



GS PERÚ

Software - Security & Services

Empresas

BOLETÍN CIBERSEGURIDAD

Enero - 2026





ESCALAR EL NEGOCIO SIN ESCALAR EL RIESGO

Enero de 2026 marca un cambio silencioso pero decisivo en la forma en que las organizaciones abordan la ciberseguridad. Los incidentes recientes ya no evidencian fallas aisladas, sino una limitación estructural: los modelos de defensa no están diseñados para operar a la velocidad ni al volumen del negocio digital actual.

Los entornos cloud-native, las identidades no humanas y la automatización masiva han multiplicado los puntos de decisión de seguridad. Cada despliegue, cada integración y cada workflow crea una condición que debe ser evaluada en tiempo real. En este contexto, los enfoques basados en revisión manual, reglas estáticas o controles post-incidente simplemente no escalan.

Los primeros análisis del año muestran que las organizaciones con menor impacto no fueron necesariamente las más protegidas, sino las que lograron operacionalizar la seguridad como un sistema continuo, capaz de adaptarse dinámicamente al cambio. Telemetría unificada, evaluación de riesgo contextual y respuestas automatizadas empiezan a dejar de ser ventajas competitivas para convertirse en requisitos mínimos.

El mercado responde a esta presión. Plataformas diseñadas para consolidar identidad, cloud, aplicaciones y red bajo un mismo modelo analítico comienzan a desplazar soluciones puntuales. La conversación deja de girar en torno a “qué herramienta usar” y pasa a centrarse en “qué tan rápido puede la seguridad acompañar al negocio”.

El inicio de 2026 no presenta una nueva amenaza, sino una nueva exigencia: la seguridad debe escalar con la operación o se convierte en fricción. En un entorno donde todo es dinámico, proteger ya no es bloquear, sino decidir mejor y más rápido.

Capacidades que definen a las organizaciones resilientes

- Seguridad diseñada como plataforma, no como conjunto de controles aislados.
- Evaluación de riesgo en tiempo real basada en contexto operativo.
- Automatización de decisiones de contención y corrección.
- Métricas alineadas a impacto de negocio, no solo a eventos técnicos.
- Integración nativa entre seguridad, TI y operaciones.

Enero de 2026 deja un mensaje claro para líderes y tomadores de decisión: la ciberseguridad entra en su fase de escala. Las organizaciones que entiendan esto no solo reducirán riesgo, sino que ganarán velocidad, confianza y ventaja competitiva.

ÍNDICE

	1. Malware	4
	1.1 Nuevo ransomware Osiris ataca a operador de servicios de alimentos en el sudeste asiático.	
	1.2 Malware de proxyware disfrazado de Notepad++ utilizado en campañas de proxyjacking.	
	1.3 Nueva ola de malware GlassWorm apunta a desarrolladores de macOS mediante extensiones maliciosas.	
	1.4 Nuevo malware VVS Stealer apunta al robo de cuentas de Discord.	
	1.5 PDFSider ataca a una empresa Fortune 100 del sector financiero.	
	1.6 Extensión maliciosa Escudo Nex bloquea navegadores y propaga malware en entornos corporativos.	
	1.7 Ataque ClickFix utiliza pantallas BSOD falsas para comprometer al sector hotelero.	
	2. Vulnerabilidades	18
	2.1 Vulnerabilidad crítica en n8n permite la ejecución de comandos del sistema.	
	2.2 Vulnerabilidades críticas en paquetes npm exponen servidores a ejecución remota de código.	
	2.3 QNAP corrige vulnerabilidades críticas en sistemas NAS que permiten ejecución de comandos y acceso no autorizado a archivos.	
	2.4 Vulnerabilidad Crítica CVE-2026-24858 en Fortinet – Bypass de Autenticación SSO Bajo Explotación Activa.	
	3. Phishing	26
	3.1 Campaña de Phishing de Múltiples Etapas Dirigida a Usuarios en Rusia con Amnesia RAT y Ransomware.	
	3.2 Campaña de Phishing Multi-Etapa Adversary-in-the-Middle (AiTM) y BEC Dirigida al Sector Energético.	
	4. Adversarios	30
	4.1 Konni implementa malware PowerShell generado por IA en campaña "Operación Poseidón".	
	4.2 Campaña Cibernética RedKitten (Vinculada a Irán) Apunta a ONG y Activistas de Derechos Humanos.	
	5. Indicadores de compromiso	34
	5.1 Direcciones IP	
	5.2 Dominios	
	5.3 Hashes	
	6. Fuentes	



1. Malware

1.1 Nuevo ransomware Osiris ataca a operador de servicios de alimentos en el sudeste asiático

Una nueva familia de ransomware denominada Osiris fue identificada tras un ataque dirigido a un importante operador de servicios de alimentos en el sudeste asiático, ocurrido en noviembre de 2025. Esta amenaza no guarda relación con una variante homónima detectada en 2016 y se atribuye a atacantes con alto nivel técnico.

Durante el ataque, los actores maliciosos utilizaron un controlador malicioso llamado Poortry, aprovechando una técnica BYOVD (Bring Your Own Vulnerable Driver) para desactivar mecanismos de seguridad del sistema. Para la exfiltración de datos, emplearon la herramienta Rclone, transfiriendo información al almacenamiento en la nube Wasabi, una táctica previamente observada en campañas del ransomware Inc.

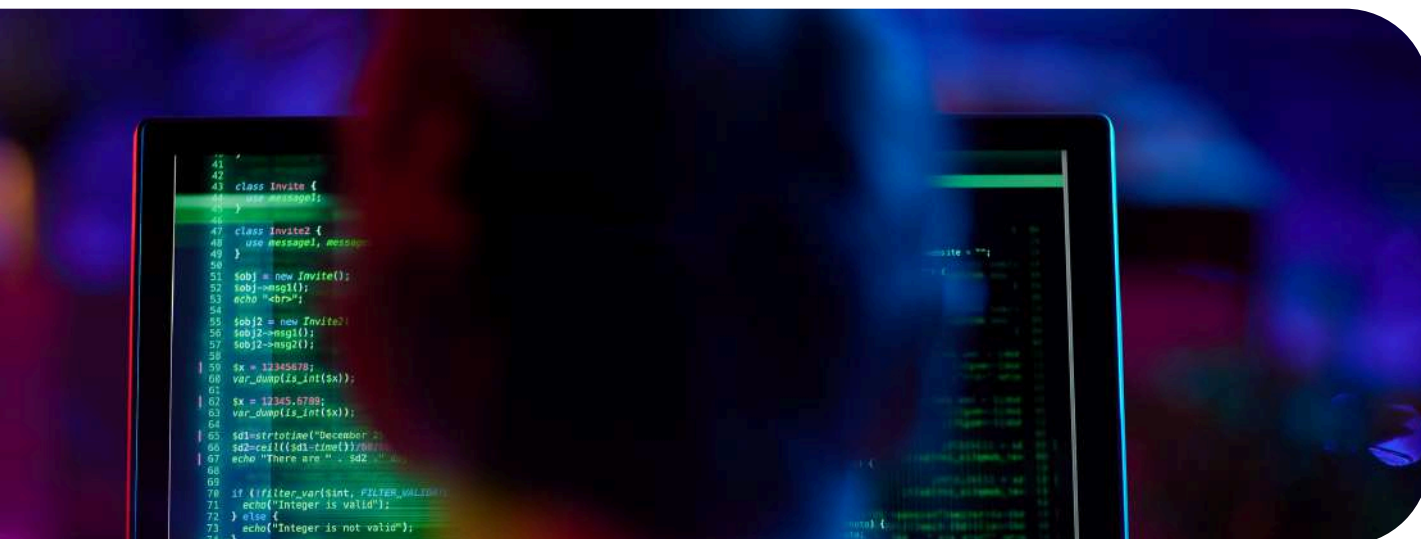
Osiris implementa cifrado híbrido (ECC + AES-128-CTR) y es capaz de cifrar archivos de forma selectiva, además de finalizar procesos y servicios críticos para maximizar el impacto. Los archivos comprometidos reciben la extensión .Osiris, y el ataque culmina con la entrega de una nota de rescate que instruye a las víctimas a iniciar negociaciones con los atacantes.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0002: Ejecución	T1106 – Native API	Ejecución directa de código malicioso a bajo nivel para desplegar el ransomware Osiris en el sistema comprometido.
TA0004: Escalada de Privilegios	T1068 – Exploitation for Privilege Escalation	Uso de un controlador vulnerable mediante la técnica BYOVD para obtener privilegios elevados en el sistema.
TA0005: Evasión de Defensa	T1562.001 – Disable or Modify Tools	Desactivación de soluciones de seguridad utilizando el driver malicioso Poortry para evadir EDR y antivirus.
TA0007: Descubrimiento	T1083 – File and Directory Discovery	Identificación de archivos y directorios específicos a cifrar dentro del entorno comprometido.
TA0009: Colección	T1005 – Data from Local System	Recolección de información sensible almacenada localmente antes del proceso de cifrado.
TA0010: Exfiltración	T1567.002 – Exfiltration to Cloud Storage	Exfiltración de datos mediante Rclone hacia almacenamiento en la nube Wasabi.
TA0040: Impacto	T1486 – Data Encrypted for Impact	Cifrado híbrido (ECC + AES-128-CTR) de archivos críticos y extensión .Osiris aplicada a los archivos afectados.
TA0040: Impacto	T1490 – Inhibit System Recovery	Finalización de procesos y servicios esenciales para impedir la recuperación normal del sistema.

