Boletín de Ciberseguridad

Fecha de Publicación
21/06/2021 - N.º 10

Mes de Junio
07/06/2021 - 21/06/2021

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 segunda quincena del mes de junio se destacan 7 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas, 1 de fraudes activos y 4 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Fallas críticas en productos de Apple
"Fuentes oficiales publican información relevante respecto a 14 vulnerabilidades recientemente descubiertas ya siendo explotadas en productos de Apple. Se destaca que dos de estas fallas en el software del proveedor son de consideración crítica."

Errores críticos en productos Microsoft
"Se han detectado cinco errores de consideración críticos que afectan a productos Microsoft, estos fueron oportunamente reportados por el proveedor de tecnología en el mes de junio, junto con las actualizaciones correspondientes para su mitigación."

Preocupación por el aumento de ataques de Phishing
"Los antecedentes de Phishing para el año 2020 ya indicaban un aumento considerable en la cantidad de ataques de phishing, en enero de este año fue superado alcanzando un récord histórico a nivel mundial, constatándose la existencia de más de 240.000 intentos de phishing entre correos enviados y sitios fraudulentos."

	Fallas críticas en productos de Apple	CRÍTICO

Descripción

Fuentes oficiales publican información relevante respecto a 14 vulnerabilidades recientemente descubiertas ya siendo explotadas en productos de Apple. Se destaca que dos de estas fallas en el software del proveedor son de consideración crítica.

Afectados

- iOS 12.5.3
- iPhone 5s
- iPhone 6
- iPhone 6 Plus
- iPad Air
- iPad mini 2
- iPad mini 3
- iPod touch

A finales de marzo de 2021 la empresa Apple contaba con 365 millones de dispositivos iOS.
Más del 80% de los usuarios de iOS actualizados a iOS 5, frente al 6% de usuarios de Android actualizados en el mismo período.

Estado

Vulnerabilidades críticas:
La primera responde a un error de corrupción de memoria, la que puede ser explotada mediante la ejecución de código remoto.

La siguiente falla se basa en un error de uso de memoria, después de ser liberada puede ser explotada para lograr ejecución arbitraria de código.

Remediación / Referencias

Para la correcta mitigación de estas vulnerabilidades se debe instalar las respectivas actualizaciones desde el sitio web del proveedor. Estas son parte del contenido de seguridad incluido en iOS 12.5.4.

Por mayor información acceder a:
https://support.apple.com/en-us/HT212548
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00455-01/

Microsoft	**Errores críticos en productos Microsoft**	CRÍTICO

Descripción

Se han detectado cinco errores de consideración críticos que afectan a productos Microsoft, estos fueron oportunamente reportados por el proveedor de tecnología en el mes de junio, junto con las actualizaciones correspondientes para su mitigación.

Afectados

Productos Microsoft:

- Microsoft Windows
- .NET Core
- Visual Studio
- Microsoft Office
- Microsoft Edge (Chromium-based y EdgeHTML)
- Microsoft SharePoint Server
- Hyper-V
- Visual Studio Code – Kubernetes Tools
- Windows HTML Platform
- Windows Remote Desktop

Estado

Por el momento no se ha podido determinar que estas vulnerabilidades estén siendo explotadas activamente.

Vulnerabilidades críticas:
Software antimalware Defender de Microsoft - Ejecución arbitraria de código
Microsoft SharePoint Server - Ejecución arbitraria de código
Video Extensions - Ejecución arbitraria de código
Windows - Ejecución arbitraria de código.
Windows MSHTML Platform - Ejecución arbitraria de código.

" El término ejecución arbitraria de código (del inglés arbitrary code execution) hace referencia, en el campo de la seguridad informática, a la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación a su antojo, aprovechando generalmente alguna vulnerabilidad (por ejemplo, un desbordamiento de búfer).”

Remediación / Referencias

Microsoft ha publicado las actualizaciones de seguridad correspondientes, las cuales incluyen el parche necesario para la remediación del problema.

Por mayor información invitamos a visitar los siguientes sitios:
https://msrc.microsoft.com/update-guide/vulnerability
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00454-01/

	**Preocupación por el aumento de ataques de Phishing**	CRÍTICO

Descripción

Los antecedentes de Phishing para el año 2020 ya indicaban un aumento considerable en la cantidad de ataques de phishing, en enero de este año fue superado alcanzando un récord histórico a nivel mundial, constatándose la existencia de más de 240.000 intentos de phishing entre correos enviados y sitios fraudulentos.

Se ha observado que estas técnicas utilizadas para vulnerar a la víctima siguen en ascenso, evolucionando e implementando nuevos recursos para un engaño exitoso.

"El termino Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima."

