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

223-2024-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°223	Fecha: 26-09-2024
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Estafas de CAPTCHA falsos que difunden malware de Lumma Stealer		
Tipo de Ataque	Stealers	Abreviatur	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:

Ya de por sí los hackers han mostrado mucha inventiva a la hora de pensar en alternativas para atacar. Pero se han superado sin duda alguna al convertir una herramienta que precisamente ha sido pensada para evitar el malware en otra herramienta que ayuda a estos a perpetrarlo, hablamos de los habituales códigos “captcha” que nos encontramos a diario en Internet.

La principal tarea de un malware es la de saltarse todos los controles de los antivirus, y por tanto poder evitar esos controles con todo tipo de artimañas que permitan que el malware se mezcle con la interfaz de los sistemas sin que los usuarios prácticamente se den cuenta.

Las pruebas CAPTCHA, piden realizar una tarea rápida para que los sitios web puedan verificar que realmente el usuario es una persona. Es una medida de seguridad utilizada para evitar que los rastreadores web automatizados, también conocidos como bots, comenten, envíen formularios o envíen spam a sitios web.

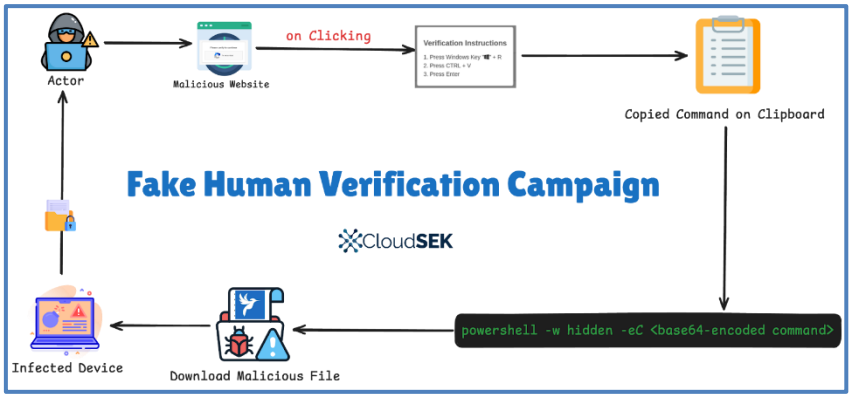
2. DETALLES:

Los ciberdelincuentes han estado distribuyendo agresivamente el malware Lumma Stealer a través de campañas de Captcha falsas, dirigidas a más de 1,4 millones de usuarios en el último mes, que está diseñado para robar datos confidenciales de los usuarios, lo que representa una grave amenaza para la seguridad en línea.

El último ataque estilo Captcha apunta a los usuarios de GitHub con un correo electrónico de phishing que afirma una vulnerabilidad de seguridad. Es decir, un usuario malintencionado de GitHub abre un nuevo "problema" en un repositorio de código abierto, afirmando falsamente que el proyecto contiene una "vulnerabilidad de seguridad" e incita a otros a visitar un dominio "GitHub Scanner" falso. Sin embargo, el dominio en cuestión no está asociado con GitHub y engaña a los usuarios para que instalen malware de Windows.

Los ataques de phishing están diseñados para engañar a los usuarios para que visiten una pantalla Captcha falsa, que luego les solicita que hagan clic en un botón que copia secretamente un script malicioso en el portapapeles del usuario al mismo tiempo.

Al seguir las instrucciones subsiguientes, que frecuentemente están disfrazadas como un paso de verificación, se dirige al usuario a ejecutar el script, lo que en última instancia resulta en una infección del sistema.



El script malicioso de PowerShell se conecta a un servidor C&C remoto para obtener malware adicional. Está diseñado para descargar y ejecutar el malware Lumma Stealer o un archivo intermediario que lo instalará más tarde, comprometiendo el sistema de la víctima.