Recomendaciones

- **Fortalecimiento de controladores y kernel (BYOVD):** Bloquear la carga de controladores vulnerables mediante políticas de Driver Blocklist, habilitar HVCI / Memory Integrity en Windows y mantener el sistema operativo y drivers permanentemente actualizados para prevenir ataques BYOVD como el uso del driver malicioso Poortry.
- **Protección avanzada contra evasión de seguridad:** Implementar y reforzar soluciones EDR/XDR con protección contra tampering, evitando la desactivación de antivirus y agentes de seguridad incluso con privilegios elevados.
- **Restricción de herramientas de exfiltración:** Monitorear y limitar el uso de herramientas legítimas como Rclone, estableciendo reglas de detección para transferencias no autorizadas hacia servicios de almacenamiento en la nube como Wasabi.
- **Segmentación y control de accesos:** Aplicar principio de mínimo privilegio, segmentar la red para limitar el alcance del ataque y restringir el acceso administrativo únicamente a sistemas y usuarios autorizados.
- **Gestión segura de copias de seguridad:** Mantener respaldos inmutables, cifrados y fuera de línea, realizando pruebas periódicas de restauración para garantizar la recuperación ante un evento de cifrado masivo.



1.2 Malware de proxyware disfrazado de Notepad++ utilizado en campañas de proxyjacking

La firma de seguridad ASEC se encuentra monitoreando una serie de ataques de proxyjacking que involucran malware disfrazado como el instalador legítimo de Notepad++, atribuidos al actor de amenazas identificado como Larva-25012. Esta campaña maliciosa busca comprometer sistemas para convertirlos en nodos proxy, permitiendo el uso indebido de los recursos de red de las víctimas.

El grupo Larva-25012 ha evolucionado sus técnicas para evadir mecanismos de detección, destacando la inyección de proxyware dentro de procesos legítimos. La distribución del malware se realiza principalmente a través de sitios falsos de descarga de software pirateado, lo que incrementa la probabilidad de infección en usuarios que buscan aplicaciones sin licencia.

En campañas recientes, los atacantes han modificado su método de entrega, pasando de instaladores MSI a archivos ZIP que contienen tanto un instalador auténtico de Notepad++ como una DLL maliciosa. Este enfoque permite que el software legítimo se ejecute normalmente, mientras el componente malicioso se carga de forma encubierta.

El malware, identificado como DPLoader, establece persistencia mediante el Programador de tareas de Windows y ejecuta scripts diseñados para instalar soluciones de proxyware como Infatica y DigitalPulse. Estas herramientas amplían la capacidad del ataque, permitiendo el enrutamiento de tráfico no autorizado a través de los sistemas comprometidos, incrementando el riesgo operativo y legal para las víctimas.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1195.002 – Compromise Software Supply Chain	Distribución de instaladores falsos de Notepad++ a través de sitios de descarga de software pirateado.
TA0002: Ejecución	T1204.002 – User Execution: Malicious File	Ejecución manual por el usuario de archivos ZIP que contienen un instalador legítimo junto con una DLL maliciosa.
TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Ejecución de scripts por parte de DPLoader para instalar componentes adicionales de proxyware.
TA0003: Persistencia	T1053.005 – Scheduled Task/Job: Scheduled Task	Registro del malware en el Programador de tareas de Windows para garantizar ejecución recurrente.
TA0005: Evasión de Defensa	T1055 – Process Injection	Inyección de proxyware dentro de procesos legítimos para ocultar la actividad maliciosa.
TA0005: Evasión de Defensa	T1036 – Masquerading	Uso de nombres y archivos asociados a software legítimo para evadir detección.
TA0006: Acceso a Credenciales	T1555 – Credentials from Password Stores	Posible acceso indirecto a credenciales almacenadas mediante la ejecución persistente del malware.
TA0011: Comando y Control	T1090 – Proxy	Uso de proxyware como Infatica y DigitalPulse para enrutar tráfico a través del sistema comprometido.

Recomendaciones:

- **Concientización y capacitación de usuarios:** Educar a los colaboradores sobre los riesgos de descargar software desde sitios no oficiales o de software pirateado, enfatizando la verificación de la fuente y la integridad de los instaladores antes de su ejecución.
- **Control estricto de aplicaciones:** Implementar Application Whitelisting (AppLocker o Windows Defender Application Control) para permitir únicamente la ejecución de software autorizado, evitando la carga de DLL maliciosas asociadas a instaladores falsos.
- **Restricción de ejecución y carpetas sensibles:** Bloquear la ejecución de archivos desde ubicaciones comúnmente abusadas, como Downloads, Temp y AppData, donde suelen desplegarse componentes de malware y proxyware.
- **Supervisión del Programador de tareas:** Monitorear y auditar de forma continua la creación y modificación de tareas programadas, ya que DPLoader utiliza este mecanismo para establecer persistencia.
- **Protección avanzada de endpoints:** Implementar soluciones EDR/XDR con capacidades de detección de process injection y masquerading, permitiendo identificar proxyware oculto dentro de procesos legítimos.

 ALTA

1.3 Nueva ola de malware GlassWorm apunta a desarrolladores de macOS mediante extensiones maliciosas

Se ha identificado una nueva campaña del malware GlassWorm dirigida específicamente a desarrolladores de macOS, utilizando extensiones maliciosas de Visual Studio Code y OpenVSX que distribuyen aplicaciones de billetera criptográfica troyanizadas. Esta actividad representa un cambio significativo respecto a campañas anteriores, las cuales estaban enfocadas principalmente en sistemas Windows.

GlassWorm emplea cargas útiles cifradas con AES-256-CBC, incrustadas dentro de código JavaScript, y ejecuta su lógica maliciosa tras un retraso de 15 minutos, una técnica diseñada para evadir mecanismos de detección estática y dinámica. A diferencia de amenazas en Windows, el malware utiliza AppleScript para establecer persistencia, apoyándose en LaunchAgents en lugar de modificar el Registro del sistema.

Como parte de su capacidad de compromiso, GlassWorm intenta reemplazar aplicaciones legítimas de billeteras de hardware, como Ledger Live y Trezor Suite, por versiones manipuladas. No obstante, esta funcionalidad presenta fallos operativos en la versión actual del malware.

A pesar del fortalecimiento de los controles de seguridad en macOS, GlassWorm mantiene capacidades activas de robo de credenciales y datos sensibles, incluyendo contraseñas almacenadas en Keychain. Los investigadores han registrado más de 33.000 instalaciones, aunque advierten que estas cifras podrían haber sido infladas artificialmente con el fin de aumentar la aparente legitimidad y confiabilidad de las extensiones maliciosas.

