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

079-2025-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°079	Fecha: 02-04-2025
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Campaña Maliciosa en Latinoamérica: AutoIt Distribuye el Infostealer Formbook		
Tipo de Ataque	Stealers	Abreviatura	Stealers
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C03
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

A mediados del primer trimestre del año, se evidenció en la telemetría de ESET, compañía de detección proactiva de amenazas, un aumento del 20% en las detecciones latinoamericanas de una familia particular de malware: Win32/Injector.Autoit.

Por lo menos el 54% de las detecciones se han concentrado en dos países de la región: Argentina y México. Completando el top de detecciones, se encuentran Colombia con 13%, Ecuador con 8%, Perú con 7% y Chile con 5%.

2. DETALLES:

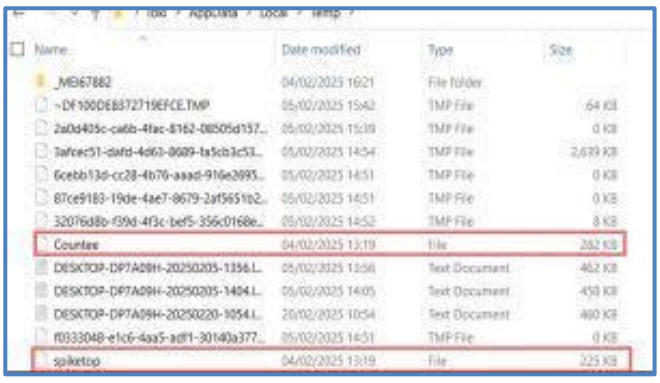
AutoIt es una herramienta utilizada por desarrolladores para automatizar tareas, pero los atacantes también pueden aprovecharla para ejecutar scripts maliciosos. En esta campaña, los ciberdelincuentes han modificado AutoIt para descargar y ejecutar Formbook en los sistemas de sus víctimas.

La campaña identificada propaga el stealer Formbook, principalmente en sistemas operativos Windows, a través de los siguientes métodos de distribución:

- Descargas disfrazadas de software legítimo en foros y páginas web fraudulentas.
- Explotación de vulnerabilidades en software desactualizado.
- Uso de publicidad maliciosa (malvertising) que redirige a los usuarios a sitios con descargas automáticas del malware.
- Correos electrónicos de phishing con archivos adjuntos maliciosos o enlaces a sitios comprometidos, dirigidos a empleados de Recursos Humanos, Finanzas o Contabilidad, quienes suelen recibir este tipo de documentos.

Al ejecutar el archivo adjunto (49fb2b8c0954cb65670a943ac017a988618b7e54), que simula ser un currículum, una cotización o formularios de pedidos, entre otros, lo que se ejecuta es un archivo compilado en Autoit que dropea un par de archivos en la ruta temporal del sistema para iniciar con el proceso de infección.

Del análisis de este archivo, detectado como una variante de Win32/Injector.Autoit, se pueden identificar las acciones que realiza la amenaza en el dispositivo de la víctima. Primero decodifica el archivo spiketop (819eaee7d4c6eeef21e32643fca172e36a97ff25), haciendo algunos reemplazos para obtener una shellcode que luego va a tratar de inyectar abusando de las características de Autoit. El objetivo es ejecutar el malware final dentro la máquina de la víctima.



Para lograrlo debe decodificar el contenido del otro archivo, Countee, copiado dentro del sistema. Para ello se vale de una cadena de bytes dentro del archivo que será utilizada como llave para descifrar el contenido del archivo.

Dentro de las algunas características de este archivo, es que contiene características de antidebugging utilizando la función GetTickCount. El binario cifrado, Countee (4e517343d6b864cdf1a88ff9167b8d03d50adfcd) es cargado en memoria para el proceso de descifrado.

Una vez que el malware final esté descifrado, se llega a una variante del infame Formbook, que será inyectado en el proceso svchost, para de esta manera realizar las acciones maliciosas sobre el dispositivo de la víctima.

Una vez activo, Formbook es capaz de robar credenciales, registrar pulsaciones de teclado, capturar pantallas y exfiltrar información confidencial hacia servidores de C2, lo que representa un riesgo crítico para la seguridad de los entornos corporativos y la integridad de los datos.

Dentro de las características de esta amenaza se pueden resaltar:

- **Robo de credenciales:** Captura credenciales y otros datos sensibles ingresados por la víctima en formularios web, de ahí su nombre.
- **Keylogging:** Registra las pulsaciones del teclado para obtener información adicional, como números de tarjetas de crédito y contraseñas.
- **Captura de pantallas:** Toma capturas de pantalla del dispositivo infectado en momentos específicos o cuando se accede a información sensible.
- **Exfiltración de datos:** Envía la información recolectada a servidores controlados por los atacantes.

