Boletín de Ciberseguridad

Fecha de Publicación
08/11/2021 - N.º 20

Mes de noviembre
25/10/2021 - 08/11/2021

Datasec

Contenido

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 las 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 noviembre se destacan 6 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas, 3 de fraudes activos y 1 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Vulnerabilidad de ejecución remota de código en WinRAR

Se ha revelado una nueva vulnerabilidad en WinRAR una vez culminado el periodo de prueba, lo que permite a atacantes maliciosos ejecutar código remoto en la computadora de la víctima. Este Software es uno de los programas más usados por los usuarios de Windows para abrir, comprimir y descomprimir archivos y ficheros.

Campaña masiva utiliza YouTube para impulsar malware que roba contraseñas

Ciberdelincuentes están comprometiendo cuentas de Google para crear canales en YouTube, subir videos a la plataforma que tienen en la descripción enlaces de descarga relacionados al tema tratado en el video y así robar credenciales por medio de la distribución de troyanos.

No seguro: SMS como método de autenticación en dos pasos

Expertos en seguridad recomiendan usar autenticación de dos factores para proteger sus cuentas en línea.
Muchos servicios utilizan la verificación por SMS de forma predeterminada, enviando códigos por mensaje de texto a su teléfono cuando intenta iniciar sesión. Pero los mensajes SMS tienen muchos problemas de seguridad y son la opción menos segura para la autenticación de dos factores.

	Vulnerabilidad de ejecución remota de código en WinRAR	CRÍTICO

Descripción

Se ha revelado una nueva vulnerabilidad en WinRAR una vez culminado el periodo de prueba, lo que permite a atacantes maliciosos ejecutar código remoto en la computadora de la víctima.

Este Software es uno de los programas más usados por los usuarios de Windows para abrir, comprimir y descomprimir archivos y ficheros.

Afectados

El software "Tryware" WinRAR, en su versión 5.70 para Windows una vez finalizado el periodo de prueba.

Estado

La versión 5.7 de WinRAR se lanzó por primera vez hace dos años, ha sido reemplazada desde entonces y puede no parecer una amenaza inmediata.

El fallo, descubierto por casualidad, presentó un error de Javascript generado por MSHTML cuando WinRAR notifica al usuario el fin de periodo de prueba gratuito. Haciéndolo por medio del dominio predeterminado «notifier.rarlab.com» que tiene contenido malicioso y que arroja

una respuesta «301 Moved Permanently», permitiendo almacenar en caché la redirección a un dominio malicioso para cualquier petición posterior.
Los expertos también observaron que un atacante con acceso al mismo dominio de la red realizaba ataques de suplantación de ARP para lanzar aplicaciones de forma remota, recuperar información del host local y ejecutar código arbitrario.

El descubrimiento determina que, una vez expirado el periodo de prueba, el Software comienza a mostrar el mensaje de error, una de cada tres ejecuciones.
Esta ventana utilizada para mostrar el error utiliza la implementación mshtml.dll para Borland C++ en la que se ha escrito WinRAR.

Los expertos señalaron que las vulnerabilidades en el software de terceros suponen graves riesgos para las organizaciones, ya que pueden ser explotadas para acceder a cualquier recurso del sistema y, potencialmente, de la red que lo aloja.

Remediación / Referencias

Si posee la versión 5.70, se recomienda descargar la última versión disponible en la página oficial de WINRAR.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2021/10/vulnerabilidad-critica-en-winrar-de.html
https://thehackernews.com/2021/10/bug-in-free-winrar-software-could-let.html

	**Zero-day explotadas activamente en Google Chrome**	CRÍTICO

Descripción

Google lanzó una actualización de emergencia para su navegador web Chrome, que incluye correcciones para dos vulnerabilidades que están siendo explotadas por atacantes de forma activa.

Afectados

Versiones de Google Chrome anteriores a 95.0.4638.69.

Estado

Uno de los fallos es de alta severidad relacionado con la insuficiente validación para inputs no confiables mediante Intents, mientras que la otra vulnerabilidad consiste en un fallo de implementación inapropiada en V8, el motor de navegador de Chrome en JavaScript.

Dado que las fallas aún están siendo explotadas, para evitar más abusos, Google aún no ha compartido detalles sobre los días cero o cómo están siendo explotados.

Sin embargo, con esta última ronda de correcciones, Google ha parcheado 15 vulnerabilidades de día cero de Chrome desde principios de 2021, muchas de las cuales estaban siendo explotadas activamente en la naturaleza, lo que indica claramente que Chrome se ha convertido en uno de los objetivos favoritos de los actores de amenazas.

