Boletín de Ciberseguridad

Fecha de Publicación
05/07/2021 - N.º 11

Mes de Julio
21/06/2021 - 05/07/2021

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 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 julio se destacan 7 noticias de relevancia: 3 sobre vulnerabilidades tecnológicas, 2 de fraudes activos y 2 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Son publicadas fallas de consideración en productos Dell
Fuentes oficiales comparten información sobre errores críticos que afectan a productos Dell. En el caso de que estas fallas fueran explotadas con éxito, los atacantes podrían ejecutar código arbitrario en los equipos de los usuarios.

Prueba de concepto filtrada para una vulnerabilidad crítica en Windows
Investigadores publicaron en GitHub un código de prueba de concepto (PoC) realizado para una vulnerabilidad de ejecución remota de código en Windows Print Spooler (cola de impresión de Windows), llamado PrintNightmare. Luego fue eliminado, aunque es probable que la PoC todavía esté disponible y pueda ser utilizada por cibercriminales para dirigir ataques específicos.

TrickBot: uno de los malware más prevalentes en la actualidad
Se trata de una botnet que está en circulación desde algunos años, los nombres por lo que se le conoce son: Trickster, TheTrick o TrickLoader. Cuando apareció en acción se observó que solamente apuntaba a robar credenciales de acceso para cuentas de banco, intentando realizar transferencias fraudulentas. En la actualidad se ha transformado en un malware multi-proposito.

Características del ransomware DarkRadiation
El ransomware fue detectado por primera vez el mes de mayo y está dirigido a las distribuciones Red Hat / CentOS y Debian Linux. Se lo conoce como DarkRadiation, y está completamente escrita en Bash, lo que resulta difícil para que la mayoría de los softwares de seguridad lo detecten como una amenaza.

DELL	**Son publicadas fallas de consideración en productos Dell**	CRÍTICO

Descripción

Fuentes oficiales comparten información sobre errores críticos que afectan a productos Dell. En el caso de que estas fallas fueran explotadas con éxito, los atacantes podrían ejecutar código arbitrario en los equipos de los usuarios del proveedor de tecnología.

"Dell es una compañía multinacional estadounidense establecida en Round Rock, la cual desarrolla, fabrica, vende y da soporte a computadoras personales, servidores, switches de red, programas informáticos, periféricos y otros productos relacionados con la tecnología."

Afectados

En 2020 Dell contaba con más de 50.2 millones de equipos desplegados en el mercado.

Productos afectados:

- Dell G15 5510
- Dell G15 5511
- Dell G3 3500
- Dell G5 5500
- Dell G7 7500

Para acceder a la lista completa de productos afectados visitar el link situado en las referencias.

Estado

No se ha podido constatar si estas vulnerabilidades han sido explotadas en la actualidad de manera activa.

"La vulnerabilidad permite al atacante evadir las protecciones de Secure Boot, controlar el proceso de booting del dispositivo y ser la puerta de entrada para el uso de las otras tres vulnerabilidades reportadas, que permiten ejecutar código arbitrario en los equipos objetivo."

Remediación / Referencias

Como medidas de mitigación instamos a instalar las respectivas actualizaciones desde el sitio web del proveedor.

Por mayor información acceder a:
https://www.dell.com/support/kbdoc/es-cl/000188682/dsa-2021-106-dell-client-platform-security-update-for-multiple-vulnerabilities-in-the-supportassist-biosconnect-feature-and-https-boot-feature
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00459-01/

Microsoft	Prueba de concepto filtrada para una vulnerabilidad crítica en Windows	CRÍTICO

Descripción

Investigadores publicaron en GitHub un código de prueba de concepto (PoC) realizado para una vulnerabilidad de ejecución remota de código en Windows Print Spooler (cola de impresión de Windows), llamado PrintNightmare. Luego fue eliminado, aunque es probable que la PoC todavía esté disponible y pueda ser utilizada por cibercriminales para dirigir ataques específicos.

Afectados

Familia de productos Windows - Es más probable que este tipo de vulnerabilidades se utilicen en ataques dirigidos.

