



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

039-2026-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 Aérea del 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 las empresas 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

CrySome RAT: el malware .NET sigiloso agrega funciones AV Killer y HVNC 4


Vulnerabilidad de ejecución remota de código en el software Cisco Secure Firewall Management Center. 6

Vulnerabilidad crítica de omisión de autenticación en Cisco Secure Firewall Management Center permite la ejecución remota de código como root..... 7

Múltiples vulnerabilidades críticas de ejecución remota de código en routers TP-Link Archer NX. 8

Nueva campaña “Ghost” compromete la cadena de suministro de npm mediante paquetes maliciosos para robo de credenciales y criptomonedas. 9

Índice alfabético 11

 Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 039		Fecha: 25-03-2026
			Página: 4 de 11
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	CrySome RAT: el malware .NET sigiloso agrega funciones AV Killer y HVNC		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

CrySome RAT es una amenaza recientemente identificada que evidencia la evolución de los troyanos de acceso remoto hacia herramientas de pos-explotación altamente persistentes y difíciles de erradicar. De acuerdo con análisis técnicos, este malware está desarrollado en C# sobre la plataforma .NET y surge en un contexto donde los atacantes priorizan el control prolongado de los sistemas comprometidos, incluso tras intentos de limpieza, reinstalación o restablecimiento del sistema operativo. Su diseño refleja un enfoque orientado a operaciones encubiertas de largo plazo, asociadas comúnmente a campañas de espionaje, fraude o control remoto permanente de equipos Windows.



Ilustración 1: CrySome RAT es un troyano de acceso remoto

2. DETALLES:

CrySome RAT se distribuye como un ejecutable empaquetado que establece comunicación persistente con un servidor de Comando y Control (C2) mediante TCP. Una vez activo, el malware recopila información del sistema y habilita módulos según órdenes del atacante. Entre sus capacidades destacan la ejecución remota de comandos, manipulación de archivos, keylogging, captura de pantalla, robo de credenciales de navegadores y control remoto mediante HVNC (Hidden Virtual Network Computing), que permite operar de forma invisible para el usuario.


Un rasgo crítico es su arquitectura de autoprotección, que incluye un módulo "AV Killer" capaz de deshabilitar soluciones de seguridad, bloquear actualizaciones y dificultar la reinstalación de defensas. Además, implementa múltiples mecanismos de persistencia: tareas programadas, servicios de Windows, procesos vigilantes y abuso de la partición de recuperación, permitiéndole sobrevivir incluso a restablecimientos de fábrica. Esto convierte a CrySome RAT en una amenaza de alta complejidad y riesgo operativo.


- **RECOMENDACIONES:**


- Implementar EDR/XDR con capacidades de detección de comportamiento y protección contra manipulación de servicios de seguridad.
- Restringir la ejecución de binarios no firmados mediante Application Control (WDAC o AppLocker).
- Supervisar conexiones salientes inusuales y aplicar filtrado de tráfico y detección de C2 a nivel de red.
- Mantener sistemas operativos y software totalmente actualizados, priorizando parches de Windows y .NET.
- Limitar privilegios de usuario y aplicar el principio de mínimo privilegio en estaciones de trabajo.
- Realizar copias de seguridad offline y protegidas, verificando periódicamente su integridad.
- Monitorear la creación de tareas programadas, servicios nuevos y cambios en el registro de inicio.
- Capacitar a los usuarios en concienciación de amenazas y detección temprana de comportamientos anómalos.
- Incluir análisis forense profundo y, de ser necesario, reinstalación segura del sistema ante infecciones confirmadas.


