



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

040-2026-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

VoidLink demuestra que el malware asistido por IA ya no es experimental..... 4


Botnet “Zerobot” explota una vulnerabilidad crítica de ejecución remota que afecta a la plataforma n8n. 6

Vulnerabilidad en productos de Cisco. 8

Vulnerabilidad crítica Zero-Day en Google Chrome. 9

Nueva campaña “EtherHiding” utiliza blockchain de Ethereum para ocultar infraestructura C2 mediante malware EtherRAT. 10

Índice alfabético 12

 Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 040		Fecha: 26-03-2026
			Página: 4 de 12
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	VoidLink demuestra que el malware asistido por IA ya no es experimental.		
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:

La alerta sobre AI-Assisted Malware surge a partir de investigaciones recientes que confirman que el uso de inteligencia artificial por parte de actores maliciosos ha dejado de ser experimental para convertirse en un recurso operativo real. Análisis publicados por GBHackers y respaldados por Check Point Research evidencian que desarrolladores con experiencia están utilizando modelos de lenguaje y entornos de desarrollo asistidos por IA para crear frameworks de malware complejos en tiempos considerablemente reducidos. Este cambio representa un punto de inflexión en el panorama de amenazas, ya que la barrera técnica para producir herramientas sofisticadas se reduce drásticamente, incrementando el volumen, la calidad y la velocidad de nuevas variantes de malware en circulación.



Ilustración 1: VoidLink demuestra que el malware asistido por IA

2. DETALLES:


El caso analizado demuestra cómo un solo desarrollador, apoyado por agentes de IA y metodologías de spec-driven development, logró construir un malware avanzado (VoidLink) con arquitectura modular, capacidades de comando y control (C2), persistencia y post-explotación en cuestión de días. La IA fue utilizada para generar especificaciones, estructuras de código, módulos completos y pruebas funcionales, sin que el binario final revele rastros evidentes de su origen asistido por IA. Además, se observa un creciente interés de los atacantes por modelos locales no censurados, evitando limitaciones, monitoreo y controles de proveedores comerciales. Este enfoque permite producir herramientas comparables a las desarrolladas por equipos completos, dificultando la atribución, acelerando campañas de ataque y desafiando seriamente los modelos tradicionales de detección basados en firmas o patrones históricos.

- **RECOMENDACIONES:**

- Adoptar plataformas XDR/EDR con detección basada en comportamiento y análisis heurístico avanzado.
- Asumir por defecto que el malware moderno puede haber sido desarrollado o adaptado con IA, enfocando la detección en TTPs y no solo en indicadores estáticos.
- Fortalecer la seguridad en entornos de IA y GenAI corporativos, controlando accesos, APIs y fugas de datos.
- Implementar Zero Trust con verificación continua de identidad, dispositivo y contexto.
- Monitorear anomalías en desarrollo de software, compilación y ejecución en entornos internos.
- Reforzar controles de egress filtering y detección de tráfico C2 cifrado o encubierto.
- Actualizar programas de Threat Intelligence para incluir amenazas emergentes asistidas por IA.
- Capacitar equipos técnicos y SOC en detección de malware modular y agentic AI-based.
- Realizar ejercicios de purple team simulando ataques con herramientas generadas dinámicamente.

Fuente de Información:

- <https://gbhackers.com/ai-assisted-malware/>

	ALERTA DE SEGURIDAD DIGITAL N°174		Fecha: 26-03-2026
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Botnet “Zerobot” explota una vulnerabilidad crítica de ejecución remota que afecta a la plataforma n8n.		
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

1. ANTECEDENTES:

Investigadores de seguridad de Intel471 han reportado la explotación activa de una vulnerabilidad **CRÍTICA** identificada por MITRE como [CVE-2025-68613](#) de tipo CWE-913: Control inadecuado de los recursos de código gestionados dinámicamente en la plataforma de automatización n8n, utilizada globalmente en entornos empresariales y de integración de servicios. La campaña fue atribuida al botnet “Zerobot”, el cual aprovechó esta falla de ejecución remota de código (RCE) para comprometer instancias expuestas a Internet. El ataque se dirige a servidores vulnerables de n8n en múltiples regiones, incluyendo infraestructuras corporativas y cloud. La explotación ocurre mediante el abuso del motor de evaluación de expresiones en workflows, permitiendo a atacantes autenticados ejecutar código arbitrario en el host. Esta técnica facilita la toma de control total del sistema, robo de credenciales y despliegue de malware adicional.