Puede encontrar una lista de complementos para identificar esta vulnerabilidad aquí:
https://www.tenable.com/plugins/search?q=cves%3A%28%22CVE-2021-1675%22%29&sort=&page=1

Estado

La explotación de esta vulnerabilidad podría dar a los atacantes remotos el control total de los sistemas vulnerables. Para lograr RCE, los atacantes deberían apuntar a un usuario autenticado en el servicio de cola de impresión. Sin autenticación, la falla podría aprovecharse para elevar los privilegios, haciendo de esta vulnerabilidad un vínculo valioso en una cadena de ataque.

Windows Print Spooler tiene un largo historial de vulnerabilidades y puede permitir un impacto serio en los objetivos. En particular, las vulnerabilidades de Print Spooler estaban vinculadas a los ataques de Stuxnet hace más de una década.

Desafortunadamente, el repositorio de GitHub estuvo disponible públicamente el tiempo suficiente para que otros lo clonaran. Es probable que la PoC todavía esté circulando y es probable que resurja públicamente, si aún no lo ha hecho.

Remediación / Referencias

La vulnerabilidad fue parcheada, aunque se indica que la actualización original no corrige las fallas ilustradas en las PoC. A partir del 1 de julio, la única solución es desactivar el servicio Print Spooler, que puede afectar operaciones importantes.

Por mayor información invitamos a visitar los siguientes sitios:
https://es-la.tenable.com/blog/cve-2021-1675-proof-of-concept-leaked-for-critical-windows-print-spooler-vulnerability?tns_redirect=true
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1675

CISCO	**Se confirman ataques a Cisco ASA**	IMPORTANTE

Descripción

Investigadores en ciberseguridad confirman ataques contra dispositivos Cisco ASA después de que fuera publicado un código de explotación PoC en Twitter para una falla XSS conocida.

También se alertó sobre ataques in-the-wild explotando esta vulnerabilidad. Las amenazas in-the-wild son amenazas que se propagan entre los distintos equipos, a diferencia de los sistemas de prueba que se realizan en un entorno aislado. El canal de infección es la vía de distribución de un malware en particular e incluye correo electrónico, IRC, bluetooth y redes peer-to-peer, entre otros.

Si el atacante lograra vulnerar los dispositivos, puede ejecutar código arbitrario dentro de la interfaz, accediendo así a información confidencial de los usuarios.

Afectados

Cisco ASA: "El software Cisco Adaptive Security Appliance (ASA) es el núcleo del sistema operativo en el que se basa la familia Cisco ASA. Proporciona funciones de firewall de clase empresarial para los dispositivos ASA en una variedad de formatos: dispositivos autónomos, módulos blade y virtuales."

Estado

Para la explotación de esta falla, el ciberdelincuente se propone a engañar a un usuario con permisos de administrador, para que de esa manera este inicie sesión y se dirija hacia el sitio web donde se implantó el código malicioso.

Remediación / Referencias

Las organizaciones deben instalar actualizaciones de seguridad que solucionen la falla para evitar ataques que aprovechen el problema.

Por mayor información invitamos a visitar los siguientes sitios:
https://blog.segu-info.com.ar/2021/06/apuntan-dispositivos-cisco-asa-despues.html
https://securityaffairs.co/wordpress/119442/hacking/cisco-asa-under-attack.html

python	**Crackonosh, el malware que utiliza paquetes de Python fraudulentos**	IMPORTANTE

Descripción

Recientemente se ha dado aviso sobre equipos con sistema operativo de Windows vulnerados, los cuales han sido infectados por un nuevo tipo de malware, generando millones de dólares en ganancias ilegales.

Fue descubierto que varios paquetes en el repositorio PyPI de Python eran utilizados para convertir equipos de usuarios vulnerables en dispositivos para minar criptomonedas. Se identificó más de 12.000 paquetes de código abierto sospechosos.

“Crackonosh, el malware se distribuye a través de copias ilegales y crackeadas de software popular, solo para deshabilitar los programas antivirus instalados en la máquina e instalar el conocido paquete de minería de monedas llamado XMRig para explotar sigilosamente los recursos del host infectado para minar Monero.”

Engañaban a desarrolladores para que descargaran los paquetes fraudulentos mediante una técnica llamada typosquatting. La cual consiste en cambiar ligeramente una cadena para suplantar un nombre legítimo a simple vista.

Afectados

Se han contabilizado más de 200.000 equipos afectados con sistema operativo de Windows y existen al menos treinta versiones diferentes del ejecutable de malware.