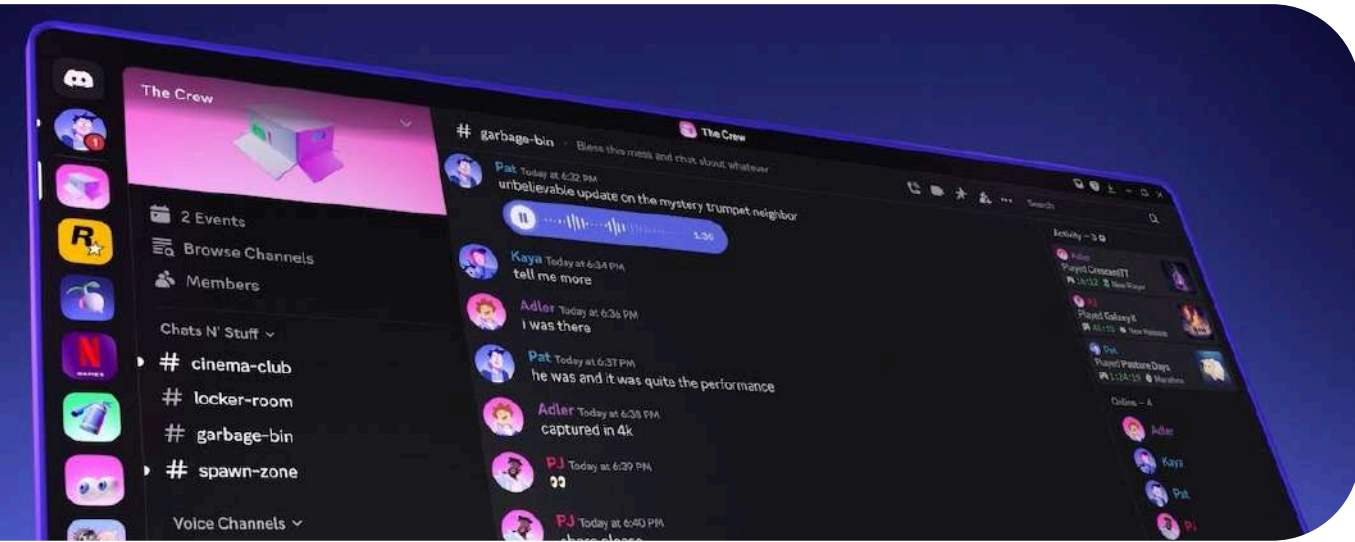
Esta campaña confirma la creciente sofisticación del malware orientado a macOS y el aumento del interés de los actores de amenazas en comprometer entornos de desarrollo, los cuales suelen manejar credenciales críticas, llaves criptográficas y acceso privilegiado a infraestructuras sensibles.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1195.002 – Compromise Software Supply Chain	Distribución de extensiones maliciosas a través de VSCode y OpenVSX, simulando herramientas legítimas para desarrolladores de macOS.
TA0002: Ejecución	T1059.007 – Command and Scripting Interpreter: JavaScript	Ejecución de cargas útiles cifradas AES-256-CBC embebidas en JavaScript tras un retraso de 15 minutos.
TA0003: Persistencia	T1543.001 – Create or Modify System Process: Launch Agent	Uso de LaunchAgents y AppleScript para mantener la ejecución persistente en macOS.
TA0005: Evasión de Defensa	T1027 – Obfuscated Files or Information	Cifrado y ofuscación de la carga maliciosa para evadir detección estática y análisis de seguridad.
TA0005: Evasión de Defensa	T1497.003 – Time Based Evasion	Retraso intencional de la ejecución (15 minutos) para evadir entornos de análisis automatizados.
TA0006: Acceso a Credenciales	T1555.001 – Credentials from Password Stores: Keychain	Robo de credenciales y contraseñas almacenadas en macOS Keychain.
TA0009: Colección	T1005 – Data from Local System	Recolección de información sensible y datos confidenciales del sistema comprometido.
TA0011: Comando y Control	T1071.001 – Application Layer Protocol: Web Protocols	Comunicación con infraestructura de comando y control utilizando protocolos web desde JavaScript.

Recomendaciones:

- **Concientización de desarrolladores y usuarios técnicos:** Capacitar a desarrolladores de macOS sobre los riesgos de instalar extensiones de VSCode/OpenVSX no oficiales, verificando siempre el editor, la reputación y la integridad de las extensiones antes de su uso.
- **Control y endurecimiento de extensiones de desarrollo:** Restringir la instalación de extensiones en entornos de desarrollo mediante políticas corporativas, permitiendo únicamente repositorios y extensiones previamente aprobadas.
- **Protección de ejecución y scripts:** Implementar controles que supervisen y restrinjan la ejecución de JavaScript y AppleScript no autorizados, especialmente aquellos que se ejecutan con retrasos temporales diseñados para evadir detección.
- **Monitoreo de persistencia en macOS:** Auditar y alertar sobre la creación o modificación de LaunchAgents y scripts de inicio, ya que GlassWorm utiliza estos mecanismos para mantener persistencia sin alterar el Registro.
- **Protección de credenciales y llaves criptográficas:** Reforzar la seguridad del Keychain de macOS, limitando el acceso a credenciales sensibles y utilizando gestores de secretos con control de acceso y auditoría.



1.4 Nuevo malware VVS Stealer apunta al robo de cuentas de Discord

Investigadores de ciberseguridad han identificado un nuevo malware desarrollado en Python, denominado VVS Stealer, diseñado específicamente para comprometer cuentas de Discord mediante el robo de credenciales y tokens de sesión. La amenaza ha sido promocionada en canales de Telegram como el "ladrón definitivo", siendo ofrecida como malware-as-a-service a través de distintos niveles de suscripción de bajo costo, lo que facilita su adopción por actores maliciosos con pocos recursos técnicos.

VVS Stealer implementa técnicas avanzadas de ofuscación mediante el uso de PyArmor, con el objetivo de evadir mecanismos de detección y análisis. Una vez ejecutado en el sistema de la víctima, el malware establece persistencia agregándose a la carpeta de Inicio de Windows, asegurando su ejecución tras cada reinicio del equipo.

Como parte de su estrategia de engaño, el malware muestra mensajes de error falsos, induciendo al usuario a reiniciar el sistema, lo que permite completar la instalación y activación de sus componentes maliciosos. Entre sus capacidades se incluye el robo de tokens de Discord, información almacenada en navegadores web, así como la captura de pantallas, ampliando el alcance de la información comprometida.

Adicionalmente, VVS Stealer puede ejecutar ataques de inyección en Discord, secuestrando sesiones activas mediante la descarga de una carga útil JavaScript maliciosa desde un servidor remoto. Esta funcionalidad permite a los atacantes mantener acceso persistente a las cuentas comprometidas, incluso después de que las víctimas cambien sus credenciales.

La aparición de VVS Stealer refuerza la tendencia creciente de malware enfocado en plataformas de comunicación y redes sociales, representando un riesgo significativo tanto para usuarios individuales como para organizaciones que utilizan Discord como canal de colaboración interna.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1204.002 – User Execution: Malicious File	Ejecución por parte del usuario de archivos maliciosos distribuidos como software atractivo o herramientas relacionadas con Discord.
TA0002: Ejecución	T1059.006 – Command and Scripting Interpreter: Python	Ejecución del malware desarrollado en Python, permitiendo el despliegue de sus módulos de robo de información.
TA0003: Persistencia	T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Establecimiento de persistencia mediante la carpeta Inicio de Windows para su ejecución automática tras reinicio.
TA0005: Evasión de Defensa	T1027 – Obfuscated Files or Information	Uso de PyArmor para ofuscar el código y evadir detección y análisis de soluciones de seguridad.
TA0006: Acceso a Credenciales	T1555 – Credentials from Password Stores	Robo de tokens de Discord y credenciales almacenadas en navegadores web.
TA0009: Colección	T1113 – Screen Capture	Captura de pantallas del sistema comprometido para recolección de información sensible.
TA0011: Comando y Control	T1071.001 – Application Layer Protocol: Web Protocols	Comunicación con servidores remotos para descarga de cargas útiles JavaScript y control de sesiones secuestradas.
TA0040: Impacto	T1565.001 – Data Manipulation	Secuestro de sesiones activas de Discord mediante inyección de código JavaScript en el cliente.

Recomendaciones:

- **Concientización de usuarios:** Capacitar a los usuarios para que eviten descargar software, scripts o “herramientas” no oficiales, especialmente aquellas que prometen mejoras, bots o utilidades para Discord.
- **Control de ejecución:** Restringir la ejecución de scripts en Python y binarios no firmados mediante políticas de control de aplicaciones (AppLocker, WDAC), con especial atención a la carpeta Inicio de Windows.
- **Protección de credenciales:** Habilitar autenticación multifactor (MFA) en cuentas de Discord y navegadores, y minimizar el almacenamiento de credenciales y tokens en el sistema.
- **Monitoreo y detección:** Implementar soluciones EDR/XDR capaces de detectar ofuscación, persistencia en el arranque y comportamientos anómalos como captura de pantalla o inyección de código en aplicaciones legítimas.

 ALTA

1.5 PDFSider ataca a una empresa Fortune 100 del sector financiero

Una nueva cepa de malware denominada PDFSider fue identificada en un ataque de ransomware dirigido contra una empresa Fortune 100 del sector financiero. El incidente se inició mediante ingeniería social, donde los atacantes se hicieron pasar por personal de soporte técnico para convencer a empleados de instalar Microsoft Quick Assist, facilitando el acceso remoto inicial.

El malware fue distribuido a través de correos electrónicos de phishing que incluían un ejecutable legítimo de PDF24 Creator acompañado de una DLL maliciosa, la cual se cargaba mediante la técnica de DLL Side-Loading. Este método permitió a PDFSider evadir controles de seguridad tradicionales al ejecutarse bajo un binario confiable.

PDFSider opera de forma altamente sigilosa, dejando mínimos artefactos en disco y utilizando exfiltración de información a través de consultas DNS. Para asegurar sus comunicaciones, emplea cifrado AES-256-GCM, característica más común en herramientas de espionaje avanzado que en malware con motivaciones puramente financieras.