Fuente de Información:

- <https://gbhackers.com/crysome-rat/>

	ALERTA DE SEGURIDAD DIGITAL N°170		Fecha: 25-03-2026
			Página: 6 de 11
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en el software Cisco Secure Firewall Management Center.		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		
Descripción			
<p>1. ANTECEDENTES:</p> <p>Cisco Systems, Inc. ha publicado una vulnerabilidad de severidad CRÍTICA clasificada como CWE-502: Deserialización de datos no confiables en la interfaz de administración web del software Cisco Secure Firewall Management Center (FMC). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código Java arbitrario como usuario root en un dispositivo afectado.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad crítica identificada por MITRE como CVE-2026-20131 en la interfaz de administración web del software Cisco Secure FMC, podría permitir que un atacante remoto no autenticado ejecute código Java arbitrario como usuario root en un dispositivo afectado.</p> <p>Esta vulnerabilidad se debe a la deserialización insegura de un flujo de bytes Java proporcionado por el usuario. Un atacante podría explotarla enviando un objeto Java serializado manipulado a la interfaz de administración web del dispositivo afectado. Una explotación exitosa permitiría al atacante ejecutar código arbitrario en el dispositivo y obtener privilegios de administrador.</p> <p>Cabe indicar que, si la interfaz de administración de FMC no tiene acceso público a Internet, la superficie de ataque asociada a esta vulnerabilidad se reduce.</p> <p>Cisco SCC Firewall Management es un servicio SaaS que Cisco actualiza como parte del mantenimiento. La solución para esta vulnerabilidad se ha implementado en los entornos de Cisco SCC Firewall Management. No se requiere ninguna acción por parte del usuario.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – Esta vulnerabilidad afecta al software Cisco Secure FMC y a la gestión de firewalls Cisco Security Cloud Control (SCC), independientemente de la configuración del dispositivo. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Cisco ha publicado actualizaciones de software que solucionan esta vulnerabilidad. No existen soluciones alternativas para corregirla. 			
Fuente de Información:	<ul style="list-style-type: none"> • https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2026-069-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2026-069-03.pdf 		

	ALERTA DE SEGURIDAD DIGITAL N°171		Fecha: 25-03-2026
			Página: 7 de 11
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica de omisión de autenticación en Cisco Secure Firewall Management Center permite la ejecución remota de código como root.		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C03
Clasificación temática familia	Intento de intrusión		
Descripción			
<p>1. ANTECEDENTES:</p> <p>Cisco Systems, Inc. ha reportado una vulnerabilidad de severidad CRÍTICA clasificada como CWE-288: omisión de autenticación mediante canal alternativo que afecta a Cisco Secure Firewall Management Center (FMC), la cual permite a un atacante remoto no autenticado evadir los mecanismos de autenticación y ejecutar scripts con privilegios de root, comprometiendo completamente el sistema subyacente. El riesgo es elevado debido a que impacta directamente el plano de gestión de los firewalls, lo que podría derivar en control total de la infraestructura de seguridad y propagación lateral dentro de la red.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad crítica identificada por MITRE como CVE-2026-20079 reside en la interfaz web de FMC y se origina por la creación incorrecta de un proceso del sistema durante el arranque (boot). Este defecto permite que ciertas rutas o flujos de ejecución queden expuestos antes de que se apliquen los controles de autenticación adecuados, generando un bypass lógico. Como resultado, un atacante puede interactuar con el sistema sin credenciales válidas, aprovechando un comportamiento anómalo en la inicialización del servicio.</p> <p>El vector de explotación consiste en el envío de peticiones HTTP especialmente diseñadas (crafted HTTP requests) hacia la interfaz de administración del FMC. Si el sistema se encuentra vulnerable, estas solicitudes permiten ejecutar scripts o comandos arbitrarios en el dispositivo, alcanzando privilegios de superusuario. Este escenario implica no solo ejecución remota de código, sino también acceso persistente, manipulación de políticas de seguridad y potencial pivoting hacia otros activos gestionados por el FMC.</p> <p>Hasta el momento de su divulgación, no existen evidencias públicas de explotación activa ni se han reportado pruebas de concepto (PoC) funcionales ampliamente disponibles; sin embargo, múltiples fuentes advierten que, debido a su criticidad y facilidad de explotación (sin autenticación y vía red), es altamente probable que actores de amenaza desarrollen exploits en el corto plazo mediante ingeniería inversa de los parches publicados.</p> <p>B. Productos afectados:</p> <ul style="list-style-type: none"> – Cisco Secure Firewall Management Center (FMC) – múltiples versiones (principalmente ramas 6.x, 7.x y algunas 10.x previas a parches). – No afectados: Cloud-Delivered FMC (cdFMC), Cisco ASA, Cisco FTD, Security Cloud Control (SCC). <p>C. Indicadores de Compromiso (IoC):</p> <ul style="list-style-type: none"> – Cisco no ha publicado IoCs específicos (hashes, IPs, dominios). <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Aplicar parches de seguridad inmediatamente (no existen workarounds). • Restringir el acceso a la interfaz FMC: Segmentación de red (zona administrativa), Acceso solo vía VPN controlada. • Implementación de jump servers. • Monitorear logs de: Acceso web, Eventos administrativos, Tráfico entrante al plano de gestión. • Realizar evaluación de compromiso si el sistema estuvo expuesto. • Validar versiones con herramientas oficiales (Cisco Software Checker). • Implementar controles compensatorios (WAF, ACLs, IDS/IPS). 			
Fuente de Información:	<ul style="list-style-type: none"> • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5Jp45V2 		