Estado

"Crackonosh funciona reemplazando archivos críticos del sistema de Windows como serviceinstaller.msi y maintenance.vbs para cubrir sus pistas y abusa del modo seguro, que evita que el software antivirus funcione, para eliminar Windows Defender (y otras soluciones instaladas) y desactivar las actualizaciones automáticas."

El malware apunta a instalar su propia versión de Windows Defender, esto lo hace para evitar medidas forenses de detección. Lo lleva a cabo colocando el ícono de Seguridad de Windows con una marca verde en la bandeja del sistema y ejecuta pruebas para determinar si se está ejecutando en una máquina virtual.

Remediación / Referencias

Una forma de mitigar este problema es iniciando en modo seguro y cambiando el nombre de sus directorios de aplicaciones antes de que se lancen los servicios correspondientes en Windows. Microsoft publicó que esta falla "no cumple con el estándar de servicios de seguridad", y señaló que el ataque se basa en tener privilegios de administrador / root.

Por mayor información al respecto se puede acceder a:
https://thehackernews.com/2021/06/crackonosh-virus-mined-2-million-of.html
https://blog.segu-info.com.ar/2021/06/malware-y-paquetes-de-python-que-minan.html

Office 365	Sitio web fraudulento busca suplantar a Office 365	IMPORTANTE

Descripción

Especialistas en ciberseguridad han informado sobre sitio web fraudulento que intenta remplazar a la plataforma de correo Office365, pudiendo robar credenciales de usuario.

Este intento de fraude representa una falsificación de la marca institucional que en caso de concretarse puede afectar a usuarios, clientes y a la entidad aludida.

Afectados

Microsoft Office 365 (Word, Excel, PowerPoint, Publisher, Access, OneNote, Outlook, etc.

Plataformas admitidas: Microsoft Windows - Mac OS X -Dispositivos Android e iOS.

Estado

Indicadores de compromiso:

URL sitio falso
https://ppi.mwavpn[.]com/

Certificado Digital
Fecha Válido: 27-05-2021
Fecha Término: 25-08-2021
Emitido: R3

Datos Alojamiento
IP: [52.165.230.236]
Número de Sistema Autónomo (AS): 8075
Etiqueta del Sistema Autónomo: MICROSOFT-CORP-MSN-AS-BLOCK
País: US
Registrador: ARIN

Datos del Dominio
Nombre de Dominio: mwavpn[.]com
Creado: 17-08-2020
Expira: 17-08-2021
Información del Registrador: GANDI SAS Gandi SAS
Correo Electrónico: abuse@support.gandi.com
Name Server: ns-158-a.gandi.net
ns-220-b.gandi.net

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).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los AntiSpam y SandBoxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

Por mayor información al respecto se puede acceder a:
https://csirt.gob.cl/alertas/8ffr21-00982-01/

TrickBot: uno de los malware más prevalentes en la actualidad

PREVENCIÓN

Descripción

Se trata de una botnet que está en circulación desde algunos años, los nombres por lo que se le conoce son: Trickster, TheTrick o TrickLoader. Cuando apareció en acción se observó que solamente apuntaba a robar credenciales de acceso para cuentas de banco, intentando realizar transferencias fraudulentas.

En la actualidad este malware se ha transformado en multi propósito y es utilizado como medio para que otros grupos de cibercriminales puedan distribuir su propio malware bajo el modelo de Malware-as-a-Service.

Algunas de las características a destacar de Trickbot son: “obtener información de equipos comprometidos (sistemas operativos, programas instalados, nombres de usuarios, nombres de dominio, etc.), robar de credenciales en navegadores, robar de credenciales del cliente Outlook, obtener credenciales de Windows, abusar de protocolos como SMB y LDAP para moverse lateralmente dentro de una red corporativa y descargar otro tipo de malware.”

Afectados

Trickbot sigue siendo una amenaza muy activa y se trata de una de las botnets más prolíficas y populares, con más de un millón de detecciones en todo el mundo.

El ransomware droppeado por excelencia por esta amenaza es Ryuk: un ransomware que suele apuntar a medianas y grandes compañías y que puso su foco en el rubro de salud durante el año 2020. Otro ransomware que ha sido distribuido por Trickbot es Conti.

Trickboot rastrea archivos de configuración locales en busca de nombres de usuarios y contraseñas para exfiltrar a sus servidores C&C: desde FTP de aplicaciones como FileZilla, Outlook, Chrome y Edge, hasta aplicaciones de control remoto como TeamViewer.

