Boletín de Ciberseguridad

Fecha de Publicación
20/06/2022- N.º 36

Mes de Junio
06/06/2022 - 20/06/2022

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 junio se destacan 6 noticias de relevancia: 4 sobre vulnerabilidades tecnológicas y 2 sobre prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Actualizaciones críticas de Microsoft corrige error Follina

Microsoft ha parcheado una vulnerabilidad de Windows que los piratas informáticos están explotando activamente. Si posee un sistema que usa Windows 7 y versiones posteriores, querrá actualizar su computadora lo antes posible.

CISA advirtió sobre vulnerabilidades críticas en los dispositivos de ADN

Se ha emitido un aviso sobre las vulnerabilidades de seguridad críticas en el software de secuenciación de próxima generación (NGS) de Illumina.

MaliBot: un nuevo troyano bancario para Android descubierto en la naturaleza

Se ha detectado una nueva variedad de malware para Android que se dirige a clientes de banca en línea y billeteras de criptomonedas en España e Italia, solo unas semanas después de que una operación coordinada de aplicación de la ley desmanteló FluBot.

Microsoft	**Actualizaciones críticas de Microsoft corrige error Follina**	CRÍTICO

Descripción

Microsoft ha parcheado una vulnerabilidad de Windows. Si posee un sistema que usa Windows 7 y versiones posteriores, deberá actualizar su computadora lo antes posible.

Estado

La falla de seguridad, llamada Follina (CVE-2022-30190), permite a los malhechores secuestrar las computadoras de los usuarios a través de programas como Microsoft Word. Los investigadores de seguridad han estado al tanto de la amenaza desde finales de mayo, pero, según los informes, Microsoft descartó sus hallazgos iniciales.

En un ataque documentado, los piratas informáticos asociados con el gobierno chino enviaron documentos de Word maliciosos a destinatarios tibetanos. Cuando se abren, estos documentos usan el exploit Follina para tomar el control de la herramienta de diagnóstico de soporte de Microsoft (MSDT) para ejecutar comandos que podrían usarse para instalar programas, crear nuevas cuentas de usuario y eliminar o cambiar datos almacenados en una computadora.

El exploit también se ha utilizado en campañas de phishing dirigidas a agencias gubernamentales estadounidenses y europeas.

La advertencia original de Microsoft sobre la amenaza ofrecía soluciones alternativas para protegerse contra la amenaza, pero esta actualización (KB5014699 para Windows 10 y KB5014697 para Windows 11) debería eliminar la necesidad de hacerlo.

Remediación / Referencias

Microsoft recomienda encarecidamente que los clientes instalen las actualizaciones para estar completamente protegidos contra la vulnerabilidad.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2022/06/actualizaciones-criticas-de-microsoft-y.html?m=1

Microsoft	Advertencia sobre la vulnerabilidad de Microsoft Windows "DogWalk" sin parches	CRÍTICO

Descripción

Se ha puesto a disposición un parche de seguridad no oficial para una nueva vulnerabilidad de día cero de Windows en la herramienta de diagnóstico de soporte de Microsoft (MSDT), incluso cuando la falla de Follina continúa siendo explotada en la naturaleza.

Estado

El problema, al que se hace referencia como DogWalk , se relaciona con una falla en el manejo de rutas y accesos a directorios por parte del sistema operativo; que se puede explotar para ocultar un archivo ejecutable malicioso en la carpeta de inicio de Windows cuando un objetivo potencial abre un archivo de almacenamiento ".diagcab", especialmente diseñado que contiene un archivo de configuración de diagnóstico.

La idea es que la carga útil se ejecute la próxima vez que la víctima inicie sesión en el sistema después de un reinicio. La vulnerabilidad afecta a todas las versiones de Windows, desde Windows 7 y Server Server 2008 hasta las últimas versiones.

Remediación / Referencias

La vulnerabilidad está siendo activamente explotada por troyanos de robo de información, especialmente Qbot.
Estos se están intentando monitorizar de forma activa.

