están alojados en dominios que se parecen mucho a sus homólogos legítimos, lo que indica que los atacantes están utilizando trucos de typosquatting para atraer a posibles víctimas a descargar el malware.

También vienen con opciones para descargar la aplicación para plataformas Android, iOS y Windows. Mientras que al hacer clic en el botón de Android se descarga un archivo APK, al hacer clic en el botón de la aplicación de Windows se activa la descarga de un script por lotes.

El script por lotes malicioso es responsable de ejecutar un script de PowerShell que, a su vez, descarga y ejecuta el troyano de acceso remoto.

Actualmente, no hay evidencia de que el actor de amenazas esté apuntando a usuarios de iOS, dado que, al hacer clic en el botón de la aplicación de iOS, el usuario accede a la lista legítima de Skype de la App Store de Apple.

"Un actor de amenazas está utilizando estos señuelos para distribuir RAT para Android y Windows, que pueden robar información confidencial, registrar pulsaciones de teclas y robar archivos", dijeron los investigadores.

El desarrollo se produce cuando investigadores revelaron que un nuevo malware denominado WogRAT dirigido tanto a Windows como a Linux está abusando de una

plataforma gratuita de bloc de notas en línea llamada aNotepad como vector encubierto para alojar y recuperar código malicioso.

Se dice que estará activo al menos desde finales de 2022 y apuntará a países asiáticos como China, Hong Kong, Japón y Singapur, entre otros. Dicho esto, actualmente no se sabe cómo se distribuye el malware en la naturaleza.

"Cuando WogRAT se ejecuta por primera vez, recopila información básica del sistema infectado y la envía al servidor C&C". "El malware admite comandos como ejecutar comandos, enviar resultados, descargar archivos y cargar estos archivos".

También coincide con campañas de phishing de gran volumen orquestadas por un actor cibercriminal con motivación financiera conocido como TA4903 para robar credenciales corporativas y probablemente seguirlas con ataques de compromiso de correo electrónico empresarial (BEC). El adversario ha estado activo desde al menos 2019, y las actividades se intensificaron después de mediados de 2023.

"TA4903 realiza habitualmente campañas que falsifican a varias entidades del gobierno de EE. UU. para robar credenciales corporativas". "El actor también falsifica a organizaciones de diversos sectores, incluidos la construcción, las finanzas, la atención sanitaria, la alimentación y las bebidas, entre otros".

Las cadenas de ataque implican el uso de códigos QR (también conocido como quishing) para el phishing de credenciales, así como la dependencia del kit de phishing EvilProxy adversary-in-the-middle (AiTM) para eludir las protecciones de autenticación de dos factores (2FA).

Una vez que un buzón de correo objetivo se ve comprometido, se ha observado que el actor de la amenaza busca información relevante sobre pagos, facturas e información bancaria, con el objetivo final de secuestrar hilos de correo electrónico existentes y realizar fraudes en las facturas.

Las campañas de phishing también han funcionado como conducto para otras familias de malware como DarkGate, Agent Tesla y Remcos RAT, el último de los cuales aprovecha señuelos esteganográficos para lanzar el malware en los hosts comprometidos.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2024/03/watch-out-for-spoofed-zoom-skype-google.html

	Apple publica actualizaciones críticas para fallas de día cero explotadas activamente	CRÍTICO

Descripción

Apple ha lanzado actualizaciones de seguridad para abordar varias fallas de seguridad, incluidas dos vulnerabilidades que, según dijo, han sido explotadas activamente en la naturaleza.

Estado

Las deficiencias se enumeran a continuación:

- Un problema de corrupción de memoria en el kernel que un atacante con capacidad arbitraria de lectura y escritura del kernel puede aprovechar para eludir las protecciones de la memoria del kernel.
- Un problema de corrupción de memoria en el sistema operativo en tiempo real (RTOS) RTKit que un atacante con capacidad arbitraria de lectura y escritura del kernel puede aprovechar para eludir las protecciones de la memoria del kernel.

Actualmente no está claro cómo se están utilizando los defectos como armas en la naturaleza. Apple dijo que ambas vulnerabilidades se abordaron con una validación mejorada en iOS 17.4, iPadOS 17.4, iOS 16.7.6 y iPadOS 16.7.6.

Las actualizaciones están disponibles para los siguientes dispositivos:

- iOS 16.7.6 y iPadOS 16.7.6: iPhone 8, iPhone 8 Plus, iPhone X, iPad de 5.ª generación, iPad Pro de 9,7 pulgadas y iPad Pro de 12,9 pulgadas de 1.ª generación
- iOS 17.4 y iPadOS 17.4: iPhone XS y posteriores, iPad Pro de 12,9 pulgadas de segunda generación y posteriores, iPad Pro de 10,5 pulgadas, iPad Pro de 11 pulgadas de primera generación y posteriores, iPad Air de tercera generación y posteriores, iPad de sexta generación y posteriores, y iPad mini de 5.ª generación y posteriores

Con el último desarrollo, Apple ha solucionado un total de tres días cero explotados activamente en su software desde principios de año. A finales de enero de 2024, solucionó un error de confusión de tipos en WebKit que afectaba a iOS, iPadOS, macOS, tvOS y el navegador web Safari y que podía provocar la ejecución de código arbitrario.

El desarrollo se produce cuando la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) agregó dos fallas a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), instando a las agencias federales a aplicar las actualizaciones necesarias antes del 26 de marzo de 2024.

