Boletín de Ciberseguridad

Fecha de Publicación
07/06/2021 - N.º 9

Mes de Junio
01/06/2021 - 07/06/2021

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 primera quincena del mes de junio se destacan 5 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas, 2 de fraudes activos y 1 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Fallas descubiertas permiten alterar a PDF con firma certificadora
"Fuentes oficiales exponen dos técnicas nuevas para atacar PDF certificados, lo que permite a los ciberdelincuentes modificar la información original del documento por contenido malicioso dejando la firma intacta, sin invalidarla."

Intento de Fraude que reemplaza al BBVA
"Fuentes oficiales del Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile (CSIRT de Gobierno), ha identificado una campaña de malware falsamente proveniente del banco BBVA. Con ella, el atacante busca persuadir a las personas de descargar el archivo adjunto y ejecutarlo."

Especificaciones y características del Ransomware Avaddon
"Se trata de un ransomware en crecimiento y con una fuerte presencia en varios países, fue detectado hace más de dos años. Para la recuperación de los archivos robados han llegado a pedir a sus víctimas la suma de USD 40.000 en su equivalente en Bitcoins. "

Fallas descubiertas permiten alterar a PDF con firma certificadora

CRÍTICO

Descripción

Fuentes oficiales exponen dos técnicas nuevas para atacar PDF certificados, lo que permite a los ciberdelincuentes modificar la información original del documento por contenido malicioso dejando la firma intacta, sin invalidarla.

"La idea del ataque explota la flexibilidad de la certificación PDF, que permite firmar o agregar anotaciones a documentos certificados bajo diferentes niveles de permiso", dijeron investigadores de Ruhr-University Bochum, que han analizado asistemáticamente la seguridad de la especificación PDF a lo largo de los años. Los hallazgos se presentaron en el 42º Simposio de IEEE sobre Seguridad y Privacidad IEEE S&P 2021) celebrado esta semana.

Evil Annotation y Sneaky Signature son las denominaciones utilizadas para ambos ataques, los cuales consisten en manipular el proceso de certificación de PDF, realizando una explotación de las vulnerabilidades descubiertas en la implementación de firmas digitales, tanto en las firmas de aprobación como en las firmas de certificación.

“Las firmas de certificación también permiten diferentes subconjuntos de modificaciones en el documento PDF según el nivel de permiso establecido por el certificador, incluida la capacidad de escribir texto en campos de formulario específicos, proporcionar anotaciones o incluso agregar varias firmas.”

Afectados

Adobe Acrobat Reader - Ataque EAA.
Foxit Reader - Ataque EAA.
Nitro Pro - Ataque EAA.
Soda PDF Desktop – Ataque SSA.
PDF Architect - Ataque SSA.

Evil Annotation Attack (EAA): funciona modificando un documento certificado que está provisto para insertar anotaciones para incluir una anotación que contiene código malicioso, que luego se envía a la víctima.

Sneaky Signature (SSA): este ataque se basa en manipular la apariencia agregando elementos de firma superpuestos a un documento que permite completar campos de formulario.

Estado

A través de estos tipos de ataques se pudo establecer también que tanto en Adobe Acrobat Pro como Adobe Reader se puede ejecutar código JavaScript aprovechándose de estas fallas, redirigiendo a la víctima a una página web maliciosa.

Lo que genera mayor preocupación en los especialistas, es la posible alteración y perdida de autenticidad de documentos PDF que están certificados mediante una firma digital. En el caso de que el exploit sea exitoso, resulta un riesgo crítico y una pérdida de credibilidad del contrato acordado entre las partes.

"También al insertar un campo de firma, el firmante puede definir la posición exacta del campo y, además, su apariencia y contenido, dijeron los investigadores". "Esta flexibilidad es necesaria ya que cada nueva firma podría contener la información del firmante. La información puede ser un gráfico, un texto o una combinación de ambos. Sin embargo, el atacante puede hacer un mal uso de la flexibilidad para manipular sigilosamente el documento e insertar contenido nuevo. "

Cuando la persona crea un contrato certificado con información sensible, mientras habilita la opción de agregar más firmas al contrato PDF, el ciberdelincuente se aprovecha de estos permisos vulnerando la información original del documento.

