



GS PERÚ

Software - Security & Services

Empresas

BOLETÍN CIBERSEGURIDAD

Febrero - 2026



ÍNDICE

	1. Malware	4
	1.1 PromptSpy: Malware Android impulsado por IA Gemini para garantizar persistencia	
	1.2 FBI alerta sobre aumento de ataques de “jackpotting” con malware Ploutus en cajeros automáticos de EE.UU.	
	1.3 Steaelite: RAT para Windows que unifica robo de datos y ransomware en un solo panel.	
	1.4 Keenadu: malware Android que puede venir preinstalado y comprometer el dispositivo desde fábrica.	
	1.5 Ransomware impacta a Advantest: proveedor clave de la industria de semiconductores.	
	1.6 Campaña ClickFix distribuye MIMICRAT mediante sitios legítimos comprometidos.	
	1.7 GhostRAT Loader facilita infecciones persistentes mediante ejecución por etapas.	
	2. Vulnerabilidades	18
	2.1 CVE-2026-21510 – Omisión de la función de seguridad de Windows Shell.	
	2.2 CVE-2026-21513 permite omitir funciones de seguridad en Internet Explorer.	
	2.3 CVE-2026-21514 permite ejecución de código mediante archivos Office maliciosos.	
	3. Phishing	24
	3.1 “Starkiller” ofrece phishing como servicio con proxy en tiempo real y evasión de MFA.	
	3.2 Campaña de phishing apunta a asistentes de la India AI Impact Summit 2026 mediante SMS y WhatsApp.	
	4. Adversarios	28
	4.1 Actor de amenazas en foco – DRAGONFLY (TA17-293A): Operaciones cibernéticas contra infraestructura crítica.	
	4.2 Google desmantela grupo de hackers vinculado a China que atacó 53 organizaciones	
	5. Indicadores de compromiso	32
	5.1 Direcciones IP	
	5.2 Dominios	
	5.3 Hashes	
	6. Fuentes	



1. Malware

1.1 PromptSpy: Malware Android impulsado por IA Gemini para garantizar persistencia

PromptSpy es un malware que utiliza IA generativa para interpretar escenarios de interfaz de usuario y ejecutar instrucciones paso a paso, permitiéndole mantenerse activo en el dispositivo. Fue desarrollado en un entorno de habla china, aunque se distribuyó principalmente a usuarios hispanohablantes en América del Sur.

El malware no se encuentra en Google Play, aunque versiones conocidas son detectadas por Google Play Protect. Solicita permisos del Servicio de Accesibilidad para capturar el contexto de la interfaz y ejecutar acciones en segundo plano sin intervención del usuario. Se bloquea en la lista de aplicaciones recientes y superpone elementos transparentes sobre botones de desinstalación, dificultando su eliminación.

La comunicación con el servidor de comando y control está cifrada y permite recibir claves API para interactuar con Gemini. La infección inicia con un dropper que simula una actualización en español, enviando capturas XML de la pantalla y recibiendo instrucciones JSON de Gemini, que ejecuta gestos automáticamente para asegurar persistencia y control completo del dispositivo.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1204 – User Execution	Distribución mediante aplicación dropper que simula una actualización legítima en español para inducir la instalación manual por parte del usuario.
TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Ejecución de instrucciones generadas dinámicamente por IA (Gemini) en formato JSON para realizar acciones automatizadas en el dispositivo.
TA0004: Escalada de Privilegios	T1548 – Abuse Elevation Control Mechanism	Abuso del Servicio de Accesibilidad de Android para obtener capacidades avanzadas de control sobre la interfaz del sistema.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Superposición de elementos transparentes sobre botones de desinstalación y bloqueo en aplicaciones recientes para impedir su eliminación.
TA0006: Acceso a Credenciales	T1555 – Credentials from Password Stores	Captura de credenciales mediante monitoreo de interfaz, registro de gestos y control remoto vía módulo VNC.
TA0007: Descubrimiento	T1010 – Application Window Discovery	Captura de instantáneas XML de la pantalla para analizar el contexto de la interfaz y adaptar acciones automáticamente.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Comunicación cifrada (AES) con servidor C2 para recibir instrucciones y claves API necesarias para interactuar con Gemini.
TA0003: Persistencia	T1542 – Pre-OS Boot / System Persistence	Uso de instrucciones de IA para mantenerse fijado en aplicaciones recientes y reactivar procesos tras intentos de cierre.

Recomendaciones

- Restringir permisos de accesibilidad: Permitir solo a aplicaciones confiables mediante políticas MDM.
- Control de instalación de apps: Bloquear fuentes desconocidas y usar listas blancas de apps autorizadas.
- Seguridad móvil avanzada: Implementar MTD/EDR para detectar comportamientos anómalos y malware.
- Monitoreo de tráfico: Analizar comunicaciones hacia dominios o IP sospechosas.
- Concientización del usuario: Evitar instalar actualizaciones fuera de tiendas oficiales y revisar permisos de apps.
- Actualización y protección: Mantener dispositivos y apps actualizadas, activar Google Play Protect y aplicar políticas de seguridad.



1.2 FBI alerta sobre aumento de ataques de “jackpotting” con malware Ploutus en cajeros automáticos de EE.UU.

En febrero de 2026, el FBI emitió una alerta IC3 FLASH advirtiendo sobre un aumento de ataques de “jackpotting” contra cajeros automáticos en Estados Unidos. Este tipo de ataque no compromete cuentas bancarias, sino que infecta directamente el cajero para forzar la dispensación de efectivo sin una transacción legítima.