Las vulnerabilidades se refieren a una falla de divulgación de información que afecta a los dispositivos Android Pixel y una falla de inyección de comandos del sistema operativo en Sunhillo SureLine que podría resultar en la ejecución de código con privilegios de root.

Remediación / Referencias

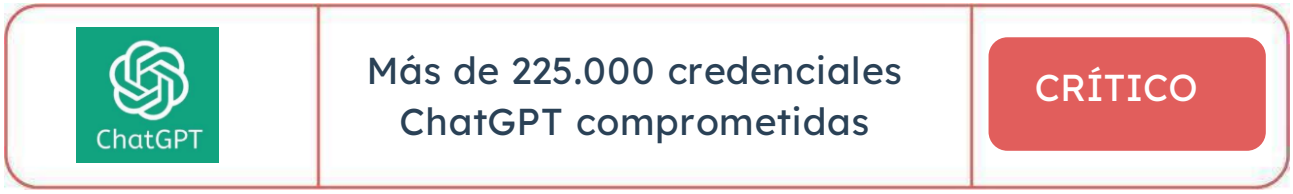
Por mayor información acceder a:

https://support.apple.com/en-us/HT214081

https://cve.mitre.org/cgi-bin/cvename.cgi?name=2024-23225

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23296

https://thehackernews.com/2024/03/urgent-apple-issues-critical-updates.html



Descripción

Más de 225.000 registros que contenían credenciales OpenAI ChatGPT comprometidas estuvieron disponibles para la venta en mercados clandestinos.

Estado

Estas credenciales se encontraron en registros de ladrones de información asociados con el malware ladrón LummaC2, Raccoon y RedLine.

"El número de dispositivos infectados disminuyó ligeramente a mediados y finales del verano, pero creció significativamente entre agosto y septiembre de 2023", informaron investigadores.

Entre junio y octubre de 2023, se infiltraron más de 130.000 hosts únicos con acceso a OpenAI ChatGPT, un aumento del 36% con respecto a lo observado durante los primeros cinco meses de 2023. El desglose por las tres principales familias de ladrones se muestra a continuación:

- LummaC2 - 70,484 hosts
- Mapache - 22,468 anfitriones
- RedLine - 15,970 hosts

"El fuerte aumento en la cantidad de credenciales ChatGPT a la venta se debe al aumento general en la cantidad de hosts infectados con ladrones de información, cuyos datos luego se ponen a la venta en los mercados o en UCL", detallaron investigadores.

El desarrollo se produce cuando Microsoft y OpenAI revelaron que actores-estado-nación de Rusia, Corea del Norte, Irán y China están experimentando con inteligencia artificial (IA) y grandes modelos de lenguaje (LLM) para complementar sus operaciones de ciberataque en curso.

Al afirmar que los adversarios pueden utilizar los LLM para generar ideas sobre nuevas técnicas comerciales, crear ataques convincentes de estafa y phishing y mejorar la productividad operativa, Group-IB dijo que la tecnología también podría acelerar el reconocimiento, facilitar la ejecución de kits de herramientas de piratería y realizar llamadas automáticas de estafadores.

"En el pasado, [los actores de amenazas] estaban interesados principalmente en computadoras corporativas y en sistemas con acceso que permitieran el movimiento a través de la red". "Ahora también se centran en dispositivos con acceso a sistemas públicos de IA.

"Esto les da acceso a registros con el historial de comunicación entre los empleados y los sistemas, que pueden utilizar para buscar información confidencial (con fines de espionaje), detalles sobre la infraestructura interna, datos de autenticación (para realizar ataques aún más dañinos) e información sobre código fuente de la aplicación (para analizarlo e identificar posibles vulnerabilidades que podrían ser explotadas)".

El abuso de credenciales de cuentas válidas por parte de actores de amenazas se ha convertido en una técnica de acceso principal, impulsada principalmente por la fácil disponibilidad de dicha información a través de malware ladrón.

"La combinación de un aumento en los robos de información y el abuso de credenciales de cuentas válidas para obtener acceso inicial ha exacerbado los desafíos de gestión de acceso e identidad de los defensores", mencionaron investigadores.

Los datos de credenciales empresariales se pueden robar de dispositivos comprometidos mediante la reutilización de credenciales, almacenes de credenciales del navegador o accediendo a cuentas empresariales directamente desde dispositivos personales.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2024/03/over-225000-compromised-chatgpt.html

Conclusiones

En un panorama cada vez más desafiante en términos de ciberseguridad, la constante capacitación y el mantenimiento de un estado de alerta son fundamentales para proteger tanto a empresas como a individuos.

Las crecientes tendencias en suplantación de sitios y los ataques coordinados por grupos de activistas malintencionados son solo algunos ejemplos de las amenazas a las que nos enfrentamos. Es imperativo que todos, desde empleados hasta altos directivos, estén bien informados y preparados para identificar y mitigar estos riesgos.
La educación continua en ciberseguridad y la adopción de prácticas de seguridad proactivas son la clave para mantenerse un paso adelante en este siempre cambiante panorama digital.

Al mantenernos alerta y actualizados, podemos fortalecer nuestra resiliencia frente a las amenazas cibernéticas y salvaguardar nuestros datos y activos críticos.

Desde el equipo de Datasec seguimos protegiendo la seguridad de nuestros clientes, socios y colaboradores.

¡Hasta la próxima!