Afectados

La industria financiera sigue siendo el sector más apuntado por los ataques de phishing, registrando el 24.9% de los intentos de phishing. En el caso de las redes sociales se determinó el 23.6% y los proveedores de servicios de correo a través de sitios web con el 19.6%.

La cantidad de empresas cuya imagen fue utilizada en estos ataques de ingeniería social superó las 400 en cada uno de los meses del primer cuarto de 2021, llegando a 465 la cantidad de marcas utilizadas en campañas de phishing en marzo.

"Los ataques de phishing apuntando a usuarios de redes sociales pasó de 11.8% en el último cuarto de 2020 a 23.6% durante los primeros tres meses de 2021, con cibercriminales lanzando ataques con el objetivo de secuestrar cuentas de redes sociales para probablemente comercializar los accesos en mercados de la dark web."

Estado

Por otra parte, también se ha visto un aumento considerable en las estafas conocidas como BEC (del inglés Business Email Compromise). Se trata de un intento de fraude dirigido a los sectores de finanzas de las empresas, el cual consiste en la utilización de correo electrónico buscando suplantar la identidad de una persona confiable, como un empleado de la propia organización o de una compañía socia, solicitando así el envío de una transferencia de dinero.

"Por último, mencionar que los ataques de ingeniería social, principalmente de phishing, son responsables del 20% de los incidentes de seguridad que registraron las empresas de América Latina durante 2020, según datos del ESET Security Report 2021."

Remediación / Referencias

Es importante destacar que ya no es suficiente con la verificación de que un sitio web es seguro o no tomado en cuenta si este es HTTPS, ya que el 83% de las paginas web detectadas utilizaban este protocolo de seguridad.

Por mayor información al respecto se puede acceder a:
https://www.welivesecurity.com/la-es/2021/06/15/2021-registro-pico-historico-cantidad-sitios-phishing/

intel	**Intel publica actualizaciones de consideración**	PREVENCIÓN

Descripción

Fueron corregidas más de 70 vulnerabilidades de seguridad. Intel tomó medidas de mitigación respecto a cinco vulnerabilidades de alta gravedad que afectan la tecnología de virtualización de Intel para productos de E / 0 dirigida (VT-d), el firmware de BIOS para algunos procesadores.

Afectados

"Hoy publicamos 29 avisos de seguridad que abordan 73 vulnerabilidades: 40 de ellos, o el 55%, se encontraron internamente a través de nuestra propia investigación de seguridad proactiva", dijo el director de Comunicaciones de Intel, Jerry Bryant."

Para ver la lista completa de productos afectados invitamos a acceder al siguiente link:
https://www.intel.com/content/www/us/en/security-center/default.html

Vector de Ataque

Es causado por una limpieza incompleta en algunos productos Intel VT-d que podría permitir a atacantes autenticados escalar privilegios a través del acceso local. Intel también corrigió cuatro errores más causados por una inicialización incorrecta, condición de carrera, validación de entrada incorrecta y administración de flujo de control insuficiente en el firmware del BIOS de la CPU que permite la escalada de privilegios a través del acceso local o físico.

"El error de alta gravedad parcheado en la Biblioteca de seguridad de Intel afecta a las versiones anteriores a la versión 3.3, y es causado por un intercambio de claves sin autenticación de entidad que permite a los atacantes autenticados escalar privilegios a través del acceso a la red."

"Intel también parcheó otras 11 vulnerabilidades de seguridad de alta gravedad que afectan a los NUC de Intel, el controlador y el asistente de soporte de Intel (DSA), el ID de Intel RealSense, el controlador del motor de aceleración programable abierto (OPAE) de la matriz de puerta programable de campo Intel (FPGA) para Linux y los controladores Intel Thunderbolt."

Remediación / Referencias

En este año 2021 Intel ha podido solucionar 132 vulnerabilidades, alguna de ellas de consideración critica ante el caso de una explotación exitosa.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/06/actualizaciones-criticas-de-intel.html
https://www.bleepingcomputer.com/news/security/intel-fixes-73-vulnerabilities-in-june-2021-platform-update/amp/

Ataques dirigidos avanzan sobre distintas industrias

PREVENCIÓN

Descripción

Especialistas en ciberseguridad manifiestan preocupación por el aumento de ataques dirigidos en el 2021 a los distintos productos y servicios que ofrecen las empresas, independientemente al rubro a que estas se dediquen.

"Aprovechando de la desestabilización global al apuntar a industrias esenciales y vulnerabilidades comunes desde el cambio al trabajo remoto. Las industrias de salud, manufactura y finanzas experimentaron un incremento en los ataques (200%, 300% y 53%, respectivamente), y estos tres sectores principales representaron un total combinado del 62% de todos los ataques en 2020, un 11% más que en 2019."