La explotación de la vulnerabilidad CVE-2025-68613 en la plataforma n8n por parte del botnet Zerobot representa un riesgo crítico y transversal para entidades públicas en Perú, especialmente aquellas que utilizan soluciones de automatización, integración de servicios o arquitecturas orientadas a APIs.

2. DETALLES:

Zerobot, una botnet basada en Mirai conocida por atacar dispositivos del Internet de las Cosas (IoT).

N8n es un software de automatización de flujos de trabajo basado en Node.js que utiliza JavaScript para la lógica interna de la plataforma y los flujos de trabajo.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-68613 corresponde a una falla crítica de tipo RCE en el motor de evaluación de expresiones de n8n, donde entradas controladas por el usuario pueden ejecutarse en un contexto no aislado del runtime subyacente.

Desde el punto de vista técnico, el vector de ataque se basa en la manipulación de workflows. Un atacante autenticado puede insertar expresiones maliciosas que son procesadas por el sistema sin sandboxing adecuado, permitiendo la ejecución de comandos arbitrarios en el servidor.

El botnet Zerobot, derivado de variantes tipo Mirai, ha sido observado explotando esta vulnerabilidad como parte de campañas automatizadas para comprometer servidores expuestos. Estas campañas utilizan escaneo masivo para identificar instancias vulnerables y ejecutar payloads de forma remota.

Una vez comprometido el sistema, el atacante obtiene privilegios equivalentes al proceso de n8n, lo que le permite ejecutar comandos del sistema operativo, acceder a archivos sensibles y modificar configuraciones internas.

Adicionalmente, debido a que n8n gestiona credenciales, tokens API e integraciones con múltiples servicios, el impacto se amplifica, permitiendo el robo de secretos y el movimiento lateral hacia otros sistemas conectados.

El ataque también habilita persistencia mediante la modificación de workflows o la inserción de lógica maliciosa, lo que puede pasar desapercibido en entornos automatizados. Esto convierte a n8n en un punto crítico dentro de la cadena de suministro digital.

Por otro lado, las entidades gubernamentales que utilizan n8n para automatizar procesos (integración entre sistemas, gestión documental, interoperabilidad) pueden sufrir ataques de RCE, la cual puede permitir a un atacante tomar control total del servidor. Esto impacta directamente a los sistemas administrativos, plataformas de atención ciudadana y servicios digitales del Estado. La explotación automatizada por botnets como Zerobot demuestra un cambio en el targeting hacia plataformas de orquestación y automatización, ampliando la superficie de ataque en infraestructuras modernas basadas en integración de servicios.

Finalmente, la vulnerabilidad CVE-2025-68613 en la plataforma n8n representa una amenaza de criticidad alta a crítica para las entidades públicas del Perú, al permitir la ejecución remota de código, el acceso a credenciales sensibles y el compromiso de sistemas interconectados. Su explotación facilita el movimiento lateral, la persistencia del atacante y la posible interrupción de servicios digitales del Estado, generando impacto operativo y riesgo reputacional. En este contexto, se recomienda su atención prioritaria mediante la identificación de activos expuestos, aplicación inmediata de parches de seguridad y el fortalecimiento de los mecanismos de control de acceso y monitoreo continuo.

A. Productos afectados:

- n8n (Workflow Automation Platform): todas las versiones anteriores a v1.120.4, v1.121.1, v1.122.0.
- Instancias desplegadas en: Servidores on-premise expuestos a Internet, entornos cloud (AWS, Azure, GCP) con acceso público y contenedores (Docker/Kubernetes) mal configurados o sin controles de acceso.
- Componentes vulnerables: motor de evaluación de expresiones (Expression Engine), módulo de workflows automatizados y gestión de credenciales e integraciones (API keys, tokens).