Además, el malware incorpora mecanismos antianálisis diseñados para evadir entornos sandbox y sistemas de detección automática, lo que incrementa su nivel de sofisticación y dificulta su identificación temprana dentro de la red comprometida.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.001 – Phishing: Adjuntos Maliciosos	Envío de correos de phishing que incluyen un ejecutable legítimo acompañado de una DLL maliciosa.
TA0001: Acceso Inicial	T1566.003 – Phishing: Ingeniería Social	Los atacantes se hicieron pasar por personal de soporte técnico para inducir a los empleados a instalar Microsoft Quick Assist.
TA0002: Ejecución	T1574.002 – Hijacking de Flujo de Ejecución: DLL Side-Loading	Carga lateral de una DLL maliciosa utilizando un binario legítimo para ejecutar PDFSider sin levantar alertas.
TA0005: Evasión de Defensa	T1027 – Archivos o Información Ofuscada	Uso de cifrado AES-256-GCM para proteger las comunicaciones y ocultar el contenido del tráfico malicioso.
TA0005: Evasión de Defensa	T1497 – Evasión de Virtualización / Sandbox	Implementación de técnicas antianálisis para evadir la detección en entornos sandbox y sistemas automatizados.
TA0011: Comando y Control (C2)	T1071.004 – C2 sobre DNS	Exfiltración de información del sistema mediante consultas DNS para evitar detección por firewalls tradicionales.
TA0010: Exfiltración	T1041 – Exfiltración sobre Canal C2	Transferencia de información del sistema hacia infraestructura controlada por el atacante usando canales cifrados.
TA0040: Impacto	T1486 – Cifrado de Datos para Impacto	Uso del malware como parte de un ataque de ransomware dirigido a una empresa Fortune 100 del sector financiero.

Recomendaciones:

- **Concientización y control de phishing:** Capacitar a los usuarios para identificar correos sospechosos y reforzar el uso de filtros de correo que bloqueen adjuntos ejecutables y técnicas de ingeniería social, especialmente aquellas que suplantan a soporte técnico.
- **Control de aplicaciones y ejecución:** Implementar listas blancas (Application Whitelisting) para permitir solo la ejecución de software autorizado y bloquear la carga lateral de DLL en aplicaciones legítimas.
- **Restricción de herramientas remotas:** Limitar y monitorear el uso de herramientas de asistencia remota como Microsoft Quick Assist, permitiendo su ejecución solo bajo necesidad justificada y con validación del área de TI.
- **Monitoreo y detección avanzada:** Desplegar soluciones EDR/XDR con capacidad de detectar comportamientos anómalos, uso de cifrado inusual y comunicaciones encubiertas a través de DNS.
- **Respaldo y recuperación:** Mantener copias de seguridad inmutables y fuera de línea, realizando pruebas periódicas de restauración para asegurar la recuperación ante incidentes de ransomware.



1.6 Extensión maliciosa Escudo Nex bloquea navegadores y propaga malware en entornos corporativos

Una extensión bloqueadora de anuncios maliciosa denominada Escudo Nex ha sido identificada como parte de una campaña de publicidad maliciosa dirigida a usuarios de Google Chrome y Microsoft Edge. Esta amenaza se distribuye mediante anuncios engañosos y se presenta como una solución legítima de bloqueo de publicidad.

Una vez instalada, la extensión provoca una denegación de servicio (DoS) al generar conexiones infinitas, lo que ocasiona fallos recurrentes, congelamiento del navegador y pérdida de respuesta del sistema. Tras el reinicio del navegador, Escudo Nex despliega una ventana emergente fraudulenta que alerta falsamente sobre supuestos problemas de seguridad en el equipo.

A través de este mensaje engañoso, se induce al usuario a ejecutar comandos maliciosos en el símbolo del sistema de Windows, los cuales activan un script de PowerShell ofuscado. Dicho script descarga e instala una herramienta de acceso remoto conocida como ModeloRAT, capaz de ejecutar múltiples actividades maliciosas dentro de redes corporativas, incluyendo control remoto del sistema comprometido.

Investigadores de ciberseguridad atribuyen esta amenaza al grupo KongTuke, el cual ha intensificado su enfoque hacia entornos empresariales desde inicios de 2025, representando un riesgo significativo para la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.002 – Phishing: Enlace Malicioso	Distribución de la extensión maliciosa Escudo Nex mediante campañas de publicidad maliciosa que simulan bloqueadores de anuncios legítimos.
TA0002: Ejecución	T1059.001 – PowerShell	Ejecución de comandos maliciosos inducidos al usuario, que lanzan scripts de PowerShell ofuscados para descargar el payload principal.
TA0005: Evasión de Defensa	T1027 – Obfuscated Files or Information	Uso de scripts PowerShell ofuscados para evadir mecanismos de detección y análisis de seguridad.
TA0005: Evasión de Defensa	T1218 – Signed Binary Proxy Execution	Abuso de funcionalidades legítimas del sistema operativo (cmd y PowerShell) para ejecutar código malicioso sin levantar alertas.
TA0011: Comando y Control	T1071.004 – Application Layer Protocol: DNS	Comunicación con infraestructura de comando y control utilizando tráfico DNS para evadir controles de red tradicionales.
TA0002: Ejecución	T1105 – Ingress Tool Transfer	Descarga e instalación de la herramienta de acceso remoto ModeloRAT desde servidores controlados por el atacante.
TA0040: Impacto	T1499 – Endpoint Denial of Service	Generación de conexiones infinitas por parte de la extensión maliciosa, causando fallos del navegador y degradación del sistema.

Recomendaciones:

- **Concientización de usuarios:** Capacitar a los colaboradores para que eviten instalar extensiones de navegador desde anuncios, enlaces patrocinados o fuentes no oficiales, y desconfíen de alertas de seguridad emergentes.
- **Control de extensiones y scripts:** Restringir la instalación de extensiones en Chrome y Edge mediante políticas corporativas y limitar la ejecución de PowerShell a usuarios y procesos autorizados.
- **Endurecimiento del endpoint:** Aplicar reglas de control de aplicaciones (AppLocker/WDAC) para bloquear la ejecución de comandos y scripts iniciados desde navegadores.
- **Monitoreo y detección:** Implementar EDR/XDR para detectar uso anómalo de PowerShell, ejecución de comandos manuales y comportamientos asociados a herramientas de acceso remoto (RAT).
- **Protección de red:** Inspeccionar y monitorear tráfico DNS para identificar comunicaciones sospechosas con infraestructura de comando y control.



1.7 Ataque ClickFix utiliza pantallas BSOD falsas para comprometer al sector hotelero

Una nueva campaña de ingeniería social conocida como ClickFix se ha dirigido al sector hotelero en Europa, utilizando pantallas falsas de Windows Blue Screen of Death (BSOD) para engañar a los usuarios y forzarlos a ejecutar malware. El ataque inicia mediante correos electrónicos de phishing que se hacen pasar por Booking[.]com, informando falsamente sobre un reembolso elevado debido a la cancelación de una reserva, generando un sentido de urgencia en las víctimas.

Los usuarios son redirigidos a un sitio web fraudulento que imita la interfaz legítima de Booking.com, donde se muestra un mensaje de error falso. Al hacer clic en el botón "Actualizar", se despliega un BSOD falso en pantalla completa, instruyendo a la víctima a ejecutar un comando malicioso de PowerShell.

Dicho comando descarga y compila DCRAT, una herramienta de acceso remoto que permite a los atacantes tomar control total del sistema comprometido. Una vez activo, el malware es capaz de robar información sensible, propagarse dentro de la red corporativa e implementar cargas maliciosas adicionales, como mineros de criptomonedas, ampliando significativamente el impacto del ataque y comprometiendo la seguridad del entorno afectado.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.002 – Phishing: Enlace Malicioso	Envío de correos electrónicos que suplantando a Booking[.]com, inducen urgencia por un reembolso falso y redirigen a sitios web fraudulentos.
TA0002: Ejecución	T1059.001 – PowerShell	Ejecución de comandos maliciosos de PowerShell inducidos mediante pantallas BSOD falsas para descargar y compilar DCRAT.
TA0005: Evasión de Defensa	T1036 – Masquerading	Uso de sitios web falsos y pantallas BSOD simuladas para engañar al usuario y evadir controles de seguridad tradicionales.
TA0005: Evasión de Defensa	T1497 – Virtualization/Sandbox Evasion	Comportamiento condicionado a la interacción del usuario para reducir la detección en entornos automatizados.
TA0003: Persistencia	T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys	DCRAT establece persistencia para ejecutarse automáticamente tras el reinicio del sistema comprometido.
TA0008: Movimiento Lateral	T1021 – Remote Services	El RAT facilita el movimiento lateral dentro de la red corporativa del hotel.
TA0010: Exfiltración	T1041 – Exfiltración Sobre Canal C2	Robo y envío de información sensible hacia servidores controlados por los atacantes.
TA0040: Impacto	T1496 – Resource Hijacking	Implementación de cargas adicionales como mineros de criptomonedas que degradan el rendimiento de los sistemas.

Recomendaciones:

- **Concientización de usuarios:** Capacitar al personal para que identifique correos de phishing que generen urgencia (reembolsos, cancelaciones) y para que nunca ejecuten comandos de PowerShell por indicación de ventanas emergentes o sitios web.
- **Restricción de PowerShell:** Implementar políticas de seguridad (AppLocker o WDAC) para limitar la ejecución de PowerShell a usuarios autorizados y bloquear su uso en contextos no administrativos.
- **Protección del navegador:** Restringir la navegación a sitios no confiables y bloquear dominios falsos que imiten plataformas legítimas como Booking[.]com mediante filtrado web y DNS seguro.
- **Monitoreo de endpoints:** Utilizar soluciones EDR/XDR para detectar comportamientos anómalos, como la ejecución de PowerShell desde el navegador o la descarga y compilación dinámica de malware.
- **Segmentación de red:** Limitar el movimiento lateral mediante segmentación de red y controles de acceso, reduciendo el impacto en caso de compromiso inicial.

