PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

127-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°127	Fecha: 31-05-2024
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	La fuga de datos expone a los líderes empresariales y a los datos de las principales celebridades		
Tipo de Ataque	Fuga de Información	Abreviatura	FugaInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K02
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

Una reciente filtración de datos que involucró a la firma Clarity.fm, con sede en San Francisco, una plataforma que conecta a empresarios con expertos de la industria, dejó información confidencial y personal sobre líderes empresariales y celebridades expuesta al acceso público sin ninguna autenticación de seguridad.

Fundada en 2012, Clarity.fm se enorgullece de facilitar consultas bajo demanda entre empresarios y profesionales establecidos, cuenta con más de 3000 expertos y tiene como clientes a Mark Cuban, Brad Feld y Eric Ries.

2. DETALLES:

El investigador de ciberseguridad Jeremiah Fowler descubrió una base de datos no protegida con contraseña que contiene aproximadamente 155.531 registros y 121.000 cuentas de miembros de empresarios, celebridades y líderes empresariales. Los registros incluían una gran cantidad de información que incluía lo siguiente:

- Nombres completos
- Números de teléfono
- Correos electrónicos
- Contenido de la consulta
- Tarifas de consulta por hora
- Registros de pago relacionados con sesiones de consultoría anteriores.

“Los perfiles mostraban direcciones de correo electrónico personales y profesionales, tarifas por hora, pagos de sesiones de consultoría anteriores y su calificación o puntuación interna (basada en los comentarios de los usuarios). Los registros se marcaron como datos de producción e indicaron si la persona era miembro, líder o mentor”, escribió Fowler en su blog en WebsitePlanet.

Líderes empresariales y celebridades confiaron a Clarity.fm detalles confidenciales. Es posible que estas personas hayan buscado orientación sobre asuntos críticos relacionados con sus negocios o carreras.

Por lo tanto, esta filtración genera serias preocupaciones sobre la seguridad de los datos y las posibles consecuencias para sus clientes de alto perfil, ya que, con los datos expuestos, enfrentan un riesgo elevado de ser blanco de ciberdelincuentes.

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos o no solicitados. En su lugar, visitar el sitio web escribiendo la dirección directamente en su navegador.
- Controlar sus cuentas para detectar cualquier actividad inusual y tener cuidado con las estafas telefónicas que podrían implicar la explotación de los datos robados.
- Practicar una higiene estricta de contraseñas. Utilizar contraseñas únicas para cada tarjeta y cambiarlas periódicamente.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.
- Implementar medidas rigurosas de evaluación y monitoreo de proveedores, cifrado de datos regular, protocolos de autenticación de usuarios, para salvar sus datos y la confianza de sus clientes.

Fuente de Información:	• hxxps://hackread.com/data-leak-exposes-business-leaders-celebrity-data/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°127	Fecha: 31-05-2024 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en productos de Luxion		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Luxion ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo desbordamiento de búfer basado en pila, elemento de ruta de búsqueda no controlada Y escritura fuera de límites en varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en instalaciones afectadas de Luxion KeyShot Viewer.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-5506 podría permitir a un atacante remoto ejecutar código arbitrario en instalaciones afectadas de Luxion KeyShot Viewer. Se requiere la interacción del usuario para aprovechar esta vulnerabilidad, ya que el objetivo debe visitar una página maliciosa o abrir un archivo malicioso. La falla específica existe en el análisis de archivos KSP. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar una escritura más allá del final de un búfer asignado. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del proceso actual.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-5507 podría permitir a un atacante remoto ejecutar código arbitrario en instalaciones afectadas de Luxion KeyShot Viewer. Se requiere la interacción del usuario para aprovechar esta vulnerabilidad, ya que el objetivo debe visitar una página maliciosa o abrir un archivo malicioso. La falla específica existe en el análisis de archivos KSP. El problema se debe a la falta de una validación adecuada de la longitud de los datos proporcionados por el usuario antes de copiarlos en un búfer basado en pila. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del proceso actual.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-5508 podría permitir a un atacante remoto ejecutar código arbitrario en instalaciones afectadas de Luxion KeyShot Viewer. Se requiere la interacción del usuario para aprovechar esta vulnerabilidad, ya que el objetivo debe visitar una página maliciosa o abrir un archivo malicioso. La falla específica existe en el análisis de archivos KSP. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar una escritura más allá del final de un búfer asignado. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del proceso actual.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-5509 podría permitir a un atacante remoto ejecutar código arbitrario en las instalaciones afectadas de Luxion KeyShot. Se requiere la interacción del usuario para aprovechar esta vulnerabilidad, ya que el objetivo debe visitar una página maliciosa o abrir un archivo malicioso. La falla específica existe en el análisis de archivos BIP. El problema se debe a la carga de una biblioteca desde una ubicación no segura. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del proceso actual.

