



GS PERÚ

Software · Security & Services

Empresas

BOLETÍN CIBERSEGURIDAD

Abril - 2026



LA SEGURIDAD ABARCA TODO EL ECOSISTEMA DIGITAL



Abril 2026: Las amenazas cibernéticas son más sofisticadas, automatizadas y difíciles de detectar.

El análisis de amenazas de abril de 2026 revela un panorama de ciberseguridad cada vez más complejo y sofisticado, donde el malware y el ciberespionaje evolucionan rápidamente en técnicas y objetivos. Se observa un incremento en ataques dirigidos a sistemas macOS con herramientas como nuevos infostealers altamente evasivos, así como incidentes críticos en la cadena de suministro de software, lo que evidencia que incluso plataformas confiables pueden ser comprometidas.

Además, destacan campañas avanzadas de ciberespionaje impulsadas por actores estatales, que utilizan exploits de día cero, rootkits y técnicas de suplantación para infiltrarse en entidades gubernamentales. Paralelamente, los atacantes están incorporando tecnologías emergentes como la inteligencia artificial para mejorar la evasión y generar malware más dinámico y difícil de detectar.

En este contexto, también surgen nuevas herramientas ofensivas y técnicas de movimiento lateral más sigilosas, lo que refuerza la necesidad de evolucionar los mecanismos de defensa, incluyendo el uso de machine learning y modelos adaptativos capaces de responder a amenazas en constante cambio.

ÍNDICE

1. Malware	4
1.1 Ataque de ransomware contra el proveedor médico ChipSoft	
1.2 JanelaRAT: Troyano bancario que roba credenciales y elude MFA en América Latina	
1.3 Cibercriminales aprovechan filtración de "Claude Code" para distribuir infostealers	
1.4 Falso parche de Windows 11 distribuye malware indetectable para el robo de datos	1.5
Nueva variante del malware móvil "SparkCat" se oculta en apps oficiales para robar criptomonedas	
2. Vulnerabilidades	14
2.1 CVE-2026-41651: Escalada de privilegios en Linux (PackageKit – Pack2TheRoot)	
2.2 CVE-2026-39987: Ejecución remota de código en Marimo	
2.3 Riesgos por sobreexposición de datos en SharePoint	
3. Phishing	20
3.1 La IA ayudó a Google a detener el 99 % de los "anuncios maliciosos"	
3.2 ¿Qué es "QRishing"?, la amenaza que se esconde detrás de un código QR	
3.3 Intervención policial de infraestructura criminal de phishing y toma de cuentas bancarias	
4. Adversarios	26
4.1 Atacantes explotan MSBuild (LOLBin) para evadir detección en ataques "Fileless"	
4.2 Sitio web de CPUID comprometido para distribuir el troyano STX RAT	
4.3 GopherWhisper: grupo APT alineado con China usó Discord y Slack para atacar organismos gubernamentales	
5. Indicadores de compromiso	32
5.1 Direcciones IP	
5.2 Dominios	
5.3 Hashes	
6. Fuentes	

1. Malware

CRÍTICA

1.1 Ataque de ransomware contra el proveedor médico ChipSoft afecta a hospitales en Países Bajos



El 7 de abril de 2026, un ataque de ransomware impactó a ChipSoft, el principal proveedor de software de registros médicos electrónicos (EHR) en los Países Bajos, cuyo sistema insignia "HiX" es utilizado por el 70 % de los hospitales del país. Como medida de precaución y contención, la empresa se vio obligada a deshabilitar múltiples plataformas digitales (Zorgportaal, HiX Mobile y Zorgplatform).

Tras la vulneración, se recomendó a los clientes cortar las conexiones VPN seguras hacia la infraestructura comprometida, lo que llevó a al menos 11 hospitales a desconectar sus sistemas.

Aunque el incidente no detuvo los procesos de atención médica crítica —los hospitales recurrieron a sistemas telefónicos y trabajo manual para su logística—, ChipSoft confirmó un "posible acceso no autorizado" y no descarta el robo de datos confidenciales de los pacientes. Este evento subraya el riesgo inminente de los ataques a la cadena de suministro dentro de los ecosistemas críticos de salud.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1199 – Trusted Relationship	Los atacantes comprometen a un proveedor tecnológico (ChipSoft) que mantiene conexiones directas y privilegiadas (VPN) con la infraestructura de múltiples hospitales.
TA0009: Recolección	T1005 – Data from Local system	Exploración y posible recopilación de registros médicos electrónicos (EHR) e información personal de los pacientes almacenada en las bases de datos.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Posible transferencia no autorizada y robo de datos médicos y personales confidenciales antes de ejecutar el despliegue del ransomware (Doble Extorsión).
TA0040: Impacto	T1486 – Data Encrypted for Impact	Despliegue del programa de ransomware (cifrado) en los servidores de la compañía, provocando la inoperatividad y caída de sus plataformas principales.
TA0040: Impacto	T1499 – Endpoint Denial of Service	Interrupción severa de los servicios digitales y logísticos entre los hospitales y los pacientes debido a la desconexión preventiva de los sistemas afectados

Recomendaciones

- Definir protocolos para desconectar de inmediato VPN e integraciones API con terceros ante indicios de compromiso en la cadena de suministro.
- Fortalecer y probar planes de continuidad que habiliten operación manual y uso de redes telefónicas en áreas críticas durante contingencias prolongadas.
- Vigilar foros y sitios de extorsión para detectar filtraciones tempranas de datos sensibles (registros de pacientes).
- Aislar integraciones con proveedores y aplicar inspección estricta del tráfico bajo un modelo de confianza cero.
- Forzar la rotación completa de credenciales, contraseñas de servicio y tokens antes de restablecer conexiones con el proveedor.