	ALERTA DE SEGURIDAD DIGITAL N°172		Fecha: 25-03-2026
			Página: 8 de 11
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades críticas de ejecución remota de código en routers TP-Link Archer NX.		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C03
Clasificación temática familia	Intento de intrusión		
Descripción			
<p>1. ANTECEDENTES:</p> <p>Microsoft Corporation ha reportado una vulnerabilidad de severidad Alta clasificada como CWE-502: Deserialización de datos no confiables que afecta a Microsoft Office SharePoint Server. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante autenticado ejecutar código arbitrario de forma remota a través de la red. El riesgo es significativo debido a que SharePoint suele operar en entornos corporativos críticos; su explotación podría comprometer datos sensibles, permitir movimientos laterales y facilitar el control del servidor afectado.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad alta identificada por MITRE como CVE-2026-20963 se origina en el manejo inseguro de datos durante procesos de deserialización, donde el sistema reconstruye objetos a partir de datos externos sin validar adecuadamente su integridad o procedencia. Este comportamiento permite que un atacante inyecte objetos maliciosos que, al ser procesados por el sistema, desencadenen la ejecución de código arbitrario. Microsoft indicó que este patrón es típico en aplicaciones empresariales que manejan grandes volúmenes de datos estructurados.</p> <p>Desde el punto de vista técnico, el vector de ataque es remoto (network-based) con baja complejidad y requiere privilegios mínimos, sin necesidad de interacción del usuario. Esto implica que un atacante con acceso autenticado básico puede explotar la vulnerabilidad mediante solicitudes manipuladas hacia los componentes vulnerables de SharePoint. El impacto es alto en los tres pilares de seguridad (confidencialidad, integridad y disponibilidad), lo que convierte esta falla en un punto crítico de compromiso dentro de redes corporativas.</p> <p>Por el momento, no existen evidencias públicas confirmadas de explotación activa ni inclusión en el catálogo KEV de CISA, y tampoco se ha divulgado un exploit público (PoC) ampliamente disponible. Sin embargo, debido a la naturaleza de la vulnerabilidad (deserialización insegura) y su facilidad relativa de explotación, existe una alta probabilidad de desarrollo de exploits en el corto plazo, especialmente en entornos donde SharePoint esté expuesto a múltiples usuarios autenticados.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – Microsoft SharePoint Server 2016 (Enterprise). – Microsoft SharePoint Server 2019. – Microsoft SharePoint Server Subscription Edition (versiones < 16.0.19127.20442). <p>B. Indicadores de Compromiso (IoC):</p> <ul style="list-style-type: none"> – No se han publicado IoCs específicos oficiales. – Indicadores indirectos: <ul style="list-style-type: none"> ▪ Ejecución de procesos anómalos en el servidor SharePoint. ▪ Actividad sospechosa en logs de aplicaciones web (IIS). ▪ Creación o modificación no autorizada de archivos/objetos. ▪ Tráfico inusual desde cuentas autenticadas de bajo privilegio. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Aplicar parches de seguridad oficiales de Microsoft (MSRC) de forma inmediata. • Restringir el acceso a SharePoint (segmentación de red / VPN). • Implementar monitoreo y logging avanzado (SIEM). • Auditar cuentas con bajos privilegios con acceso al sistema. • Validar integridad de aplicaciones y objetos serializados. <p>Aplicar principios de mínimo privilegio y control de acceso estricto.</p>			
Fuente de Información:	<ul style="list-style-type: none"> • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20963 		