Vector de Ataque

"Botnet: Se trata de un programa malicioso que puede ser controlado remotamente por un atacante. Este tipo de código malicioso está compuesto por un panel de control desde el cual se ejecutan las acciones a realizar y una aplicación de servidor que establece la comunicación con el centro de control del atacante. La particularidad de las botnets es que permite a un atacante ejecutar instrucciones en muchos equipos infectados con el malware de manera simultánea."

Este malware es distribuido mediante correos de phishing dirigidos, utilizando como punto de engaño noticias de actualidad, problemas o envíos relacionados al dominio corporativo del correo de la víctima o cuestiones financieras (facturas, cobro de bonos, multas de tránsito impagas, entre otros).

Los mails que reciben las victimas contienen enlaces a páginas web fraudulentas, con archivos adjuntos de tipos varios: Excel, Word o ZIP. Estos envíos provienen de múltiples localizaciones alrededor del mundo, utilizando frecuentemente las cuentas de víctimas comprometidas en campañas antiguas para distribuirse sin apuntar a un blanco en particular.

Remediación / Referencias

Recomenedaciones para protegernos de esta amenaza:

- Estar alerta a cualquier comunicación sospechosa: Verificar el remitente, la veracidad y motivo de la comunicación, aún si proviene de una dirección de correo legítima.
- En caso de recibir un correo sospechoso, no ingresar a un sitio aunque parezca real.
- Para archivos adjuntos, sospechar de aquellos que son de tipo Word, Excel, PDF o ZIP protegidos con contraseña, y no descargarlos.
- Contar con una política que establezca cambios de contraseña periódicos.
- Mantener dispositivos y aplicaciones actualizados, tanto servidores, equipos como computadoras o laptops, o dispositivos móviles.

Por mayor información al respecto se puede acceder a:
https://www.welivesecurity.com/la-es/2021/06/25/trickbot-caracteristicas-malware-mas-activos-peligrosos/

Características del ransomware DarkRadiation

PREVENCIÓN

Descripción

El ransomware fue detectado por primera vez el mes de mayo y está dirigido a las distribuciones Red Hat / CentOS y Debian Linux. Se lo conoce como DarkRadiation, y está completamente escrita en Bash, lo que resulta difícil para la mayoría de los softwares de seguridad lo detecten como una amenaza.

"El malware utiliza el algoritmo AES de OpenSSL con modo CBC para cifrar archivos en varios directorios. También utiliza la API de Telegram para enviar un estado de infección a los actores de la amenaza y se encuentra ofuscado con node-bash-obfuscate".

Afectados

Distribuciones: Red Hat / CentOS - Debian Linux
Sus objetivos principales son los contenedores de Linux y Docker Cloud.También se ha confirmado que utiliza Telegram para iniciar la comunicación con su servidor C&C.

Vector de Ataque

"La cadena de infección de DarkRadiation es un proceso que comprende un conjunto complejo de scripts Bash y alrededor de seis C&C, todos sin conexión. El ransomware utiliza API codificadas para comunicarse con los bots de Telegram, y los scripts tienen varias dependencias, como curl, wget, OpenSSL, sshpass y pssh."

DarkRadiation obtiene una lista de usuarios del equipo vulnerado, luego sobrescribe sus contraseñas con una megacontraseña y elimina todos los usuarios de shell después de crear un nuevo usuario con el ID "Ferrum" y la contraseña "MegPw0rD3"."

Remediación / Referencias

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/06/darkradiation-dirigido-distribuciones.html
https://www.hackread.com/redhat-debian-linux-distributions-darkradiation-ransomware/

Conclusiones

En esta edición exhortamos a tener especial cuidado sobre la vulnerabilidad descubierta en Windows. A través de la filtración de una prueba de concepto realizada y publicada en distintos repositorios, se observa que su explotación exitosa puede dar lugar a actores malintencionados a tomar el control total de los sistemas vulnerables.

La falla podría aprovecharse para elevar privilegios, haciendo de esta vulnerabilidad un vínculo valioso en una cadena de ataque. La recomendación es que en los entornos corporativos de servidores se desactive el servicio de Print Spooler (cola de impresión de Windows).

Finalmente destacamos estar en constante conocimiento respecto a intentos de fraudes activos, actualización de vulnerabilidades recién descubiertas, así como las características y especificaciones de los ransomware que prevalecen en la actualidad.