El malware identificado incluye la familia Ploutus, que interactúa con la capa XFS para enviar comandos directos al hardware y ordenar la salida de dinero sin autorización. Muchos incidentes inician con acceso físico al cajero, donde los atacantes manipulan o reemplazan el disco duro para instalar el código malicioso. Los equipos con Windows son un objetivo frecuente, ya que el malware puede adaptarse entre distintos fabricantes.

Entre los indicadores de compromiso se incluyen ejecutables sospechosos, herramientas de acceso remoto no autorizadas y persistencia anómala en el sistema. El FBI recomienda validar la integridad de los sistemas con imágenes de referencia, restringir el uso de USB, reforzar controles físicos y monitorear señales de manipulación para prevenir nuevos ataques.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1200 – Hardware Additions	Instalación del malware mediante acceso físico al cajero automático, manipulando o reemplazando el disco duro e introduciendo dispositivos USB maliciosos.
TA0002: Ejecución	T1106 – Native API	Envío de comandos directos a la capa XFS del cajero para interactuar con el hardware y ordenar la dispensación de efectivo.
TA0003: Persistencia	T1547 – Boot or Logon Autostart Execution	Configuración de ejecutables o servicios personalizados en Windows para mantener el malware activo tras reinicios.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Uso de herramientas de acceso remoto no autorizadas y binarios disfrazados para evadir controles de seguridad locales.
TA0007: Descubrimiento	T1018 – Remote System Discovery	Identificación del entorno del cajero y validación del sistema operativo Windows para adaptar el malware al fabricante.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Comunicación con herramientas remotas (ej. AnyDesk/TeamViewer) para control operativo del sistema comprometido.
TA0040: Impacto	T1071 – Application Layer Protocol	Comunicación cifrada (AES) con servidor C2 para recibir instrucciones y claves API necesarias para interactuar con Gemini.
TA0003: Persistencia	T1496 – Resource Hijacking	Manipulación directa del hardware del cajero para forzar la dispensación de efectivo sin autorización bancaria.

Recomendaciones:

- Controles físicos en cajeros: Mejorar cerraduras, sensores, alarmas y videovigilancia con retención adecuada.
- Control de USB y dispositivos: Permitir solo hardware autorizado y deshabilitar puertos no esenciales.
- Hardening de Windows: Validar integridad con imagen dorada, cifrado de disco, arranque seguro y TPM.
- Restricción de acceso remoto: Bloquear o monitorear AnyDesk, TeamViewer y alertar ante instalaciones no autorizadas.
- Monitoreo de integridad: Detectar ejecutables no firmados, cambios en servicios o en el registro.

 ALTA

1.3 Steaelite: RAT para Windows que unifica robo de datos y ransomware en un solo panel

Steaelite es un malware como servicio que integra acceso remoto, recolección de credenciales, exfiltración de información y un módulo de ransomware en desarrollo dentro de una única plataforma web de administración.

La herramienta fue identificada por investigadores de BlackFog y se comercializa en foros clandestinos desde noviembre, incluyendo material promocional en YouTube.

Permite ejecución remota de código, administración de archivos, transmisión en vivo del escritorio y activación de cámara y micrófono en equipos comprometidos.

Incluye funciones de keylogging, monitoreo del portapapeles, recuperación de contraseñas y enumeración de programas instalados en el sistema.

El panel avanzado ofrece desactivación de Windows Defender, evasión de UAC, persistencia, acceso RDP oculto y capacidad de propagación mediante dispositivos USB.

El robo de datos puede comenzar de forma automatizada incluso antes de que el operador interactúe manualmente con la víctima.

Su modelo de suscripción mensual facilita que un único actor ejecute campañas completas de doble extorsión sin cambiar de herramienta.

Una vez desplegado el módulo de cifrado, permitirá exfiltrar información y posteriormente cifrar los sistemas afectados desde el mismo entorno de control.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1200 – Hardware Additions	Distribución del malware mediante ingeniería social o instalación encubierta disfrazada de software legítimo para comprometer equipos Windows.
TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Ejecución remota de comandos y cargas útiles VB.NET desde el panel web para controlar el sistema infectado.
TA0003: Persistencia	T1547 – Boot or Logon Autostart Execution	Configuración de mecanismos de inicio automático y servicios persistentes para mantener el acceso tras reinicios.
TA0006: Credential Access	T1056 – Input Capture	Implementación de keylogging y monitoreo del portapapeles para capturar credenciales y datos sensibles.
TA0007: Descubrimiento	T1082 – System Information Discovery	Enumeración de programas instalados, procesos activos y reconocimiento del entorno comprometido.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Extracción automatizada de documentos y credenciales a través del canal de comando y control.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Gestión centralizada desde un panel basado en navegador con comunicación remota para control total del sistema.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Gestión centralizada desde un panel basado en navegador con comunicación remota para control total del sistema.

Recomendaciones:

- EDR/XDR y anti-tampering: Proteger endpoints y evitar desactivación de defensas incluso con privilegios elevados.
- Control de privilegios y credenciales: Aplicar mínimo privilegio, MFA y monitoreo de accesos críticos.
- Bloqueo de accesos remotos no autorizados: Restringir RDP, AnyDesk, TeamViewer y alertar ante conexiones no aprobadas.
- Prevención de exfiltración de datos: Implementar DLP, monitorear tráfico saliente y detectar transferencias sospechosas.
- Hardening de Windows: Deshabilitar servicios innecesarios, usar listas blancas y mantener parches actualizados.
- Respallos y segmentación de red: Mantener backups inmutables, probar restauraciones y segmentar la red para limitar daños.