B. Indicadores de Compromiso (IoC):

Dirección IP:

- 103.59.160.237.
- 140.233.190.96.
- 144.172.100.228.
- 172.86.123.179.
- 216.126.227.101.

Dominio:

- 0bot.qzz.io.
- andro.notemacro.com/inihiddenngentod/zerobotv9.
- pivot.notemacro.com/inihiddenngentod/zerobotv9.

SHA-256:

- c8e8b627398ece071a3a148d6f38e46763dc534f9bfd967ebc8ac3479540111f.
- 360467c3b733513c922b90d0e222067509df6481636926fa1786d0273169f4da.
- cc1efbca0da739b7784d833e56a22063ec4719cd095b16e3e10f77efd4277e24.
- 045a1e42cb64e4aa91601f65a80ec5bd040ea4024c6d3b051cb1a6aa15d03b57.
- d024039824db6fe535ddd51bc81099c946871e4e280c48ed6e90dada79ccfcc7.
- deb70af83a9b3bb8f9424b709c3f6342d0c63aa10e7f8df43dd7a457bda8f060.
- 6e4e797262c80b9117aded5d25ff2752cd83abe631096b66e120cc3599a82e4e.
- 2fdb2a092f71e4eba2a114364dc8044a7aa7f78b32658735c5375bf1e4e8ece3.
- 263a363e2483bf9fd9f915527f5b5255daa42bbfa1e606403169575d6555a58c.
- d7112dd3220ccb0b3e757b006acf9b92af466a285bbb0674258bcc9ad463f616.

C. Datos clave del incidente:

- Tipo de ataque: Ejecución remota de código (RCE) + propagación de botnet
- Nivel de criticidad: Crítico (CVSS 9.9)
- Organización afectada: Usuarios/empresas que utilizan n8n
- Productos afectados: n8n (versiones < 1.120.4 / 1.121.1 / 1.122.0)
- Actor de amenaza: Zerobot (botnet tipo Mirai)
- Impacto: Compromiso total del sistema, robo de datos, movimiento lateral
- Fecha del incidente: Explotación activa reportada en marzo de 2026.


3. RECOMENDACIONES:


- Actualizar inmediatamente a versiones parcheadas: 1.120.4, 1.121.1, 1.122.0 o superiores.
- Restringir permisos de creación/edición de workflows.
- Implementar principio de mínimo privilegio.
- No exponer instancias n8n directamente a Internet.
- Aplicar segmentación de red y control de acceso.
- Monitorear logs y tráfico en busca de anomalías.
- Implementar WAF/EDR para detección de explotación.


Rotar credenciales almacenadas en n8n.

Fuente de Información:

- <https://www.intel471.com/blog/cve-2025-68613-zerobot-botnet-exploits-critical-vulnerability-impacting-n8n-ai-orchestration-platform>
- <https://www.akamai.com/blog/security-research/2026/feb/zerobot-malware-targets-n8n-automation-platform>