 ALTA

2. Vulnerabilidades

2.1 Vulnerabilidad crítica en n8n permite la ejecución de comandos del sistema

Se ha identificado una vulnerabilidad de seguridad crítica en n8n, una plataforma de automatización de flujos de trabajo de código abierto ampliamente utilizada, que permite a usuarios autenticados ejecutar comandos arbitrarios del sistema operativo en el servidor donde se ejecuta la aplicación.

La vulnerabilidad, identificada como CVE-2025-68668 y calificada con un puntaje CVSS de 9,9, afecta a las versiones 1.0.0 hasta la 1.111.0. El fallo se origina en el mecanismo de protección del nodo de código Python, el cual utiliza Pyodide para la ejecución de scripts. Debido a una validación insuficiente, los atacantes pueden crear o modificar flujos de trabajo maliciosos y ejecutar comandos del sistema con los mismos privilegios del proceso n8n.

Este comportamiento representa un riesgo elevado, ya que permite el control total del host, facilitando la instalación de malware adicional, la exfiltración de información sensible o el movimiento lateral dentro del entorno corporativo. El ataque requiere credenciales válidas, pero no privilegios administrativos adicionales dentro de la plataforma.

El proveedor ha mitigado la vulnerabilidad en la versión n8n 2.0.0, la cual introduce una implementación nativa de Python basada en un ejecutor de tareas, mejorando significativamente el aislamiento y la seguridad del entorno de ejecución.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1078 – Cuentas Válidas	Uso de credenciales legítimas de usuarios autenticados en n8n para acceder a la plataforma y crear o modificar flujos de trabajo maliciosos.
TA0002: Ejecución	T1059.006 – Command and Scripting Interpreter: Python	Ejecución de comandos arbitrarios del sistema mediante la explotación del nodo de código Python basado en Pyodide.
TA0004: Escalada de Privilegios	T1068 – Explotación para Escalada de Privilegios	Aprovechamiento de la ejecución de código con los privilegios del proceso n8n para obtener control avanzado sobre el host.
TA0005: Evasión de Defensa	T1622 – Debugger Evasion / Sandbox Evasion	Ejecución de comandos a través de flujos legítimos de n8n, evitando detecciones basadas en comportamiento tradicional.
TA0008: Movimiento Lateral	T1021 – Servicios Remotos	Uso del acceso al sistema comprometido para interactuar con otros servicios o sistemas accesibles desde el host de n8n.
TA0010: Exfiltración	T1041 – Exfiltración sobre Canal C2	Posible extracción de información sensible mediante comandos del sistema o scripts Python ejecutados desde el flujo comprometido.
TA0040: Impacto	T1485 – Destrucción de Datos	Ejecución de comandos del sistema que pueden afectar la disponibilidad e integridad de los datos y servicios automatizados.

Recomendaciones

- **Actualización inmediata (Patch Management):** Migrar de forma prioritaria a n8n versión 2.0.0 o superior, ya que corrige la ejecución arbitraria de comandos mediante el nodo Python vulnerable.
- **Control de accesos y privilegios:** Restringir la creación y modificación de flujos de trabajo solo a usuarios estrictamente necesarios, aplicando el principio de mínimo privilegio.
- **Monitoreo de actividad sospechosa:** Implementar EDR/XDR en el host de n8n para detectar ejecuciones anómalas de comandos del sistema iniciadas por procesos de automatización.
- **Segmentación del entorno:** Aislar el servidor de n8n de otros sistemas críticos para reducir el impacto y movimiento lateral en caso de compromiso.
- **Auditoría de flujos existentes:** Revisar y validar todos los flujos de trabajo activos en busca de nodos Python o ejecuciones no autorizadas.

 ALTA

2.2 Vulnerabilidades críticas en paquetes npm exponen servidores a ejecución remota de código

Se han identificado vulnerabilidades críticas en paquetes ampliamente utilizados del ecosistema npm, las cuales representan un alto riesgo para aplicaciones web y servicios backend que dependen de estas bibliotecas.

La primera vulnerabilidad afecta al paquete `@adonisjs/bodyparser`, rastreada como CVE-2026-21440, con una puntuación CVSS de 9,2. Esta falla permite a atacantes remotos escribir archivos arbitrarios en el servidor mediante un problema de recorrido de ruta en la función `MultipartFile().move`. Las versiones afectadas incluyen AdonisJS hasta la 10.1.1 y 11.0.0-next.5. La explotación exitosa podría derivar en ejecución remota de código (RCE) al sobrescribir archivos sensibles del sistema. El problema ha sido corregido en versiones posteriores del framework.⁴

De forma paralela, se detectó otra vulnerabilidad crítica en el paquete `jsPDF`, identificada como CVE-2025-68428, también con una puntuación CVSS de 9,2. Esta falla permite a los atacantes acceder a rutas no saneadas y recuperar el contenido de archivos arbitrarios, comprometiendo la confidencialidad de la información. La vulnerabilidad fue mitigada en la versión 4.0.0 de `jsPDF`.

Ambas vulnerabilidades representan un riesgo significativo para entornos productivos, especialmente aquellos expuestos a Internet, y subrayan la importancia de una gestión activa de dependencias y parches dentro de la cadena de suministro de software.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Explotación de vulnerabilidades de recorrido de ruta en aplicaciones web que utilizan paquetes npm vulnerables expuestos a Internet.
TA0002: Ejecución	T1059.007 – JavaScript	Ejecución de código malicioso aprovechando la escritura de archivos arbitrarios o la carga de dependencias manipuladas en entornos Node.js.
TA0003: Persistencia	T1505.003 – Web Shell	Inserción de archivos maliciosos persistentes en el servidor mediante la sobrescritura de archivos de la aplicación o del backend.
TA0004: Escalada de Privilegios	T1068 – Exploitation for Privilege Escalation	Uso de archivos sobrescritos para ejecutar procesos con privilegios elevados del servicio Node.js.
TA0005: Evasión de Defensa	T1036 – Masquerading	Uso de archivos con nombres y rutas legítimas para evadir controles de seguridad y revisiones manuales.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Acceso y extracción de información sensible desde archivos arbitrarios leídos en el sistema afectado.
TA0040: Impacto	T1499 – Endpoint Denial of Service	Alteración o eliminación de archivos críticos de la aplicación que provoca caída del servicio o corrupción de datos.

Recomendaciones:

- **Gestión de vulnerabilidades y parches:** Establecer un proceso continuo de identificación, evaluación y remediación de vulnerabilidades, aplicando parches de seguridad según criticidad (CVSS), priorizando activos críticos y sistemas expuestos a Internet.
- **Control de la cadena de suministro de software:** Implementar herramientas de análisis de dependencias (SCA) para identificar vulnerabilidades en paquetes npm utilizados por aplicaciones web y servicios backend, integrando estos controles dentro del ciclo de desarrollo (CI/CD).
- **Hardening de aplicaciones Node.js:** Restringir permisos de escritura y acceso al sistema de archivos para los procesos de la aplicación, minimizando el impacto de posibles ataques de Path Traversal o escritura de archivos arbitrarios.
- **Monitoreo de comportamiento y detección de explotación:** Supervisar logs de aplicaciones y tráfico HTTP para detectar patrones anómalos asociados a intentos de carga de archivos maliciosos, acceso a rutas no autorizadas o explotación de vulnerabilidades conocidas.
- **Segmentación y aislamiento de servicios:** Aislar aplicaciones web y servicios backend en entornos segmentados, evitando que un compromiso por ejecución remota de código permita el movimiento lateral hacia otros sistemas críticos.
- **Protección de servidores y runtime:** Implementar soluciones EDR/XDR en servidores que ejecuten aplicaciones Node.js para detectar ejecución de código malicioso, cargas no autorizadas y mecanismos de persistencia posteriores a la explotación.



2.3 QNAP corrige vulnerabilidades críticas en sistemas NAS que permiten ejecución de comandos y acceso no autorizado a archivos

QNAP abordó recientemente múltiples vulnerabilidades críticas de seguridad que afectan a sus sistemas de almacenamiento conectados a la red, las cuales podrían ser explotadas por atacantes remotos para ejecutar comandos no autorizados o acceder a información sensible.

La vulnerabilidad más grave corresponde a una inyección SQL, identificada como CVE-2025-59387, que afecta al Servicio de recuperación de aplicaciones múltiples (MARS). Esta falla permite a un atacante ejecutar comandos no autorizados dentro del sistema afectado, comprometiendo la integridad y seguridad del dispositivo. El problema fue corregido a partir de la versión 1.2.1.1686, actualmente renombrada como HDP para WordPress.

