



GS PERÚ

Software - Security & Services

Empresas

BOLETÍN CIBERSEGURIDAD

Mayo - 2026





LA SEGURIDAD ABARCA TODO EL ECOSISTEMA DIGITAL

Mayo de 2026 consolida una realidad ineludible: el riesgo cibernético ha trascendido los límites internos para distribuirse por todo el ecosistema digital. Los atacantes priorizan comprometer a terceros, dependencias de código abierto y plataformas SaaS globales para impactar a múltiples organizaciones de forma simultánea.

La superficie de ataque abarca ahora cada integración externa de la operación diaria. El envenenamiento de cadenas de suministro mediante paquetes maliciosos (en npm, PyPI y Crates.io), el secuestro de aplicaciones y las vulnerabilidades de día cero son vectores estratégicos para el espionaje, el robo de secretos y el despliegue de ransomware.

Los enfoques de seguridad perimetral resultan insuficientes frente a un escenario donde un solo compromiso provoca un impacto en cascada a nivel sectorial. Para mitigar estos riesgos, las organizaciones deben desarrollar una visibilidad estricta sobre sus dependencias, aislar proactivamente los entornos que interactúan con Inteligencia Artificial y prepararse de manera coordinada para incidentes extorsivos.

La explotación activa de componentes críticos como Microsoft Defender o plataformas como Langflow refleja claramente esta transformación. Ante amenazas masivas impulsadas por botnets resilientes y campañas de Phishing-as-a-Service con IA, la respuesta automatizada y el monitoreo exhaustivo de identidades han dejado de ser diferenciadores tecnológicos para convertirse en requisitos básicos y obligatorios de resiliencia empresarial.

ÍNDICE



1. MALWARE 04

- 1.1 Paquete malicioso de NPM roba archivos de usuarios del directorio de Claude AI
- 1.2 Ataque de ransomware a la plataforma Canvas por ShinyHunters impacta masivamente al sector educativo de EE. UU.
- 1.3 El malware "Remus Stealer" despliega sofisticadas técnicas de evasión y robo de datos en Windows
- 1.4 CloudZ RAT explota Windows Phone Link para robar credenciales y códigos OTP
- 1.5 La campaña multinivel TrapDoor distribuye malware de robo y credenciales a través de npm, PyPI y Crates.io



2. VULNERABILIDADES 14

- 2.1 Explotación de vulnerabilidad Zero-Day en PAN-OS Captive Portal permite ejecución remota de código sin autenticación
- 2.2 Vulnerabilidades activamente explotadas en Langflow y Trend Micro Apex One
- 2.3 Explotación activa de vulnerabilidades en Microsoft Defender permite escalada a SYSTEM y denegación de servicio



3. PHISHING 20

- 3.1 La IA y Phishing-as-a-Service impulsan el aumento masivo de ataques por correo electrónico
- 3.2 Alertan por estafas digitales y transmisiones falsas con IA a semanas del Mundial 2026
- 3.3 Incremento del fraude digital en Perú: phishing, smishing y vulnerabilidades por robo de dispositivos móviles



4. ADVERSARIOS 26

- 4.1 Desmantelamiento coordinado de botnet "Glassworm" dirigida a desarrolladores
- 4.2 Grupo "Deface Perú" vulnera el sistema y emite falsas alertas de tsunami y fraude electoral
- 4.3 Hackers irrumpen en Canvas y afectan a universidades en plena semana de exámenes



5. INDICADORES DE COMPROMISO 32

- 5.1 Direcciones IP
- 5.2 Dominios
- 5.3 Hashes



6. FUENTES 34

1. Malware

ALTA

1.1 [ALTA] Paquete malicioso de NPM roba archivos del directorio de usuarios de Claude AI



Investigadores de OX Security descubrieron un nuevo paquete malicioso en el registro npm denominado "mouse5212-super-formatter" (campana Malware-Slop), el cual se disfraza de una utilidad de sincronización interna pero está diseñado para robar información del directorio local /mnt/user-data de la herramienta Claude AI de Anthropic.

Durante la fase de postinstalación, el malware utiliza tokens de acceso de GitHub encontrados en el entorno de la víctima, o un token codificado por defecto, para autenticarse y subir recursivamente todos los archivos a repositorios controlados por el atacante, ocultando la actividad mediante un falso registro de red.

Este incidente, en el que el atacante filtró accidentalmente su propio token privado de GitHub, evidencia una tendencia creciente de actores de amenazas que utilizan IA para generar código malicioso "descuidado", omitiendo prácticas básicas de seguridad operativa (OPSEC).

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

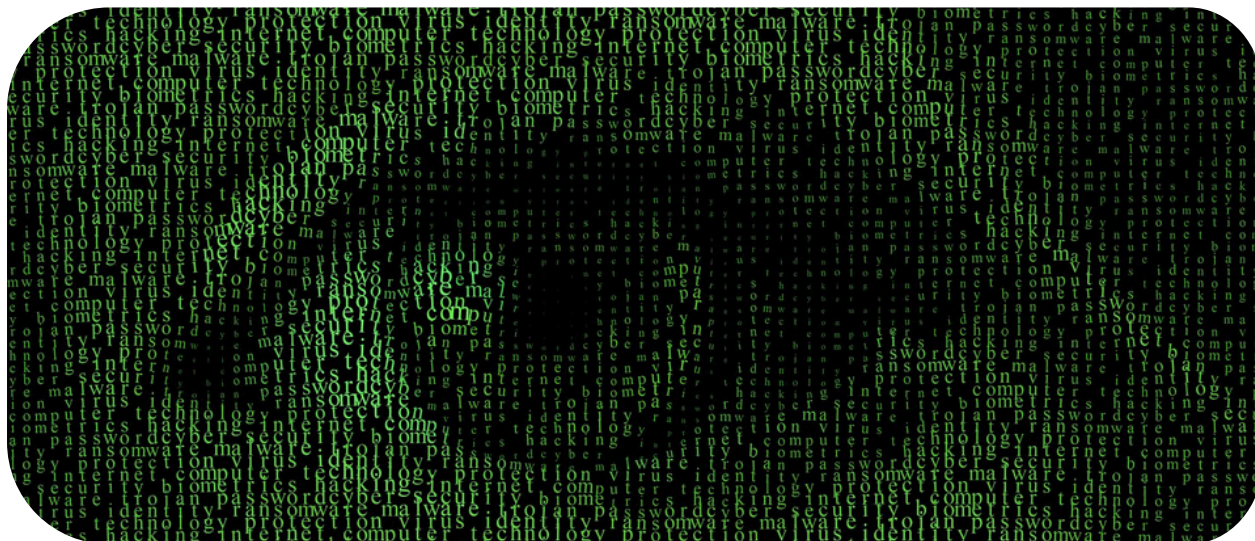
Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1195.001 – Supply Chain Compromise: Compromise Software Dependencies and Development Tools	Publicación del paquete malicioso "mouse5212-super-formatter" en el registro público de dependencias de npm.
TA0002: Ejecución	T1059.007 – Command and Scripting Interpreter: JavaScript	Ejecución automática de la lógica de autenticación y robo de información durante el gancho de instalación postinstall del paquete.
TA0006: Acceso a Credenciales	T1552 – Unsecured Credentials	Búsqueda y recolección de tokens de acceso personales (PAT) de GitHub almacenados en el entorno operativo del desarrollador afectado.
TA0009: Recolección	T1005 – Data from Local System	Rastreo exhaustivo y copia de archivos contenidos en la ruta crítica /mnt/user-data vinculada a la actividad del asistente Claude AI.
TA0010: Exfiltración	T1567.001 – Exfiltration to Code Repository	Envío y sincronización estructurada de los archivos locales sustraídos hacia una cuenta de GitHub externa controlada por el atacante.

Recomendaciones

- **Bloqueo de Paquetes en el Registro Local:** Restringir de forma inmediata la descarga o resolución del paquete "mouse5212-super-formatter" en los gestores de dependencias internos de la organización y auditar si se encuentra presente en los entornos de desarrollo locales.
- **Aislamiento de Volúmenes de IA:** Configurar los contenedores o entornos donde se ejecutan herramientas de desarrollo de IA para que directorios compartidos o de almacenamiento temporal de datos de usuario (como /mnt/user-data) tengan permisos estrictamente limitados y aislados de procesos externos de Node.js/npm.
- **Rotación y Auditoría de Tokens de GitHub:** Forzar la invalidación y el cambio inmediato de cualquier token de acceso personal a repositorios si se sospecha que una estación de trabajo ejecutó la instalación del paquete comprometido durante su ventana de disponibilidad.
- **Detección de Archivos de Configuración Ofuscados:** Utilizar herramientas de monitorización en los terminales (EDR) para identificar scripts de dependencias que generen logs falsos de red o conexiones salientes inesperadas hacia las APIs de repositorios de código abiertos durante la construcción de proyectos.