ALTA

1.2 JanelaRAT: Troyano bancario que roba credenciales y elude MFA en América Latina



En abril de 2026, investigadores de GREAT detallaron las tácticas de JanelaRAT, una variante modificada del malware BX RAT diseñada para atacar a usuarios de instituciones financieras y de criptomonedas en América Latina, con especial foco en Brasil y México, donde se registraron más de 26 000 ataques en el último año.

La cadena de infección comienza con correos electrónicos de suplantación (phishing) que simulan facturas pendientes, llevando a la víctima a descargar archivos MSI. Estos instaladores actúan como "droppers" que preparan el terreno utilizando la técnica de DLL Sideload: ejecutan un archivo legítimo (nevasca.exe) que a su vez carga silenciosamente la biblioteca maliciosa de JanelaRAT (PixelPaint.dll).

Una vez activo, el troyano monitorea el título de las ventanas del navegador y, al detectar un banco objetivo, despliega un sofisticado sistema de pantallas superpuestas (overlays). Estas ventanas falsas imitan actualizaciones de Windows o portales bancarios para bloquear la interacción del usuario y robar contraseñas, tokens de autenticación multifactor (MFA) e interceptar la sesión bancaria en tiempo real, comunicándose con un servidor de Comando y Control (C2) que rota diariamente.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.001 / T1566.002 – Phishing: Spearphishing Attachment and Link	Envío de correos electrónicos engañosos sobre facturas pendientes que incluyen enlaces a archivos PDF maliciosos y sitios web para descargar el empaquetado (ZIP/MSI).
TA0002: Ejecución	T1574.002 – Hijack Execution Flow: DLL Side-Loading	Uso de un ejecutable legítimo (nevasca.exe) introducido por el dropper MSI para cargar subrepticamente la DLL maliciosa que contiene a JanelaRAT.
TA0003: Persistencia	T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Creación de un acceso directo (LNK) y un script en la carpeta de Inicio de Windows del usuario para garantizar la ejecución silenciosa en cada inicio de sesión.
TA0005: Evasión de Defensa	T1027 – Obfuscated Files or Information	Protección del código con Eazfuscator, aplanamiento de flujo de control (CFF) y cifrado de cadenas mediante AES (Rijndael) y Base64.
TA0006: Acceso a Credenciales	T1056.001 / T1056.002 – Input Capture: Keylogging / GUI Input Capture	Captura de pulsaciones de teclado y despliegue de ventanas superpuestas (overlays) que simulan sitios legítimos para interceptar contraseñas y tokens MFA.
TA0011: Comando y Control	T1568.002 – Dynamic Resolution: Domain Generation Algorithms / Fast Flux	Rotación diaria de dominios de C2 contruidos dinámicamente utilizando servicios DNS dinámicos (DDNS) sobre el puerto 443 (sin TLS).
TA0040: Impacto	T1499 – Endpoint Denial of Service (Temporal)	Despliegue de falsas pantallas de "Actualización de Windows" a pantalla completa para distraer y bloquear temporalmente la interacción del usuario con el sistema operativo mientras roban datos en segundo plano.

ALTA

1.3 Cibercriminales aprovechan filtración de "Claude Code" para distribuir infostealers



El 8 de abril de 2026, investigadores de Zscaler reportaron una campaña de ciberataques que aprovechó la reciente filtración del código interno de "Claude Code" (herramienta de IA de Anthropic) ocurrida el 31 de marzo.

Los atacantes utilizaron este incidente de alto perfil como señuelo, creando múltiples repositorios falsos en GitHub que prometían acceso a funciones empresariales sin restricciones de la herramienta. El objetivo principal fue engañar a desarrolladores y usuarios curiosos para que descargaran un archivo ZIP infectado (promovido por usuarios como idbzoomh).

Al ejecutarse, este archivo instalaba dos programas maliciosos de forma silenciosa: Vidar, un infostealer diseñado para extraer contraseñas, cookies de sesión, datos bancarios y archivos sensibles; y GhostSocks, un malware que convierte el equipo comprometido en un proxy para redirigir tráfico y ocultar el origen de futuros ataques. Este caso resalta la extrema rapidez con la que los ciberdelincuentes arman campañas (weaponization) basadas en noticias tecnológicas de gran impacto.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0002: Ejecución	T1204.002 – User Execution: Malicious File	Los usuarios y desarrolladores descargan y ejecutan voluntariamente el archivo ZIP infectado, creyendo que contiene el código legítimo o funciones avanzadas de la herramienta.
TA0005: Evasión de Defensa	T1036 – Masquerading	Creación de repositorios falsos en GitHub que suplantan la identidad visual y el contenido del código filtrado de "Claude Code" para generar confianza.
TA0006: Acceso a Credenciales	T1555 – Credentials from Password Stores	El infostealer Vidar extrae silenciosamente contraseñas guardadas, cookies de sesión y datos bancarios almacenados en los navegadores web de la víctima.
TA0009: Recolección	T1005 – Data from Local System	Búsqueda y recopilación de archivos e información sensible directamente desde el disco duro de la computadora comprometida sin mostrar alertas.
TA0011: Comando y Control	T1090.003 – Connection Proxy	Despliegue del malware GhostSocks para redirigir el tráfico malicioso a través del dispositivo infectado, utilizándolo para ocultar el rastro de los atacantes.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Envío de todos los datos personales, credenciales y cookies recopilados hacia los servidores de mando controlados por los ciberdelincuentes.

Recomendaciones

- Capacitar a desarrolladores sobre los riesgos de descargar código o herramientas desde repositorios no verificados, especialmente aquellos que ofrezcan "software filtrado" o funciones premium gratuitas.
- Implementar protección de endpoints con detección de firmas y comportamiento en memoria de malware como Vidar y GhostSocks.
- Ante sospecha de infostealer, invalidar sesiones activas y rotar contraseñas, considerando evasión de MFA mediante robo de cookies.
- Analizar conexiones a IP sospechosas o patrones de uso como proxy no autorizado en equipos internos.
- Exigir pruebas de software, scripts o herramientas de terceros en entornos aislados antes de su ejecución en estaciones principales.