	ALERTA DE SEGURIDAD DIGITAL N°175		Fecha: 26-03-2026
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en productos de Cisco.		
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 publicado una vulnerabilidad de severidad ALTA de tipo CWE-124: Desbordamiento de búfer (Buffer Underflow) en el bootloader de Cisco IOS XE, que permite la evasión del mecanismo Secure Boot. Este tipo de vulnerabilidad se origina por una validación insuficiente de los binarios durante el proceso de arranque del sistema, lo que rompe la cadena de confianza (chain of trust). En términos técnicos, el fallo permite que código no firmado o manipulado sea cargado en etapas tempranas del boot, afectando directamente la integridad del firmware del dispositivo.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad alta identificada por MITRE como CVE-2026-20104 de tipo CWE-124: Desbordamiento de búfer (Buffer Underflow), podría permitir a un atacante ejecutar código que eluda el requisito de ejecutar imágenes firmadas por Cisco.</p> <p>El impacto potencial de esta vulnerabilidad es alto, ya que un atacante puede lograr la ejecución de código arbitrario en tiempo de arranque, eludiendo controles críticos de seguridad como la verificación criptográfica de imágenes firmadas por el fabricante. Esto implica que el atacante puede instalar firmware persistente malicioso, comprometiendo completamente el dispositivo a nivel de sistema operativo base, con impacto directo en la confidencialidad e integridad de la información procesada por equipos de red críticos.</p> <p>El método de explotación requiere condiciones específicas: un atacante con privilegios elevados (nivel 15) o acceso físico al dispositivo puede manipular los binarios cargados durante el proceso de arranque. Mediante esta técnica, se alteran los mecanismos de validación de integridad, permitiendo la carga de código arbitrario sin necesidad de firmar las imágenes. Aunque no es un vector remoto directo, su explotación es crítica en escenarios de acceso interno o compromisos previos, especialmente en infraestructuras OT o entornos industriales.</p> <p>El riesgo es alto, particularmente para organizaciones que dependen de dispositivos Cisco en su infraestructura de red (switches de acceso, industriales o backbone). La posibilidad de comprometer el proceso de arranque permite ataques persistentes difíciles de detectar, incluyendo implantas a nivel firmware, bypass de controles de seguridad y manipulación del tráfico de red. Además, este tipo de vulnerabilidad puede ser utilizada como punto de apoyo en campañas avanzadas (APT), afectando la confianza en la infraestructura de comunicaciones.</p> <p>A. Productos afectados:</p> <p>Cisco IOS XE Software en:</p> <ul style="list-style-type: none"> – Catalyst 9200 Series Switches. – Catalyst ESS9300 Embedded Series. – Catalyst IE9310 / IE9320 Rugged Series. – Cisco IE3500 / IE3505 Series. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Actualizar el producto afectado a la última versión de software disponible que corrige esta vulnerabilidad. • Restringir el acceso físico a dispositivos de red críticos. • Limitar el acceso privilegiado (nivel 15) mediante controles AAA. • Implementar Secure Boot y validación de firmware en su última versión disponible. • Monitorear integridad de imágenes y procesos de arranque. • Integrar controles de detección de anomalías en firmware (Firmware Integrity Monitoring). <p>Segmentar redes OT/IT para reducir exposición en entornos industriales.</p>			
Fuente de Información:		<ul style="list-style-type: none"> • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xe-secureboot-bypass-B6uYxYSZ?utm_source=chatgpt.com 	

	ALERTA DE SEGURIDAD DIGITAL N°176		Fecha: 26-03-2026
			Página: 9 de 12
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica Zero-Day en Google Chrome.		
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>Google ha reportado una vulnerabilidad de severidad ALTA clasificada como implementación incorrecta / bypass de restricciones de seguridad (CWE-284 / CWE-693: control de acceso inapropiado o protección insuficiente) que afecta al motor V8 de Google Chrome. Esta falla permite a un atacante remoto ejecutar código arbitrario dentro del sandbox del navegador mediante contenido web malicioso. El riesgo es elevado debido a que el navegador es un vector de ataque masivo en entornos corporativos, pudiendo ser utilizado como punto de entrada inicial para compromisos más amplios.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad alta identificada por MITRE como CVE-2026-3910 reside en una implementación incorrecta dentro del motor V8 (JavaScript/WebAssembly), encargado de procesar código activo en páginas web. Un atacante puede aprovechar esta debilidad mediante la creación de una página HTML especialmente diseñada que, al ser visitada por la víctima, desencadena la ejecución de código arbitrario dentro del contexto del navegador.</p> <p>Desde una perspectiva técnica, el fallo permite romper ciertas restricciones del sandbox del navegador o manipular su comportamiento interno, facilitando la ejecución de código controlado por el atacante. Aunque inicialmente la ejecución ocurre dentro del sandbox, este tipo de vulnerabilidades suele combinarse con otras (chain exploits) para lograr escape del sandbox y comprometer completamente el sistema operativo subyacente.</p> <p>Se ha confirmado que esta vulnerabilidad está siendo explotada activamente en el mundo real (zero-day), aunque los detalles técnicos del exploit no han sido divulgados completamente para evitar abusos adicionales. No obstante, la existencia de explotación “in-the-wild” implica que ya existen herramientas o exploits funcionales, aunque los PoC públicos son limitados o restringidos.</p> <p>El riesgo de esta vulnerabilidad es alto, especialmente en entornos empresariales donde Chrome es ampliamente utilizado. La explotación activa como zero-day incrementa la probabilidad de ataques dirigidos y campañas masivas, convirtiendo la navegación web en un vector crítico de compromiso inicial dentro de la cadena de ataque.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – Google Chrome versiones anteriores a 146.0.7680.75/76 (Windows/macOS). – Google Chrome versiones anteriores a 146.0.7680.75 (Linux). – Navegadores basados en Chromium (potencialmente afectados): Microsoft Edge, Brave, Opera y Vivaldi. <p>B. Indicadores de Compromiso (IoC):</p> <ul style="list-style-type: none"> – Redirecciones a sitios web maliciosos o comprometidos. – Ejecución de código sospechoso tras navegación web. – Actividad anómala del navegador (crashes, comportamiento inusual). – Descarga o ejecución de payloads sin interacción adicional. – Tráfico hacia dominios de comando y control (C2) tras visitar páginas web. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Actualizar Google Chrome a versiones \geq 146.0.7680.75/76 y forzar reinicio del navegador tras la actualización. • Aplicar políticas de seguridad en endpoints (EDR/XDR). • Restringir navegación a sitios no confiables. • Implementar aislamiento del navegador (Browser Isolation). <p>Monitorear actividad web y eventos del navegador en SIEM.</p>			
Fuente de Información:	<ul style="list-style-type: none"> • https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html • https://issues.chromium.org/issues/491410818 		