CRÍTICA

1.2 [CRÍTICA] Ataque de ransomware a la plataforma Canvas por ShinyHunters impacta masivamente al sector educativo de EE. UU.



El 12 de mayo de 2026, se reportó un masivo ataque de ransomware y robo de datos vinculado al grupo de amenazas ShinyHunters contra el sistema de gestión de aprendizaje (LMS) Canvas, provocando interrupciones generalizadas en múltiples instituciones educativas de Estados Unidos.

El incidente ha sido catalogado como uno de los robos de datos más significativos en el ámbito educativo hasta la fecha, evidenciando de forma alarmante el riesgo sistémico que genera la dependencia concentrada de un sector entero en un número reducido de proveedores de Software como Servicio (SaaS).

Debido a que ShinyHunters acostumbra operar a gran escala liberando y monetizando la información de manera progresiva, se anticipa que la lista de organizaciones afectadas continúe expandiéndose conforme avancen las investigaciones, lo que obliga a las instituciones a reevaluar urgentemente la resiliencia y seguridad de su cadena de suministro digital.

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

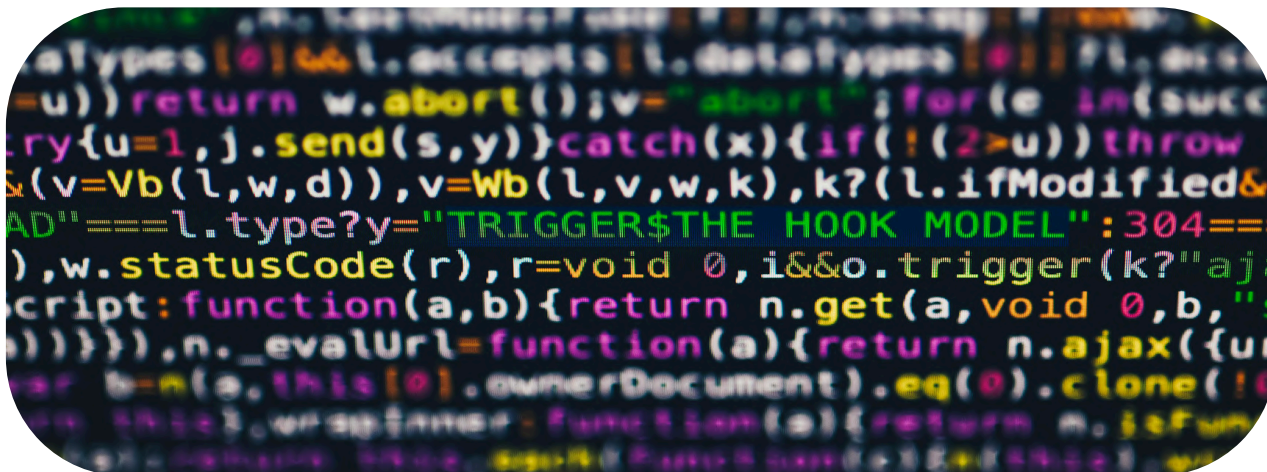
Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1195 – Supply Chain Compromise / T1078 – Valid Accounts	Compromiso en cascada a nivel sectorial mediante la intrusión y explotación de debilidades en una plataforma SaaS ampliamente adoptada.
TA0002: Exfiltración	T1567 – Exfiltration Over Web Service	Extracción masiva de datos confidenciales correspondientes a estudiantes, docentes e instituciones globales para su posterior monetización.
TA0003: Impacto	T1486 – Data Encrypted for Impact / T1489 – Service Stop	Despliegue de ransomware que interrumpe la continuidad operativa de los sistemas centrales de enseñanza y gestión educativa.

Recomendaciones

- Auditoría de Cuentas y Accesos: Revisar minuciosamente las cuentas de usuario, configuraciones de permisos e integraciones de terceros junto con los accesos a través de APIs en la plataforma Canvas.
- Rotación Preventiva de Credenciales: Implementar la rotación de contraseñas y tokens de acceso donde se considere apropiado para neutralizar el uso de identidades potencialmente filtradas.
- Monitoreo Proactivo de Eventos: Incrementar los niveles de supervisión y detección en búsqueda de comportamientos inusuales o actividades anómalas en el entorno educativo y SaaS de la organización.
- Activación de Planes de Respuesta: Asegurar que los canales internos de reporte de incidentes estén claros para el personal y que los planes de comunicación ante crisis estén listos en caso de confirmarse una afectación directa.
- Evaluación de Compromiso (Compromise Assessment): En caso de sospechar que el incidente haya servido como vector para vulnerar sistemas internos adyacentes, realizar una evaluación formal de compromiso para obtener certeza y seguridad técnica.
- Reforzamiento de Controles de Identidad: Robustecer los mecanismos de autenticación (como la aplicación rigurosa de MFA) y exigir auditorías de seguridad y contratos de aseguramiento claros a los proveedores tecnológicos estratégicos

ALTA

1.3 [ALTA] El malware "Remus Stealer" despliega sofisticadas técnicas de evasión y robo de datos en Windows



El análisis de muestras del malware "Remus Stealer" ha revelado un sofisticado patrón de ejecución en múltiples etapas diseñado para operar de manera encubierta en entornos Windows.

La amenaza se inicia mediante un cargador a nivel de usuario que despliega componentes secundarios en directorios temporales, utilizando de forma temprana la Interfaz de Línea de Comandos de Administración de Windows (WMI) a través de `wmiprvse.exe` y `wmiadap.exe` para perfilar el sistema y detectar entornos virtualizados o sandboxes.

Para evadir el control del usuario, eleva sus privilegios abusando de manejadores COM auto-elevados (específicamente modificando rutas del registro asociadas al CLSID 4590F811-1D3A-11D0891F-00AA004B2E24) e interfiere activamente con mecanismos de inspección de seguridad como `amsi.dll`.

Finalmente, mediante el desempaquetado en memoria, la ofuscación de cadenas y la inyección de procesos, logra ocultarse dentro de procesos legítimos del sistema para acceder a carpetas del escritorio y datos de Microsoft Outlook, preparando canales de comunicación encubiertos y conexiones hacia el dominio `cheapoca.biz` en puertos no estándar.

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

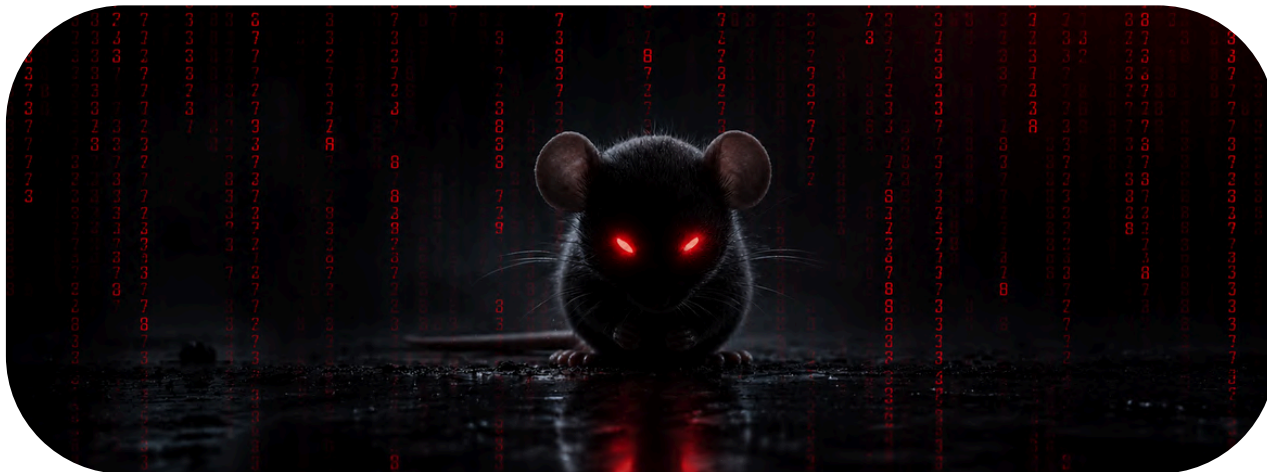
Táctico	Técnicas / Subtécnicas	
TA0002: Ejecución	T1059 – Command and Scripting Interpreter / T1047 – Windows Management Instrumentation	Uso de un cargador por etapas para ejecutar componentes desde carpetas temporales e invocación de herramientas WMI para realizar consultas en ROOT\CIMV2.
TA0004: Escalada de Privilegios	T1546.015 – Event Triggered Execution: Component Object Model Hijacking	Manipulación del flujo de ejecución del sistema mediante la explotación del Moniker de Elevación COM y el abuso de controladores auto-elevados en el registro.
TA0005: Evasión de Defensas	T1027 – Obfuscated Files or Information / T1055 – Process Injection	Uso de descodificación en tiempo de ejecución para evitar firmas estáticas en disco e inyección de código funcional dentro de procesos legítimos de Windows. Interferencia con amsi.dll y claves de compatibilidad de aplicaciones.
TA0007: Descubrimiento	T1082 – System Information Discovery / T1497 – Virtualization/Sandbox Evasion	Enumeración de las características del sistema operativo y controladores de video para realizar un reconocimiento del entorno físico o virtual antes de proceder con la infección.
TA0009: Recolección	T1005 – Data from Local System	Rastreo y exploración de rutas accesibles por el usuario, apuntando específicamente a ubicaciones del escritorio y carpetas de datos de correo electrónico (Outlook).
TA0011: Comando y Control	T1071.001 – Application Layer Protocol: Web Traffic / T1102 – Web Service	Descifrado dinámico de indicadores de red en memoria para establecer comunicaciones encubiertas con el dominio cheapoca.biz a través de puertos no estándar (500, 5003–5007) y tráfico UDP hacia la IP 162.159.36.2:53.