CRÍTICA**1.4 Falso parche de Windows 11 distribuye malware indetectable para el robo de datos**

El 13 de abril de 2026, investigadores de Malwarebytes alertaron sobre una sofisticada campaña global que distribuye un software malicioso disfrazado de una actualización de Windows 11 (versión 24H2).

Los atacantes utilizan correos electrónicos y enlaces engañosos (typosquatting) para dirigir a las víctimas a un portal web falso que imita a la perfección la estética de Microsoft. Al descargar el supuesto parche de optimización y seguridad, el usuario ejecuta un instalador limpio que oculta su lógica maliciosa dentro de un código JavaScript, logrando evadir la detección de al menos 69 motores antivirus.

Una vez activo, el malware extrae la IP y geolocalización del equipo, modifica el registro de Windows para simular ser una función de seguridad legítima y se enmascara como un acceso directo de Spotify para garantizar su ejecución en cada reinicio (persistencia). Su objetivo final es robar información sensible, principalmente credenciales de inicio de sesión y datos de medios de pago (tarjetas de crédito) almacenados en los navegadores web, exfiltrándolos hacia un servidor externo.

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

Táctico	Técnicas / Subtécnicas	
TA0001: Acceso Inicial	T1566.002 – Phishing: Spearphishing Link	Envío de correos electrónicos con enlaces hacia dominios maliciosos (con errores ortográficos) que imitan el sitio oficial de descargas de Microsoft.
TA0002: Ejecución	T1059.007 – Command and Scripting Interpreter: JavaScript	Uso de lógica maliciosa incrustada dentro de código JavaScript ejecutado por el instalador para evadir los análisis de los antivirus tradicionales.
TA0003: Persistencia	T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Creación de un falso acceso directo de Spotify que se ejecuta automáticamente cuando el sistema operativo se inicia.
TA0005: Evasión de Defensa	T1036 – Masquerading	Suplantación de portales de Microsoft, modificación del registro para simular una función de seguridad y camuflaje como la aplicación de Spotify.
TA0009: Recolección	T1555.003 – Credentials from Password Stores: Credentials from Web Browsers	Extracción de credenciales de inicio de sesión e información de medios de pago almacenados en los navegadores web de la víctima.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Comunicación con un servidor externo para gestionar la infraestructura de ataque e instalar paquetes maliciosos adicionales en el equipo.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Envío de la información robada (credenciales, tarjetas de crédito, IP y geolocalización) a la infraestructura controlada por los atacantes.

Recomendaciones

- Forzar mediante GPO que Windows se actualice solo por Windows Update y bloquear descargas de actualizaciones desde navegadores.
- Usar soluciones que detecten comportamientos anómalos en tiempo real (registro, scripts de inicio, etc.).
- Aplicar filtrado DNS y de correo para detectar URLs con typosquatting.
- Evitar que se guarden contraseñas y tarjetas; usar gestores corporativos cifrados.
- Revisar periódicamente claves Run/RunOnce y accesos sospechosos, especialmente en apps comunes.

ALTA

1.5 Nueva variante del malware móvil "SparkCat" se oculta en apps oficiales para robar criptomonedas



El 13 de abril de 2026, especialistas de la firma Kaspersky alertaron sobre una nueva y sofisticada generación del malware móvil denominado "SparkCat". Esta variante ha logrado evadir los controles de seguridad y posicionarse dentro de aplicaciones aparentemente legítimas disponibles tanto en la App Store como en Google Play. El objetivo principal de este malware es el robo de fondos en criptomonedas mediante la exposición de datos sensibles.

Una vez que el usuario instala la aplicación infectada, esta solicita acceso a la galería del dispositivo. Si se le conceden los permisos, SparkCat escanea silenciosamente las fotografías utilizando tecnología de reconocimiento de texto (OCR) para identificar contraseñas y frases de recuperación (seed phrases) de billeteras digitales.

Al encontrar información coincidente, los datos son exfiltrados directamente a los servidores de los ciberdelincuentes. Esta amenaza destaca por su alto nivel de adaptación y el uso de técnicas avanzadas para ocultarse en los ecosistemas móviles oficiales.

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

Táctico	Técnicas / Subtécnicas	
TA0001: Acceso Inicial	T1204.002 – User Execution: Malicious File	Los usuarios descargan e instalan voluntariamente las aplicaciones infectadas creyendo que son herramientas o juegos legítimos desde las tiendas oficiales.
TA0005: Evasión de Defensa	T1036 – Masquerading	El malware se empaqueta y oculta dentro de aplicaciones funcionales para evadir los procesos de revisión automáticos de la App Store y Google Play.
TA0007: Descubrimiento	T1083 – File and Directory Discovery	Solicitud y abuso de los permisos del sistema operativo móvil para acceder a la galería de fotos y explorar el almacenamiento local del dispositivo.
TA0006: Acceso a Credenciales	T1552 – Unsecured Credentials	Uso de tecnología de reconocimiento óptico de caracteres (OCR) sobre las imágenes almacenadas para extraer claves privadas y frases de recuperación de criptomonedas.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Envío silente de las fotografías clave o del texto plano identificado hacia la infraestructura de mando y control (C2) de los atacantes.