"Aunque ni la EAA ni la SSA pueden cambiar el contenido en sí, siempre permanece en el PDF, las anotaciones y los campos de firma se pueden usar como una superposición para agregar contenido nuevo. Las víctimas que abren el PDF no pueden distinguir estas adiciones del contenido normal. Y lo que es peor: las anotaciones pueden incrustar código JavaScript de alto privilegio que puede agregarse a ciertos documentos certificados"

Remediación / Referencias

Para prevenir un posible ataque los investigadores en ciberseguridad recomiendan no utilizar las anotaciones de FreeText, Stamp y Redact en Adobe. También cerciorarse que los campos de texto para firmar estén configurados en ubicaciones definidas en el archivo PDF antes de la certificación.

Como medida de mitigación ha sido creada una herramienta en Python llamada PDF-Detector, la cual analiza documentos certificados para identificar la aparición de elementos sospechosos en un documento PDF.

Por mayor información acceder a:
https://thehackernews.com/2021/05/researchers-demonstrate-2-new-hacks-to.html
https://blog.segu-info.com.ar/2021/05/demuestran-vulnerabilidades-que.html

Bluetooth	**Errores en Bluetooth pueden suplantar un dispositivo legitimo**	IMPORTANTE

Descripción

Han sido publicadas distintas vulnerabilidades en Bluetooth, que en caso de un exploit exitoso puede llevar a que un atacante simule ser un dispositivo genuino mientras se da el proceso de emparejamiento.

“Los investigadores identificaron que estas fallas podrían permitir a un atacante (actuando como un MITM (Man-in-the-Middle) en el procedimiento de autenticación mediante clave) utilizar una serie de respuestas creadas por el mismo para determinar cada bit de la clave de acceso generada aleatoriamente y seleccionada por el iniciador de emparejamiento en cada ronda del procedimiento de emparejamiento, y una vez identificada, hacer uso de estos bits de la clave durante la misma sesión de emparejamiento para completar con éxito el procedimiento de emparejamiento autenticado con el respondedor”, dice el aviso de seguridad de Bluetooth SIG.

Afectados

Bluetooth SIG: Bluetooth Special Interest Group es una asociación privada sin ánimo de lucro con sede en Kirkland, Washington. A fecha de septiembre de 2007, el SIG estaba formado por más de 9000 compañías de telecomunicaciones, informática, automovilismo, música, textil, automatización industrial y tecnologías de red.

Empresas afectadas: Android, Cisco, Microchip Technology, Cradlepoint, Intel y Red Hat.

Estado

El éxito del exploit está en que primero el atacante se encuentre en el rango inalámbrico de dos equipos que intenten conectarse entre sí. Luego de que se termine la autenticación y al participar del proceso de emparejamiento, el equipo de respuesta queda autenticado con el ciberdelincuente y no con el iniciador de la conexión, permitiendo que el ciberdelincuente pueda interceptar y recabar información confidencial del usuario.

Aun no hay información de si estas vulnerabilidades han sido explotadas por algún atacante.

Remediación / Referencias

Bluetooth SIG ya ha publicado recomendaciones al respecto, ahora se espera que las empresas vulneradas también lancen las actualizaciones y parches de mitigación correspondientes.

Por mayor información invitamos a visitar los siguientes sitios:
https://www.welivesecurity.com/la-es/2021/05/28/vulnerabilidades-bluetooth-permitir-atacantes-hacerse-pasar-dispositivo-de-otro/

BBVA	**Intento de Fraude que reemplaza al BBVA**	CRÍTICO

Descripción

Fuentes oficiales del Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile (CSIRT de Gobierno), ha identificado una campaña de malware falsamente proveniente del banco BBVA. Con ella, el atacante busca persuadir a las personas de descargar el archivo adjunto y ejecutarlo.