Debido a que las empresas se esfuerzan por ofrecer más acceso virtual y remoto a través del uso de portales de clientes, se ha visto un aumento del 67% en los ataques dirigidos a aplicaciones web.

"La atención médica sufrió la peor parte de estos ataques debido a su cambio a la telesalud y la atención remota, con el 97% de toda la actividad hostil dirigida a esta industria, siendo ataques a aplicaciones web o ataques a aplicaciones específicas."

Afectados

Los ataques contra el sector manufactura aumentaron del 7% el año pasado al 22%; el sector salud incrementó del 7% al 17%; y el sector financiero ha aumentado del 15% al 23%.

Empresas de múltiples industrias tuvieron ataques relacionados con la vacuna COVID-19 y las cadenas de suministro asociadas.

"El oportunismo ciberdelincuente del COVID-19 se intensificó, con grupos como Ozie Team, Agent Tesla y TA505, junto con actores estatales como Vicious Panda, Mustang Panda y Cozy Bear muy activos en 2020."

Los tipos de malware más reconocidos son Mineros: 41%; Troyanos: 26%; Gusanos: 10%, ransomware 6%.

En Europa, Oriente Medio, África y América los criptomineros dominaron la actividad, pero fueron poco comunes en Asia.

"El 50% de las organizaciones a nivel mundial están priorizando la protección de sus servicios en la nube, lo que la convierte en el principal centro de atención de ciberseguridad durante los próximos 18 meses."

"Los servicios empresariales y profesionales fueron la industria más atacada en América, representando el 26% de todos los ataques. Estados Unidos presentó dos de las tasas más altas de actividad de reconocimiento de todos los países analizados."

En el ámbito de la educación, el 58% de toda la actividad hostil fue de reconocimiento. América observó el 8% de todos los ataques como ataques DoS/DDoS.

Vector de Ataque

Durante el último año con el incremento del malware multifunción, el malware se está volviendo más masificado y diverso en cuanto a características y funcionalidades.

Los criptomineros han reemplazado al software espía como el malware más común en el mundo, pero el uso de ciertas variantes de malware contra industrias específicas continúa evolucionando.

Los gusanos aparecieron con mayor frecuencia en los sectores financiero y manufacturero. La atención médica se vio afectada por los troyanos de acceso remoto, mientras que la industria de la tecnología fue atacada por el ransomware. El sector educativo se vio afectado por los criptomineros debido a la popularización de la minería entre los estudiantes que explotan infraestructuras desprotegidas.

Remediación / Referencias

"Los cambios en los modelos operativos o la adopción de nuevas tecnologías presentan oportunidades para los actores malintencionados y con un creciente mercado de criptomonedas popular entre los estudiantes sin experiencia; los ataques estaban destinados a suceder. Ahora, a medida que entremos a una fase más estable de la pandemia, tanto las organizaciones como las personas deben priorizar la higiene de la ciberseguridad en todas las industrias, incluida la cadena de suministro."

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/06/los-ataques-oportunistas-dirigidos.html
https://diarioti.com/estudio-global-los-ataques-oportunistas-dirigidos-aumentan-hasta-300/116740

AVADDON RANSOMWARE	**Avaddon finaliza sus operaciones y entrega claves a sus víctimas**	PREVENCIÓN

Descripción

El grupo de cibercriminalas ransomware Avaddon ha finalizado sus operaciones, entregando las claves de descifrado de sus víctimas a BleepingComputer, un sitio web que cubre noticias de tecnología y ofrece ayuda informática gratuita a través de sus foros. En el pasado, se lanzaron claves de descifrado para TeslaCrypt, Crysis, AES-NI, Shade, FilesLocker, Ziggy, y FonixLocker.

"BleepingComputer recibió un aviso anónimo que pretendía ser del FBI y que contenía una contraseña y un enlace a un archivo ZIP protegido por contraseña. Este archivo decía ser "Decryption Keys Ransomware Avaddon" y contenía los tres archivos y se confirmaron que las claves eran legítimas."

Afectados

Los ataques de Avaddon han afectado a empresas y organizaciones de todo el mundo, incluidos varios países de América Latina. Son 2.934 las claves de descifrado entregadas, donde cada clave corresponde a una víctima específica. Emsisoft ya publicó descifrador gratuito con esas claves.

Vector de Ataque

"Avaddon lanzó su operación en junio de 2020 a través de una campaña de phishing que sólo contenía un guiño sonriente. Con el tiempo, Avaddon se ha convertido en una de las operaciones de ransomware más importantes, y el FBI y la policía australiana publicaron recientemente avisos relacionados con el grupo."