Recomendaciones

- **Monitoreo de Actividad WMI:** Implementar reglas de detección basadas en comportamiento para identificar consultas inusuales o masivas a las clases de ROOT\CIMV2 ejecutadas por procesos del sistema como wmiiprvse.exe y wmiadap.exe
- **Protección del Registro y Objetos COM:** Monitorear y restringir modificaciones no autorizadas en las claves del registro que involucren configuraciones de manejadores de Elevación COM, prestando especial atención al CLSID 4590F811-1D3A-11D0891F-00AA004B2E24
- **Detección de Inyección en Memoria (EDR/XDR):** Desplegar soluciones de seguridad avanzadas en los endpoints capaces de identificar técnicas de vaciado de procesos (process hollowing), desempaquetado de código en tiempo de ejecución y manipulaciones de la interfaz AMSI (amsi.dll).
- **Control de Red de Puertos No Estándar:** Configurar los firewalls perimetrales y de host para bloquear o alertar sobre conexiones salientes dirigidas a puertos inusuales (como el rango 5003–5007) y aplicar filtrado DNS estricto contra el dominio identificado cheapoca.biz y la dirección IP 162.159.36.2.
- **Evaluación de Compromiso (Compromise Assessment):** En caso de sospechar que el incidente haya servido como vector para vulnerar sistemas internos adyacentes, realizar una evaluación formal de compromiso para obtener certeza y seguridad técnica.
- **Políticas de Acceso a Archivos de Usuario:** Monitorear el acceso concurrente o la lectura masiva de archivos confidenciales dentro del perfil de usuario, especialmente en directorios de almacenamiento de bases de datos de aplicaciones de mensajería o correo como Microsoft Outlook.

ALTA

1.4 [ALTA] CloudZ RAT explota Windows Phone Link para robar credenciales y códigos OTP



El 6 de mayo investigadores de Cisco Talos han revelado una nueva campaña de intrusión, que utiliza el troyano de acceso remoto CloudZ en conjunto con un plugin indocumentado llamado "Pheno" para robar credenciales y contraseñas de un solo uso (OTP).

La novedad de este ataque radica en que secuestra la aplicación legítima Microsoft Phone Link (integrada en Windows 10 y 11) para monitorear e interceptar datos móviles confidenciales, como mensajes SMS, leyendo directamente la base de datos SQLite del programa en la PC. Esto permite a los atacantes eludir la autenticación de dos factores (2FA) sin necesidad de infectar o comprometer el dispositivo móvil de la víctima.

La cadena de ataque inicia con un ejecutable falso de ConnectWise ScreenConnect que establece persistencia mediante una tarea programada de PowerShell, la cual descarga un cargador .NET responsable de desplegar el RAT modular CloudZ, establecer comunicaciones cifradas con el servidor C2 y ejecutar comandos para la exfiltración de datos.

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

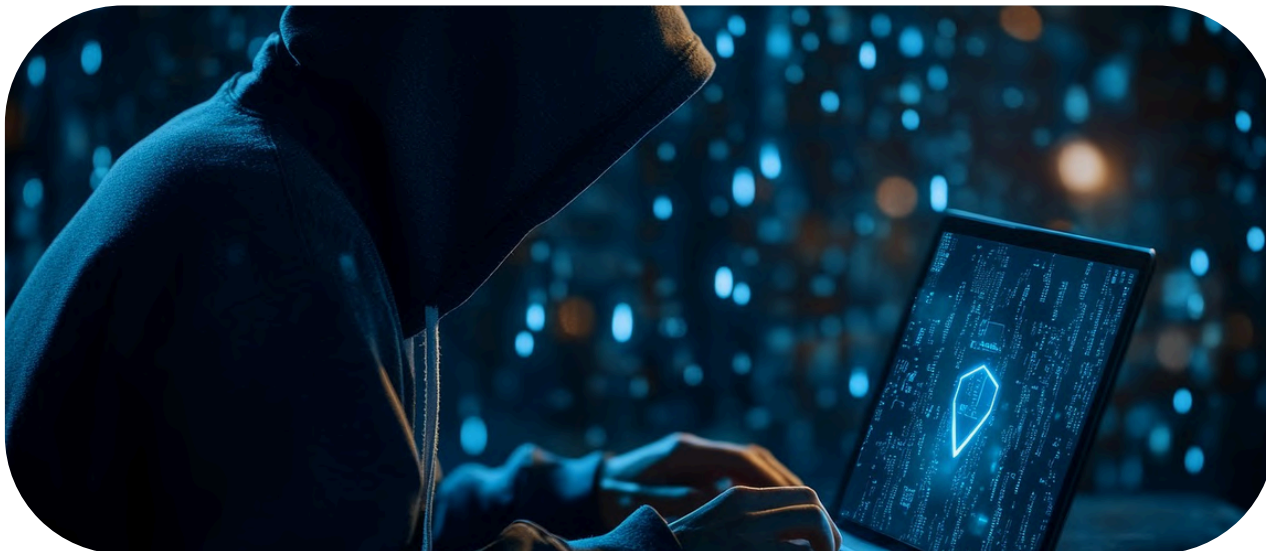
Táctico	Técnicas / Subtécnicas	
TA0002: Ejecución	T1059.001 – Command and Scripting Interpreter: PowerShell	Uso de un script de PowerShell incrustado para ejecutar el cargador malicioso basado en .NET en la máquina de la víctima.
TA0003: Persistencia	T1053.005 – Scheduled Task/Job: Scheduled Task	Creación de tareas programadas en Windows para garantizar la ejecución continua del dropper inicial.
TA0005: Evasión de Defensas	T1036.005 – Masquerading: Match Legitimate Name or Location	Suplantación de software legítimo mediante la distribución de un instalador falso de la herramienta ConnectWise ScreenConnect.
TA0009: Recolección	T1005 – Data from Local System	Uso del plugin personalizado "Pheno" para monitorear los procesos de Microsoft Phone Link y extraer información confidencial (como SMS y OTPs) desde su base de datos SQLite local.
TA0011: Comando y Control	T1132.001 – Data Encoding: Standard Encoding	Establecimiento de conexiones a través de sockets cifrados con el C2 y recepción de comandos codificados en Base64 (ej. recolección de metadatos, carga de plugins, grabación de pantalla).