Remediación / Referencias

Se recomienda a los usuarios de Chrome que actualicen a la última versión para Windows, Mac y Linux para mitigar cualquier riesgo potencial de explotación activa.

Fuentes:
https://cve.mitre.org/cgi-https://www.welivesecurity.com/la-es/2021/10/29/google-chrome-dos-nuevas-zero-day-explotadas-activamente/
bin/cvename.cgi?name=CVE-2021-38000
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38003

Aplicaciones sobre “El juego del calamar” que contienen malware

IMPORTANTE

Descripción

Profesionales en ciberseguridad encontraron que en aplicaciones relacionadas con la serie de El Juego del Calamar disponibles en Google Play Store había varios malwares que infectaban los dispositivos.
El principal malware encontrado es Joker, un troyano que se encontró por primera vez en 2017 y que es capaz de ejecutar una librería nativa de Android.

Afectados

Usuarios de Android que descargaron esta aplicación.

Estado

La popular serie coreana "El juego del calamar" ha servido como plataforma para atacar personas.
Un ejemplo de esto es la aplicación “Squid Game Wallpaper 4K HD”, para Android en Google Play.

Ciberdelincuentes distribuyeron por medio de la aplicación el virus troyano Joker. Este puede hacer que aparezca publicidad sin control en tu dispositivo o crear suscripciones no deseadas

de SMS. También logran enganchar a las víctimas por medio de falsos enlaces a episodios gratuitos, y al intentar descargar estos es cuando se infectan los equipos.
La aplicación, que ya ha sido eliminada de la tienda, fue descargada por al menos cinco mil cuentas.

Respecto al malware Joker, este puede infectar a muchos usuarios al ocultarse dentro de aplicaciones con la capacidad de realizar múltiples acciones en el equipo de la víctima como ser: leer mensajes de texto, suscribirse a servicios pagos a través de sitios web o instalar spyware.

Remediación / Referencias

Se recomienda descargar aplicaciones desde las cuentas oficiales, revisar los permisos que solicitan, así como los comentarios de los usuarios que ya la descargaron y la cantidad de descargas. Además, considera fundamental utilizar una solución antivirus para prevenir la descarga de malware (software malicioso).

Por mayor información al respecto se puede acceder a:
https://www.welivesecurity.com/la-es/2021/10/26/aplicaciones-relacionada-juego-calamar-buscan-infectar-malware/

	Campaña masiva utiliza YouTube para impulsar malware que roba contraseñas	IMPORTANTE

Descripción

Ciberdelincuentes están comprometiendo cuentas de Google para crear canales en YouTube, subir videos a la plataforma que tienen en la descripción enlaces de descarga relacionados al tema tratado en el video y así robar credenciales por medio de la distribución de troyanos.

Afectados

Los usuarios de cuentas de Google que acceden a los enlaces en la descripción de los videos en YouTube.

Estado

Mediante enlaces que acompañan la descripción de videos en la plataforma YouTube, los atacantes están distribuyendo un malware con el que pretenden robar las credenciales de los usuarios.

Los videos cubren una amplia gama de temas, desde cracks de software, guías sobre cómo sortear licencias de software, criptomonedas, piratería de software, trampas de juegos y software VPN. Estos contienen un enlace que los autores del video afirman que es una herramienta que ayudará al espectador en su búsqueda relacionada con el tema del video. Sin

embargo, el enlace conduce a la descarga de troyanos que se esconden en el equipo de la víctima para robar credenciales.

La campaña propaga específicamente dos tipos de malware, el Racoon Stealer y el RedLine. "En el caso de los videos que distribuyen el troyano RedLine el enlace suele ser de un acortador, como bit.ly, el cual redirige al usuario a un sitio de descarga de archivos que aloja el malware. En el caso de los videos que distribuyen Racoon Stealer, los enlaces suelen no estar acortados y redirigen a un dominio llamado "taplink" que aloja el código malicioso."

Este tipo de malware se introduce en el sistema informático de forma secreta. A continuación, extrae silenciosamente la información personal del usuario en segundo plano, que incluye contraseñas, credenciales de tarjetas de crédito, cookies e incluso capturas de pantalla de las ventanas activas.

Dicho esto, estos troyanos podrían exponer significativamente la información privada de la víctima a los actores de la amenaza.