Dado que se trata de una vulnerabilidad Zero Day sin una solución oficial disponible del proveedor, el equipo 0patch proporciono micro–parches de forma gratuita hasta que dicha solución esté disponible.
Mantener la base de datos de virus actualizada de su agente Antivirus/EDR.

Por mayor información acceder a:
https://csirt.telconet.net/comunicacion/noticias-seguridad/vulnerabilidad-zero-day-en-microsoft-windows-dogwalk/
https://blog.0patch.com/2022/06/microsoft-diagnostic-tools-dogwalk.html

	CISA advirtió sobre vulnerabilidades críticas en los dispositivos de ADN	CRÍTICO

Descripción

Se ha emitido un aviso sobre las vulnerabilidades de seguridad críticas en el software de secuenciación de próxima generación (NGS) de Illumina.

Estado

Tres de las fallas tienen una calificación de 10 sobre 10 en gravedad en el Sistema de puntuación de vulnerabilidad común (CVSS), y otras dos tienen calificaciones de gravedad de 9.1 y 7.4.

Los problemas afectan el software en los dispositivos médicos que se utilizan para "uso de diagnóstico clínico en la secuenciación del ADN de una persona o pruebas de diversas afecciones genéticas, o solo para uso en investigación", según la FDA.

Los dispositivos e instrumentos afectados incluyen NextSeq 550Dx, MiSeq Dx, NextSeq 500, NextSeq 550, MiSeq, iSeq 100 y MiniSeq con las versiones 1.3 a 3.1 del software Local Run Manager (LRM).

La lista de fallas es la siguiente:

- CVE-2022-1517 (puntaje CVSS: 10.0): una vulnerabilidad de ejecución remota de código a nivel del sistema operativo que podría permitir que un atacante altere la configuración y acceda a datos confidenciales o API.
- CVE-2022-1518 (puntuación CVSS: 10.0): una vulnerabilidad transversal de directorio que podría permitir que un atacante cargue archivos maliciosos en ubicaciones arbitrarias.

- CVE-2022-1519 (puntaje CVSS: 10.0): un problema con la carga sin restricciones de cualquier tipo de archivo, lo que permite a un atacante lograr la ejecución de código arbitrario.
- CVE-2022-1521 (puntuación CVSS: 9,1): falta de autenticación en LRM de forma predeterminada, lo que permite a un atacante inyectar, modificar o acceder a datos confidenciales.
- CVE-2022-1524 (puntaje CVSS: 7.4): falta de cifrado TLS para las versiones 2.4 y anteriores de LRM que podría ser objeto de abuso por parte de un atacante para organizar un ataque de intermediario (MitM) y acceder a las credenciales.

Remediación / Referencias

Si bien no hay evidencia de que las fallas se estén explotando en la naturaleza, se recomienda que se aplique el parche de software lanzado por Illumina el mes pasado para mitigar cualquier riesgo potencial.

Para saber más invitamos a visitar el siguiente sitio:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1517

Microsoft	Vulnerabilidad descubierta de Microsoft Office 365 que podría ser abusada	CRÍTICO

Descripción

Se ha descubierto una "funcionalidad peligrosa" en la suite de Microsoft 365 que podría ser potencialmente abusada por un actor malicioso para rescatar archivos almacenados en SharePoint y OneDrive y lanzar ataques a la infraestructura de la nube.

Estado

El ataque depende de una función de Microsoft 365 llamada AutoSave que crea copias de versiones de archivos anteriores cuando los usuarios realizan ediciones en un archivo almacenado en OneDrive o SharePoint Online.

Comienza con la obtención de acceso no autorizado a la cuenta de un usuario objetivo, seguido por el abuso del acceso para cifrar archivos. Las tres vías más comunes para obtener el punto de apoyo inicial implican la violación directa de la cuenta a través de ataques de phishing o de fuerza bruta, engañar a un usuario para que autorice una aplicación OAuth de terceros no autorizada o tomar el control de la sesión web de un usuario que ha iniciado sesión.