Recomendaciones

- Evitar almacenar capturas con contraseñas, códigos o seed phrases en la galería del dispositivo, por su alto riesgo como vector de ataque.
- Revisar y restringir permisos de apps; denegar acceso a galería/almacenamiento si no es esencial para su función.
- Validar reputación, reseñas y volumen de descargas antes de instalar apps, incluso desde tiendas oficiales.
- Bloquear instalaciones desde orígenes desconocidos y evitar descargas desde enlaces o sitios no confiables.
- Implementar soluciones MTD para detectar comportamiento anómalo, exfiltración en segundo plano y malware como SparkCat.

2. Vulnerabilidades

ALTA

2.1 Vulnerabilidad "Pack2TheRoot" permite obtener privilegios root en múltiples distribuciones Linux



Se reportó una vulnerabilidad crítica en sistemas Linux denominada "Pack2TheRoot" (CVE-2026-41651), la cual afecta al componente PackageKit, utilizado para la gestión de paquetes en múltiples distribuciones. La falla, clasificada con una severidad alta (CVSS 8.8), permite que usuarios locales sin privilegios obtengan acceso root mediante una condición de carrera tipo TOCTOU (Time-of-Check to Time-of-Use), explotando errores en la validación de transacciones del sistema.

Investigadores de Deutsche Telekom confirmaron que el problema afecta versiones de PackageKit desde la 1.0.2 hasta la 1.3.4, impactando distribuciones como Ubuntu, Debian, Fedora y Rocky Linux. La explotación permitiría instalar paquetes maliciosos, ejecutar código arbitrario y comprometer completamente el sistema afectado.

Aunque la vulnerabilidad ya fue corregida en PackageKit 1.3.5 y mediante parches de seguridad distribuidos por distintos proveedores, se recomienda actualizar inmediatamente los sistemas y verificar la presencia de versiones vulnerables para evitar accesos no autorizados y escaladas de privilegios.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0004: Escalada de Privilegios	T1068 – Exploitation for Privilege Escalation	Explotación de una condición de carrera (TOCTOU) en el componente PackageKit para elevar los permisos de un usuario estándar a privilegios de root.
TA0002: Ejecución	T1059.004 – Command and Scripting Interpreter: Unix Shell	Ejecución de código arbitrario y comandos con altos privilegios tras lograr la explotación exitosa.
TA0003: Persistencia	T1543.002 – Create or Modify System Process: Systemd	Instalación de paquetes de software malicioso a nivel de sistema para garantizar permanencia en la infraestructura comprometida.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Aprovechamiento de errores en el mecanismo de validación de transacciones del gestor de paquetes para eludir los controles de acceso locales.

Recomendaciones

- Verificar inmediatamente si la versión comprometida del paquete fue instalada en servidores, contenedores o entornos de desarrollo durante la ventana de exposición.
- Rotar de forma preventiva todas las credenciales, tokens, claves API y accesos cloud que pudieron haber sido expuestos.
- Implementar controles de validación de integridad y firma digital para paquetes, imágenes Docker y dependencias utilizadas en entornos CI/CD.
- Restringir privilegios y accesos de cuentas utilizadas en pipelines automatizados, evitando permisos excesivos sobre repositorios y servicios cloud.
- Habilitar monitoreo y alertas sobre conexiones salientes sospechosas, exfiltración de información y actividades anómalas en sistemas de desarrollo.
- Realizar auditorías periódicas de dependencias y aplicar herramientas de análisis de vulnerabilidades y supply chain security.
- Mantener actualizados los sistemas, librerías y componentes utilizados en entornos de desarrollo y automatización.
- Implementar segmentación de red y controles de acceso para limitar el movimiento lateral y el impacto ante posibles compromisos.

CRÍTICA**2.2 CVE-2026-39987: Vulnerabilidad RCE en Marimo explotada en menos de 10 horas**

El 13 de abril de 2026, se reportó la explotación activa de una falla crítica de Ejecución Remota de Código (RCE), registrada como CVE-2026-39987 (CVSS 9.3), en la plataforma de notebooks de Python de código abierto Marimo.

Investigadores de Sysdig detectaron ataques en la naturaleza apenas 9 horas y 41 minutos después de la publicación del aviso de seguridad. La vulnerabilidad reside en el endpoint WebSocket del terminal de la aplicación (/terminal/ws) en las versiones 0.20.4 y anteriores, el cual omite por completo la verificación de autenticación de sesión.

Esto permite a cualquier atacante remoto obtener un shell interactivo persistente con los máximos privilegios del proceso. La rapidez del ataque subraya una preocupante tendencia en la que los actores de amenazas (presumiblemente asistidos por IA) desarrollan exploits directamente desde la descripción técnica, sin requerir una Prueba de Concepto (PoC) pública.

Tras obtener el acceso inicial mediante scripts automatizados, operadores humanos lograron explorar el sistema de archivos y exfiltrar archivos .env con credenciales críticas de infraestructura en la nube (claves de AWS) en tan solo tres minutos.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Explotación del endpoint WebSocket /terminal/ws expuesto y carente de autenticación en la plataforma Marimo.
TA0002: Ejecución	T1059.004 – Command and Scripting Interpreter: Unix Shell	Obtención y uso de un pseudo-terminal (shell interactivo) que se ejecuta con todos los privilegios del proceso de la aplicación subyacente.
TA0007: Descubrimiento	T1083 – File and Directory Discovery	Exploración manual del sistema de archivos local de la víctima tras el acceso inicial para localizar información valiosa (ej. comandos ls, cat).
TA0006: Acceso a Credenciales	T1552.001 – Unsecured Credentials: Credentials In Files	Búsqueda, lectura y extracción de archivos de configuración y variables de entorno (.env) que almacenan claves de AWS sin cifrar.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Robo y transferencia de los archivos .env y las credenciales de infraestructura en la nube fuera del entorno comprometido.