La mayoría de las credenciales robadas como claves de inicio de sesión en navegadores web, clientes FTP, aplicaciones de correo, o VPN fueron recolectadas por RedLine, y actualmente se encuentran a la venta en la dark web.

En tanto, Google es consciente de esta campaña masiva y expresó que están tomando medidas para frenar esta actividad.

Remediación / Referencias

- Evitar la descarga de aplicaciones desde un mero enlace en la descripción de un video de YouTube.
- Revisar la seguridad de las contraseñas y crear hábitos saludables en cuanto a la gestión de las contraseñas.
- Implementar la autenticación en dos pasos en Google.

Por mayor información:
https://www.welivesecurity.com/la-es/2021/10/22/propagan-malware-robar-credenciales-videos-youtube/

	**Descubren la mayor red de bots con 1.6 millones de dispositivos infectados**	IMPORTANTE

Descripción

Expertos en ciberseguridad reportan la detección de una nueva botnet masiva capaz de lanzar poderosos ataques de denegación de servicio (DoS) gracias a que ha infectado más de 1.6 millones de dispositivos conectados a Internet.

Identificada como Pink, esta botnet primordialmente opera en China.

Estado

Pink se ha utilizado para lanzar más de 100 ataques DDoS hasta la fecha, lo que la convierte en la botnet más grande que el equipo de seguridad de Netlab de Qihoo 360 ha observado en la naturaleza durante unos seis años.

La botnet en cuestión ha sido nombrada 'Rosa' por los investigadores de seguridad después de que una muestra recolectada a fines de 2019 tuviera varios nombres de funciones que comenzaran con rosa.

Se estima que ha infectado a alrededor de 1,6 millones de personas en todo el mundo, (siendo el 96% de China) irrumpiendo en computadoras para agregar dispositivos a la red, explotando vulnerabilidades de día cero en puertas de enlace de red de dispositivos de banda ancha producidos por corporaciones específicas.

Pink, tiene una arquitectura muy fuerte y robusta, que utiliza una combinación de servicios de terceros, P2P (redes peer-to-peer) y C2 centrales para sus comunicaciones de bots a controladores que se dirige principalmente a enrutadores basados en MIPS.

La botnet Pink se ha centrado en gran medida en orquestar ataques DDoS (denegación de servicio distribuida). Los ataques DDoS a menudo se utilizan para abrumar una red, servidor u organización con una cantidad de tráfico inmanejable (que también es tráfico falso), lo que hace que se bloquee o se vuelva inutilizable para visitantes o usuarios genuinos.

"También se ha descubierto que Pink adoptó DNS-Over-HTTPS (DoH), un protocolo utilizado para realizar la resolución remota del sistema de nombres de dominio a través del protocolo HTTPS, para conectarse al controlador especificado en un archivo de configuración que se entrega a través de GitHub o Baidu Tieba, o mediante un nombre de dominio integrado y codificado en algunas de las muestras"

Los investigadores observaron más de 103.000 nodos que aún estaban activos a finales de octubre y esto es uno de los indicios de como las botnets pueden ofrecer una infraestructura poderosa para que los delincuentes monten una variedad de intrusiones.

Referencias

Para más información:
https://blog.segu-info.com.ar/2021/11/pink-botnet-con-16-millones-de.html

	**No seguro: SMS como método de autenticación en dos pasos**	PREVENCIÓN

Descripción

Expertos en seguridad recomiendan usar autenticación de dos factores para proteger sus cuentas en línea.
Muchos servicios utilizan la verificación por SMS de forma predeterminada, enviando códigos por mensaje de texto a su teléfono cuando intenta iniciar sesión. Pero los mensajes SMS tienen muchos problemas de seguridad y son la opción menos segura para la autenticación de dos factores.

Vector de Ataque

La autenticación de dos factores (2FA) aporta una capa adicional de seguridad que las contraseñas por sí solas no pueden proporcionar. Al requerir un paso adicional para que el usuario demuestre su identidad, se reduce la posibilidad de que un mal actor acceda a los datos.

Uno de los métodos más comunes de 2FA son los mensajes de texto SMS.
El problema es que los SMS no son un medio seguro ya que los piratas informáticos tienen varias herramientas en su arsenal que pueden interceptar, suplantar y falsificar los SMS. A pesar de este fallo de seguridad y de las mejores opciones de autenticación, varias instituciones siguen utilizando la 2FA basada en SMS.