Avaddon logra acceso a una red realizando primero tareas de reconocimiento para identificar principalmente bases de datos, backup y copias shadow, y también buscando la forma escalar privilegios dentro de la red.

Utiliza técnicas para dificultar el análisis: anti-VM, anti-debugging, utilización de tablas de strings cifradas encapsuladas en objetos.

Remediación / Referencias

En comparación con otros grupos de ciberdelincuentes que finalizan sus operaciones a través de mensajes publicados en la web, Avaddon ha desaparecido sin dar indicio alguno más que la entrega de las claves de sus víctimas.

Se cree que Avaddon puede estar entrando en una fase de "cambio de marca", algo que muchs otros grupos criminales han hecho antes, como Nemty-to-Nefilim y Gandcrab-to-REvil. De esta manera puede lograr evadir el rastro que van dejando y ocultarse del seguimiento de la justicia.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/06/ransomware-avaddon-cierra-su-operacion.html
https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/

	**Prevención y cuidado de los datos personales**	PREVENCIÓN

Descripción

Recientemente en Argentina se detectó un problema de seguridad y un manejo inadecuado de los datos personales de los usuarios, que dándose a conocer dejaría expuestos datos confidenciales e información sensible.

“Un sitio.com.ar (no gubernamental) estaba siendo enviado por Whatsapp a los pacientes que se realizan exámenes médicos en los hospitales públicos de la zona un enlace que apunta a un archivo PDF dentro del directorio "/constancias" del sitio mencionado. Al momento de encontrar el directorio había más de 20.000 archivos PDF almacenados”

Cada país tiene una ley de protección de datos personales y a nivel global existen distintos estándares regulatorios y de calidad de servicio que velan por el tratamiento adecuado de la información personal de los usuarios.

Es muy importante en seguridad de la información tener en cuenta la autenticidad de los usuarios que acceden a la información, la disponibilidad e integridad de la misma y la confidencialidad, la que en este caso puntual está siendo vulnerada.

"La Ley 25.326 es el mecanismo existente de protección de los datos personales en Argentina, que incluye los datos sensibles y de salud. En particular el art. 9 de la Ley donde señala que "El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado..." y sigue "Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad."

Afectados

El PDF tiene todos los datos personales y de salud del paciente: como la dirección de domicilio, su teléfono personal, enfermedades prevalentes, etc.

Vector de Ataque

El inconveniente aparece cuando el dueño del sitio olvida proteger el directorio "/constancias" y permite el listado abierto de todos los archivos PDF. Cualquiera que acceda al directorio abierto, sin autenticación previa, puede acceder a todos los resultados.

"Al llamar directamente a su teléfono personal, el dueño del sitio.com.ar procedió a bloquear la navegación de directorio inmediatamente, aunque eliminar el listado de directorios no soluciona el problema definitivamente. Luego, al reportar el problema de forma personal a un directivo del sitio este fue bloqueado temporalmente y luego los archivos sí fueron eliminados por el dueño del sitio."

Remediación / Referencias

Como medidas preventivas se recomienda:

- Constatar la confiabilidad del sitio de hosting que se está utilizando para guardar datos sensibles.

- Estar informado respecto a si el proveedor realiza el tratamiento correcto de la información y si el servicio ofrecido está apegado tanto a los estándares regulatorios de su país como a las normas internacionales.

- Se debe apuntar y concientizar por que haya un responsable de la información a quien se pueda consultar y sea responsable de la información privada de terceros.

Conclusiones

Vistas las amenazas y técnicas delictivas a las que nos enfrentamos y vemos diariamente en las noticias, es como responsables de organizaciones y de información asociada que debemos seguir teniendo en cuenta la relevancia de la información que publicamos, sobre todo cuando la misma contiene información sensible de forma directa.

Los casos de phishing, engaños a través de correo electrónico y redes sociales continúan en aumento, aquí no solo recomendamos la habilitación de doble factor de autenticación en todas las cuentas de usuarios de la organización, sino que también estar muy atentos como usuarios de tecnología, sobre todo cuando existen mensajes con promociones, sorteos o regalos, estos siguen siendo los principales temas de inicio de ataques falsificados.

Es importante ser muy precavido en estos casos, sobre todo ante los errores de "typos", sobre este tema publicamos una nota en dónde explicamos que son y como prevenir diversos ataques en nuestras organizaciones a través del bloqueo efectivo de los mismos.

Estas protecciones son cada vez más relevantes de incorporarlas a medida que los adversarios aumentan en cantidad y capacidad, y las defensas sobre algunos aspectos siempre se pueden reforzar para trabajar con seguridad y tranquilidad.

¡Sigan protegiéndose!