Al aprovechar el acceso a la cuenta, un atacante puede crear demasiadas versiones de un archivo o, alternativamente, reducir el límite de versiones de una biblioteca de documentos a un número bajo como "1" y luego cifrar cada archivo dos veces.

Remediación / Referencias

Para mitigar tales ataques, se recomienda aplicar una política de contraseña segura, exigir la autenticación multifactor (MFA), evitar descargas de datos a gran escala en dispositivos no administrados y mantener copias de seguridad externas periódicas de archivos en la nube con datos confidenciales.

Por mayor información acceder a:

https://support.microsoft.com/es-es/office/detecci%C3%B3n-de-ransomware-y-recuperaci%C3%B3n-de-archivos-0d90ec50-6bfd-40f4-acc7-b8c12c73637f

android	**MaliBot: Descubierto nuevo troyano bancario para Android**	PREVENCIÓN

Descripción

Se ha detectado una nueva variedad de malware para Android que se dirige a clientes de banca en línea y billeteras de criptomonedas en España e Italia.

Estado

El troyano de robo de información, cuyo nombre en código es MaliBot, tiene tantas funciones como sus contrapartes, lo que le permite robar credenciales y cookies, omitir los códigos de autenticación multifactor (MFA) y abusar del Servicio de accesibilidad de Android para monitorear la pantalla del dispositivo de la víctima.

Se sabe que MaliBot se disfraza principalmente de aplicaciones de minería de criptomonedas que se distribuyen a través de sitios web fraudulentos diseñados para atraer a visitantes potenciales para que las descarguen.

También saca otra hoja del libro de jugadas del troyano bancario móvil, ya que emplea smishing como vector de distribución para propagar el malware accediendo a los contactos de un teléfono inteligente infectado y enviando mensajes SMS que contienen enlaces al malware. SOVA, que se detectó por primera vez en agosto de 2021, se destaca por su capacidad para realizar ataques superpuestos, que funcionan al mostrar una página fraudulenta usando

WebView con un enlace proporcionado por el servidor C2 en caso de que una víctima abra una aplicación bancaria incluida en su lista de objetivos activos.

Remediación / Referencias

Las instituciones financieras deben implementar mejores controles de seguridad y detecciones activas de amenazas para adelantarse a amenazas de rápida evolución como estas.

Para saber más invitamos a visitar el siguiente sitio:
https://revistabyte.es/ciberseguridad/malibot-banca-online/

	**Un paso más cerca de un futuro sin contraseña**	PREVENCIÓN

Descripción

Muchas empresas tecnológicas líderes están abandonando el nombre de usuario y la contraseña.

Estado

Los piratas informáticos no solo ingresan, a veces, todo lo que necesitan hacer es iniciar sesión. Lo cual es fácil, dado el estado actual de la seguridad de las contraseñas.

El enfoque más común de administración de identidades y accesos (nombre de usuario y contraseña), no ha funcionado bien durante mucho tiempo. Los piratas informáticos lanzan un promedio de 50 millones de ataques de contraseña todos los días, o alrededor de 580 por segundo.

El costo promedio de una violación de datos se estima en $4.2 millones, y las credenciales comprometidas obtienen los máximos honores como el vector de ataque más común, lo que representa el 20 % de todas las violaciones. Además, el restablecimiento de contraseñas es una de las principales razones por las que los trabajadores llaman a los servicios de asistencia de TI, y eso le cuesta a las empresas hasta $70 por cada llamada. Las grandes organizaciones de EE. UU. asignan más de $1 millón anualmente para restablecer contraseñas.

Pero eso finalmente podría estar cambiando ahora que los líderes empresariales están reconociendo los límites de la seguridad de las contraseñas. Con las herramientas de autenticación mejorando y la confianza cero convirtiéndose en el modelo dominante de ciberseguridad, más organizaciones están comenzando a implementar enfoques sin contraseña, como la autenticación multifactor (MFA), la biometría y las herramientas de inicio de sesión único (SSO).