 ALTA

1.4 Keenadu: malware Android que puede venir preinstalado y comprometer el dispositivo desde fábrica

Keenadu es un malware para Android identificado en febrero de 2026 que puede integrarse en el firmware del dispositivo, en aplicaciones del sistema o distribuirse mediante tiendas oficiales, afectando el equipo incluso antes de su primer uso.

Se emplea principalmente para fraude publicitario, generando clics invisibles en anuncios, aunque algunas variantes permiten a los atacantes obtener control avanzado del sistema.

Hasta la fecha se han detectado más de 13.000 dispositivos comprometidos a nivel global, con mayor impacto en América Latina, especialmente en Brasil.

Cuando está integrado en el firmware, funciona como puerta trasera con privilegios elevados, capaz de instalar aplicaciones sin autorización y modificar las existentes.

Puede acceder a archivos, mensajes, credenciales bancarias, datos de ubicación e incluso monitorear actividad del navegador, representando un riesgo significativo para la privacidad del usuario.

Su presencia en componentes críticos del sistema y en aplicaciones distribuidas por tiendas oficiales refuerza la gravedad del incidente dentro de la cadena de suministro tecnológica.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1195 – Supply Chain Compromise	Integración del malware en el firmware del dispositivo durante fabricación o distribución, comprometiendo el equipo antes de su venta.
TA0001: Acceso Inicial	T1476 – Deliver Malicious App	Distribución mediante aplicaciones infectadas en Google Play o apps de sistema preinstaladas.
TA0002: Ejecución	T1402 – Broadcast Receivers (Android)	Ejecución automática del malware tras eventos del sistema, como inicio del dispositivo o instalación de apps.
TA0003: Persistencia	T1547 – Boot or Logon Autostart Execution	Integración en componentes críticos del sistema (launcher o desbloqueo facial) para mantenerse activo tras reinicios.
TA0005: Evasión de Defensa	T1622 – Debugger Evasion	Activación selectiva según idioma o zona horaria para evitar detección en ciertos entornos.
TA0006: Acceso a Credenciales	T1555 – Credentials from Password Stores	Recolección de credenciales almacenadas en el dispositivo, incluyendo datos bancarios y cuentas guardadas en apps.
TA0009: Colección	T1513 – Screen Capture / Input Capture	Monitoreo de actividad del usuario, incluyendo búsquedas en navegador y posible acceso a datos biométricos.
TA0040: Impacto	T1496 – Resource Hijacking	Uso del dispositivo para fraude publicitario generando clics invisibles en segundo plano.

Recomendaciones:

- Cadena de suministro segura: Comprar solo a fabricantes y distribuidores autorizados, verificando firmas de firmware y parches.
- Auditoría de firmware y apps: Revisar dispositivos nuevos para detectar apps sospechosas o permisos excesivos.
- MDM y control de apps: Restringir instalaciones no autorizadas, auditar privilegios y controlar apps del sistema.
- Protección móvil avanzada (MTD/EDR): Detectar malware, puertas traseras y comportamientos persistentes.
- Monitoreo de tráfico y actividad: Analizar conexiones salientes y consumo anómalo de recursos.
- Actualizaciones y seguridad del sistema: Mantener SO, Google Play Services y apps críticas actualizados.
- Control de permisos críticos: Limitar accesos innecesarios de apps relacionadas con biometría o administración del dispositivo.



1.5 Ransomware impacta a Advantest: proveedor clave de la industria de semiconductores

En febrero de 2026, Advantest Corporation, fabricante japonés de equipos de prueba para semiconductores, confirmó un incidente de ransomware que afectó parte de su infraestructura de TI. La compañía detectó actividad inusual el 15 de febrero en su red corporativa, activando de inmediato sus protocolos internos de respuesta a incidentes y aislamiento de sistemas comprometidos.

Los análisis preliminares indican que un tercero no autorizado obtuvo acceso a segmentos de la red e implementó malware para cifrar sistemas internos. Advantest contrató expertos externos en ciberseguridad para apoyar la investigación forense, contención del incidente y evaluación del posible alcance del compromiso.

Hasta el 23 de febrero no se había confirmado filtración de datos, aunque la compañía notificará directamente a clientes o empleados si se determina afectación de información sensible. Advantest, proveedor de soluciones de prueba para chips de 5G, IoT, vehículos autónomos e inteligencia artificial, no detalló qué servicios fueron impactados ni el efecto operativo sobre clientes.

El incidente evidencia el riesgo creciente del ransomware sobre infraestructuras críticas y cadenas de suministro estratégicas a nivel global.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Posible explotación de servicios expuestos o credenciales comprometidas para obtener acceso inicial a la red corporativa.
TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Uso de scripts o comandos para desplegar el ransomware dentro de sistemas comprometidos.
TA0003: Persistencia	T1547 – Boot or Logon Autostart Execution	Configuración de servicios o tareas programadas para mantener acceso tras reinicios del sistema.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Desactivación o alteración de herramientas de seguridad para evitar detección antes del cifrado.
TA0007: Descubrimiento	T1083 – File and Directory Discovery	Enumeración de archivos, servidores y recursos compartidos dentro de la red antes de ejecutar el cifrado.
TA0008: Movimiento Lateral	T1021 – Remote Services	Propagación del ransomware a otros sistemas mediante servicios remotos internos (RDP, SMB, etc.).
TA0011: Comando y Control	T1071 – Application Layer Protocol	Comunicación con infraestructura externa para recibir instrucciones o transmitir información previa al cifrado.
TA0040: Impacto	T1486 – Data Encrypted for Impact	Cifrado de sistemas y archivos corporativos para interrumpir operaciones y forzar negociación de rescate.