Recomendaciones

- **Auditoría de Aplicaciones Vinculadas:** Evaluar la necesidad comercial de utilizar Microsoft Phone Link en entornos corporativos. Si no es estrictamente necesario, deshabilitar la aplicación mediante Políticas de Grupo (GPO) para reducir drásticamente la superficie de ataque y evitar la sincronización de mensajes confidenciales en los equipos de escritorio.
- **Monitoreo de Tareas Programadas y PowerShell:** Configurar alertas en plataformas SIEM o EDR para detectar la creación de tareas programadas inusuales, prestando especial atención a aquellas que invoquen scripts de PowerShell de forma oculta o desde rutas temporales.
- **Detección de Suplantación de Identidad:** Vigilar la descarga y ejecución de herramientas de administración remota (RMM) como ConnectWise ScreenConnect. Verificar sistemáticamente las firmas digitales y los hashes de los instaladores para identificar binarios falsificados.
- **Protección de Bases de Datos Locales:** Implementar reglas de monitoreo para detectar accesos inusuales o concurrentes a archivos de bases de datos locales (como los archivos SQLite utilizados por Phone Link o navegadores web) por parte de procesos no reconocidos o plugins inyectados.
- **Refuerzo de Mecanismos MFA:** Dado que esta amenaza permite interceptar códigos enviados por SMS y eludir la autenticación de dos factores (2FA), se recomienda migrar hacia métodos de autenticación más robustos, como llaves de seguridad físicas (FIDO2/WebAuthn) o aplicaciones de autenticación (TOTP) que no dependan de la sincronización de mensajes de texto en la PC.

CRÍTICA

1.5 [CRÍTICA] La campaña multinivel TrapDoor distribuye malware de robo de credenciales a través de npm, PyPI y Crates.io



El 25 de mayo de 2026, investigadores de Socket reportaron una sofisticada campaña coordinada de ataque a la cadena de suministro, denominada TrapDoor, que ha afectado simultáneamente a los ecosistemas de npm, PyPI y Crates.io a través de más de 34 paquetes maliciosos distribuidos en 384 versiones.

Registrada inicialmente el 22 de mayo de 2026, la operación está dirigida de forma específica a desarrolladores de las comunidades de criptomonedas, DeFi, Solana e Inteligencia Artificial (IA).

Los paquetes maliciosos suplantán herramientas legítimas de configuración, IA o flujos web3, ejecutando vectores de ataque adaptados a cada ecosistema (scripts build.rs en Rust, ganchos postinstall en npm y ejecución al importar en Python) para sustraer secretos de desarrollo, billeteras cripto, claves SSH, variables de entorno y credenciales de la nube.

Una de las características más disruptivas de la campaña es la introducción de archivos de configuración. cursorrules y CLAUDE.md mediante solicitudes de extracción (pull requests) falsas en repositorios populares de IA (como langchain o langflow).

Estos archivos contienen instrucciones ocultas diseñadas para engañar a los asistentes de codificación de IA, manipulando las herramientas para que ejecuten un supuesto "escaneo de seguridad" que, en realidad, descubre y exfiltra los secretos locales del desarrollador.

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

Táctico	Técnicas / Subtécnicas	
TA0001: Acceso Inicial	T1195.001 – Supply Chain Compromise: Compromise Software Dependencies and Development Tools	Publicación coordinada y masiva de paquetes maliciosos con nombres engañosos orientados a crypto e IA en npm, PyPI y Crates.io.
TA0002: Ejecución	T1204.002 – User Execution: Malicious File T1059.007 – JavaScript	Uso de ganchos postinstall, scripts build.rs y delegación a través de comandos de node (node -e) desde Python para descargar y ejecutar cargas de JavaScript remotas.
TA0003: Persistencia	T1547 – Boot or Logon Autostart Execution T1137 – Office Application Startup	Implantación de persistencia local a través de servicios de systemd, ganchos de Git, tareas programadas (cron) y la manipulación de archivos de instrucciones de IA corporativas (.cursorrules, CLAUDE.md).
TA0006: Acceso a Credenciales	T1552 – Unsecured Credentials	Escaneo automático de secretos locales y validación proactiva de tokens mediante llamadas directas a las APIs oficiales de AWS y GitHub.
TA0008: Movimiento Lateral	T1021.004 – Remote Services: SSH	Intentos automatizados de propagación y movimiento lateral a través de la red corporativa aprovechando las llaves SSH descubiertas en la máquina comprometida.
TA0010: Exfiltración	T1567.001 – Exfiltration to Code Repository	Recolección de almacenes de claves locales, cifrado mediante operaciones XOR de clave fija y exfiltración de los datos hacia GitHub Gists y dominios externos administrados.

Recomendaciones

- **Bloqueo Inmediato de Repositorios de Carga:** Restringir las conexiones de red salientes hacia el dominio de GitHub Pages del atacante (ddjidd564.github[.]io), utilizado para alojar de forma externa la lógica maliciosa de ejecución en Python.
- **Auditoría de Contribuciones Externas y Pull Requests:** Inspeccionar rigurosamente cualquier Pull Request entrante en proyectos de la organización, especialmente aquellas que modifiquen o introduzcan de manera inesperada archivos de contexto o reglas para IA como .cursorrules o CLAUDE.md.
- **Revisión de Dependencias Cruzadas:** Verificar que los entornos locales no tengan instalados paquetes sospechosos incluidos en la lista de alerta, tales como move-analyzer-build (Crates.io), crypto-credential-scanner o defi-env-auditor (npm), y cryptowallet-safety (PyPI).
- **Monitoreo de APIs de Proveedores de Nube:** Establecer alertas ante llamadas inusuales de validación de tokens o actividades de aprovisionamiento en las APIs de AWS y GitHub originadas desde estaciones de trabajo de desarrolladores individuales.
- **Aislamiento de Flujos de Construcción:** Configurar los entornos de desarrollo para deshabilitar o restringir la ejecución automática de scripts de compilación de dependencias de terceros (como deshabilitar scripts postinstall en npm mediante ignore-scripts=true y verificar la procedencia de los scripts build.rs de Rust)

2. Vulnerabilidades

CRÍTICA

2.1 [CRÍTICA] Explotación de vulnerabilidad Zero-Day en PAN-OS Captive Portal permite ejecución remota de código sin autenticación



El 6 de mayo de 2026, se alertó sobre la explotación activa de la vulnerabilidad CVE-2026-0300, un fallo de desbordamiento de búfer (buffer overflow) en el servicio de Portal de Autenticación User-ID (Captive Portal) del software PAN-OS de Palo Alto Networks, que afecta a los cortafuegos de las series PA y VM.

La vulnerabilidad permite a un atacante remoto no autenticado ejecutar código arbitrario con privilegios de root mediante el envío de paquetes de red especialmente diseñados. Unit 42 está rastreando al grupo de amenazas posiblemente respaldado por un Estado, CL-STA-1132, el cual ha logrado inyectar código malicioso (shellcode) en procesos de trabajadores de nginx.

Las actividades de post-explotación documentadas incluyen el robo de credenciales de la cuenta de servicio del firewall para realizar la enumeración de Active Directory, ataques de inundación SAML para forzar la conmutación por error hacia un segundo dispositivo y comprometerlo, el despliegue de herramientas de tunelización de código abierto (EarthWorm y ReverseSocks5) y la eliminación sistemática de registros y evidencias de compromiso.

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

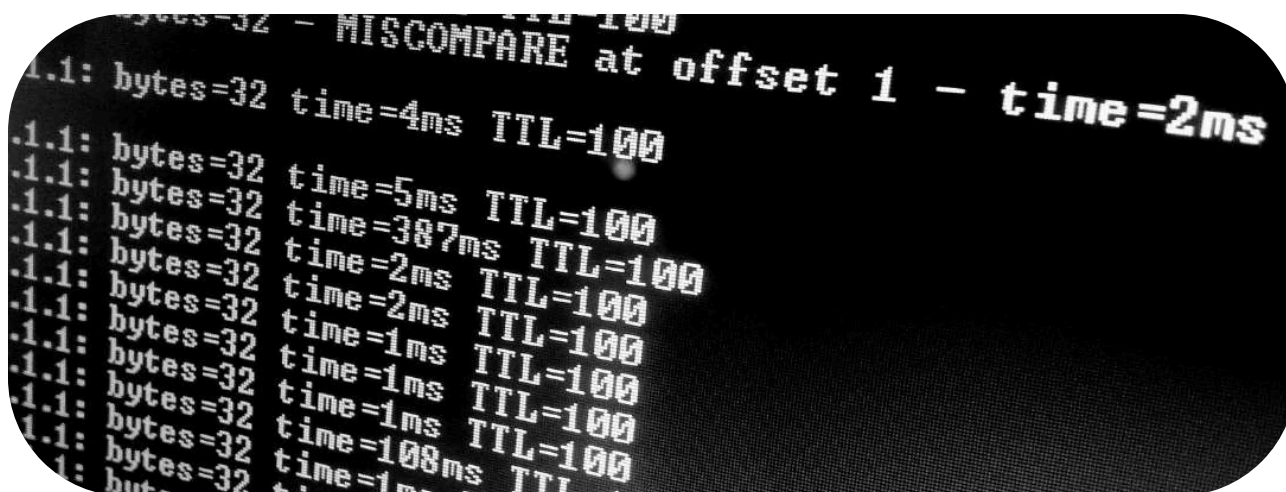
Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Explotación de la vulnerabilidad de día cero CVE-2026-0300 en el Portal de Autenticación expuesto a redes no confiables o a Internet.
TA0002: Ejecución	T1203 – Exploitation for Client Execution T1059 – Command and Scripting Interpreter	Inyección exitosa de shellcode en el proceso de un trabajador de nginx y ejecución de scripts/binarios con privilegios de root.
TA0005: Evasión de Defensas	T1070 – Indicator Removal on Host	Limpieza sistemática de registros del sistema mediante el borrado de mensajes del kernel, eliminación de registros de fallas de nginx, remoción de archivos core dump y eliminación del binario SUID utilizado para escalada.
TA0007: Descubrimiento	T1087.002 – Account Discovery: Domain Account T1482 – Domain Trust Discovery	Enumeración de Active Directory apuntando a la raíz del dominio y a DomainDnsZones utilizando credenciales legítimas sustraídas del firewall.
TA0008: Movimiento Lateral	T1090.003 – Proxy: Connection Proxy	Despliegue de las herramientas EarthWorm y ReverseSocks5 para establecer servidores proxy y túneles SOCKS5 inversos que evaden los controles perimetrales y permiten pivotar hacia la red interna.