A. Productos afectados:

- Luxion KeyShot Viewer.
- Luxion KeyShot.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://www.keyshot.com/csirt/ • hxxps://www.zerodayinitiative.com/advisories/ZDI-24-538/ • hxxps://www.zerodayinitiative.com/advisories/ZDI-24-539/ • hxxps://www.zerodayinitiative.com/advisories/ZDI-24-540/ • hxxps://www.zerodayinitiative.com/advisories/ZDI-24-541/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°127	Fecha: 31-05-2024
		Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Actores de amenazas utilizan versiones crackeadas de MS Office para distribuir malware		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código malicioso		

Descripción

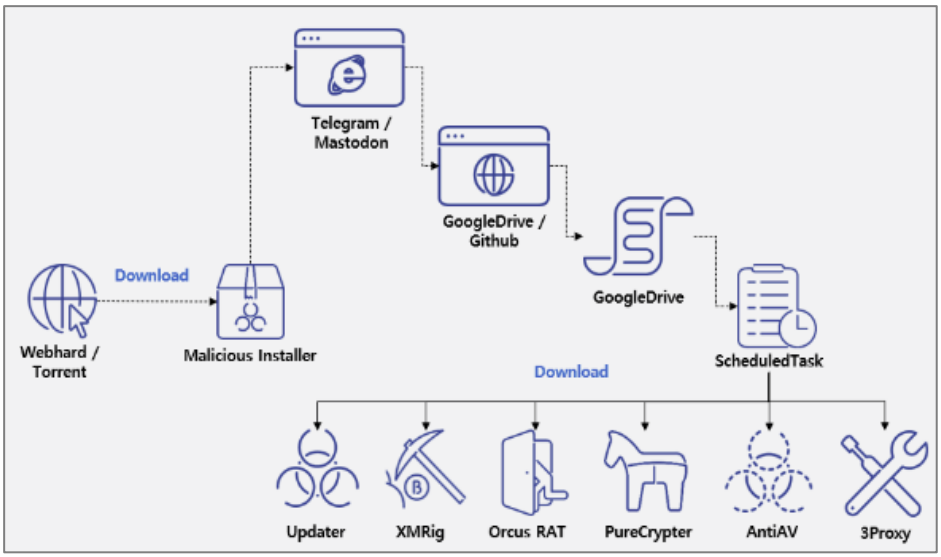
1. ANTECEDENTES:

El Centro de inteligencia de seguridad AhnLab (ASEC), ha detectado una nueva campaña de distribución de malware disfrazado de MS Office. Los actores de amenazas están aprovechando las plataformas de intercambio de archivos para distribuir malware disfrazado de MS Office, que recupera la URL de descarga y la plataforma de destino durante la infección, lo que les permite personalizar los ataques y evadir la detección.

2. DETALLES:

Los atacantes distribuyen malware disfrazado de software (Windows, MS Office, Hangul) a través de sitios para compartir archivos, y el malware evita la detección de archivos con actualizaciones frecuentes y utiliza el Programador de tareas para su persistencia, lo que provoca infecciones repetidas al eliminarlo.

Los ciberdelincuentes distribuyen malware disfrazado de software crackeado. El malware, desarrollado en .NET, utiliza ofuscación para ocultar su código malicioso e inicialmente accedió a Telegram para recuperar una URL de descarga.



Las versiones más nuevas contienen dos URL de Telegram y una URL de Mastodon, cada una con una cadena vinculada a una URL de Google Drive o GitHub. El operador del malware oculta comandos maliciosos de PowerShell dentro de estas ubicaciones de almacenamiento en la nube, utilizando codificación Base64 para una mayor ofuscación y, una vez ejecutados, estos comandos instalan cepas de malware adicionales.