Recomendaciones:

- Segmentación y Zero Trust: Separar entornos críticos y limitar movimiento lateral con controles de identidad y mínimo privilegio.
- Protección de endpoints (EDR/XDR): Detectar comportamientos previos al cifrado y bloquear desactivación de defensas.
- Gestión de parches y servicios expuestos: Mantener sistemas y dispositivos actualizados para reducir la superficie de ataque.
- Control de accesos privilegiados (PAM): MFA y monitoreo continuo de cuentas administrativas.
- Backups inmutables y recuperación: Mantener copias cifradas y aisladas, probando restauraciones periódicamente.



1.6 Campaña ClickFix distribuye MIMICRAT mediante sitios legítimos comprometidos

En febrero de 2026, Elastic Security Labs reportó una campaña ClickFix que utiliza sitios web legítimos comprometidos, como bincheck.io, para distribuir MIMICRAT (AstarionRAT), un troyano de acceso remoto previamente no documentado.

La operación destaca por su sofisticación técnica: emplea cadenas de ejecución PowerShell en múltiples etapas que desactivan mecanismos de seguridad de Windows como ETW y AMSI, antes de desplegar un cargador en Lua que ejecuta el malware en memoria. La víctima es inducida a copiar y ejecutar un comando en "Ejecutar", descargando scripts adicionales desde servidores C2 vía HTTPS simulando tráfico legítimo.

MIMICRAT, desarrollado en C++, ofrece 22 comandos de pos explotación, incluyendo suplantación de tokens, inyección de shellcode, acceso interactivo y tunelización por proxy SOCKS5. Se observan similitudes con campañas previas de Matanbuchus 3.0, sugiriendo posibles fines de ransomware o exfiltración de datos.

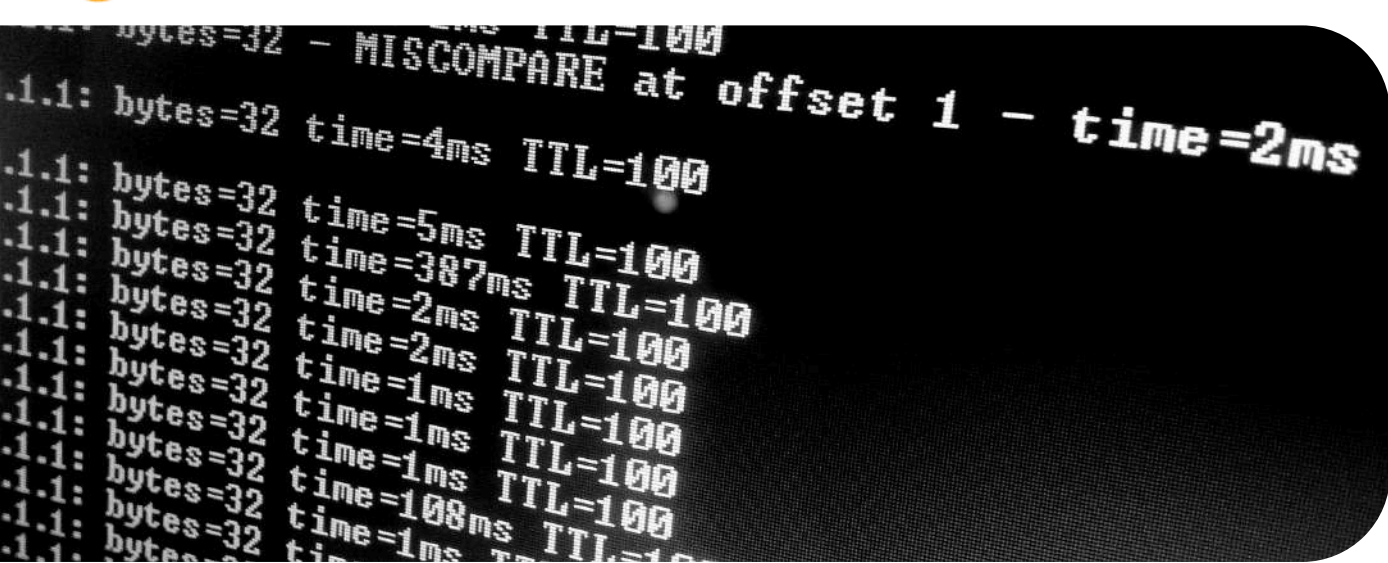
La campaña soporta 17 idiomas, adapta su contenido según la región del navegador y afecta víctimas globales, incluidas universidades en EE.UU. y usuarios de habla china, mostrando un alcance oportunista y amplio.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1189 – Drive-by Compromise	Compromiso de sitios legítimos (ej. bincheck[.]io) mediante inyección de JavaScript malicioso que redirige a la víctima a un señuelo ClickFix con falsa verificación de Cloudflare.
TA0002: Ejecución	T1059.001 – Command and Scripting Interpreter: PowerShell	Inducción a la víctima para ejecutar manualmente un comando PowerShell desde el cuadro “Ejecutar”, iniciando la cadena de infección en múltiples etapas.
TA0005: Evasión de Defensa	T1562.001 – Impair Defenses	Desactivación/parcheo de mecanismos de seguridad de Windows como ETW (Event Tracing for Windows) y AMSI antes de desplegar el implante final.
TA0002: Ejecución	T1055 – Process Injection	Descarga y ejecución en memoria de shellcode descifrado mediante un cargador basado en Lua para evitar detección en disco.
TA0003: Persistencia	T1134 – Access Token Manipulation	Uso de suplantación de tokens de Windows para mantener privilegios y facilitar movimiento lateral o ejecución privilegiada.
TA0007: Descubrimiento	T1082 – System Information Discovery	Recopilación de información del sistema y entorno de la víctima para adaptar comandos de posexplotación.
TA0011: Comando y Control	T1071.001 – Application Layer Protocol: Web Protocols	Comunicación con el servidor C2 mediante HTTPS por el puerto 443, utilizando perfiles HTTP que imitan tráfico legítimo de análisis web.
TA0008: Movimiento Lateral	T1090 – Proxy	Implementación de tunelización SOCKS5 para redirigir tráfico y facilitar acceso a otros sistemas internos.
TA0040: Impacto (Potencial)	T1486 – Data Encrypted for Impact / T1041 – Exfiltration Over C2 Channel	Posible despliegue posterior de ransomware o exfiltración de datos, según superposiciones con campañas vinculadas a Matanbuchus 3.0.