De manera paralela, se identificó una vulnerabilidad de recorrido de ruta en Qfiling, registrada como CVE-2025-59384, que permite el acceso no autorizado a archivos confidenciales del sistema. Esta falla fue mitigada en la versión 3.13.1 y posteriores.

Adicionalmente, QNAP reportó una vulnerabilidad de recorrido de ruta de menor gravedad que afecta a Qfinder Pro, Qsync y QVPN Device Client para macOS, lo que podría facilitar accesos indebidos en entornos específicos. Asimismo, se corrigieron vulnerabilidades adicionales en el Centro de licencias de QNAP, incluyendo una lectura fuera de límites y un desbordamiento de búfer, fortaleciendo la seguridad general de su ecosistema de software.

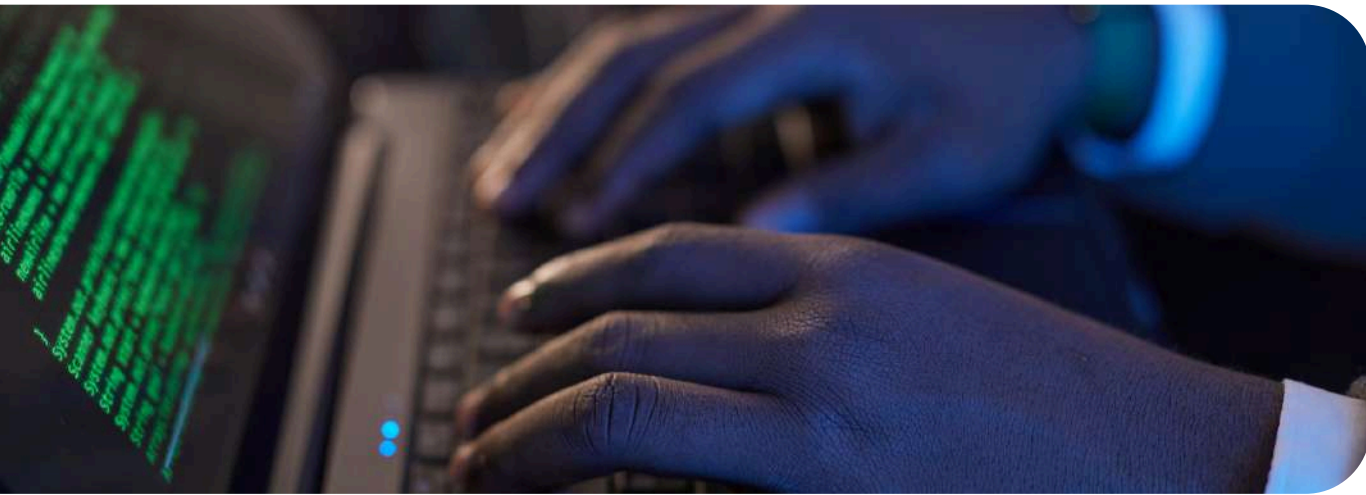
Estas vulnerabilidades representan un riesgo significativo para entornos empresariales y domésticos, especialmente aquellos con dispositivos NAS expuestos a Internet, reforzando la necesidad de aplicar parches de seguridad de manera oportuna y mantener una gestión activa de actualizaciones.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Explotación de servicios expuestos en dispositivos QNAP NAS mediante vulnerabilidades de inyección SQL y recorrido de ruta en aplicaciones como MARS y Qfiling.
TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Ejecución de comandos no autorizados en el sistema NAS tras explotar la vulnerabilidad de inyección SQL (CVE-2025-59387).
TA0003: Persistencia	T1505.003 – Server Software Component: Web Shell	Posible instalación de web shells o scripts persistentes aprovechando el acceso obtenido a través de aplicaciones vulnerables.
TA0004: Escalada de Privilegios	T1068 – Exploitation for Privilege Escalation	Aprovechamiento de fallas en servicios internos del NAS para elevar privilegios tras el acceso inicial.
TA0005: Evasión de Defensa	T1562.001 – Impair Defenses: Disable or Modify Tools	Modificación o desactivación de mecanismos de seguridad y registros del sistema NAS para evitar detección.
TA0006: Acceso a Credenciales	T1555 – Credentials from Password Stores	Acceso a archivos de configuración o almacenes de credenciales expuestos mediante fallas de recorrido de ruta.
TA0009: Recolección	T1005 – Data from Local System	Lectura y recopilación de archivos confidenciales almacenados en el NAS explotando vulnerabilidades de path traversal.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Extracción de información sensible desde el NAS hacia infraestructura controlada por el atacante.
TA0040: Impacto	T1485 – Data Destruction	Posible eliminación, modificación o corrupción de archivos críticos almacenados en el sistema NAS comprometido.

Recomendaciones

- **Patch Management y actualización de firmware:** Aplicar de forma inmediata las actualizaciones de seguridad publicadas por QNAP, priorizando MARS, Qfiling, Qfinder Pro, Qsync y QVPN Device Client. Asegurar que todos los dispositivos NAS en producción ejecuten versiones parcheadas y soportadas.
- **Reducción de superficie de ataque:** Restringir la exposición de servicios QNAP a Internet, deshabilitando aplicaciones innecesarias y limitando el acceso administrativo únicamente a redes internas o mediante VPN segura.
- **Segmentación de red:** Ubicar los dispositivos NAS en segmentos de red aislados, controlando el acceso únicamente a servidores y usuarios autorizados, con el fin de limitar movimientos laterales ante una posible intrusión.
- **Monitorización y detección temprana:** Implementar monitoreo continuo de logs y tráfico hacia/desde los dispositivos QNAP para detectar patrones anómalos, intentos de explotación de inyección SQL, accesos a rutas no autorizadas o ejecución de comandos sospechosos.
- **Endurecimiento de aplicaciones y servicios:** Aplicar principios de hardening en servicios NAS, incluyendo control de permisos, deshabilitación de cuentas por defecto, uso de autenticación multifactor (MFA) y validación estricta de entradas en aplicaciones web integradas.
- **Protección y respaldo de la información:** Mantener copias de seguridad periódicas, cifradas y fuera de línea (offline/immutable backups) para garantizar la recuperación ante incidentes de destrucción o corrupción de datos.

 CRÍTICA

2.4 Vulnerabilidad Crítica CVE-2026-24858 en Fortinet – Bypass de Autenticación SSO Bajo Explotación Activa

Fortinet lanzó actualizaciones de seguridad para corregir una vulnerabilidad crítica de autenticación en su sistema FortiOS que estaba siendo explotada activamente en el mundo real. La falla permite el bypass de autenticación SSO de FortiCloud, lo que podría permitir que un atacante con una cuenta FortiCloud y un dispositivo registrado inicie sesión en dispositivos de otros clientes si la función SSO está habilitada. La vulnerabilidad también afecta a otros productos como FortiManager y FortiAnalyzer.

Fortinet confirmó que actores maliciosos estaban abusando de esta ruta de ataque para acceder sin autenticación, crear cuentas administrativas locales persistentes y realizar cambios de configuración, incluidos accesos VPN no autorizados y extracción de configuraciones de firewall. La explotación de esta vulnerabilidad fue lo suficientemente seria como para que la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. Agregara la CVE-2026-24858 a su Catálogo de Vulnerabilidades Conocidas Explotadas, con una fecha límite de remediación para agencias federales.

Fortinet tomó medidas temporales deshabilitando el servicio FortiCloud SSO a nivel de nube para frenar los abusos, e instó a los usuarios a actualizar inmediatamente a versiones parcheadas y verificar posibles compromisos en sus dispositivos.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Explotación activa de la vulnerabilidad SSO para obtener acceso administrativo sin autenticación correcta.
TA0003: Persistencia	T1543.003 – Create or Modify System Process	Creación de cuentas administrativas locales persistentes dentro del dispositivo comprometido.
TA0004: Evasión de Defensa	T1550.003 – Use Alternate Authentication Material	Abuso de la autenticación SSO de FortiCloud como vía alternativa para omitir controles de seguridad estándar.
TA0011: Comando y Control	T1071.001 – Application Layer Protocol: Web Traffic	Comunicación con la plataforma para ejecutar cambios de configuración y escalado de acceso.
TA0040: Impacto	T1489 – Service Stop	Deshabilitación y reconfiguración del servicio SSO para mitigar ataques, alterando el funcionamiento esperado del sistema

Recomendaciones

- Actualizar inmediatamente todos los dispositivos FortiOS, FortiManager, FortiAnalyzer, FortiProxy y FortiWeb a las versiones que corrigen CVE-2026-24858 para restaurar funciones SSO seguras.
- Auditar configuraciones y credenciales de administración para detectar cambios no autorizados y rotar contraseñas si se sospecha compromiso.
- Revisar acceso FortiCloud SSO y, de ser innecesario, deshabilitarlo temporalmente hasta aplicar parches.
- Implementar controles de acceso restringido a interfaces de administración, restringir acceso sólo desde redes internas o IPs de confianza.
- Monitorear registros de eventos y alertas de seguridad para detectar patrones inusuales de inicio de sesión o creación de cuentas administrativas.
- Correlacionar los eventos de firewall, sistema y autenticación para identificar signos tempranos de explotación o movimiento lateral.