	ALERTA DE SEGURIDAD DIGITAL N°177		Fecha: 26-03-2026
			Página: 10 de 12
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Nueva campaña "EtherHiding" utiliza blockchain de Ethereum para ocultar infraestructura C2 mediante malware EtherRAT.		
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			
<p>1. ANTECEDENTES:</p> <p>El 24 de marzo de 2026, la Unidad de Respuesta a Amenazas (TRU) de eSentire reportó una campaña activa de malware denominada "EtherHiding", observada en entornos globales mediante infraestructura distribuida tipo CDN, donde actores de amenaza emplean la red blockchain de Ethereum para ocultar direcciones de comando y control (C2). La investigación revela que el actor —aún no atribuido formalmente— utiliza el malware "EtherRAT", específicamente su módulo Sys-Info, para recolectar información del sistema y seleccionar objetivos de alto valor. La campaña se caracteriza por el uso de contratos inteligentes y transacciones en Ethereum como mecanismo de resolución dinámica de C2, dificultando su detección y desmantelamiento. El vector inicial involucra la distribución de cargas maliciosas a través de recursos aparentemente legítimos que imitan tráfico CDN, logrando evasión avanzada de controles perimetrales.</p> <p>2. DETALLES:</p> <p>La campaña identificada introduce una evolución significativa en tácticas de ocultamiento de infraestructura C2 mediante el uso de blockchain pública. A diferencia de modelos tradicionales de C2 centralizado, el actor almacena direcciones de servidores maliciosos dentro de datos codificados en transacciones de Ethereum, lo que permite una resiliencia excepcional frente a takedowns y listas negras. Este enfoque descentralizado elimina puntos únicos de falla y complica la atribución.</p> <p>EtherRAT es una puerta trasera basada en Node.js que, según informes, Sysdig vincula con un grupo de amenazas persistentes avanzadas (APT) de Corea del Norte debido a importantes coincidencias con las tácticas, técnicas y procedimientos (TTP) de la "Contagious Interview".</p> <p>El malware EtherRAT integra un módulo denominado Sys-Info, cuya función es realizar reconocimiento exhaustivo del host comprometido. Este módulo recopila información como nombre del equipo, usuario, arquitectura del sistema, procesos activos y configuraciones de red. Estos datos son posteriormente utilizados para clasificar a la víctima y determinar si es un objetivo de interés estratégico, lo que evidencia un enfoque de ataque selectivo.</p> <p>Una vez validado el objetivo, el malware consulta la blockchain de Ethereum para recuperar dinámicamente la dirección del C2. Esto se logra mediante la lectura de datos incrustados en contratos inteligentes o transacciones específicas, que actúan como repositorios encubiertos. Este mecanismo evita el uso de dominios o IPs estáticas, reduciendo la efectividad de controles tradicionales como DNS filtering o bloqueo de IP.</p> <p>La campaña también implementa técnicas de ofuscación y camuflaje de tráfico, simulando patrones de comunicación similares a redes de distribución de contenido (CDN). Esto permite que el tráfico malicioso pase desapercibido dentro de flujos legítimos, dificultando su detección mediante análisis de comportamiento o inspección profunda de paquetes (DPI).</p> <p>En términos de persistencia, EtherRAT emplea mecanismos comunes como claves de registro, tareas programadas o modificación de servicios del sistema, asegurando su ejecución continua tras reinicios. Además, se ha observado que el malware puede descargar módulos adicionales, lo que sugiere capacidades de expansión modular y posible evolución hacia funcionalidades de espionaje o ransomware.</p> <p>Desde la perspectiva de evasión, el uso de infraestructura descentralizada como Ethereum representa un cambio paradigmático. Las soluciones de seguridad tradicionales no están diseñadas para inspeccionar o bloquear transacciones en blockchain pública, lo que crea una superficie de ataque difícil de controlar. Este enfoque podría ser replicado por otros actores en futuras campañas.</p>			