Indicadores de compromiso:

Ruta utilizada para persistir en la máquina de una víctima:

C:\Users\<NOMBRE_USUARIO>\AppData\Local\Temp

Hashes, URLs y C&C

Hashes de muestras analizadas:

- e396b7e8cebd7ad85137c54bbda9dac97f04eec2 | Win32/Formbook.AA
- 517b2a5d16bcbc5ca09463f806a7be9866be2904 | Win32/Formbook.AA
- 389643635ea3a1a0e76d097f3724c8df18e95823 | Win32/Injector.Autoit.GVH
- 49fb2b8c0954cb65670a943ac017a988618b7e54 | Win32/Injector.Autoit.GVH

3. RECOMENDACIONES:

- Procurar que el sistema operativo, navegadores y aplicaciones estén siempre actualizados con los últimos parches de seguridad para mitigar vulnerabilidades explotadas por los atacantes.
- Evitar descargar archivos sospechosos adjuntos en correos electrónicos de remitentes desconocidos ni descargar software de fuentes no oficiales.
- Implementar software antivirus y herramientas de detección de amenazas que puedan identificar y bloquear la ejecución de scripts maliciosos.
- Limitar el uso de AutoIt en entornos corporativos y monitorear su ejecución para evitar usos indebidos.
- Capacitar a los empleados sobre las técnicas de ingeniería social utilizadas para distribuir malware, como correos de phishing y descargas engañosas.
- Utilizar autenticación multifactor (MFA) en todas las plataformas que sean posibles, para evitar que las credenciales comprometidas sean utilizadas por atacantes.

Fuente de Información:	• hxxps://devel.group/blog/campana-maliciosa-en-latinoamerica-autoit-distribuye-el-infostealer-formbook/ • hxxps://www.welivesecurity.com/es/investigaciones/autoit-distribuye-infostealer-formbook-empresas-latinoamerica/ • hxxps://t21.pe/ciberataques-latinoamerica-malware-formbook • hxxps://csirtasobancaria.com/alertas-de-seguridad/nueva-campana-de-distribucion-del-stealer-formbook

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°079	Fecha: 02-04-2025 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en aplicación de Apache Tomcat		
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:

Apache Software Foundation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo ejecución remota de código (RCE), que afecta a las versiones 11.0.0-M1 a 11.0.2, 10.1.0-M1 a 10.1.34 y 9.0.0-M1 a 9.0.98 de Apache Tomcat. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante eludir las restricciones de seguridad y ejecutar código arbitrario sin autenticación en condiciones específicas.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-24813 de tipo ejecución remota de código (RCE), podría permitir a un atacante eludir las restricciones de seguridad y ejecutar código arbitrario sin autenticación en condiciones específicas.

Aprovecha el manejo inadecuado de los archivos de sesión cargados y los mecanismos de deserialización. Al cargar una carga útil manipulada en un directorio con permisos de escritura (p. ej., /uploads/../sessions/), un atacante puede activar la deserialización, lo que resulta en la ejecución de comandos arbitrarios en el servidor objetivo.

A. Productos afectados:

- Apache Tomcat 11.0.0-M1 a 11.0.2.
- Apache Tomcat 10.1.0-M1 a 10.1.34.
- Apache Tomcat 9.0.0.M1 a 9.0.98.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Actualizar a las versiones parcheadas de Apache Tomcat (9.0.99, 10.1.35 o 11.0.3).

Fuente de Información:	• hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/10/5 • hxxps[:]//github[.]com/absholi7ly/POC-CVE-2025-24813/blob/main/README.md • hxxps[:]//lists[.]apache[.]org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°079	Fecha: 02-04-2025 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en software de FreeType		
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:

Se ha publicado una vulnerabilidad de severidad **ALTA** de tipo Escritura fuera de límites, que afecta a las versiones 2.13.0 y anteriores de the FreeType Project. La explotación exitosa de esta vulnerabilidad podría permitir que un atacante remoto comprometa el sistema vulnerable.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-27363 de tipo Escritura fuera de límites, podría permitir que un atacante remoto comprometa el sistema vulnerable.

La vulnerabilidad implica una falla de escritura fuera de límites que puede ocurrir al analizar estructuras de subglifos de fuentes relacionadas con archivos de fuentes TrueType GX y variables. Esta falla puede provocar la ejecución de código arbitrario, lo que potencialmente permite a los atacantes ejecutar código malicioso de forma remota.

A. Productos afectados:

- FreeType 2.13.0 y anteriores.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Actualizar a FreeType versión 2.13.3 o posterior.

Fuente de Información:	• hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/13/1 • hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/13/11 • hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/13/12 • hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/13/2 • hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/13/3 • hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/13/8 • hxxps[:]//www[.]Facebook[.]com/security/advisories/cve-2025-27363

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°079	Fecha: 02-04-2025 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad que afecta a productos de Apple		
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:

Apple Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo control inadecuado de la generación de código (inyección de código), que afecta varios productos de Apple específicamente aquellos que utilizan el componente AudioToolbox. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-24243 de tipo control inadecuado de la generación de código (inyección de código), podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad existe debido a un error de límite en el audio. Un atacante remoto puede crear un archivo especialmente diseñado, engañar a la víctima para que lo abra, provocar corrupción de memoria y ejecutar código arbitrario en el sistema objetivo.

A. Productos afectados:

- VisionOS 2.4.
- MacOS Ventura 13.7.5.
- TvOS 18.4.
- IPadOS 17.7.6.
- IOS 18.4.
- IPadOS 18.4.
- MacOS Sonoma 14.7.5.

3. RECOMENDACIÓN:

- Actualizar sus dispositivos Apple a las últimas versiones de software que incluyan la corrección.

Fuente de Información:	• hxxps://support.apple.com/en-us/122373

Índice alfabético