Recomendaciones

- Actualizar Marimo a versión $\geq 0.23.0$ para mitigar el endpoint vulnerable.
- Revocar y regenerar claves cloud (AWS), credenciales de BD y tokens expuestos en .env o variables de entorno.
- Analizar logs de red y servidor en busca de tráfico no autorizado hacia /terminal/ws desde el 08/04/2026.
- Aislar notebooks (Marimo/Jupyter) y restringir acceso vía VPN o ZTNA, evitando exposición pública.
- Ejecutar servicios y contenedores sin permisos de root para reducir impacto ante compromiso.

ALTA

2.3 Riesgos críticos por sobreexposición de datos y permisos ocultos en SharePoint



Microsoft SharePoint se ha convertido en el núcleo de colaboración y almacenamiento de la mayoría de las organizaciones, volviéndolo un objetivo de alto valor. Sin embargo, el riesgo más subestimado proviene desde adentro: la acumulación orgánica de permisos excesivos a lo largo del tiempo.

En una empresa promedio, esto puede traducirse en millones de archivos y cientos de miles de derechos de acceso imposibles de rastrear manualmente. Esta brecha de visibilidad es aprovechada mediante grupos anidados que ocultan quién tiene acceso real, etiquetas de permisos falsificadas (como nombrar "Leer" a un acceso de control total), enlaces compartidos anónimos que persisten por defecto y bibliotecas de documentos ocultas.

Esta falta de higiene en los permisos permite que empleados descontentos o atacantes externos con una sola cuenta comprometida mantengan accesos persistentes y ejecuten exfiltraciones de datos masivas y silenciosas, superando con creces el radio de impacto inicial.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0003: Persistencia	T1098 – Account Manipulation	Uso de estructuras de grupos anidados (en Entra ID y SharePoint heredado) para enterrar y mantener el de acceso de usuarios incluso tras intentos revocación.
TA0005: Evasión de Defensa	T1036 – Masquerading	Cambio de nombre en las etiquetas de los niveles de permiso (ej. etiquetar como "Lectura" un permiso de Control Total) para engañar a los administradores durante las auditorías visuales.
TA0005: Evasión de Defensa	T1564 – Hide Artifacts	Creación de bibliotecas de documentos que son invisibles para otros miembros de la organización para ocultar archivos confidenciales copiados.
TA0001: Acceso Inicial	T1199 – Trusted Relationship / T1133 – External Remote Services	Explotación de enlaces para compartir anónimos y persistentes generados por Microsoft 365/Teams, los cuales sobreviven a los procesos de salida de empleados.
TA0010: Exfiltración	T1567.002 – Exfiltration to Cloud Storage	Uso de bibliotecas ocultas y enlaces de invitados externos para sostener una exfiltración encubierta de datos sin dejar un registro de auditoría obvio.

Recomendaciones

- Gestionar y revisar permisos en SharePoint como control proactivo y permanente.
- Usar herramientas o scripts para desglosar membresías en Microsoft Entra ID y SharePoint, identificando accesos efectivos.
- Revisar y revocar enlaces de invitados o comparticiones anónimas obsoletas.
- Verificar la configuración real de permisos, no solo las etiquetas de visualización.
- Aplicar controles de intercambio externo con aprobación y expiración automática para accesos de invitados.

3. Phishing

MEDIA

3.1 La IA ayudó a Google a detener el 99 % de los "anuncios maliciosos"



Google reportó que, gracias al uso de inteligencia artificial con Gemini, logró bloquear aproximadamente 8 200 millones de anuncios maliciosos en 2025, interceptando más del 99 % antes de que llegaran a los usuarios.

El sistema analiza grandes volúmenes de señales (comportamiento, antigüedad de cuentas, patrones de campañas) para identificar actividades sospechosas, incluso cuando los atacantes utilizan IA generativa para evadir controles.

Además, Google reforzó sus políticas publicitarias con múltiples actualizaciones y mecanismos como la verificación de anunciantes, enfrentando amenazas como fraudes, campañas engañosas y uso de deepfakes.

En conjunto, esto demuestra una evolución hacia modelos de detección preventiva y análisis basado en intención, impulsados por IA.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566 – Phishing	Uso de anuncios engañosos para redirigir usuarios a sitios maliciosos o robar información.
TA0002: Ejecución	T1204 – User Execution	El usuario interactúa con anuncios fraudulentos que desencadenan descargas o ejecución de contenido malicioso.
TA0005: Evasión de Defensa	T1036 – Masquerading	Creación de anuncios que aparentan ser legítimos (marcas, servicios reales).
TA0006: Acceso a Credenciales	T1556 – Modify Authentication Process	Manipulación de formularios o páginas falsas para capturar credenciales.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Envío de datos recolectados desde sitios fraudulentos hacia servidores controlados por atacantes.
TA0040: Impacto	T1657 – Data Manipulation / Fraud	Generación de fraudes mediante anuncios falsos, deepfakes o suplantación de identidad.

Recomendaciones

- Implementar soluciones de detección basadas en comportamiento e inteligencia artificial para identificar campañas maliciosas y anomalías en tráfico web.
- Aplicar controles de filtrado web y DNS para bloquear dominios asociados a publicidad maliciosa o redirecciones sospechosas.
- Fortalecer la concientización de usuarios frente a anuncios engañosos, phishing y contenido generado con IA como deepfakes.
- Integrar mecanismos de verificación de identidad y reputación en plataformas digitales para reducir el riesgo de suplantación.
- Mantener monitoreo continuo del tráfico HTTP/HTTPS mediante herramientas SIEM o proxy seguro para detectar comunicaciones con infraestructuras maliciosas.
- Actualizar políticas de seguridad y controles de navegación para adaptarse a amenazas emergentes impulsadas por IA generativa.

CRÍTICA**3.2 ¿Qué es "QRishing"?, la amenaza que se esconde detrás de un código QR**

Las autoridades europeas han alertado sobre el aumento del QRishing, una variante del phishing que utiliza códigos QR maliciosos para redirigir a las víctimas a sitios fraudulentos.