 ALTA

3 . Phishing

3.1 Campaña de Phishing de Múltiples Etapas Dirigida a Usuarios en Rusia con Amnesia RAT y Ransomware

En enero de 2026, Fortinet FortiGuard Labs detectó una campaña masiva de phishing de múltiples etapas que apuntó principalmente a usuarios en Rusia, desplegando tanto Amnesia RAT como ransomware tras deshabilitar las defensas del sistema afectado. Esta campaña combina ingeniería social, abuso de servicios legítimos en la nube y técnicas para inutilizar Microsoft Defender, logrando un compromiso profundo de los sistemas infectados.

Los atacantes distribuían archivos ZIP con documentos que aparentaban ser rutinarios y un acceso directo malicioso con doble extensión diseñado para engañar al usuario. Al ejecutarse, este acceso directo lanzaba un script de PowerShell desde GitHub que establecía una fase inicial de compromiso y, posteriormente, permitía la descarga y ejecución de cargas maliciosas, incluyendo Amnesia RAT para control remoto y un ransomware derivado de la familia Hakuna Matata para cifrar datos. Además, se utilizó la herramienta "defendnot" para forzar la desactivación de Microsoft Defender y así evadir detecciones.

La campaña exhibe un flujo de ataque sofisticado que demuestra la eficacia de combinar vectores tradicionales con la explotación de servicios legítimos para hospedar y ejecutar etapas adicionales del ataque, complicando la detección temprana y respuesta.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.002 – Phishing: Link/ Archivo	Distribución de archivos ZIP con documentos de ingeniería social y accesos directos maliciosos para inducir ejecución.
TA0002: Ejecución	T1204.002 – User Execution: Malicious File	Ejecución de atajos que inician scripts de PowerShell descargados desde GitHub.
TA0004: Evasión de Defensa	T1562.001 – Disable or Modify Tools	Uso de “defendnot” y PowerShell para deshabilitar Microsoft Defender y evitar detecciones.
TA0005: Persistencia	T1547.001 – Registry Run Keys	Configuración de mecanismos para mantener presencia a través del RAT.
TA0011: Comando y Control	T1071.001 – Application Layer Protocol: Web Traffic	Comunicación de RAT y exfiltración de datos en HTTPS camuflado como tráfico legítimo.
TA0040: Impacto	T1486 – Data Encrypted for Impact	Despliegue de ransomware para cifrar activos y forzar pago/impactar operaciones.

Recomendaciones

- Monitorear y analizar actividad de PowerShell y descargas desde servicios en la nube, correlacionando con alertas de comportamiento anómalo.
- Capacitar de forma continua al personal sobre campañas que utilizan documentos empresariales aparentemente legítimos como señuelos y enseñar signos de archivos con dobles extensiones u otros engaños.
- Correlacionar registros de red, endpoint y autenticación para detectar etapas tempranas de compromiso y responder rápidamente a comportamientos inusuales.
- Implementar y reforzar filtros de correo y antiphishing para bloquear archivos adjuntos sospechosos y campañas con ingeniería social avanzada
- Habilitar MFA en todos los accesos críticos y asegurar que las protecciones de seguridad no puedan ser fácilmente desactivadas por scripts o herramientas externas.



3.2 Campaña de Phishing Multi-Etapa Adversary-in-the-Middle (AiTM) y BEC Dirigida al Sector Energético

En enero de 2026, Microsoft advirtió sobre una campaña sofisticada de phishing de múltiples etapas con técnicas Adversary-in-the-Middle combinada con Business Email Compromise que se dirigió a organizaciones del sector energético. La campaña abusó de servicios legítimos como SharePoint para alojar enlaces de phishing, envió correos desde cuentas previamente comprometidas y creó reglas maliciosas en bandejas de entrada para mantener persistencia y evadir la detección del usuario.

El ataque comenzó con correos electrónicos aparentemente legítimos provenientes de organizaciones confiables comprometidas, que incluían enlaces a supuestos documentos SharePoint. Estos enlaces redirigían a las víctimas a páginas de captura de credenciales falsas, permitiendo a los atacantes robar sesiones y credenciales de Microsoft 365. Con acceso a las cuentas, los adversarios crearon reglas automatizadas para borrar correos, marcar mensajes como leídos y enviar phishing adicional desde las propias cuentas comprometidas, extendiendo así el alcance de la campaña.

En un caso observado, un solo buzón comprometido fue utilizado para enviar más de 600 correos maliciosos a contactos internos y externos de la víctima. Microsoft señaló que restablecer contraseñas no es suficiente para mitigar este tipo de ataque: es crucial revocar cookies de sesión activas y eliminar reglas sospechosas creadas por el atacante para detener la persistencia.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.002 – Phishing: Spearphishing Link	Uso de correos desde cuentas legítimas comprometidas con enlaces a SharePoint para inducir a las víctimas a autenticarse.
TA0002: Ejecución	T1204.002 – User Execution: Malicious Link	Redirección a páginas de phishing para capturar credenciales de Microsoft 365.
TA0004: Evasión de Defensa	T1137.001 – Office 365 Exchange Rules	Creación de reglas en bandejas de entrada para borrar correos y ocultar actividad del atacante.
TA0011: Comando y Control	T1071.001 – Application Layer Protocol: Web Traffic	Comunicación y exfiltración de credenciales a través de tráfico web cifrado camuflado como legítimo.
TA0040: Impacto	T1586 – Phishing	Uso de cuentas comprometidas para ampliar la campaña de phishing y escalar acceso dentro de la organización.

Recomendaciones

- Implementar MFA resistente a phishing para reducir la efectividad de credenciales robadas durante ataques AiTM.
- Revisar y monitorear reglas de bandeja de entrada sospechosas, especialmente aquellas que borran o redirigen correos sin interacción explícita del usuario.
- Configurar políticas de acceso condicional y evaluación continua que reduzcan el riesgo de acceso persistente tras el robo de credenciales o sesiones.
- Utilizar soluciones de antiphishing avanzadas que analicen enlaces y páginas visitadas, detectando redireccionamientos maliciosos incluso si están alojados en servicios confiables.
- Capacitar al personal para identificar engaños que abusan de plataformas legítimas y reforzar protocolos de reporte de correos sospechosos.



4. Adversarios

4.1 Konni implementa malware PowerShell generado por IA en campaña “Operación Poseidón”

El grupo de amenazas norcoreano Konni ha sido observado utilizando malware basado en PowerShell generado mediante inteligencia artificial en una campaña de espionaje dirigida contra desarrolladores de blockchain en Japón, Australia e India. Esta operación, denominada Operación Poseidón, tiene como objetivo comprometer entornos de desarrollo para obtener acceso persistente y control remoto de los sistemas afectados.

La campaña se inicia a través de ingeniería social, empleando correos electrónicos maliciosos que se hacen pasar por avisos financieros o comunicados relacionados con inversiones, diseñados para inducir a las víctimas a descargar archivos ZIP maliciosos. Dichos archivos contienen un acceso directo de Windows que ejecuta de forma encubierta un cargador PowerShell integrado.

Una vez ejecutado, el cargador despliega una puerta trasera denominada EndRAT, la cual establece persistencia en el sistema comprometido y permite a los atacantes ejecutar comandos remotos, recolectar información sensible y ampliar el acceso dentro del entorno de desarrollo. El uso de scripts PowerShell generados por IA contribuye a variar dinámicamente el código, dificultando la detección mediante firmas tradicionales.

Además, la operación incorpora técnicas de evasión de detección y ofuscación, lo que reduce la visibilidad del malware en soluciones de seguridad y complica su análisis. Esta combinación de ingeniería social avanzada, automatización mediante IA y malware sin archivos persistentes tradicionales refleja un alto nivel de sofisticación, posicionando a Konni como un adversario relevante en el panorama de amenazas de enero de 2026.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.001 – Phishing: Adjuntos Maliciosos	Envío de correos de ingeniería social que simulan avisos financieros o comunicados de inversión, induciendo a las víctimas a descargar archivos ZIP maliciosos.
TA0002: Ejecución	T1059.001 – PowerShell	Ejecución encubierta de scripts PowerShell mediante archivos de acceso directo que cargan malware generado con apoyo de IA.
TA0003: Persistencia	T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Implementación de mecanismos de persistencia para mantener el acceso tras reinicios del sistema comprometido.
TA0005: Evasión de Defensa	T1027 – Obfuscated/Encrypted Files or Information	Uso de scripts PowerShell ofuscados y variantes dinámicas generadas por IA para evadir detección basada en firmas.
TA0005: Evasión de Defensa	T1562.001 – Disable or Modify Tools	Reducción de visibilidad frente a soluciones de seguridad mediante técnicas de evasión y ejecución sin archivos persistentes tradicionales.
TA0011: Comando y Control	T1059.001 – PowerShell (C2)	Comunicación con infraestructura de comando y control para recibir instrucciones remotas y ejecutar comandos en el sistema infectado.
TA0009: Recolección	T1005 – Data from Local System	Recolección de información sensible desde entornos de desarrollo comprometidos, incluyendo datos técnicos y credenciales.
TA0008: Movimiento Lateral	T1021 – Remote Services	Expansión del acceso dentro del entorno de desarrollo una vez obtenida persistencia inicial.