Afectados

BBVA: La entidad financiera contaba con 35,6 millones de clientes a nivel mundial (a septiembre de 2020), frente a los 15,3 millones de 2015.

Estado

El fraude se encuentra activo al día de hoy y en el caso de que sea exitoso puede resultar en un perjuicio económico para los usuarios y un daño en la imagen reputacional de la empresa.

“El mensaje del correo indica que existe un aviso de pago emitido a petición del cliente. En realidad, el atacante adjunta un archivo con malware, con el objetivo de que sea descargado y ejecutado en el equipo del receptor, lo que gatillara la infección del equipo.”

Observación: Tener en consideración las señales de compromiso en su conjunto.

- IoC Correo Electrónico
- Datos del encabezado del correo
- Servidores SMTP: bizcloud-power.gsi.co.jp [159.203.164.34]
- Asunto: Aviso de pago: Ref. [GLV223170768] / Créditos ACH / Ref. Cliente: [18325_PK] / Ref. Segunda parte: [80015757]
- Archivos que se encuentran en la amenaza:

  Nombre: MTC103 PAYMENT.dat

  SHA256: d6e727f3c218dcf962d1adcb709f689ee22d8c4f9f69ee2f4bfa39a3e763f376

  Nombre: LQiJd4ry3xmoC7C.exe

  SHA256: bbc0947ca657f753eae1ed44b9cef04c730e8ef76d84c41901b243939dc25006

Remediación / Referencias

Recomendaciones:

- 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:
El informe oficial publicado por el CSIRT del Gobierno de Chile está disponible en el siguiente enlace:
https://www.csirt.gob.cl/media/2021/05/2CMV21-00187-01.pdf

Por mayor información invitamos a visitar los siguientes sitios:
https://www.csirt.gob.cl/alertas/2cmv21-00187-01/

AnyDesk	**Malware utiliza publicidad falsa en Google dirigida a AnyDesk**	IMPORTANTE

Descripción

Especialistas en ciberseguridad advierten por una publicidad engañosa en Google dirigida a AnyDesk. Mediante ingeniería social se promueve la descarga de un instalador malicioso que suplanta al programa original. Cuando se busca descargar el software, este aparece como opción en el navegador a través de publicidad no autorizada por el proveedor. Cuando la víctima entra al enlace es redirigido a un sitio web que es igual a la página legitima de AnyDesk e insta al usuario a descargar un instalador que contiene un troyano.

Afectados

AnyDesk: es un software de escritorio remoto que provee acceso remoto bidireccional entre computadoras personales y está disponible para todos los sistemas operativos comunes.

Hasta el momento no se tiene información exacta sobre la cantidad de clics sobre la publicidad fraudulenta, pero si se estima de quienes visitaron el sitio falso, una gran mayoría realizaron la descarga del instalador infectado.

Estado

Se trata de una técnica que tiene características de una puerta trasera. Esta busca vulnerar al usuario accediendo a información sensible además de obtener control remoto sobre el equipo, mediante la utilización de Ingeniería Social.

“Se cree que la campaña comenzó el 21 de abril de 2021, involucra un archivo malicioso que se hace pasar por un ejecutable de AnyDesk (AnyDeskSetup.exe), que, al ejecutarse, descarga un implante de PowerShell para acumular y exfiltrar información del sistema infectado.”

Remediación / Referencias

El proveedor del software comunicó informar a Google para borrar e invalidar la publicidad engañosa, a lo cual aseguran ya se están tomando medidas de mitigación.

“Este uso malintencionado de Google Ads es una forma eficaz e inteligente de lograr un despliegue masivo de shells, ya que proporciona al actor de amenazas la capacidad de elegir libremente sus objetivos de interés.”