Los atacantes manipulan códigos QR (por ejemplo, con pegatinas sobre códigos legítimos) para dirigir a páginas falsas que imitan servicios reales, donde solicitan datos personales o bancarios.

Este tipo de ataque se ha expandido debido al uso masivo de códigos QR en la vida cotidiana (restaurantes, pagos, multas, paquetes). Una vez obtenida la información, los atacantes pueden realizar fraude, robo de identidad o incluso desplegar malware.

Organismos como el Instituto Nacional de Ciberseguridad (INCIBE) recomiendan verificar los enlaces antes de acceder y desconfiar de códigos QR de origen dudoso.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566 – Phishing	Uso de códigos QR para engañar a usuarios y redirigirlos a sitios maliciosos.
TA0005: Evasión de Defensas	T1036 – Masquerading	Creación de páginas falsas que imitan servicios legítimos (bancos, empresas).
TA0006: Acceso a Credenciales	T1556 – Modify Authentication Process	Captura de credenciales a través de formularios falsos.
TA0009: Recolección	T1005 – Data from Local System	Obtención de información personal ingresada (correo, teléfono, datos bancarios).
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Envío de datos robados hacia servidores controlados por atacantes.
TA0040: Impacto	T1657 – Fraud / Identity Theft	Uso de la información robada para fraude financiero o suplantación de identidad.

Recomendaciones

- Evitar escanear códigos QR de origen desconocido y verificar visualmente que no hayan sido manipulados (ej. pegatinas sobrepuestas).
- Configurar los dispositivos móviles para mostrar la URL completa antes de acceder, validando el dominio del sitio.
- Implementar soluciones de seguridad móvil (MTD/Mobile Security) que analicen enlaces maliciosos en tiempo real.
- Capacitar a los usuarios sobre riesgos de QRishing, enfatizando la verificación de sitios web antes de ingresar información sensible.
- Mantener actualizadas las herramientas de protección del dispositivo (antivirus, navegador seguro, filtros web).
- Aplicar controles de filtrado DNS/URL en redes corporativas para bloquear dominios fraudulentos.

ALTA

3.3 Intervención policial de infraestructura criminal de phishing y toma de cuentas bancarias mediante apps maliciosas



La Policía Nacional desarticuló en Magdalena del Mar (Lima) una red de fraude digital tras detectar transferencias bancarias sospechosas. Cinco personas fueron capturadas en flagrancia cuando intentaban retirar dinero obtenido mediante engaños virtuales.

La organización operaba mediante phishing, suplantando entidades bancarias y utilizando técnicas como el enmascaramiento de llamadas para generar confianza. Las víctimas eran inducidas a descargar aplicaciones falsas, lo que permitía a los atacantes obtener credenciales y tomar control de sus cuentas bancarias.

Posteriormente, realizaban transferencias y retiraban el dinero mediante intermediarios. El operativo permitió recuperar aproximadamente S/ 10 000, evidenciando una estructura organizada con roles definidos.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1649 – Steal or Forge Authentication Certificates / Caller ID Spoofing	Enmascaramiento de números telefónicos para aparentar legitimidad.
TA0002: Ejecución	T1204 – User Execution	Inducción a la víctima para descargar aplicaciones maliciosas.
TA0005: Evasión de Defensas	T1406 – Obfuscated Files or Information (Mobile)	Ocultamiento de comportamiento malicioso en apps móviles.
TA0006: Acceso a Credenciales	T1555 – Credentials from Password Stores	Obtención de credenciales almacenadas en el dispositivo.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Envío de credenciales y datos a una infraestructura controlada por atacantes.
TA0040: Impacto	T1657 – Fraud / Financial Theft	Transferencias no autorizadas y retiro de dinero mediante intermediarios.

Recomendaciones

- Evitar descargar aplicaciones fuera de tiendas oficiales y validar siempre que pertenezcan realmente a entidades bancarias.
- Implementar autenticación multifactor (MFA) en cuentas bancarias para mitigar el uso indebido de credenciales.
- Capacitar a los usuarios para identificar intentos de phishing y llamadas fraudulentas, especialmente aquellas que soliciten acciones urgentes.
- Utilizar soluciones de seguridad móvil (antimalware) que detecten aplicaciones maliciosas y comportamientos sospechosos.
- Monitorear transacciones bancarias en tiempo real y activar alertas ante movimientos inusuales.
- Aplicar controles de seguridad como bloqueo de instalación de apps desconocidas en dispositivos corporativos.

4. Adversarios

CRÍTICA

4.1 Atacantes explotan MSBuild (LOLBin) para evadir detección en ataques "Fileless"



El 13 de abril de 2026, reportes de seguridad destacaron el uso creciente de MSBuild.exe, una herramienta de desarrollo nativa y firmada digitalmente por Microsoft, como un binario de tipo LOLBin (Living Off the Land Binary) para ejecutar intrusiones sigilosas y sin archivos (fileless).

Al abusar de esta herramienta, los atacantes logran incrustar y ejecutar código C# malicioso directamente desde archivos de proyectos XML (.csproj) en la memoria, eludiendo por completo las defensas basadas en firmas y los análisis de comportamiento de Windows Defender.

En febrero de 2026, la firma Lab52 reportó una campaña de phishing que utilizaba esta técnica: los atacantes enviaron un archivo ZIP simulando una invitación a una reunión que contenía un MSBuild.exe renombrado y un proyecto malicioso.