	ALERTA DE SEGURIDAD DIGITAL N°173		Fecha: 25-03-2026
			Página: 9 de 11
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Nueva campaña “Ghost” compromete la cadena de suministro de npm mediante paquetes maliciosos para robo de credenciales y criptomonedas.		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C03
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Investigadores de Huntress han reportado una campaña activa mediante “*device code phishing*” dirigida a más de 340 organizaciones que utilizan Microsoft 365 en países como EE.UU., Canadá, Australia, Nueva Zelanda y Alemania. El ataque, detectado inicialmente el 19 de febrero de 2026, consiste en el envío de correos de phishing que inducen a las víctimas a autenticarse en una página legítima de Microsoft (device login) introduciendo un código proporcionado por el atacante. Esta técnica permite a los adversarios abusar del flujo OAuth para generar tokens de acceso persistentes, incluso tras cambios de contraseña. La campaña utiliza infraestructura de redirección (Cloudflare Workers, sitios comprometidos y servicios PaaS como Railway) para evadir controles de seguridad y facilitar el robo de sesiones. El impacto incluye toma de cuentas, acceso persistente a servicios cloud y posible exfiltración de datos.

La campaña de “*device code phishing*” contra entornos de Microsoft 365 representa un riesgo alto a crítico para entidades públicas peruanas debido a su fuerte dependencia de servicios cloud como correo institucional, gestión documental y autenticación centralizada (Microsoft Entra ID). Este tipo de ataque permite el compromiso de cuentas legítimas con MFA habilitado, lo que rompe uno de los principales controles de seguridad adoptados por el Estado peruano.

2. DETALLES:

La técnica de “*device code phishing*” es una variante avanzada de phishing que abusa del flujo legítimo de autenticación OAuth denominado Device Authorization Grant (o device code flow), diseñado para dispositivos con capacidades limitadas de entrada (como Smart TVs o IoT).

Esta campaña emplea la técnica de “*device code phishing*”, que explota el flujo de autorización OAuth diseñado para dispositivos con entrada limitada. A diferencia del phishing tradicional, no requiere páginas falsas, sino que utiliza portales legítimos de autenticación de Microsoft, lo que incrementa la tasa de éxito y reduce la detección.

El vector inicial es un correo de phishing que incorpora enlaces maliciosos disfrazados mediante servicios legítimos (Cisco, Trend Micro, Mimecast), generando una cadena de redirecciones (multi-hop) que culmina en una página controlada por el atacante.

Estas páginas generan dinámicamente códigos de autenticación (*device code*) y persuaden a la víctima para ingresarlos en el portal oficial de Microsoft. Este enfoque elimina la necesidad de que el atacante envíe manualmente el código, automatizando el proceso y aumentando la escalabilidad del ataque.

Una vez que la víctima introduce el código junto con sus credenciales y MFA, Microsoft genera tokens OAuth (access y refresh tokens). Estos tokens son accesibles por el atacante, quien ya conoce el “*device code*” asociado, permitiendo la toma de control de la sesión sin necesidad de credenciales adicionales.

Cabe indicar que el impacto se extiende a todo el ecosistema federado de autenticación, afectando no solo Microsoft 365 sino también aplicaciones de terceros integradas con Entra ID.