Recomendaciones

- **Restricción de Accesos al Portal:** Limitar el acceso al Portal de Autenticación User-ID exclusivamente a zonas e IPs internas de confianza, asegurándose de que la interfaz no sea accesible de forma directa desde el Internet público o redes no seguras.
- **Deshabilitar Páginas de Respuesta:** Desactivar la opción de "Páginas de Respuesta" en el Perfil de Gestión de Interfaz vinculado a cualquier interfaz de Capa 3 por donde pueda ingresar tráfico no confiable o proveniente de Internet.
- **Desactivación del Servicio:** Si las operaciones de la organización no requieren el uso del Portal de Autenticación User-ID, se recomienda proceder a su desactivación completa como medida de reducción de la superficie de ataque.
- **Activación de Firmas de Prevención de Amenazas:** Para los clientes con suscripciones activas de Advanced Threat Prevention, habilitar de forma estricta el ID de Amenaza 510019 (disponible en las versiones de contenido de Aplicaciones y Amenazas 9097-10022 o superiores). Es importante considerar que las capacidades de decodificación requieren contar con PAN-OS 11.1 o una versión posterior.
- **Monitoreo de Indicadores de Red y Host:** Implementar reglas de detección para identificar conexiones salientes sospechosas hacia los dominios e IPs reportados, como 146.70.100[.]69 (utilizado para la descarga de herramientas) y solicitudes con cadenas de Agente de Usuario (User Agent) anómalas.
- **Auditoría de Procesos e Inyecciones:** Examinar de manera exhaustiva las estaciones de trabajo y firewalls en busca de anomalías en procesos como nginx, la presencia de archivos binarios de tunelización en directorios temporales (/var/tmp/linuxap, /tmp/R5, etc.) o manipulación de privilegios SUID.

CRÍTICA

2.2 [CRÍTICA] Vulnerabilidades activamente explotadas en Langflow y Trend Micro Apex One



El 21 de mayo de 2026, CISA incorporó dos vulnerabilidades al catálogo KEV tras confirmarse su explotación activa. La primera, CVE-2025-34291 (CVSS 9.4), afecta a la plataforma de agentes de IA Langflow.

Se trata de un fallo de validación de origen (combinación de políticas CORS excesivamente permisivas y falta de protección CSRF) que permite la ejecución remota de código (RCE). El mayor riesgo de esta vulnerabilidad es el "compromiso en cascada": los atacantes pueden robar todos los tokens y API-keys del espacio de trabajo para penetrar en los diversos servicios SaaS y cloud integrados.

Por otro lado, la CVE-2026-34926 (CVSS 6.7) es una vulnerabilidad de salto de directorio (directory traversal) en las versiones locales de Trend Micro Apex One. Permite a un atacante (que ya posea credenciales administrativas previas) modificar las tablas de actualización del servidor para inyectar código malicioso, utilizando la propia solución de seguridad para distribuir malware a todos los agentes conectados, en un claro escenario de ataque a la cadena de suministro interna.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application T1078 – Valid Accounts	Explotación del API de Langflow mediante omisión de autenticación (CORS/CSRF). En el caso de Apex One, uso de credenciales administrativas previamente comprometidas.
TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Aprovechamiento del endpoint de Langflow, diseñado originalmente para lanzar agentes de usuario, convirtiéndolo en un vector para ejecutar código arbitrario.
TA0006: Acceso a Credenciales	T1552 – Unsecured Credentials	Extracción masiva de tokens de acceso y API-keys almacenados en los espacios de trabajo comprometidos de la plataforma Langflow.
TA0008: Movimiento Lateral	T1021 – Remote Services	Abuso de las credenciales y tokens extraídos para pivotar y comprometer de forma subyacente otros servicios SaaS o en la nube.
TA0040: Impacto	T1554 – Compromise Client Software Binary	Modificación de la tabla de despliegue en el servidor de Trend Micro Apex One para forzar la distribución de código malicioso hacia los agentes de los endpoints.

Recomendaciones

- Actualización Prioritaria: Aplicar los parches de seguridad emitidos por los fabricantes para ambas plataformas de manera inmediata (CISA establece como fecha límite el 4 de junio de 2026).
- Rotación Masiva de Secretos (Langflow): Tras aplicar el parche, es estrictamente necesario realizar una rotación completa de todas las API-keys, tokens de acceso y credenciales almacenadas en los espacios de trabajo, asumiendo que ya han sido expuestos.
- Restricción de API (Langflow): Mientras se gestiona la actualización, aislar y restringir el acceso de red a las instancias de Langflow, bloqueando específicamente las conexiones externas no confiables dirigidas hacia su API.
- Auditoría de Cuentas (Apex One): Dado que la explotación en Trend Micro requiere de acceso previo, se debe realizar una auditoría exhaustiva de las cuentas administrativas del servidor para identificar el vector de intrusión inicial.
- Verificación de Integridad (Apex One): Revisar las tablas de despliegue en el servidor central y analizar los registros de acceso en busca de inyecciones de código, alteraciones o actividades anómalas distribuidas hacia las estaciones de trabajo.

CRÍTICA

2.3 [CRÍTICA] Explotación activa de vulnerabilidades en Microsoft Defender permite escalada a SYSTEM y denegación de servicio



Microsoft ha confirmado la explotación activa de dos vulnerabilidades en Microsoft Defender (CVE-2026-41091 y CVE-2026-45498), las cuales fueron añadidas por CISA a su catálogo de Vulnerabilidades Conocidas Explotadas (KEV) con fecha límite de mitigación obligatoria para el 3 de junio de 2026.

La falla más grave, CVE-2026-41091 (CVSS 7.8), es un error de resolución incorrecta de enlaces simbólicos (link following) que permite a un atacante local autorizado redirigir las operaciones del antivirus hacia archivos arbitrarios y obtener el control total del equipo con privilegios SYSTEM.

Por otro lado, la vulnerabilidad CVE-2026-45498 (CVSS 4.0) permite provocar una denegación de servicio (DoS). La explotación simultánea de ambas sugiere el uso de cadenas de ataque donde primero se desactiva la protección mediante el DoS y luego se ejecuta la escalada de privilegios.

Adicionalmente, CISA incluyó en el catálogo KEV cinco vulnerabilidades históricas (2008-2010) de Microsoft y Adobe, indicando que los actores de amenazas están atacando activamente sistemas obsoletos en entornos industriales e infraestructuras críticas.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0004: Escalada de Privilegios	T1068 – Exploitation for Privilege Escalation	Explotación de la vulnerabilidad CVE-2026-41091 manipulando la resolución de enlaces simbólicos antes del acceso a archivos para alcanzar el nivel de SYSTEM.
TA0040: Impacto	T1489 – Service Stop	Uso de la vulnerabilidad CVE-2026-45498 para causar una denegación de servicio (DoS) en los componentes de Microsoft Defender.
TA0005: Evasión de Defensas	T1562.001 – Impair Defenses: Disable or Modify Tools	Desactivación de la protección antivirus (mediante DoS) como fase preparatoria antes del despliegue de malware o la explotación de otros fallos.
TA0008: Movimiento Lateral	T1021 – Remote Services	Aprovechamiento potencial de los privilegios SYSTEM obtenidos en estaciones de trabajo de dominio para extraer credenciales y comprometer controladores de dominio.