Al ejecutarse, MSBuild contactaba servidores externos, descargaba cargas útiles en directorios temporales y, mediante la carga lateral de DLL (DLL Sideload), ejecutaba el malware PlugX de manera encubierta, logrando que tanto el endpoint como el antivirus percibieran toda la cadena de ejecución como legítima.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.001 – Phishing: Spearphishing Attachment	Distribución inicial a través de una campaña de phishing utilizando un archivo ZIP adjunto disfrazado de una invitación a una reunión.
TA0005: Evasión de Defensa	T1218.011 – System Binary Proxy Execution: MSBuild	Abuso del binario legítimo y firmado MSBuild.exe para compilar y ejecutar código C# malicioso en memoria eludiendo alertas de seguridad.
TA0002: Ejecución	T1059.009 – Command and Scripting Interpreter: C#	Ejecución directa de lógica maliciosa (fileless) incrustada dentro de archivos de configuración de proyectos XML (.csproj).
TA0011: Comando y Control	T1105 – Ingress Tool Transfer	Uso de la lógica del script de MSBuild para contactar servidores controlados por el atacante y descargar cargas útiles codificadas en carpetas temporales.
TA0005: Evasión de Defensa	T1574.002 – Hijack Execution Flow: DLL Side-Loading	Ejecución de un programa aparentemente legítimo diseñado para cargar en memoria una DLL maliciosa y desplegar el malware PlugX de manera encubierta.

Recomendaciones

- Alertar sobre ejecución de MSBuild.exe en estaciones no dev, o desde rutas temporales o inusuales.
- Detectar y bloquear cadenas anómalas donde MSBuild.exe genere procesos como PowerShell.exe, cmd.exe u otros no asociados a compilación legítima.
- Impedir la ejecución directa de .csproj o .xml desde directorios como Temp o Downloads.
- Detectar conexiones salientes de MSBuild.exe hacia IPs o dominios externos no autorizados.
- Aplicar controles para identificar carga de DLLs no estándar desde directorios temporales o asociados a payloads.

CRÍTICA**4.2 Sitio web de CPUID comprometido para distribuir el troyano STX RAT mediante falsas descargas**

Entre el 9 y el 10 de abril de 2026, el popular sitio web de utilidades de hardware CPUID (creadores de software como CPU-Z y HWMonitor) fue víctima de un ataque de tipo watering hole. Los atacantes comprometieron una API secundaria del sitio, provocando que los enlaces de descarga legítimos redirigieran aleatoriamente a los usuarios hacia repositorios maliciosos alojados en buckets de Cloudflare R2.

Las víctimas descargaron archivos que contenían el ejecutable original firmado junto con una biblioteca maliciosa (CRYPTBASE.dll). Al iniciar la aplicación, se desencadenaba una carga lateral (DLL Sideload) que, tras realizar comprobaciones para evadir entornos sandbox, instalaba el troyano de acceso remoto STX RAT.

Este malware está diseñado para robar credenciales, cookies de navegadores, billeteras de criptomonedas y claves de clientes FTP, enviándolas a un servidor C2 (supp0v3[.]com).

Se han identificado más de 150 víctimas — incluyendo organizaciones de manufactura, telecomunicaciones y retail— y los investigadores sugieren que el ataque fue perpetrado por un actor de amenazas con vínculos rusos.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1189 – Drive-by Compromise	Compromiso de una API en el sitio web legítimo de CPUID para redirigir aleatoriamente a los usuarios a descargas maliciosas (Watering Hole).
TA0002: Ejecución	T1204.002 – User Execution: Malicious File	Descarga y ejecución voluntaria por parte de la víctima del instalador malicioso creyendo que se trata de una utilidad de sistema legítima.
TA0005: Evasión de Defensa	T1574.002 – Hijack Execution Flow: DLL Side-Loading	Abuso del ejecutable legítimo y firmado para cargar en memoria la biblioteca maliciosa CRYPTBASE.dll adjunta en el mismo paquete.
TA0005: Evasión de Defensa	T1497.001 – Virtualization/Sandbox Evasion: System Checks	Ejecución de verificaciones del entorno del sistema para confirmar que no está siendo analizado en un sandbox antes de conectar con el C2.
TA0006: Acceso a Credenciales	T1555 – Credentials from Password Stores	Robo sistemático de credenciales, cookies de navegadores web, billeteras de criptomonedas y contraseñas de clientes FTP.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Comunicación con la infraestructura maliciosa (supp0v3[.]com y ai.supp0v3[.]com) para gestionar la infección y exfiltrar datos.

Recomendaciones

- Revisar logs de DNS, proxy y firewall en busca de conexiones a supp0v3[.]com y ai.supp0v3[.]com desde el 09/04/2026.
- Detectar descargas recientes de herramientas CPUID o similares (p. ej., HWiNFO_Monitor_Setup.exe) y la presencia de CRYPTBASE.dll en directorios asociados.
- Ante sospecha de STX RAT, aislar equipos afectados y rotar credenciales, tokens, cookies y accesos corporativos.
- Configurar EDR/XDR para alertar sobre carga de DLLs no firmadas o no estándar desde rutas temporales o de usuario.
- Mantener listas de bloqueo para dominios de hosting bulletproof y certificados SSL inconsistentes o no válidos para la entidad emisora.

CRÍTICO**4.3 GopherWhisper: grupo APT alineado con China usó Discord y Slack para atacar organismos gubernamentales**

Investigadores de ESET Research han identificado a un nuevo grupo de Amenaza Persistente Avanzada (APT) denominado "GopherWhisper", alineado con China y enfocado en atacar entidades gubernamentales, con especial énfasis en Mongolia.

Sumado a la inyección de código en procesos del sistema operativo como `svchost.exe`, GopherWhisper logra operar de manera extremadamente sigilosa, ocultando su tráfico malicioso dentro del flujo de red habitual de las organizaciones.

Activo al menos desde 2024, el grupo destaca por su alto nivel de desarrollo técnico, utilizando un sofisticado ecosistema de herramientas maliciosas personalizadas programadas en lenguaje Go (como los inyectores JabGopher, el loader FriendDelivery y múltiples backdoors como LaxGopher y SSLORDoor).