Un aspecto crítico es la persistencia: los tokens OAuth permanecen válidos incluso tras el cambio de contraseña, lo que permite mantener acceso prolongado (persistencia post-compromiso). Esto representa una evolución significativa frente al phishing convencional.

La infraestructura del ataque incluye el uso de Cloudflare Workers, Vercel y sitios comprometidos como intermediarios, junto con backend en Railway, dificultando el bloqueo por reputación y permitiendo evasión de filtros de seguridad empresarial.

La campaña presenta múltiples técnicas de ingeniería social: suplantación de DocuSign, notificaciones de voz, formularios de Microsoft y señuelos relacionados a licitaciones o documentos, lo que amplía la superficie de ataque y mejora la efectividad del engaño.

Finalmente, el “*device code phishing*” no es un vector tradicional sino un abuso de autenticación legítima, lo que lo convierte en una amenaza especialmente peligrosa para el sector público peruano. Su impacto potencial incluye compromiso total de identidad digital, persistencia avanzada y acceso a infraestructura crítica del Estado, con baja probabilidad de detección si no se aplican controles específicos sobre OAuth y monitoreo de sesiones.

A. Productos afectados:

- Microsoft 365 (Office 365) – Servicios de correo (Exchange Online), colaboración (SharePoint, OneDrive, Teams).
- Microsoft Entra ID (Azure Active Directory) – Gestión de identidades y autenticación basada en OAuth.
- Aplicaciones integradas con OAuth – Cualquier aplicación que utilice el flujo de autorización “*device code*”.
- Servicios cloud asociados – Plataformas SaaS conectadas mediante Single Sign-On (SSO) con Microsoft.

B. Datos clave del incidente:

- Tipo de ataque: Phishing avanzado (*device code* Phishing / OAuth Abuse).
- Nivel de criticidad: Alto / Crítica.
- Organización afectada: Usuarios de Microsoft 365 (más de 340 organizaciones).
- Productos afectados: Microsoft 365, Microsoft Entra ID (Azure AD).
- Actor de amenaza: Grupos múltiples (Storm-2372, APT29, UTA0304, UTA0307).
- Impacto: Compromiso de cuentas, persistencia mediante tokens, acceso a datos corporativos.
- Fecha del incidente: Desde 19 de febrero de 2026 (actividad activa en marzo 2026).

C. Indicadores de Compromiso (IoC):

Direcciones IP (Railway):

- 162.220.234[.]41
- 162.220.234[.]66
- 162.220.232[.]57
- 162.220.232[.]99
- 162.220.232[.]235

TTPs (MITRE ATT&CK):

- T1566.002 – Phishing (Spearphishing Link)
- T1078.004 – Valid Accounts (Cloud Accounts)

Infraestructura:

- Cloudflare Workers (workers[.]dev)
- Railway (PaaS)
- Redirecciones vía servicios de seguridad (Cisco, Mimecast, Trend Micro).

3. RECOMENDACIONES:

- Revocar inmediatamente refresh tokens en cuentas comprometidas.
- Monitorear logs de autenticación (Azure AD / Entra ID) en busca de IPs sospechosas (Railway).
- Implementar Conditional Access Policies (bloqueo por geolocalización/IP).
- Restringir o auditar el uso del flujo “*device code*”.
- Capacitación contra phishing avanzado (OAuth abuse).
- Habilitar detección de anomalías en tokens y sesiones.
- Bloquear dominios/infraestructura asociada (Cloudflare Workers sospechosos).

Fuente de Información:

- <https://www.huntress.com/blog/railway-paas-m365-token-replay-campaign>
- <https://thehackernews.com/2026/03/device-code-phishing-hits-340-microsoft.html>
- <https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/>
- <https://www.proofpoint.com/us/blog/threat-insight/access-granted-phishing-device-code-authorization-account-takeover>

Índice alfabético

Malware 4,9

Explotación de vulnerabilidades conocidas 6,7,8