Así es como funciona la verificación por SMS: cuando intentas iniciar sesión, el servicio envía un mensaje de texto al número de teléfono móvil que les has proporcionado anteriormente. Obtienes ese código en tu teléfono y lo ingresas para iniciar sesión. Ese código solo es válido para un uso y se utiliza para garantizar que solo tú puedes acceder a tus datos por lo que activar la verificación en dos pasos es necesario.

Aunque el SMS 2FA elimina la simple contraseña de la ecuación, abre otra vulnerabilidad para que los atacantes la exploten, una que requiere incluso menos habilidad que la de descifrar contraseñas: El puerto SIM/intercambio donde lo que se busca es engañar a los operadores para que porten un número de teléfono a un nuevo dispositivo en un movimiento llamado intercambio de SIM.

Podría ser tan fácil como conocer tu número de teléfono y los cuatro últimos dígitos de tu número de la Seguridad Social. Una vez que un hacker ha redirigido tu número de teléfono, ya no necesita tu teléfono físico para acceder a tus códigos 2FA.

También están los puntos débiles del propio sistema de telecomunicaciones móviles. En lo que se denomina un ataque SS7, un ciberdelincuente puede espiar a través del sistema de telefonía móvil, escuchando las llamadas, interceptando los mensajes de texto y viendo la ubicación de su teléfono.

Los ataques a los números de teléfono incluyen malware que los usuarios instalan sin darse cuenta y que busca las contraseñas de los SMS de un solo uso y las envía al atacante.

En definitiva, utilizar la autenticación de dos factores basada en SMS no es lo ideal, pero es conveniente ya que muchos servicios aún no disponen de otros métodos de 2FA.

Remediación / Referencias

Un esquema de autenticación de dos factores que no se basa en SMS es superior, porque la compañía de telefonía celular no podrá darle a otra persona acceso a sus códigos.

Aplicaciones como Authy, Microsoft Authenticator o Google Authenticator generan códigos en su dispositivo por lo que Incluso si un atacante engañara a su compañía de telefonía celular para que transfiriera su número de teléfono a su teléfono, no podría obtener sus códigos de seguridad.
Los datos necesarios para generar esos códigos permanecerían de forma segura en su teléfono.

Informate más en:
https://blog.segu-info.com.ar/2021/10/por-que-no-es-seguro-usar-sms-como.html
https://www.genbeta.com/seguridad/por-que-no-debes-confiar-en-la-autenticacion-en-dos-pasos-a-traves-de-sms

Conclusiones

Una vez más, en esta quincena de días, en la que vamos actualizándonos de las noticias más relevantes en cuanto a seguridad de la información, vemos la creciente necesidad de las organizaciones modernas en acompañar los crecimientos tecnológicos con personas capacitadas que crezcan con las nuevas tecnologías, ya que de lo contrario observamos que podemos ser engañados con diferentes fraudes a través de las tecnologías en las que confiamos.

Más allá de todos los mecanismos técnicos que podamos implementar, al final del día cada persona de la organización tiene un poder sobre la información de la misma, es por eso que actualizar periódicamente las políticas y mejores usos y prácticas que existan sobre los mismos es relevante comunicarlo a todas las áreas de trabajo.

A través de campañas perpetuas de concientización se puede mejorar día a día en la postura de seguridad. Por ejemplo, entre las noticias vimos fraudes por YouTube y teléfono en la que los atacantes potencian las capacidades de machine learning e inteligencia artificial, para al fin y al cabo poder tener una conversación con otro colaborador en tiempo real y que este confíe realmente por el tono de voz, pausas y demás.

Este tipo de ataques pueden ser críticos en organizaciones dónde no solo no existan campañas de concientización que aborden estas problemáticas, y más aún si las únicas formas de confiar y tomar acción se toman por vía telefónica, así como sucedía históricamente vía mail en dónde los atacantes impresionaban ya sea realmente o de forma ofuscada la dirección del remitente, para que los destinatarios confiaran en el atacante que falsifica en vez de los originales.

Es por eso que identificar estas situaciones y actuar en consecuencia para prevenirlas es cada vez más el trabajo que los oficiales de seguridad de las organizaciones modernas tienen como objetivo empujar desde diferentes perspectivas y casi de forma pedagógica guiar y encaminar los esfuerzos de forma óptima para lograr la protección necesaria.

Desde Datasec seguimos de cerca estos desafíos, así generamos y difundimos elementos y artefactos que ayuden estos procesos de mejoría.
¡Juntos nos protegemos!
Hasta la próxima.