Recomendaciones

- **Verificación Manual de Versiones:** Comprobar localmente desde la aplicación Seguridad de Windows (Configuración → Acerca de) que la versión del cliente antimalware (Antimalware Client Version) sea 1.1.26040.8, 4.18.26040.7 o superior.
- **Asegurar Actualizaciones Automáticas:** En entornos corporativos con gestión centralizada (WSUS, SCCM, Intune), verificar exhaustivamente que las directivas no estén bloqueando la actualización automática de firmas y del motor Microsoft Malware Protection Engine.
- **Priorización de Activos Críticos:** Dada la explotación activa y el plazo límite del 3 de junio de 2026 establecido por CISA, parchear de inmediato todos los sistemas con Microsoft Defender activo, dando máxima prioridad a servidores y estaciones de trabajo con acceso a datos sensibles o cuentas privilegiadas.flow, bloqueando específicamente las conexiones externas no confiables dirigidas hacia su API.
- **Auditoría de Sistemas Obsoletos:** Evaluar la infraestructura heredada (legacy), especialmente en entornos industriales, para aplicar controles compensatorios o parches contra las vulnerabilidades históricas (2008-2010) recientemente reactivadas por atacantes.
- **Confirmación de Estado en Antivirus de Terceros:** Aunque los sistemas con soluciones antivirus de terceros (donde Defender está deshabilitado) no son vulnerables, se recomienda verificar el estado real del servicio en todos los endpoints para descartar configuraciones incorrectas que expongan la red.

3. Phishing

ALTA

3.1 [ALTA] La IA y el Phishing-as-a-Service impulsan el aumento masivo de ataques por correo electrónico



El "Email Threats Report 2026" publicado por Barracuda Networks revela que la ingeniería social impulsada por Inteligencia Artificial y el modelo de Phishing-as-a-Service (PhaaS) están acelerando drásticamente el volumen y la tasa de éxito de los ciberataques.

Según el análisis de más de 3.000 millones de correos electrónicos, los atacantes están migrando de los tradicionales archivos adjuntos maliciosos hacia métodos de distribución más sigilosos, tales como cargas útiles basadas en URL y códigos QR incrustados en documentos PDF (presentes en el 70% de los PDFs maliciosos detectados).

Además, el 34% de las empresas experimenta al menos un incidente de usurpación de cuentas (Account Takeover) al mes, permitiendo a los ciberdelincuentes eludir las defensas tradicionales al enviar mensajes convincentes desde bandejas de entrada legítimas comprometidas.

Con el 90% de las campañas masivas utilizando kits de PhaaS, el correo electrónico se consolida como la primera línea de defensa de la identidad y la continuidad del negocio.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.002 – Phishing: Spearphishing Link / T1566.001 – Spearphishing Attachment	Envío de correos electrónicos de ingeniería social mejorados con IA que incluyen enlaces maliciosos o archivos adjuntos HTML comprometedores (más del 10% de los adjuntos HTML son maliciosos).
TA0001: Acceso Inicial	T1078 – Valid Accounts	Usurpación de cuentas de correo electrónico corporativas para eludir los filtros de seguridad perimetral y distribuir ataques internamente o hacia socios de confianza.
TA0002: Ejecución	T1204.002 – User Execution: Malicious File	Interacción del usuario al abrir documentos PDF aparentemente confiables y escanear códigos QR maliciosos (QRishing) que redirigen a sitios fraudulentos.
TA0005: Evasión de Defensas	T1036 – Masquerading	Ocultamiento de los destinos maliciosos (cargas útiles) detrás de códigos QR incrustados en formatos de documentos que tradicionalmente se consideran seguros.

Recomendaciones

- **Protección Multicapa e Integrada:** Implementar soluciones de seguridad de correo electrónico que no dependan únicamente de firmas tradicionales, sino que utilicen análisis de comportamiento e IA para detectar anomalías, enlaces maliciosos y técnicas de ofuscación como los códigos QR.
- **Protección de la Identidad:** Desplegar controles robustos de gestión de identidades, incluyendo Autenticación Multifactor (MFA) resistente a la suplantación de identidad (FIDO2), para prevenir y mitigar los crecientes incidentes de usurpación de cuentas.
- **Respuesta Automatizada ante Incidentes:** Integrar herramientas de detección y respuesta rápida que permitan identificar y aislar automáticamente correos electrónicos maliciosos distribuidos desde bandejas de entrada internas comprometidas antes de que afecten a otros usuarios.
- **Concientización Actualizada:** Capacitar a los empleados específicamente sobre las nuevas tácticas de los atacantes, haciendo énfasis en los riesgos de interactuar con archivos adjuntos HTML y la prohibición de escanear códigos QR incrustados en documentos PDF corporativos.

ALTA

3.2 [ALTA] Alertan por estafas digitales y transmisiones falsas con IA a semanas del Mundial 2026



A pocos días del inicio del Mundial 2026 en Estados Unidos, México y Canadá, especialistas de FortiGuard Labs de Fortinet advirtieron sobre un incremento masivo de estafas digitales que explotan la urgencia de los aficionados.

Los ciberdelincuentes están utilizando herramientas de inteligencia artificial para diseñar campañas de phishing altamente convincentes, con textos impecables e imágenes que imitan a la perfección las plataformas oficiales de la FIFA y sus socios.

Estas amenazas se dividen principalmente en la venta de entradas falsas, paquetes turísticos VIP inexistentes y vuelos truchos.

Adicionalmente, se ha detectado el uso de páginas de streaming ilegal para los partidos; al intentar acceder a la transmisión o descargar supuestos reproductores, se instala malware de forma silenciosa capaz de tomar el control del dispositivo, robar credenciales bancarias y vaciar billeteras virtuales.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.002 – Phishing: Spearphishing Link / T1566.003 – Spearphishing SMS	Distribución de enlaces maliciosos mediante correos electrónicos, WhatsApp y SMS simulando ofertas exclusivas de pasajes o entradas para el Mundial.
TA0002: Ejecución	T1204.001 – User Execution: Malicious Link T1204.002 – Malicious File	El usuario interactúa con reproductores de video falsos o descarga archivos de verificación para ver los partidos gratis, activando el malware.
TA0005: Evasión de Defensas	T1036 – Masquerading	Uso de inteligencia artificial para clonar la estética, logotipos e interfaces de los portales legítimos de la FIFA y aerolíneas.
TA0006: Acceso a Credenciales	T1555 – Credentials from Password Stores	El malware desplegado o los formularios falsos capturan contraseñas de homebanking, datos de tarjetas de crédito y claves de billeteras digitales.
TA0040: Impacto	T1657 – Financial Theft / Fraud	Robo financiero directo mediante transacciones no autorizadas y suplantación de identidad de los aficionados.

Recomendaciones

- **Adquisición Exclusiva en Canales Oficiales:** Comprar entradas, hospedajes y paquetes de viaje únicamente a través de las plataformas legítimas de la FIFA o de sus socios comerciales autorizados, desconfiando de ofertas con precios inusualmente bajos.
- **Verificación de URL e Indicadores:** Revisar minuciosamente la dirección web (dominio) antes de realizar cualquier pago o ingresar datos personales, evitando hacer clic en enlaces recibidos por redes sociales o servicios de mensajería.
- **Evitar Descargas de Fuentes Desconocidas:** No instalar aplicaciones, archivos ejecutables ni extensiones de navegador que sean exigidas por páginas web de origen dudoso para poder visualizar las transmisiones en vivo de los partidos.
- **Activación de Autenticación de Doble Factor (2FA):** Habilitar el segundo factor de autenticación en todas las aplicaciones sensibles, tales como correos electrónicos, WhatsApp y billeteras virtuales, para mitigar el impacto en caso de robo de contraseña.
- **Uso de Redes Seguras y Monitoreo:** Evitar realizar transacciones financieras conectados a redes Wi-Fi públicas o abiertas y monitorear de forma constante los movimientos de las cuentas bancarias tras realizar compras de última hora.

MEDIA

3.3 [MEDIA] Incremento del fraude digital en Perú: phishing, smishing y vulnerabilidades por robo de dispositivos móviles



Especialistas en derecho digital y regulación alertaron sobre el alarmante incremento de los delitos informáticos en el país, registrándose más de 31,000 denuncias ante la Fiscalía Especializada en Ciberdelincuencia, lideradas ampliamente por el fraude informático y el smishing.