El botón “No soy un robot” activa un script de JavaScript que copia un comando de PowerShell en el portapapeles del usuario. Una vez pegado y ejecutado, este comando descarga y ejecuta otro script de PowerShell desde hxxps://github-scanner[.]com/download.txt.

El script se conecta a un servidor remoto de comando y control, recupera un ejecutable malicioso llamado l6E.exe, lo guarda como SysSetup.exe en un directorio temporal y luego ejecuta el archivo descargado, lo que potencialmente puede provocar un mayor compromiso del sistema.

Se revela una propagación global de campañas de Captcha falsas, con Italia, Argentina, Francia, España y Brasil experimentando la mayor concentración de ataques. Más de 1,4 millones de usuarios únicos fueron protegidos en las últimas cuatro semanas, lo que subraya la naturaleza generalizada de estas amenazas.

Los IoC proporcionados indican un posible ciberataque que involucra un servidor C&C alojado en github-scanner.com, un script de PowerShell para actividad maliciosa y el malware Lumma Stealer, lo que sugiere un esfuerzo coordinado para comprometer sistemas y robar datos confidenciales.

C&C:

- https://github-scanner[.]com

PowerShell script:

- 10d4e15b63a07368299f2245661d7a4626cd1a91a9950a3cbed5b4276d2dc31f

Lumma Stealer:

- d737637ee5f121d11a6f3295bf0d51b06218812b5ec04fe9ea484921e905a207

URL falsas maliciosas

- hxxps[://]heroic-genie-2b372e[.]netlify[.]app/please-verify-z[.]html
- hxxps[://]fipydslaongos[.]b-cdn[.]net/please-verify-z[.]html
- hxxps[://]sdkjhfdskjnck[.]s3[.]amazonaws[.]com/human-verify-system[.]html
- hxxps[://]verifyhuman476[.]b-cdn[.]net/human-verify-system[.]html
- hxxps[://]pub-9c4ec7f3f95c448b85e464d2b533aac1[.]r2[.]dev/human-verify-system[.]html
- hxxps[://]verifyhuman476[.]b-cdn[.]net/human-verify-system[.]html
- hxxps[://]newvideozones[.]click/veri[.]html
- hxxps[://]ch3[.]dlvideosfre[.]click/human-verify-system[.]html
- hxxps[://]newvideozones[.]click/veri[.]html
- hxxps[://]ofsetvideofre[.]click

3. RECOMENDACIONES:

- Realizar el bloqueo de los indicadores de compromiso listados.
- Ser escéptico con los correos electrónicos no solicitados. Verificar siempre la autenticidad de los correos electrónicos inesperados, especialmente aquellos que le solicitan que tome medidas inmediatas en sus repositorios.
- No ejecutar scripts desconocidos ni comandos de fuentes no confiables. Verificar el contenido y el origen del script antes de ejecutarlo.
- Habilitar la autenticación de dos factores (2FA) siempre que sea posible.
- Utilizar una solución antivirus oficial y confiable, instalada y actualizada regularmente en sus dispositivos. Estas soluciones brindan protección esencial contra malware como Lumma Stealer, detectando y bloqueando scripts y cargas útiles maliciosas antes de que puedan causar algún daño. Incluso si interactúa accidentalmente con un intento de phishing, contar con una solución de seguridad confiable puede actuar como una red de seguridad crucial.

Fuente de Información:	• hxxps://cyberpress.org/fake-captcha-scams-spreading-lumma-stealer-malware/ • hxxps://www.gendigital.com/blog/news/innovation/global-surge-in-fake-captcha-attacks • https://www.cloudsek.com/blog/unmasking-the-danger-lumma-stealer-malware-exploits-fake-captcha-pages

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°223	Fecha: 26-09-2024 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en productos Cisco		
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:

Cisco ha publicado múltiples vulnerabilidades de severidad **ALTA** de tipo falsificación de solicitud entre sitios (CSRF), gestión inadecuada del estado del sistema, desbordamiento de búfer basado en pila, desreferencia de puntero NULL, validación de entrada incorrecta y error en la lógica de precedencia del operador que afectan a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado realizar un ataque CSRF, ejecutar comandos en la CLI y generar una condición de denegación de servicio (DoS) en un dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20437 de tipo falsificación de solicitud entre sitios (CSRF), en la interfaz de administración basada en web del software Cisco IOS XE, podría permitir que un atacante remoto no autenticado realice un ataque de falsificación de solicitud entre sitios (CSRF) y ejecute comandos en la CLI de un dispositivo afectado. Esta vulnerabilidad se debe a que no hay suficientes protecciones CSRF para la interfaz de administración basada en web de un dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario ya autenticado para que siga un enlace creado. Si lo logra, podría permitir al atacante realizar acciones arbitrarias en el dispositivo afectado con los privilegios del usuario objetivo.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20455 de tipo gestión inadecuada del estado del sistema en el proceso que clasifica el tráfico que se dirige al componente Unified Threat Defense (UTD) del software Cisco IOS XE en modo controlador, podría permitir que un atacante remoto no autenticado generar una condición de DoS en un dispositivo afectado. Esta vulnerabilidad existe porque UTD maneja incorrectamente ciertos paquetes cuando estos salen de un túnel IPsec SD-WAN. Un atacante podría aprovechar esta vulnerabilidad enviando tráfico diseñado a través de un túnel IPsec SD-WAN que esté configurado en un dispositivo afectado. Una explotación exitosa podría permitir al atacante hacer que el dispositivo se recargue, lo que resultaría en una condición de DoS.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20433 de tipo desbordamiento de búfer basado en pila en la función de Protocolo de reserva de recursos (RSVP) del software Cisco IOS y del software Cisco IOS XE, podría permitir que un atacante remoto no autenticado haga que un dispositivo afectado se recargue inesperadamente, lo que genera una condición de DoS. Esta vulnerabilidad se debe a un desbordamiento de búfer al procesar paquetes RSVP creados. Un atacante podría aprovechar esta vulnerabilidad enviando tráfico RSVP a un dispositivo afectado. Si lo logra, podría hacer que el atacante recargue el dispositivo afectado, lo que provocaría una condición de DoS.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20464 de tipo validación de entrada incorrecta en la función de multidifusión independiente del protocolo (PIM) del software Cisco IOS XE, podría permitir que un atacante remoto no autenticado provoque una condición de DoS en un dispositivo afectado. Esta vulnerabilidad se debe a una validación insuficiente de los paquetes PIMv2 IPv4 recibidos. Un atacante podría aprovechar esta vulnerabilidad enviando un paquete PIMv2 diseñado a una interfaz habilitada para PIM en un dispositivo afectado. Una explotación exitosa podría permitir al atacante hacer que un dispositivo afectado se reinicie, lo que resultaría en una condición de DoS. Esta vulnerabilidad puede explotarse con un paquete de unidifusión o multidifusión IPv4.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20480 de tipo error en la lógica de precedencia del operador en la función DHCP Snooping del software Cisco IOS XE en los nodos de borde de la estructura de acceso definido por software (SD-Access), podría permitir que un atacante remoto no autenticado provoque un alto uso de la CPU en un dispositivo afectado, lo que resulta en una condición de DoS que requiere una recarga manual para recuperarse. Esta vulnerabilidad se debe a un manejo inadecuado de los paquetes DHCP de IPv4. Un atacante podría aprovechar esta vulnerabilidad enviando determinados paquetes DHCP de IPv4 a un dispositivo afectado. Si lo logra, el atacante podría hacer que el dispositivo agote los recursos de la CPU y deje de procesar el tráfico, lo que provocaría una situación de DoS que requeriría una recarga manual para recuperarse.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20436 de tipo desreferencia de puntero NULL en la función de servidor HTTP del software Cisco IOS XE cuando la función de servicio de telefonía está habilitada podría permitir que un atacante remoto no autenticado provoque una condición de DoS en un dispositivo afectado. Esta vulnerabilidad se debe a una desreferencia de puntero nulo al acceder a URL específicas. Un atacante podría aprovechar esta vulnerabilidad enviando tráfico HTTP diseñado a un dispositivo afectado. Una explotación exitosa podría permitir al atacante hacer que el dispositivo afectado se recargue, lo que provocaría una condición de DoS en el dispositivo afectado.