El malware actualizador, "software_reporter_tool.exe", aprovecha un script de PowerShell para descargar y mantener la persistencia, lo que crea un ejecutable malicioso en "C:\ProgramData\KB5026372.exe" y utiliza una instalación 7zip comprometida ("C:\ProgramData\Google \7z.exe") para descomprimir un archivo protegido con contraseña de GitHub o Google Drive (contraseña: "x") replicando tácticas de una campaña anterior.

Además, el actualizador se registra en el Programador de tareas para garantizar un funcionamiento continuo después de un reinicio, y la tarea programada activa el script de PowerShell para obtener más actualizaciones y una posible instalación de malware. Los atacantes implementaron Orcus RAT y XMRig en el sistema comprometido.

Orcus RAT puede robar información mediante registro de teclas, cámara web y captura de pantalla, mientras que XMRig extrae criptomonedas. XMRig está configurado para detener la minería cuando se ejecutan programas que consumen muchos recursos y para finalizar procesos que compiten por los recursos, como los instaladores de software de seguridad, mientras que 3Proxy se usa para convertir la máquina infectada en un servidor proxy agregando una regla de firewall e inyectándose en un proceso legítimo.

A. Indicadores de compromiso (IoC):

MD5:

- 77a5bd4e03fc9a653b4e8c33996d19a0: Malware disfrazado de software crackeado (oinstall.exe).
- 3a4d761de4fac0c2e47a5c84fca78c0f: Descargador (software_reporter_tool.exe).
- 5dd8cdd4e80185b60d43511987b254cd: Descargador (software_reporter_tool.exe).
- 6a648b7d0e4ae16f6beb170decd5b0b6: Descargador (software_reporter_tool.exe).
- 08299a45472f501644b4daa458336428: Descargador (software_reporter_tool.exe.
- 27623130a8e8b792fc99cbdcecee3177: 3Proxy – Dropper (dwm.exe).
- abdbfe7b8f4976935b87a0a0e67d1da0: 3Proxy (dwm.exe).
- 93899d3008af9df6b7d261445b3e8f59: Orcus RAT (dwm.exe).
- 151cd4702bc15421c24fd5930f119a48: PureCrypter (dwm.exe).
- d00feba624fa6fdcbad1b1219f3f2da7: AntiAV (dwm.exe).
- 1b5393ac3eceda9b16836039f7d04c5e: XMRig (InstallUtil.exe).
- c9cdc0c746fa9095bd87b455f8f9c3c8: XMRig – codificado.
- f836a133490929ea0185d50e10bd11c0: XMRig – decodificado.

C&C:

- minecraftrpgserver[.]com:80: PureCrypter.
- minecraftrpgserver[.]com:27036: Orcus RAT.
- minecraftrpgserver[.]com:27037: XMRig.

URL de descarga:

- hxxps://t[.]me/dRidulEDhRQYNREkN: Malware disfrazado de software crackeado.
- hxxps://t[.]me/IXvMGsiyPuHoPSSiD: Malware disfrazado de software crackeado.
- hxxps://mastodon[.]social/@ dRidulEDhRQYNREkN: Malware disfrazado de software crackeado.
- hxxps://drive.usercontent.google[.]com/download?id=1kFPqJkzWKIIQzC3b0b6nunctXKHPeJNi&export=download: Comandos de PowerShell codificados en Base64.
- hxxps://drive.usercontent.google[.]com/download?id=1SFoSCa4PhCsR7ACj8HUlfrU7L1i8YwiR&export=download:
  Comandos de PowerShell codificados en Base64.
- hxxps://gist.github[.]com/thamanarya/6510d9e6b96adfea6b9422a3fd22ef82/raw/Power:
  Comandos de PowerShell codificados en Base64.

3. RECOMENDACIONES:

- Tener cuidado al ejecutar archivos ejecutables descargados de sitios para compartir archivos.
- Descargar productos como programas de utilidad y juegos sólo desde sus sitios web oficiales.
- Actualizar V3 a la última versión para evitar la infección de malware.
- Prevenir infecciones repetidas de malware reparando el Programador de tareas después de instalar V3.

Fuente de Información:	• hxxps://asec.ahnlab.com/en/66017/

Índice alfabético