Recomendaciones:

- Bloqueo de comandos sospechosos: Restringir ejecución en “Ejecutar” o PowerShell sin privilegios elevados.
- Endurecimiento de PowerShell: Activar Constrained Language Mode, registro de scripts y ejecución firmada.
- Protección AMSI/ETW: Usar EDR que detecte manipulación y ejecución de código en memoria.
- Monitoreo de tráfico HTTPS: Revisar conexiones cifradas a dominios desconocidos o sospechosos.
- Control de integridad web: Monitorear portales y detectar inyecciones JavaScript no autorizadas.
- Filtrado DNS: Bloquear dominios asociados a C2 o categorizados como maliciosos.

 ALTA

1.7 GhostRAT Loader facilita infecciones persistentes mediante ejecución por etapas

En febrero de 2026, investigadores de seguridad identificaron GhostRAT Loader, un malware que actúa como cargador para desplegar GhostRAT, un troyano diseñado para mantener acceso remoto prolongado en sistemas Windows.

La infección se desarrolla en múltiples etapas: tras su ejecución inicial, el loader inicia procesos en segundo plano y descarga componentes adicionales, evitando comportamientos visibles que puedan alertar al usuario. Este enfoque permite una permanencia silenciosa dentro del entorno comprometido.

GhostRAT Loader implementa persistencia mediante modificaciones en el registro y configuraciones de inicio automático, asegurando su ejecución tras reinicios. También intenta escalar privilegios mediante manipulación de tokens de acceso para consolidar el control del sistema.

El malware utiliza intérpretes de comandos y módulos compartidos del sistema para ejecutar código sin depender de archivos evidentes, combinando técnicas de ofuscación y alteración de permisos para evadir detección. Posteriormente, realiza descubrimiento del entorno, recopila información del sistema y puede capturar datos del portapapeles o comunicarse con servidores externos para recibir instrucciones o transferir información.

Su comportamiento refleja un modelo de amenaza enfocado en sigilo, persistencia y control remoto sostenido, aumentando el riesgo de exposición prolongada de datos y credenciales.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Uso de intérpretes de comandos del sistema (línea de comandos / scripts) para iniciar la carga del malware y ejecutar componentes adicionales.
TA0002: Ejecución	T1129 – Shared Modules	Carga dinámica de módulos compartidos del sistema para ejecutar código sin depender de ejecutables evidentes.
TA0003: Persistencia	T1112 – Modify Registry	Modificación de claves del registro de Windows para asegurar permanencia tras reinicios.
TA0003: Persistencia	T1547 – Boot or Logon Autostart Execution	Configuración de mecanismos de inicio automático que permiten la ejecución del malware al arrancar el sistema o iniciar sesión.
TA0004: Escalada de Privilegios	T1134 – Access Token Manipulation	Manipulación de tokens de acceso para elevar privilegios y mantener mayor control sobre el sistema comprometido.
TA0005: Evasión de Defensa	T1027 – Obfuscated Files or Information	Uso de ofuscación, alteración de permisos y ejecución en segundo plano para evitar detección por herramientas de seguridad.
TA0007: Descubrimiento	T1082 – System Information Discovery	Recolección de información del sistema operativo, aplicaciones instaladas y entorno del dispositivo.
TA0007: Descubrimiento	T1083 – File and Directory Discovery	Exploración de archivos y directorios para identificar información relevante.
TA0009: Colección	T1115 – Clipboard Data	Captura de datos almacenados en el portapapeles del usuario.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Comunicación con servidores externos para recibir instrucciones remotas o transferir información.
TA0040: Impacto	T1529 – System Shutdown/Reboot	Posible reinicio o apagado forzado del sistema como parte de su lógica operativa o encubrimiento de actividad.

Recomendaciones:

- Zero Trust y MFA: Implementar confianza cero y autenticación multifactor en accesos críticos para proteger credenciales.
- Endurecimiento de configuraciones: Aplicar políticas robustas de autenticación, cifrado y gestión de accesos privilegiados (PAM).
- Gestión de parches: Mantener sistemas y software de seguridad actualizados para mitigar vectores de malware por etapas.
- Monitoreo SIEM/EDR: Detectar cambios sospechosos en registro, inicio automático, tokens y ejecución inusual de comandos.
- Supervisión de tráfico y C2: Revisar comunicaciones salientes a dominios o IP desconocidas asociadas a comando y control.
- Respallos y recuperación: Mantener copias periódicas, aisladas y probadas para restauración rápida ante incidentes.