Las principales señales de alerta incluyen correos electrónicos con mensajes amenazantes, enlaces sospechosos o solicitudes urgentes de información personal que buscan engañar al usuario corporativo o particular.

La situación se agrava drásticamente ante el hurto físico de teléfonos celulares (con más de 1.5 millones de reportes de robo), lo que expone de forma inmediata bases de datos de identidad, permitiendo a los delincuentes realizar la suplantación de identidad, el vaciado completo de cuentas bancarias, extorsiones y la generación de créditos instantáneos no autorizados.

Ante este escenario, se destaca la urgencia de fortalecer la educación digital desde etapas tempranas y agilizar la regulación de normativas como la Ley Antispam para mitigar las comunicaciones fraudulentas.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.002 – Phishing: Spearphishing Link / T1566.003 – Spearphishing SMS	Distribución de correos electrónicos con enlaces maliciosos o amenazas urgentes (phishing), y envío masivo de mensajes de texto fraudulentos (smishing).
TA0001: Acceso Inicial	T1078 – Valid Accounts	Acceso ilegítimo a las sesiones y aplicaciones financieras activas del usuario aprovechando la vulnerabilidad del robo físico del dispositivo móvil.
TA0006: Acceso a Credenciales	T1555 – Credentials from Password Stores	Extracción de información personal y contraseñas guardadas expuestas directamente en el almacenamiento o aplicaciones del teléfono sustraído.
TA0040: Impacto	T1657 – Financial Theft / Fraud	Ejecución de fraudes financieros mediante el vaciado ilícito de cuentas bancarias, solicitudes de créditos instantáneos a nombre de la víctima y extorsiones.

Recomendaciones

- Implementación de Claves Robustas y Biometría: Utilizar contraseñas sofisticadas, largas y complejas para el bloqueo de pantalla de los dispositivos móviles, asegurando además que el acceso a aplicaciones bancarias requiera de autenticación biométrica obligatoria independiente
- Bloqueo Inmediato ante Pérdida o Robo: Establecer protocolos claros para los colaboradores de la organización que incluyan el reporte inmediato del robo del terminal a las operadoras de telecomunicaciones y entidades financieras para congelar las cuentas y bloquear el código IMEI.
- Capacitación Continua en Ingeniería Social: Informar de manera constante a los usuarios sobre las señales de alerta de los mensajes fraudulentos, instruyendo al personal a nunca interactuar con enlaces sospechosos o responder a solicitudes que exijan datos confidenciales bajo pretextos de urgencia.
- Seguridad de Datos Corporativos en Móviles: Implementar soluciones de Gestión de Dispositivos Móviles (MDM) en entornos empresariales que permitan el borrado remoto de los datos del dispositivo en caso de extravío o hurto, evitando la exposición de la información corporativa.
- Cumplimiento de Medidas de Seguridad de Datos: Garantizar que todas las organizaciones que gestionen datos personales apliquen estrictamente medidas de seguridad técnica y organizativa para proteger la privacidad de sus clientes y cumplir con el marco legal penal vigente (el cual sanciona el hurto de información mediante robo de celulares con penas de hasta 8 o 10 años).

4. Adversarios

CRÍTICA

4.1 [CRÍTICA] Desmantelamiento coordinado de la botnet "Glassworm" dirigida a desarrolladores



El 26 de mayo de 2026, el equipo de Operaciones Contra Adversarios de CrowdStrike, en colaboración con Google y Shadowserver Foundation, ejecutó el desmantelamiento de la botnet global Glassworm.

Esta amenaza, activa desde principios de 2025 y presuntamente operada desde Rusia (debido a la evasión de sistemas en países de la CEI y comentarios en ruso en el código), apuntaba sistemáticamente a desarrolladores de software.

Los atacantes comprometieron la cadena de suministro de código abierto distribuyendo extensiones troyanizadas en el mercado OpenVSX (afectando a VSCode, Cursor, VSCodium, entre otros), inyectando código en paquetes de npm y Python, y envenenando más de 300 repositorios de GitHub con credenciales robadas.

Para asegurar su resiliencia, Glassworm utilizaba una arquitectura de Comando y Control (C2) de cuatro capas, ocultando sus direcciones en transacciones de la blockchain de Solana, la red P2P BitTorrent DHT y eventos de Google Calendar.

El operativo logró interrumpir simultáneamente los cuatro canales, aislando a los atacantes de las máquinas infectadas.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1195.001 – Supply Chain Compromise: Compromise Software Dependencies and Development Tools	Infección a través de extensiones de IDEs falsificadas, scripts de instalación y ganchos postinstall maliciosos en paquetes de dependencias (npm, PyPI).
TA0005: Evasión de Defensas	T1614 – System Location Discovery / T1027 – Obfuscated Files or Information	Verificación del idioma, configuración regional y zona horaria del sistema para evitar infectar máquinas ubicadas en países de la CEI, sumado al uso de código ofuscado.
TA0006: Acceso a Credenciales	T1552 – Unsecured Credentials	Recolección de credenciales de desarrolladores para comprometer de forma encubierta repositorios de GitHub mediante modificaciones forzadas (force-push) en las ramas principales.
TA0011: Comando y Control	T1102 – Web Service / T1090.003 – Connection Proxy	Uso de canales redundantes y descentralizados (blockchain de Solana, red BitTorrent DHT y Google Calendar) como puntos muertos de entrega (dead-drops) para enmascarar las rutas hacia los servidores C2.

Recomendaciones

- **Monitoreo Inmediato de IoCs en Red:** Revisar los registros de red y la telemetría de los terminales en busca de conexiones salientes hacia la dirección IP benigna 164.92.88[.]210 (operada por CrowdStrike), ya que cualquier beacon hacia esta IP confirma una infección activa por Glassworm que requiere remediación urgente.
- **Búsqueda de Amenazas en Endpoints (Threat Hunting):** Implementar las reglas YARA publicadas por la investigación (como CrowdStrike_GlasswormRat_01 y CrowdStrike_GlasswormDownloader_01) en las herramientas EDR para identificar las cadenas características del troyano (GlasswormRAT) y sus instaladores ofuscados de Python en los discos duros y la memoria.
- **Refuerzo en Estaciones de Desarrollo:** Limitar y auditar rigurosamente la instalación de extensiones de editores de código (VSCode, Cursor, Positron) descargadas de mercados de terceros como OpenVSX, comprobando la reputación y autenticidad del autor.
- **Defensa Proactiva en CI/CD:** No depender exclusivamente de detecciones post-instalación, ya que las dependencias maliciosas comprometen el sistema en segundos; se debe asegurar los repositorios de código y las canalizaciones de compilación contra inyecciones no autorizadas.

CRÍTICA

4.2 [CRÍTICA] Grupo "Deface Perú" vulnera el sistema Sismate y emite falsas alertas de tsunami y fraude electoral



El 21 de mayo de 2026, el grupo de hacktivistas denominado "Deface Perú" vulneró exitosamente la infraestructura del Sistema de Mensajería de Alerta Temprana (Sismate), enviando notificaciones falsas a los teléfonos celulares de millones de usuarios a nivel nacional.

Los atacantes lograron manipular el canal de Cell Broadcast, una tecnología habilitada por el Ministerio de Transportes y Comunicaciones (MTC) y gestionada por la empresa concesionaria Everbridge, la cual opera independientemente del control de las operadoras móviles tradicionales (SMS). Durante el ataque se difundieron dos mensajes masivos: el primero generó pánico al advertir sobre un falso sismo de magnitud 8.7 con inminente peligro de tsunami en todo el litoral peruano; minutos después, un segundo mensaje transmitió una consigna política alegando un supuesto "fraude electoral".

El Instituto Nacional de Defensa Civil (INDECI) se vio obligado a intervenir rápidamente para desmentir la emergencia, evidenciando el grave riesgo físico y psicológico que supone la toma de control de los sistemas críticos de comunicación del Estado.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application / T1078 – Valid Accounts	Posible explotación de vulnerabilidades en la infraestructura web del MTC o uso de credenciales comprometidas de la plataforma de la concesionaria (Everbridge) para acceder al panel de control de alertas.
TA0008: Movimiento Lateral	T1021 – Remote Services	Desplazamiento y escalada dentro de la red del proveedor de comunicaciones para alcanzar los servidores responsables de la emisión de señales Cell Broadcast.
TA0040: Impacto	T1491.002 – Defacement: Internal Defacement	Alteración y manipulación no autorizada del contenido del sistema de notificaciones de emergencia para difundir propaganda política y desinformación (pánico colectivo).
TA0040: Impacto	T1489 – Service Stop / Disruption	Interrupción de la confiabilidad operativa del sistema de alertas tempranas (Sismate), socavando la confianza pública en los mecanismos oficiales de prevención de desastres.