Recomendaciones:

- **Concientización y control de correo electrónico:** Fortalecer la capacitación de desarrolladores y personal técnico frente a campañas de ingeniería social, enfocándose en la detección de correos que simulan avisos financieros o inversiones. Implementar filtros avanzados para bloquear adjuntos ZIP y archivos .LNK provenientes de fuentes externas no confiables.
- **Restricción de ejecución de PowerShell:** Aplicar políticas de control de aplicaciones para limitar la ejecución de scripts PowerShell no firmados, especialmente en estaciones de trabajo de desarrollo y entornos críticos.
- **Protección de endpoints (EDR/XDR):** Implementar soluciones EDR/XDR con capacidades de detección de comportamiento que identifiquen ejecución anómala de PowerShell, cargas en memoria y variación dinámica de código generada por IA.
- **Seguridad en entornos de desarrollo:** Aislar los entornos de desarrollo de la red corporativa mediante segmentación, restringiendo el acceso a recursos críticos y reduciendo el impacto del movimiento lateral en caso de compromiso.
- **Monitoreo y respuesta automatizada:** Integrar capacidades SOAR para ejecutar playbooks automáticos que permitan el aislamiento inmediato del endpoint afectado, la revocación de credenciales comprometidas y el bloqueo de indicadores asociados a la campaña Konni.

 ALTA

4.2 Campaña Cibernética RedKitten (Vinculada a Irán) Apunta a ONG y Activistas de Derechos Humanos

Se identificó una campaña de ciberespionaje sofisticada denominada RedKitten, atribuida a un actor de amenazas que habla farsi y está alineado con intereses estatales iraníes. Esta campaña está dirigida a organizaciones no gubernamentales dedicadas a derechos humanos y a activistas que documentan abusos recientes, aprovechando el contexto de protestas y represión en Irán a finales de 2025.

Los atacantes utilizan correos con archivos comprimidos que contienen documentos Excel con macros maliciosos disfrazados de listas de víctimas de protestas. Cuando los usuarios habilitan las macros, se ejecuta un dropper que instala un backdoor modular llamado SloppyMIO, el cual puede ejecutar comandos arbitrarios, recolectar y exfiltrar archivos, descargar cargas adicionales y establecer persistencia mediante tareas programadas. La campaña abusa de servicios legítimos como GitHub y Google Drive para distribución de módulos, y usa Telegram para su canal de comando y control.

Se ha observado además que partes del código VBA muestran indicios de haber sido generadas con modelos de lenguaje de IA, lo que evidencia una tendencia creciente de adversarios que adoptan herramientas automatizadas para generar malware más rápidamente.

Objetivos principales:

- Recolectar información sensible de ONG, activistas de derechos humanos y periodistas, especialmente datos relacionados con protestas, víctimas, contactos y documentación.
- Exfiltrar archivos y comunicaciones que puedan servir para vigilancia, identificación y seguimiento de personas u organizaciones críticas del gobierno iraní.
- Obtener inteligencia estratégica, no dinero. A diferencia del ransomware o fraude, aquí no buscan extorsión, sino información y control.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.002 – Phishing: Link/Archivo	Distribución de ZIPs con documentos Excel maliciosos como señuelo para inducir a la víctima a habilitar macros.
TA0002: Ejecución	T1204.002 – User Execution: Malicious File	Macro VBA malicioso que actúa como dropper para instalar la implantación SloppyMIO cuando se habilitan.
TA0004: Evasión de Defensa	T1027 – Obfuscated Files or Information	Uso de VBA ofuscado y servicios legítimos para ocultar la carga útil maliciosa.
TA0011: Comando y Control	T1071.001 – Application Layer Protocol: Web Traffic	Comunicación con el operador a través de Telegram Bot API para recibir órdenes y enviar datos exfiltrados.
TA0003: Persistencia	T1547.001 – Registry Run Keys / T1053.003 – Scheduled Task	Creación de tareas programadas para ejecutar cargas persistentes y módulos adicionales.
TA0040: Impacto	T1486 – Data Encrypted for Impact	Robo y exfiltración de archivos sensibles, ejecución remota de comandos que comprometen la confidencialidad e integridad de los sistemas

Recomendaciones

- Educar y concienciar a equipos sobre correos con contenidos relacionados a derechos humanos o crisis internacionales que contengan archivos adjuntos antes de habilitar macros.
- Configurar filtros de correo electrónico avanzados y sandboxing para examinar anexos sospechosos.
- Restringir la habilitación de macros por política corporativa y sólo permitir las en archivos firmados o provenientes de fuentes de confianza.
- Implementar monitoreo de C2 y detección de tráfico inusual, especialmente hacia plataformas como Telegram, GitHub o Google Drive.
- Asegurar mecanismos de seguridad en endpoints con EDR y correlación de eventos para detectar comportamientos anómalos como creación de tareas programadas no autorizadas.
- Segmentar y proteger datos sensibles de ONG y activistas con controles de acceso fuerte y cifrado para reducir el impacto de una posible exfiltración de datos.

5. Indicadores de Compromiso

5.1 Direcciones IP

198[.]50[.]117[.]55
 45[.]148[.]10[.]121
 84[.]53[.]229[.]179
 39[.]35[.]221[.]85
 152[.]32[.]170[.]230
 146[.]190[.]27[.]211
 165[.]154[.]162[.]102
 45[.]148[.]10[.]141
 120[.]27[.]154[.]152
 218[.]248[.]19[.]102
 80[.]94[.]92[.]182

5.2 Dominio

- leaseweb[.]com
- adsl-229-179.elcom[.]ru
- ptcl.net[.]pk
- ucloud[.]cn
- digitalocean[.]com
- alibabacloud[.]com
- sancharnet[.]in
- dmzhost[.]co
- hosting25.tronicsat[.]com
- ttcldata[.]net
- unmanaged[.]uk

5.3 Hashes

49980dbb7cd975261b6e19b49fd2f6c6f7
 80e7831624ec5e8b728a14ab928336

95e905566ec8556ffbb9b909719ae505d
 66a53c33513434366d354f7248462a1

8b5d5b7d29590f6700afe2300561b4d62
 466038a000c5f328b93ce2129a21a82

3406a744f369fa8743761b568a5904853
 eeb12ba732bda92478330b280fa3283

93a20b4053f77a503602816a0c36cd7e4
 4eb2c66c50ffcf688dadecdd0596d1d7

9b3ac5f7f52633479bcc2d5d853ab38bb
 326ed52a7b9acca47a80cfb403909bd

9b026b8f0b5e85aec2143e4688b8e6bef
 572605dfed562af0acd35d160a8b2ab

94456a74ff20f531e6fc9b8c43086e5af01
 98f550edf699415bda40c6a7f9f18

8fbfa523a9ea5d080c945ed43bbacbdb
 9a3846a55d6cd0e3c1b3f2fb0a00e074

3cacdf6058f10e1040cle4a72c71bfe06d5
 d54ebec0aa5063933d62362b3ellc

35f42e78296f3e8635799d75a697e44a0
 b3a2d1d53dd9507d29f05fcc54922eb

2faf6730d2a2f1d41b62763050900e9b82f
 b7e62df352624645b9064abc847ac

6. Fuentes

- 6.1 <https://urlhaus.abuse.ch/browse.php?search=pinaton.ru&page=1>
- 6.2 <https://www.abuseipdb.com/check/>
- 6.3 <https://www.cyware.com/resources/threat-briefings/daily-threat-briefing/cyware-daily-threat-intelligence-january-23-2026>
- 6.4 <https://www.cyware.com/resources/threat-briefings/daily-threat-briefing/cyware-daily-threat-intelligence-january-06-2026>
- 6.5 <https://www.cyware.com/resources/threat-briefings/daily-threat-briefing/cyware-daily-threat-intelligence-january-20-2026>
- 6.6 <https://www.cyware.com/resources/threat-briefings/daily-threat-briefing/cyware-daily-threat-intelligence-january-05-2026>
- 6.7 <https://thehackernews.com/2026/01/microsoft-flags-multi-stage-aitm.html>
- 6.8 <https://thehackernews.com/2026/01/multi-stage-phishing-campaign-targets.html>
- 6.9 <https://thehackernews.com/2026/01/fortinet-patches-cve-2026-24858-after.html>
- 6.10 <https://thehackernews.com/2026/01/iran-linked-redkitten-cyber-campaign.html>