 ALTA

2. Vulnerabilidades

2.1 CVE-2026-21510 – Omisión de la función de seguridad de Windows Shell

En febrero de 2026, investigadores de Microsoft y Google Threat Intelligence Group alertaron sobre CVE-2026-21510, una vulnerabilidad crítica que permite eludir las protecciones de Windows SmartScreen y Shell. La falla persuade a los usuarios a abrir enlaces maliciosos o archivos de acceso directo, requiriendo únicamente un clic para ser explotada.

Microsoft calificó la vulnerabilidad como importante, con una puntuación CVSS de 8,8, y advirtió que podría ser utilizada en ataques sofisticados para ejecutar código no autorizado y evadir los mecanismos de defensa predeterminados del sistema operativo.

El hallazgo se divulgó públicamente antes de que se liberara un parche oficial, lo que aumenta el riesgo para entornos corporativos y usuarios finales. Por ello, se recomienda implementar mitigaciones temporales, como restricciones en la ejecución de accesos directos y enlaces de origen desconocido, junto con monitoreo activo de sistemas potencialmente afectados.

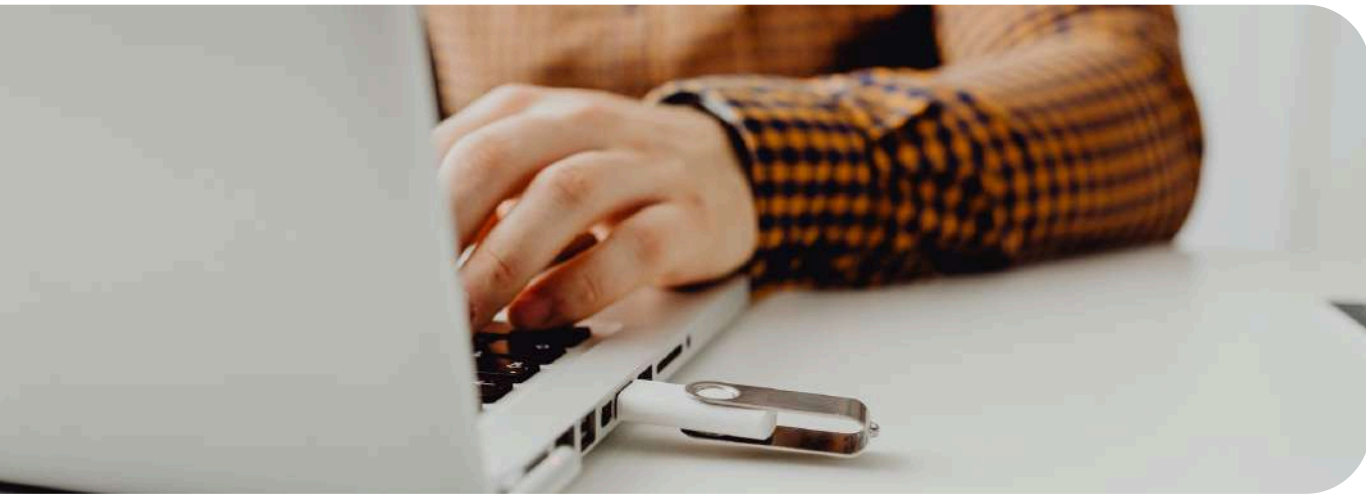
La situación destaca la importancia de mantener actualizados los sistemas y aplicar medidas preventivas para reducir la exposición frente a vulnerabilidades de alto impacto en Windows.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.002 – Phishing: Link	Envío de enlaces o archivos de acceso directo manipulados para inducir al usuario a hacer clic y activar la omisión de SmartScreen.
TA0002: Ejecución	T1204.001 – User Execution: Malicious Link	La explotación se activa con un solo clic del usuario al abrir el enlace o archivo especialmente diseñado.
TA0005: Evasión de Defensa	T1553.005 – Subvert Trust Controls: Mark-of-the-Web Bypass	Elusión de advertencias de seguridad de Windows SmartScreen y Windows Shell para permitir la ejecución sin alertas visibles.
TA0007: Descubrimiento	T1082 – System Information Discovery	Identificación básica del entorno Windows comprometido para adaptar acciones posteriores.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Posible establecimiento de comunicaciones salientes a través de protocolos web estándar tras la ejecución inicial.
TA0040: Impacto	T1203 – Exploitation for Client Execution	Ejecución de contenido no autorizado en el sistema afectado, comprometiendo la integridad y seguridad del entorno.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Comunicación cifrada (AES) con servidor C2 para recibir instrucciones y claves API necesarias para interactuar con Gemini.
TA0003: Persistencia	T1542 – Pre-OS Boot / System Persistence	Uso de instrucciones de IA para mantenerse fijado en aplicaciones recientes y reactivar procesos tras intentos de cierre.