Finalmente, la campaña demuestra un alto nivel de sofisticación técnica, combinando técnicas de malware avanzado, evasión de detección y uso innovador de tecnologías emergentes. Esto posiciona a EtherHiding como una amenaza relevante para organizaciones públicas y privadas, especialmente aquellas con infraestructura crítica o datos sensibles.

A. Vulnerabilidades explotadas:

- No se identifican CVEs específicos explotados en esta campaña.
- El vector de infección parece depender de ingeniería social o descarga de software malicioso.
- Posible abuso de configuraciones débiles o falta de controles EDR.

B. Indicadores de Compromiso (IoC):

- Hashes asociados a muestras de EtherRAT (no publicados completamente en fuente abierta).
- Tráfico hacia nodos públicos de Ethereum (RPC endpoints).
- Consultas a contratos inteligentes específicos (direcciones variables).
- Procesos sospechosos relacionados con recolección de información del sistema.
- Conexiones salientes cifradas con patrones similares a CDN.
- Creación de tareas programadas o claves de persistencia inusuales.
- Ver [lista completa](#) de IoC.

C. Datos clave del incidente:

- Tipo de ataque: Malware avanzado con C2 descentralizado (Blockchain-based C2 / RAT).
- Nivel de criticidad: Alto / Crítico.
- Organización afectada: No específica (campaña global dirigida).
- Productos afectados: Sistemas Windows (principalmente endpoints corporativos).
- Actor de amenaza: No atribuido (probable cibercrimen avanzado con capacidades APT-like).
- Impacto: Exfiltración de información, control remoto del sistema, evasión de detección, posible pivoting lateral.
- Fecha del incidente: marzo de 2026.

3. RECOMENDACIONES:

- Implementar soluciones EDR/XDR con क्षमता de análisis de comportamiento.
- Monitorear tráfico hacia nodos blockchain públicos (Ethereum RPC).
- Aplicar Zero Trust Network Access (ZTNA) para limitar comunicaciones salientes.
- Bloquear ejecución de binarios no firmados o desconocidos.
- Fortalecer controles de correo y navegación web (sandboxing).
- Capacitar a usuarios en detección de ingeniería social.
- Integrar inteligencia de amenazas (TI) enfocada en técnicas emergentes como blockchain abuse.
- Auditar procesos que acceden a APIs externas no comunes.

Fuente de Información:

- <https://www.esentire.com/blog/etherrat-sys-info-module-c2-on-ethereum-etherhiding-target-selection-cdn-like-beacons>
- <https://www.sysdig.com/blog/etherrat-dprk-uses-novel-ethereum-implant-in-react2shell-attacks>
- <https://www.esentire.com/blog/muddywater-apt-tsundere-botnet-etherhiding-the-c2>

Índice alfabético

Malware	4,10
Explotación de vulnerabilidades conocidas	6,8,9