



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

001-2026-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

El ransomware Interlock explota el día cero en el controlador antitrampas de juegos para desactivar EDR y AV. 4

Vulnerabilidad en productos BeyondTrust. 6

Vulnerabilidad de Inyección de código en Endpoint Manager Mobile de Ivanti. 7

Índice alfabético 8

 Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°001		Fecha: 02-02-2026
			Página: 4 de 8
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El ransomware Interlock explota el día cero en el controlador antitrampas de juegos para desactivar EDR y AV.		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Interlock es un grupo de ransomware no RaaS (sin afiliados) activo desde 2024, con foco oportunista en Norteamérica y Europa —especialmente en el sector educativo— y con tácticas de doble extorsión (robo y cifrado de datos). Su cadena de ataque suele iniciar mediante descargas drive-by desde sitios legítimos comprometidos o la técnica ClickFix (engañar al usuario para ejecutar PowerShell), usando loaders como MintLoader y backdoors en JavaScript (NodeSnakeRAT/Interlock RAT) para persistencia y control remoto; se apoya en RDP, ScreenConnect/AnyDesk y exfiltra con AzCopy antes de cifrar. Organismos como CISA/FBI y proveedores como Fortinet y Cisco Talos han documentado su evolución, incluidos encryptors para Windows/Linux/entornos virtualizados y un DLS (“Worldwide Secrets Blog”) para presión pública.



Ilustración 1: El ransomware Interlock explota el día cero en el controlador antitrampas de juegos para desactivar EDR y AV.

2. DETALLES:

Investigaciones recientes muestran que Interlock incorporó una herramienta de “kill-switch” de procesos, apodada Hotta Killer, que carga un driver anti-cheat legítimo renombrado (UpdateCheckerX64.sys) vulnerable (GameDriverx64.sys, CVE-2025-61155) para terminar procesos de EDR/AV a nivel kernel (IOCTL 0x222040 y bandera 0xFA123456, con llamadas a ZwTerminateProcess).

El vector inicial observado enlaza a MintLoader y la ejecución de un runtime Node.js que activa implants JavaScript (NodeSnakeRAT/Interlock RAT), con capacidades de persistencia, discovery, SOCKS5 y ejecución de comandos; luego, despliegan ScreenConnect y reglas de firewall para moverse lateralmente.

En campañas de 2025–2026 contra educación, mantuvieron dwell time prolongado, exfiltraron >250 GB con AzCopy y, tras cegar defensas, cifraron endpoints Windows y hipervisores (p. ej., Nutanix) con binarios dedicados; el grupo opera sin nota con monto inicial, forzando negociación vía onion.


A nivel de TTPs, además de drive-by/ClickFix, emplean LOLBins, RDP, creación masiva de cuentas y stealers (Lumma/Berserk) según distintos informes.


3. RECOMENDACIONES:

- Implementar programas continuos de sensibilización en ciberseguridad para reconocer intentos de engaño comunes como falsos avisos de actualización, mensajes urgentes o captchas manipulados, que siguen siendo uno de los principales vectores de acceso inicial.
- Asegurar la actualización periódica de sistemas operativos, aplicaciones y firmware reduce significativamente la superficie de ataque y minimiza la explotación de vulnerabilidades conocidas. Limitar los privilegios de los usuarios únicamente a lo necesario para sus funciones diarias reduce el impacto de una posible intrusión y dificulta el movimiento del atacante dentro de la red.
- Disponer de respaldos periódicos, protegidos y desconectados del entorno principal, garantiza la recuperación de la información ante incidentes de cifrado sin depender de pagos a actores maliciosos.
- Utilizar mecanismos de autenticación robusta, como contraseñas seguras y autenticación multifactor, para disminuir el riesgo de accesos no autorizados mediante credenciales comprometidas.
- Establecer controles básicos de monitoreo y revisión de eventos ayuda a detectar comportamientos anómalos tempranamente, reduciendo el tiempo de permanencia del atacante. Evitar la instalación de software remoto o utilidades externas sin validación previa disminuye el riesgo de que estos sean utilizados como puerta trasera por actores maliciosos.
- Contar con procedimientos claros para la gestión de incidentes de ciberseguridad permite responder de manera ordenada, reducir el impacto operativo y facilitar la recuperación del servicio. La seguridad digital no depende solo del área técnica; debe integrarse como una responsabilidad transversal en todos los niveles de la organización.