A. Productos afectados:

- La vulnerabilidad CVE-2024-20437 afecta a los productos Cisco si ejecutan una versión vulnerable del software Cisco IOS XE y tienen habilitada la función de servidor HTTP y el comando de configuración interna del servicio.
- La vulnerabilidad CVE-2024-20455 afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco IOS XE en modo controlador, tienen UTD instalado y habilitado y tienen túneles SD-WAN configurados para usar Ipsec.
  - Enrutadores de servicios integrados (ISR) de la serie 1000.
  - Software de borde Catalyst 8000v.
  - Plataformas perimetrales de la serie Catalyst 8200.
  - Plataformas perimetrales de la serie Catalyst 8300.
  - Plataformas Catalyst 8500L Edge.
  - Enrutadores de la serie resistente Catalyst IR8300.
- La vulnerabilidad CVE-2024-20433 afecta al software Cisco IOS e IOS XE si la función RSVP está habilitada.
- La vulnerabilidad CVE-2024-20464 afecta a los dispositivos Cisco si ejecutan el software Cisco IOS XE versión 17.13.1 o 17.13.1a y tienen PIM configurado.
- La vulnerabilidad CVE-2024-20480 afecta al software Cisco IOS XE si se ejecuta en un dispositivo que está configurado como nodo de borde de estructura SD-Access y que tiene habilitada la función DHCP Snooping.
- La vulnerabilidad CVE-2024-20436 afecta a los productos Cisco si ejecutan una versión vulnerable del software Cisco IOS XE y tienen habilitadas las funciones de servidor HTTP y de servicio de telefonía.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-csrf-ycUYxkKO • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-utd-dos-hDATqxs • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rsvp-dos-OypvgVZf • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pim-APbVfySJ • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sda-edge-dos-MBcbG9k • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-httpsrvr-dos-yOZThut

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°223	Fecha: 26-09-2024 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en ADAM-5550 de Advantech		
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:

Aarón Flecha Menéndez y Luis Villalba Pérez de S21sec han reportado dos vulnerabilidades de severidad **ALTA** de tipo codificación débil de contraseñas y secuencias de comandos entre sitios que afecta al controlador industrial ADAM-5550 de Advantech. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado interceptar las credenciales fácilmente decodificables de un usuario legítimo para obtener acceso completo al dispositivo y cargar código malicioso en la página web del dispositivo.

2. DETALLES:

El ADAM-5550 es un controlador industrial versátil diseñado para aplicaciones de automatización de máquinas y sistemas SCADA, aunque ya se está descontinuando.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-37187 de tipo codificación débil de contraseñas, se debe a que las credenciales de usuario se comparten con un nivel bajo de cifrado, que consiste en codificación base 64.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-38308 de tipo secuencias de comandos entre sitios, se debe a que la aplicación web de Advantech ADAM 5550 incluye una página de "registros" en la que se muestran al usuario todas las solicitudes HTTP recibidas. El dispositivo no neutraliza correctamente el código malicioso al analizar las solicitudes HTTP para generar la salida de la página.

A. Productos afectados:

- Advantech ADAM 5550: Todas las versiones.

3. RECOMENDACIÓN:

- Actualizar el firmware del ADAM-5630 a la versión 2.5.2 o superior, considerando que el ADAM-5550 se está descontinuando.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-270-01

Índice alfabético