Boletín de Ciberseguridad

Fecha de Publicación
29/08/2022 - N.º 41

Mes de Agosto
15/08/202 - 29/08/2022

Datasec

Índice

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 segunda quincena del mes de agosto se destacan 6 noticias de relevancia: 1 sobre vulnerabilidades tecnológicas, 4 de fraudes activos y 1 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Vulnerabilidad encontrada en Linux

Se encontró una vulnerabilidad en Linux de hace 8 años.

Ataque AiTM a usuarios de Google Suite

Ataques AiTM están dirigidos específicamente a los directores ejecutivos y otros miembros senior de varias organizaciones que usan Google Workspace.

Falsas Ofertas de Trabajo

Se han encontrado diversos ataques de phishing o personas que quieren ingresar a una empresa para colocar malware dentro.

	Vulnerabilidad encontrada en Linux	CRÍTICO

Descripción

Se encontró una vulnerabilidad en Linux de hace 8 años.

Estado

Investigadores académicos encontraron una vulnerabilidad en Linux de escalamiento de privilegios previamente desconocida que afecta al kernel de Linux.

La falla de seguridad se puede explotar para aumentar los privilegios y también puede conducir a un escape del contenedor. Los académicos dicen que la vulnerabilidad ha estado presente en Linux durante ocho años.

Remediación / Referencias

Se recomienda actualizar las plataformas Linux.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2022/08/dirtycred-vulnerabilidad-presente-en.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2588

	Estafas Bancarias mediante SMS y Llamadas telefónicas	CRÍTICO

Descripción

Bancos como Santander, BBVA, Unicaja o Bankinter identificaron estafas mediante sms y llamadas telefónicas para robar claves bancarias.

Estado

Los ciberdelincuentes comienzan con un mensaje de móvil haciéndose pasar por el banco, en este mensaje se lee una transferencia de cierta cantidad de dinero y debajo de él, el enunciado, *«Si no* reconoce esa actividad, verifique inmediatamente» seguido por un link a una página web falsa, haciéndose pasar por la página oficial del banco. Al ingresar al link, se pide ingresar la cédula de identidad y firma electrónica, seguido por una llamada telefónica, por donde los ciberdelincuentes piden un código que llega al celular de la víctima para poder finalizar el hackeo de la cuenta.

Remediación / Referencias

Consejos para prevenir ataques de Phishing, no ingreses a links que no sean seguros, no envíes información personal usando mensajes de correo electrónico y verifique el emisor del correo si es el correcto.

Por mayor información al respecto se puede acceder a:
https://cybersecuritynews.es/las-nuevas-ciberestafas-bancarias-combinan-sms-y-llamadas-falsas/
https://www.bancosantander.es/glosario/smishing

G Suite	**Ataque AiTM a usuarios de Google Suite**	IMPORTANTE

Descripción

Ataques AiTM están dirigidos específicamente a los directores ejecutivos y otros miembros senior de varias organizaciones que usan Google Workspace.

Estado

La campaña de phishing de Gmail AiTM implica el uso de los correos electrónicos comprometedores de los directores ejecutivos para realizar ingeniería social, los ataques utilizan varios dominios comprometidos para llevar a las víctimas a la página de destino final, la cual es falsa. El ataque implica el envío de correos electrónicos de caducidad de contraseña, el cual contiene un enlace malicioso incrustado para supuestamente "ampliar su acceso", lleva al destinatario a abrir páginas de redirección de Google Ads y Snapchat para cargar la URL de la página de phishing.

Remediación / Referencias

AiTM: ataque de intermediario, el atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas y procurar que ninguna de las víctimas conozca que el enlace entre ellos ha sido violado.

Por mayor información al respecto se puede acceder a:
https://thehackernews.com/2022/08/researchers-warn-of-aitm-attack.html

	Google Chrome identifica amenaza ZeroDay	IMPORTANTE

Descripción

Se identificaron 11 vulnerabilidades, de la cual una de ellas es categorizada como zero-day.

Estado

No se hacen públicos muchos detalles sobre la vulnerabilidad de día cero hasta que la mayoría de los usuarios hayan tenido tiempo de asegurarse de que la actualización esté instalada y activada.

Se sabe sobre esta vulnerabilidad que está relacionada a como Google Chrome procesa la entrada de usuarios.

Remediación / Referencias

Se recomienda realizar una actualización de Google Chrome manualmente.
Por mayor información al respecto se puede acceder a:
https://www.forbes.com/sites/daveywinder/2022/08/20/google-confirms-chrome-zero-day-5-as-attacks-begin-update-now/?sh=163d04be39cc
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2856

	Ransomware accede a datos de CISCO	IMPORTANTE

Descripción

El atacante intentó filtrar archivos robados en línea.

Estado

Cisco experimentó un incidente de seguridad e inmediatamente tomamos medidas para contener y erradicar la amenaza.

No se identificó ningún impacto resultante de este incidente, incluidos servicios o productos, datos confidenciales de cliente o información confidencial.

Los atacantes obtuvieron acceso a la red de Cisco utilizando las credenciales robadas de un empleado después de secuestrar la cuenta personal de Google del empleado que contenía las credenciales sincronizadas desde su navegador.

Remediación / Referencias

Se recomienda no dar información personal o confidencial antes de saber de dónde proviene el usuario que la pide.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2022/08/grupo-de-ransomware-accede-datos-no.html

CSIRT	**Falsa Oferta de Trabajo**	PREVENCIÓN

Descripción

Se encontró un ataque de phishing con un CV por una falta oferta de trabajo.

Estado

El atacante adjunta un archivo ZIP, disfrazado como un CV de un postulante a una oferta laboral. Dentro de este archivo ZIP nos encontramos con un tipo de malware y un RAT (troyano de acceso remoto). Posee un keylogger, un tipo de herramienta que se utiliza para robar contraseñas, ya que registra cada tecla que presionas.

Remediación / Referencias

No abrir correos ni mensajes de dudosa procedencia, desconfiar de los enlaces y archivos en los mensajes o correo, mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).

Por mayor información al respecto se puede acceder a:
https://www.csirt.gob.cl/alertas/2cmv22-00332-01/

Conclusiones

Estamos viendo amenazas que afectan a las corporaciones debido a sus débiles controles de seguridad en las incorporaciones de personal.

Una parte esencial que puede comprometer a la empresa y a los accesos de confianza son las personas y la información digital presente en diversos medios.

Por tanto, las organizaciones cada vez más, deben obtener información más precisa y completa de sus nuevas contrataciones. De lo contrario son propensas a compromisos de insiders o diversos actores maliciosos que tendrán accesos confiados internos y podrán desbaratar operaciones de forma más simple.

Por ejemplo, colocar malware interno o desviar comunicaciones, entre otros casos.

El equipo de Datasec queda a las órdenes ante cualquier consulta o requerimientos de mayor información.