Recomendaciones

- Auditoría Forense Integral: Iniciar de inmediato una investigación técnica profunda en conjunto con la empresa Everbridge y el MTC para identificar el vector de acceso exacto (falla de software, robo de credenciales o ataque a la cadena de suministro) que permitió la intrusión en la red de Cell Broadcast.
- Control de Accesos y MFA Estricto: Implementar Autenticación Multifactor (MFA) obligatoria, políticas de acceso condicional por geolocalización y el principio de doble autorización (regla de dos personas) para cualquier operador que intente emitir o programar una alerta nacional.
- Segmentación de Infraestructura Crítica: Aislar las redes y servidores que controlan el sistema Sismate del resto de la infraestructura TI del ministerio y de los proveedores de telecomunicaciones, aplicando principios estrictos de Confianza Cero (Zero Trust).
- Protocolos de Gestión de Crisis y Desinformación: Establecer canales de comunicación de contingencia redundantes y predefinidos entre el MTC, INDECI y los medios de comunicación para desmentir falsas alarmas en tiempo real, mitigando el pánico o el riesgo de daño físico durante episodios de alteración del orden público.
- Monitoreo de Integridad del Sistema: Desplegar herramientas de monitoreo continuo (SIEM/SOC) con alertas automatizadas frente a inicios de sesión inusuales en las consolas de administración del Sismate o envíos de notificaciones masivas fuera de los protocolos de simulacro programados.

CRÍTICA

4.3 [CRÍTICA] Hackers irrumpen en Canvas y afectan a universidades en plena semana de exámenes



El 7 de mayo de 2026, el grupo de ciberdelincuentes ShinyHunters vulneró la popular plataforma educativa en la nube Canvas (propiedad de Instructure), afectando a más de 8.000 instituciones y 30 millones de usuarios a nivel global, incluyendo prestigiosas universidades y distritos escolares de Estados Unidos en plena semana de exámenes finales.

Los atacantes publicaron una nota de rescate en la página principal de los sitios de Canvas exigiendo pagos bajo la amenaza de nuevas filtraciones de datos y dando como plazo a la empresa hasta el 12 de mayo de 2026.

La interrupción masiva dejó a estudiantes y profesores sin acceso a calificaciones, materiales de estudio, cuestionarios y herramientas de comunicación, forzando a algunas instituciones (como la Universidad James Madison) a modificar y posponer sus calendarios de exámenes, y exponiendo la profunda dependencia del sector educativo hacia unas pocas plataformas digitales centralizadas.

Este ataque representa el segundo incidente de seguridad del mes para Instructure, tras confirmarse que el 1 de mayo un ataque distinto comprometió nombres de usuario, direcciones de correo electrónico y números de identificación estudiantil.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1195 – Supply Chain Compromise / T1078 – Valid Accounts	Acceso no autorizado a la infraestructura en la nube de Instructure (Canvas), lo que repercutió de forma masiva en las instituciones educativas cliente.
TA0040: Impacto	T1491.002 – Defacement: Internal Defacement	Alteración y modificación de la página principal de Canvas en múltiples instituciones para mostrar un mensaje extorsivo y nota de rescate directamente a los usuarios.
TA0040: Impacto	T1489 – Service Stop	Interrupción del acceso de los estudiantes a recursos críticos como calificaciones, materiales de estudio y cuestionarios, interrumpiendo el flujo operativo de las universidades.
TA0010: Exfiltración	T1005 – Data from Local System	Robo y compromiso de información de los usuarios (nombres de usuario, correos electrónicos y números de identificación) durante la filtración inicial ocurrida el 1 de mayo.

Recomendaciones

- Planes de Continuidad Académica: Desarrollar protocolos de contingencia que no dependan exclusivamente de Canvas para la entrega de tareas o evaluaciones, garantizando el uso del correo electrónico institucional u otras plataformas como canales alternativos de comunicación.
- Alerta por Filtración de Datos: Notificar de manera urgente a toda la comunidad estudiantil y docente sobre el compromiso de sus correos electrónicos y números de identificación estudiantil para prevenir futuros ataques de ingeniería social o suplantación de identidad.
- Evaluación de Proveedores SaaS: Revisar los acuerdos de nivel de servicio (SLA) y exigir a proveedores como Instructure auditorías de seguridad transparentes, garantizando que apliquen medidas robustas en lugar de solo "parches de seguridad" superficiales.
- Rotación Preventiva de Credenciales: Exigir a estudiantes, profesores y personal administrativo el cambio inmediato de contraseñas utilizadas para acceder a los portales universitarios y reforzar las políticas de autenticación multifactor (MFA) ante el riesgo de cuentas comprometidas.

5. Indicadores de Compromiso

5.1 Direcciones IP

80[.]94[.]92[.]184	40[.]124[.]175[.]60	130[.]131[.]225[.]103
103[.]172[.]20[.]218	27[.]150[.]170[.]101	130[.]131[.]225[.]103
45[.]88[.]138[.]44	52[.]32[.]214[.]226	65[.]191[.]211[.]33
118[.]196[.]4[.]129	66[.]132[.]195[.]47	89[.]124[.]113[.]107

5.2 Dominios

avsvmcloud[.]com	Usrpubtrk[.]com
digitalcollege[.]org	voruftuiov[.]com
freescanonline[.]com	so6lavern[.]garden
thedoccloud[.]com	yxponte[.]com
virtualwebdata[.]com	effectivegatecpm[.]com
rnicrosoft[.]com	

5.3 Hashes

0001a7e82ccc41a89d7792159ce3e936a91dbe8ce2781edd742ea0943c84093d
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
0003cdf49cc31f363db1517330bf7f0f30923b435675bcb63686db57bd34b34c
027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
0005ead0e5bc5ed7d40c6f2c90c0f8d1574c6039feed79c7e78b967ccf8652c
64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1
0007edc2bd1af15dacfe156f6cbfaa0368fb81b6e78ec1a7e3c4e120a73b9bd1
d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e
000b7a6edad313848002761d0bda643c455da7f65a37f1ef5603209da7b24d59
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
000abccf991307ca36d4d410c78ce6d04cccb071a4e43ac65ddfcc2d7bc8ca1
00086f0430284109783541481fd4021522d56c0ffcd34d279e1f73f17fca32ab

6. Fuentes

- 6.1 <https://thehackernews.com/2026/05/malicious-npm-package-stole-files-from.html>
- 6.2 <https://www.nccgroup.com/newsroom/news-reaction-us-education-ransomware-attack-on-canvas-shinyhunters/>
- 6.3 <https://www.cyfirma.com/news/weekly-intelligence-report-22-may-2026/>
- 6.4 <https://thehackernews.com/2026/05/windows-phone-link-exploited-by-cloudz.html>
- 6.5 <https://thehackernews.com/2026/05/trapdoor-supply-chain-attack-spreads.html>
- 6.6 <https://unit42.paloaltonetworks.com/captive-portal-zero-day/>
- 6.7 <https://cybersecurefox.com/es/cisa-vulnerabilidades-langflow-trend-micro-kev/>
- 6.8 <https://es.barracuda.com/company/news/2026/ai-phishing-service-drive-increase-email-attacks-barracuda-reports>
- 6.9 <https://tn.com.ar/tecno/novedades/2026/05/26/mundial-2026-alertan-por-estafas-digitales-que-ofrecen-entradas-falsas-vuelos-truchos-y-ver-partidos-gratis/>
- 6.10 <https://especial.larepublica.pe/peru-conectado/2026/2026/01/28/fraude-digital-en-aumento-senales-de-alerta-y-medidas-de-proteccion-1605968>
- 6.11 <https://especial.larepublica.pe/peru-conectado/2026/2026/01/28/fraude-digital-en-aumento-senales-de-alerta-y-medidas-de-proteccion-1605968>
- 6.12 <https://www.crowdstrike.com/en-us/blog/inside-crowdstrike-takedown-of-a-developer-targeting-botnet/>
- 6.13 <https://www.atv.pe/noticia/hackean-sismate-falsas-alertas-terremoto-2/>
- 6.14 <https://cnnespanol.cnn.com/2026/05/07/eeuu/ciberataque-canvas-hackers-examenes-trax>