Fuente de Información:

- <https://gbhackers.com/interlock-ransomware/>

	ALERTA DE SEGURIDAD DIGITAL N°054		Fecha: 02-02-2026
			Página: 6 de 8
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en productos BeyondTrust.		
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>BeyondTrust Inc. ha publicado una vulnerabilidad de severidad MEDIA clasificada como CWE-693: Falla del mecanismo de protección que afecta al software BeyondTrust Privilege Management para Windows. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario local autenticado que ya posea privilegios elevados y evadir las protecciones del producto.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad media identificada por MITRE como CVE-2026-1232 de tipo Falla del mecanismo de protección que afecta al software BeyondTrust Privilege Management para Windows, podría permitir a un usuario local autenticado que ya posea privilegios elevados y evadir las protecciones del producto. Esto le permitiría modificar la configuración del software o acceder a componentes protegidos de la aplicación.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – BeyondTrust Privilege Management para Windows en versiones anteriores o iguales a la 25.7. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad. • verificar la versión instalada a través de la consola de administración de BeyondTrust y aplicar los parches o actualizaciones recomendados por el fabricante para mitigar el riesgo de manipulación local 			
Fuente de Información:		<ul style="list-style-type: none"> • https://www.beyondtrust.com/trust-center/security-advisories/bt26-01 • https://beyondtrustcorp.service-now.com/csm?id=kb_article_view&sysparm_article=KB0023100 	

	ALERTA DE SEGURIDAD DIGITAL N°055		Fecha: 02-02-2026
			Página: 7 de 8
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de Inyección de código en Endpoint Manager Mobile de Ivanti.		
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>Ivanti ha publicado una vulnerabilidad de severidad CRÍTICA clasificada como CWE-94: Control inadecuado de la generación de código (Inyección de código) en Endpoint Manager Mobile (anteriormente MobileIron Core). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad crítica identificada por MITRE como CVE-2026-1340 de tipo control inadecuado de la generación de código (Inyección de código) en Endpoint Manager Mobile, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el servidor EPMM sin credenciales, obtener control del sistema o manipular datos críticos del entorno administrado y facilitar movimientos laterales dentro de la red afectada.</p> <p>La vulnerabilidad existe debido a una validación de entrada incorrecta. Un atacante remoto no autenticado puede enviar una solicitud especialmente diseñada a la aplicación y ejecutar código arbitrario en el sistema objetivo. Tenga en cuenta que la vulnerabilidad se está explotando activamente.</p> <p>Esta vulnerabilidad puede explotarse a través de la red, sin privilegios ni interacción del usuario, con impacto total en confidencialidad, integridad y disponibilidad.</p> <p>Varios informes de seguridad señalan que esta vulnerabilidad, junto con CVE-2026-1281, ha sido explotada en ataques reales ("zero-day") antes de que muchos sistemas estuvieran parchados.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – Endpoint Manager Mobile, versiones 12.5.x, 12.6.x y 12.7.x (y anteriores) del producto, usado para la gestión de dispositivos móviles corporativos. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • La vulnerabilidad se soluciona en el parche RPM 12.x.0.x: https://support.mobileiron.com/mi/vsp/AB1771634/ivanti-security-update-1761642-1.0.0S-5.noarch.rpm. • La vulnerabilidad se soluciona en el parche RPM 12.x.1.x: https://support.mobileiron.com/mi/vsp/AB1771634/ivanti-security-update-1761642-1.0.0L-5.noarch.rpm. • La solución permanente para esta vulnerabilidad se incluirá en la próxima versión del producto: 12.8.0.0. • Revisar y monitorizar los sistemas EPMM para detectar indicios de explotación (logs, conexiones inusuales, cambios de configuración). • Asegurar que los despliegues expuestos a Internet estén filtrados o segmentados adecuadamente. 			
Fuente de Información:	<ul style="list-style-type: none"> • https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340 		

Índice alfabético

Ransomware 4

Explotación de vulnerabilidades conocidas 6,7