Recomendaciones

- Aplicación de parches: Mantener Windows, Shell y software actualizado para cerrar CVE-2026-21510 y otros vectores.
- Bloqueo de archivos sospechosos: Restringir apertura de accesos directos o enlaces de fuentes no confiables.
- Monitoreo EDR: Detectar ejecuciones anómalas y bypass de SmartScreen en tiempo real.
- Educación del usuario: Capacitar sobre riesgos de enlaces y archivos desconocidos y verificar su legitimidad antes de hacer clic.
- Segmentación de entornos críticos: Limitar privilegios y accesos de usuarios a sistemas sensibles.

 ALTA

2.2 CVE-2026-21513 permite omitir funciones de seguridad en Internet Explorer

En febrero de 2026, investigadores de Microsoft y Google Threat Intelligence Group (GTIG) revelaron la vulnerabilidad CVE-2026-21513, una omisión de funciones de seguridad en el framework MSHTML que afecta a Internet Explorer, pese a su desaprobación oficial.

La falla permite a atacantes convencer a usuarios de abrir archivos HTML o accesos directos LNK especialmente diseñados, lo que podría derivar en la ejecución remota de código con privilegios del usuario. Microsoft calificó la vulnerabilidad con una puntuación CVSS de 8,8 y confirmó que se explotó activamente antes de que los parches estuvieran disponibles.

Esta explotación destaca la importancia de mantener entornos heredados actualizados y la necesidad de implementar estrategias preventivas contra archivos y enlaces no confiables. Ataques coordinados podrían usar esta falla para comprometer sistemas corporativos, acceder a información sensible y realizar movimientos laterales dentro de redes internas.

El incidente refuerza la relevancia de aplicar mitigaciones, monitoreo activo y capacitación del usuario para minimizar riesgos en entornos con software discontinuado o componentes heredados.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1204 – User Execution	Convencer al usuario de abrir un archivo HTML o LNK malicioso diseñado específicamente para explotar la omisión de funciones de seguridad de MSHTML.
TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Ejecución de código a través del motor de scripting de Internet Explorer al procesar contenido malicioso en archivos HTML o accesos directos LNK.
TA0003: Persistencia	T1547 – Boot or Logon Autostart Execution	Aprovechamiento de accesos directos persistentes para mantener la capacidad de ejecución si el usuario interactúa nuevamente con el archivo comprometido.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Omisión de alertas de Windows SmartScreen y funciones de seguridad de Windows Shell para evitar notificaciones y bloquear mecanismos de defensa del sistema.
TA0040: Impacto	T1499 – Endpoint Denial of Service	Posible ejecución de código no autorizado que compromete la integridad del sistema afectado y facilita actividades maliciosas coordinadas sin detección inmediata.

Recomendaciones:

- Actualizar MSHTML/Internet Explorer: Aplicar los parches de Microsoft para cerrar la omisión de seguridad y prevenir ejecución de código.
- Bloquear archivos HTML y LNK sospechosos: Restringir la apertura de archivos de fuentes no confiables o correos externos.
- Monitoreo de scripts y accesos directos: Usar EDR para registrar y alertar sobre ejecución inusual de contenido HTML o LNK.
- Restringir ejecución de contenido legado: Deshabilitar componentes de IE y MSHTML en sistemas que no requieren compatibilidad con aplicaciones antiguas.
- Concientización de usuarios: Capacitar al personal sobre riesgos de abrir enlaces y accesos directos no verificados, incluso de remitentes aparentemente confiables.

 ALTA

2.3 CVE-2026-21514 permite ejecución de código mediante archivos Office maliciosos

En febrero de 2026, investigadores de Microsoft y Google Threat Intelligence Group alertaron sobre la vulnerabilidad CVE-2026-21514, que elude las mitigaciones OLE en Microsoft 365 y Office, exponiendo a los usuarios a controles COM/OLE inseguros al abrir documentos maliciosos.

La falla, con una puntuación CVSS de 7,8, fue explotada activamente antes de la liberación del parche. Aunque el panel de vista previa no constituye un vector de ataque, los usuarios frecuentemente abren archivos recibidos por correo electrónico, lo que incrementa el riesgo de compromiso. La explotación requiere únicamente la interacción del usuario, lo que la hace práctica y efectiva para campañas de entrega de código malicioso en entornos corporativos.

El descubrimiento se acreditó a Google Threat Intelligence Group, equipos de seguridad interna de Microsoft y un investigador anónimo, subrayando la necesidad de aplicar mitigaciones inmediatas. Se recomienda monitoreo continuo de documentos Office sospechosos, educación del usuario y restricciones de apertura de archivos desconocidos para reducir el riesgo de explotación y proteger la integridad de los sistemas corporativos.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1204 – User Execution	El atacante induce al usuario a abrir un archivo de Microsoft Office malicioso enviado por correo electrónico o compartido en entornos corporativos, iniciando la explotación de COM/OLE.
TA0002: Ejecución	T1059 – Command and Scripting Interpreter	La vulnerabilidad permite la ejecución de código malicioso dentro de Office al aprovechar controles COM/OLE inseguros sin necesidad de interacción adicional más allá de abrir el documento.
TA0003: Persistencia	T1547 – Boot or Logon Autostart Execution	Archivos maliciosos pueden ser configurados para ejecución repetida mediante macros o enlaces incrustados que se activan al abrir documentos, manteniendo la amenaza activa hasta parcheo.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	La omisión de mitigaciones OLE evita que mecanismos de seguridad como Protected View y otros controles internos de Office detecten la actividad maliciosa.
TA0007: Descubrimiento	T1083 – File and Directory Discovery	Documentos maliciosos pueden incluir payloads que recopilan información sobre archivos locales y rutas de sistema para facilitar ejecución de código adicional o reconocimiento del entorno.
TA0040: Impacto	T1499 – Endpoint Denial of Service	La explotación de archivos Office puede comprometer la disponibilidad del sistema o interrumpir operaciones normales si se ejecutan múltiples cargas maliciosas que interfieren con Office y servicios relacionados.