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/05/instaladores-de-anydesk-promocionados.html
https://thehackernews.com/2021/05/malvertising-campaign-on-google.html?m=1#click=https://t.co/TUC23ZAaeY

AVADDON RANSOMWARE	**Especificaciones y características del Ransomware Avaddon**	PREVENCIÓN

Descripción

Se trata de un ransomware en crecimiento y con una fuerte presencia en varios países, fue detectado hace más de dos años. Para la recuperación de los archivos robados han llegado a pedir a sus víctimas la suma de USD 40.000 en su equivalente en Bitcoins

Mediante un programa llamado Ransomware-as-a-Service (RaaS) han logrado reclutar adeptos en la deep-weeb en todas partes del mundo, sumándose a los ataques dirigidos.

“Muchos grupos de ransomware adoptaron la modalidad extorsiva del doxing; es decir, el robo de información de los sistemas comprometidos previo al cifrado para luego amenazar a las víctimas con publicar la información en caso de no querer llegar a un acuerdo para el pago del rescate. En el caso de Avaddon, si bien de acuerdo con las muestras analizadas y los hashes públicos que observamos no detectamos la capacidad de robar información desde el equipo infectado, los operadores detrás de este ransomware cuentan con un sitio en la red TOR creado principalmente para este fin en el que publicaron supuesta información de las víctimas.”

Otro de los ataques que se han podido constatar es mediante la denegación de servicios (DDoS), buscando interrumpir el buen funcionamiento de la página web de sus víctimas, no permitiendo a los usuarios el acceso al sitio consultado.

Afectados

Los ataques de Avaddon han afectado a empresas y organizaciones de todo el mundo, incluidos varios países de América Latina.

Vector de Ataque

"Mediante la técnica de phishing envía a sus víctimas correos que incluyen un archivo JScript malicioso adjunto que utiliza una segunda extensión ".ZIP" para hacerle creer a la potencial víctima que se trata de un archivo comprimido que contiene una foto comprometedora que ha sido descubierta en la web. El código JScript a su vez ejecuta comandos de Powershell para descargar el ransomware de un servidor web y guardarlo en el directorio %TEMP% del equipo de la víctima para luego ejecutar el malware."

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

Teniendo esto en cuenta, algunas recomendaciones son:

- Hacer backup de la información de manera periódica.
- Instalar una solución de seguridad confiable.
- Utilizar una solución de cifrado de archivos.
- Capacitar al personal sobre los riesgos que existen en Internet y cómo evitarlos.
- Mostrar las extensiones ocultas de los archivos por defecto.
- Analizar los adjuntos de correos electrónicos.
- Deshabilitar los archivos que se ejecutan desde las carpetas AppData y LocalAppData.
- Deshabilitar RDP cuando no sea necesario.
- Actualizar el software de dispositivos de escritorio, móviles y de red.
- Crear políticas de seguridad y comunicarlas a los empleados.

Por mayor información al respecto se puede acceder a:
https://www.welivesecurity.com/la-es/2021/05/31/ransomware-avaddon-principales-caracteristicas/

Conclusiones

Las noticias contenidas en este boletín advierten sobre las nuevas modalidades y distintos ataques utilizados por ciberdelincuentes para alterar documentación digitalizada, falsificando y afectando la autenticidad de los mismos.

También destacamos a estar atentos y mantenerse informado respecto al phishing y a otras modalidades de ingeniería social, ya que se observa un incremento constante de intentos de engañar a las víctimas, mediante correos que buscan suplantar instituciones de manera ilegitima para robar y manipular información sensible de los clientes.

Finalmente podemos concluir que hacer un seguimiento y una correcta identificación de los ransomware que persisten y avanzan sobre distintos países, permite tomar medidas preventivas de mitigación para no ser vulnerados.

Nuestro principal objetivo es concientizar sobre los riesgos crecientes y proveer de herramientas útiles, para mejorar la postura de seguridad digital de las organizaciones.

El equipo de Datasec queda a las órdenes ante cualquier consulta o requerimientos de mayor información y apoyo para remediar cualquier situación detectada.