Remediación / Referencias

Este alejamiento gradual de la seguridad basada en contraseñas no sorprende dado el alto volumen de robo de credenciales. Con el número de incidentes anuales de derrame de credenciales casi duplicándose entre 2016 y 2020, ha contribuido a las razones por las que el 92 % de las organizaciones cree que la autenticación sin contraseña es el futuro.

Para saber más invitamos a visitar el siguiente sitio:
https://blog.segu-info.com.ar/2022/06/el-futuro-es-passwordless.html

Conclusiones

Cada vez quedan más lejos los tiempos de la inocencia, aquellos en los que los teléfonos móviles y demás dispositivos como PC; eran seguros, por la sencilla razón de que no existían amenazas de seguridad a su alrededor. Tiempos en los que instalar un antivirus en un teléfono móvil no era necesario, y en los que podíamos confiar en que descargar software desde cualquier origen no nos plantearía problemas.
Eran otros tiempos, no digo que mejores, pero sí mucho más tranquilos.

Los ecosistemas de gestión de información son tan variados y cada vez más inmersos en nuestra vida diaria moderna, que ahora nuestros electrodomésticos, nuestro auto, casa y hasta la misma ciudad, se comunican; transfieren información que nos permite lograr cuotas de eficiencia y comodidad jamás antes vista. Esto implica que las amenazas resurjan en cada nueva manera de hacer o de compartir información valiosa.

Este ecosistema genera día a día nuevas amenazas en muchas tecnologías diferentes, y alrededor del mundo las mismas técnicas se globalizan, entonces tenemos desarrolladores de exploits y "zero-days" (exploits de día cero) que trabajan día a día en encontrar fallas de seguridad diversas, lo hacen a través de análisis de documentación, pruebas demo de software, revisión de código, descompilación, fuzzing, entre otras técnicas, que luego de encontradas las vías para ejecutar un compromiso, se trazan posibles prácticas de explotación y se desarrollan programas que simplifiquen los procesos; a estos últimos les llamamos "exploits".
Los exploits tienen como todo software; un tiempo de vida. La primera vez que se crean, cuando se hacen públicos, se suelen comercializar de alguna forma sobre todo los que impacten a grandes cantidades de usuarios, por eso los sistemas operativos son históricamente los softwares más atacados desde comienzos de la historia en ciberseguridad.
Aunque los tipos de amenazas son distintos, todos han seguido la misma evolución, y los zero day exploits no iban, claro, a ser una excepción. Me refiero a que nacen como un concepto a investigar, pero que con el tiempo terminan por convertirse en un producto comercial que encuentra un buen encaje en determinados mercados.

Esto genera diversos ecosistemas de negocios digitales, las finanzas crecen por y mediante el uso de tecnologías de la información que se comunican por canales digitales.
Los delincuentes se han adaptado para aprovechar todas estas debilidades, para hacer lo mismo que nos puede pasar en persona, pero por medios digitales; extorsión, fraude, violación de la privacidad, robo de billeteras, etc. Para prevenir esto en los medios digitales, necesitamos que todo el ecosistema de personas que trabajamos en él, sepamos de los ciclos de ciberseguridad y porqué son relevantes para reducir las amenazas, riesgos y peligros del uso de los mismos.
Arquitectos de software y hardware, desarrolladores, gerentes de proyectos de tecnología, administradores de redes y sistemas, particularmente.

Todo esto es parte del ciclo de desarrollo de software que toda aplicación o sistema va a experimentar en el transcurso de su existencia útil y es muy importante que este conocimiento esté arraigado para una cultura infosegura. Los procesos de descarte, son el punto final, que pasa muchas veces desapercibido por las organizaciones y es muy importante considerar, por sus implicaciones en la seguridad de la información.

El borrado seguro y destrucción de datos es importante como parte del proceso final de eliminación de datos sensibles o confidenciales, ese es otro gran capítulo que analizaremos en la siguiente quincena de noticias. ¡Hasta entonces!