La principal amenaza de este grupo radica en su técnica de evasión: abusan de servicios legítimos y de confianza —incluyendo Slack, Discord, file.io y Microsoft 365 Outlook (utilizando la API de Microsoft Graph para comunicarse a través de borradores de correo)— para camuflar sus comunicaciones de Comando y Control (C2) y la exfiltración de datos.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1195 – Supply Chain Compromise	Uso potencial de software o recursos comprometidos para infiltración.
TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Ejecución de comandos mediante cmd.exe desde los backdoors.
TA0003: Persistencia	T1547 – Boot or Logon Autostart Execution	Uso de loaders y DLLs maliciosas para mantener persistencia.
TA0005: Evasión de Defensas	T1036 – Masquerading	Uso de archivos disfrazados (ej. whisper.dll) para ocultar malware.
TA0008: Movimiento Lateral	T1021 – Remote Services	Expansión a otros sistemas dentro de la red comprometida.
TA0011: Comando y Control	T1102 – Web Service	Abuso de servicios legítimos como Slack, Discord y Microsoft 365.

Recomendaciones

- Implementar monitoreo avanzado de tráfico hacia servicios legítimos (Slack, Discord, Microsoft 365), ya que pueden ser utilizados como canales C2.
- Aplicar soluciones EDR/XDR capaces de detectar inyección de procesos y ejecución en memoria.
- Restringir el uso de aplicaciones no autorizadas mediante políticas de control de aplicaciones (whitelisting).
- Supervisar el uso de APIs como Microsoft Graph para detectar comportamientos anómalos en cuentas de correo.
- Implementar segmentación de red para limitar el movimiento lateral en caso de compromiso.
- Correlacionar eventos en SIEM para identificar patrones de actividad APT (comandos remotos, exfiltración, uso de servicios cloud).

5. Indicadores de Compromiso

5.1 Direcciones IP

59[.]36[.]233[.]74	40[.]124[.]175[.]60	91[.]191[.]209[.]198
172[.]94[.]9[.]50	193[.]163[.]125[.]142	34[.]76[.]250[.]139
104[.]252[.]175[.]235	101[.]206[.]107[.]245	209[.]99[.]189[.]177
2[.]57[.]122[.]193	182[.]109[.]0[.]59	66[.]132[.]195[.]47

5.2 Dominios

careers[-]medtronic[.]com	go[-]connect[.]work
css[.]xcss[.]me	usrpubtrk[.]com
ads[.]tiogolhd[.]com	fj0r8[-]chain[.]so6lavern[.]garden
dyncorear[.]so6lavern[.]garden	ycout[.]yxponte[.]com
tvtvhd[.]com	pl28819760[.]effectivegatecpm[.]com
bulddiamond[.]net	ql24[.]com

5.3 Hashes

f6303471df0eb6393fbb84b151f0629bcd9677c1035598a464ebac7e7e4bcd
99d038a345d0db462629537744627a9e72ec490b6bbac47f8ed240db53e6eb46
97fb83007d6112a56c66d18bb2314d5eae12d83ef512c976b8b0b9ea33bbcaa6
fe44ddb7f980df41ed4d42c98a68583a2cf35a93fd9cc842ff44f74d2a19f7fc
ce32ad6ee5e9302329f9af9b1d7b748ca8f94983bab0f5fa4c3cdd846960bd7d
5c2819ebc600adc7fcad0002e6056e824e1af35d1e16334e16199712850a208f
2c651833512a0dba3213a82bf3cfd847cf71bab288bbef8c8d207f8cba86c3c2
4bb245ba8dcd49d077f713c1de90a977cc61eb231e92975abc4928ed9a2f3d0f
7f866eb81a5422af576b17bad6e7a3301591377b869b50df17c061784d72286a
f25fa9c1dbe672deafec34e8ca211002dfb41a412013daae5de3c0056bc3c6ea
e60ab99da105ee27ee09ea64ed8eb46d8edc92ee37f039dbc3e2bb9f587a33ba
a35d9ec6dbd33257d6e38c1ccf46ebd2ee36691a04cb119c99bea80257ba02b5
015d31611fbf8aa1e503bddfa99798d848c93760bd499af719e610547ddb8837

6. Fuentes

- 6.1 <https://therecord.media/chipsoft-ransomware-attack-disrupts-dutch-hospitals>
- 6.2 <https://securelist.com/janelarat-financial-threat-in-latin-america/119332/>
- 6.3 <https://www.hornetsecurity.com/en/blog/monthly-threat-report/>
- 6.4 https://computerhoy.20minutos.es/ciberseguridad/una-nueva-vulnerabilidad-linux-bautizada-como-pack2theroot-permite-obtener-acceso-como-administrador-forma-muy-sencilla_6963744_0.html
- 6.5 <https://elcomercio.pe/tecnologia/ciberseguridad/que-es-qrishing-la-amenaza-que-se-esconde-detras-de-un-codigo-qr-malware-virus-noticia/>
- 6.6 <https://elcomercio.pe/tecnologia/inteligencia-artificial/la-ia-ayudo-a-google-a-bloquear-millones-de-anuncios-maliciosos-noticia/>
- 6.7 <https://tn.com.ar/tecno/novedades/2026/04/08/cibercriminales-usaron-el-codigo-filtrado-de-claude-para-distribuir-virus-infostealers-en-internet/>
- 6.8 <https://gbhackers.com/msbuild-lolbin/>
- 6.9 <https://www.americatv.com.pe/noticias/actualidad/caen-cyberinjertos-sur-fraude-digital-n517727>
- 6.10 <https://www.welivesecurity.com/es/investigaciones/gopherwhisper-apt-china-discord-slack/>