Recomendaciones

- Bloqueo de macros y OLE inseguro: Configurar políticas de Office y Microsoft 365 para deshabilitar macros y controles OLE en documentos recibidos de fuentes externas.
- Filtrado de archivos adjuntos y contenido malicioso: Implementar soluciones de seguridad de correo electrónico que inspeccionen archivos Office y bloqueen documentos sospechosos antes de llegar al usuario final.
- Segmentación de entornos críticos: Limitar la apertura de documentos en estaciones de trabajo con acceso a información sensible, usando contenedores o máquinas virtuales para previsualización segura.
- Monitoreo de comportamiento en Office: Activar soluciones EDR que detecten ejecución de código inesperado, manipulación de COM/OLE y actividad anómala de aplicaciones Office.
- Concientización del usuario: Capacitar a empleados para no abrir documentos de fuentes desconocidas y revisar cuidadosamente cualquier solicitud inesperada de habilitar contenido o macros.

 CRÍTICA

3 . Phishing

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

En febrero de 2026, investigadores de Abnormal AI alertaron sobre "Starkiller", una nueva plataforma de phishing como servicio que actúa como proxy inverso, cargando en tiempo real páginas legítimas de marcas como Apple, Google, Facebook y Microsoft. A diferencia de los kits tradicionales, retransmite la sesión completa entre la víctima y el sitio auténtico, capturando credenciales, códigos MFA, cookies y tokens de sesión.

El sistema genera enlaces engañosos que imitan dominios legítimos, utilizando símbolos "@" y acortadores de URL para ocultar la dirección real. En segundo plano, despliega contenedores Docker con instancias de Chrome sin cabeza que registran cada interacción del usuario.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1204 – Phishing	Envío de enlaces engañosos que imitan dominios legítimos (uso del símbolo "@" y acortadores de URL) para redirigir a víctimas hacia el proxy controlado por el atacante.
TA0002: Ejecución	T1204 – User Execution	La víctima interactúa voluntariamente con la página de inicio de sesión real cargada a través del proxy, ingresando credenciales y códigos MFA.
TA0006: Acceso a Credenciales	T1056 – Input Capture	Captura de cada pulsación de tecla (keylogging) y envío de formularios mientras el usuario interactúa con la sesión autenticada.
TA0006: Acceso a Credenciales	T1557 – Adversary-in-the-Middle	Uso de proxy inverso en contenedor Docker con navegador sin cabeza para retransmitir en tiempo real credenciales y tokens MFA entre víctima y sitio legítimo.
TA0005: Evasión de Defensa	T1036 – Masquerading	Generación de URLs visualmente similares a dominios oficiales y carga dinámica del sitio auténtico para evadir detección basada en páginas estáticas.
TA0006: Acceso a Credenciales	T1539 – Steal Web Session Cookie	Intercepción y robo de cookies y tokens de sesión tras autenticación exitosa para toma directa de cuenta.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Monitoreo de sesiones en tiempo real y envío de credenciales robadas mediante infraestructura controlada por el atacante y alertas automatizadas (ej. Telegram).
TA0043: Reconocimiento	T1598 – Phishing for Information	Recopilación de correos electrónicos y datos de contacto desde sesiones comprometidas para reutilización en campañas futuras.

Recomendaciones

- Autenticación resistente a phishing: Usar FIDO2 o Passkeys para proteger credenciales y tokens MFA frente a proxies maliciosos.
- Protección de correo y URLs: Implementar gateways y análisis en tiempo real para detectar redirecciones, acortadores y símbolos engañosos como "@".
- Aislamiento del navegador: Ejecutar sesiones sospechosas en entornos seguros para evitar exposición directa de credenciales corporativas.
- Monitoreo de sesiones: Detectar secuestro de sesión, anomalías en tokens y cambios simultáneos de IP o dispositivo tras autenticaciones.
- Políticas de acceso condicional: Aplicar autenticación adaptativa basada en riesgo y revalidar accesos ante comportamientos anómalos.



3.2 Campaña de phishing apunta a asistentes de la India AI Impact Summit 2026 mediante SMS y WhatsApp

El 22 de febrero de 2026, los organizadores del India AI Impact Summit emitieron una alerta tras detectar una campaña de phishing dirigida a asistentes del evento, celebrado del 16 al 20 de febrero en Bharat Mandapam, Nueva Delhi. Los mensajes fraudulentos, distribuidos por SMS y WhatsApp, afirmaban falsamente gestionar “reembolsos” e instaban a los destinatarios a compartir información financiera confidencial.

Los atacantes solicitaban datos de tarjetas bancarias, códigos CVV, contraseñas de un solo uso (OTP) y números de contacto, redirigiendo además a enlaces sospechosos diseñados para recolectar credenciales. Los organizadores recalcaron que ningún reembolso legítimo requiere enviar información sensible por plataformas de mensajería y que dichas comunicaciones no estaban autorizadas.

Expertos indicaron que grandes conferencias tecnológicas se han convertido en objetivos atractivos para ingeniería social, aprovechando el volumen de asistentes y la exposición mediática. Esta edición contó con más de 50.000 participantes de 118 países, incluidos líderes gubernamentales y ejecutivos del sector tecnológico.

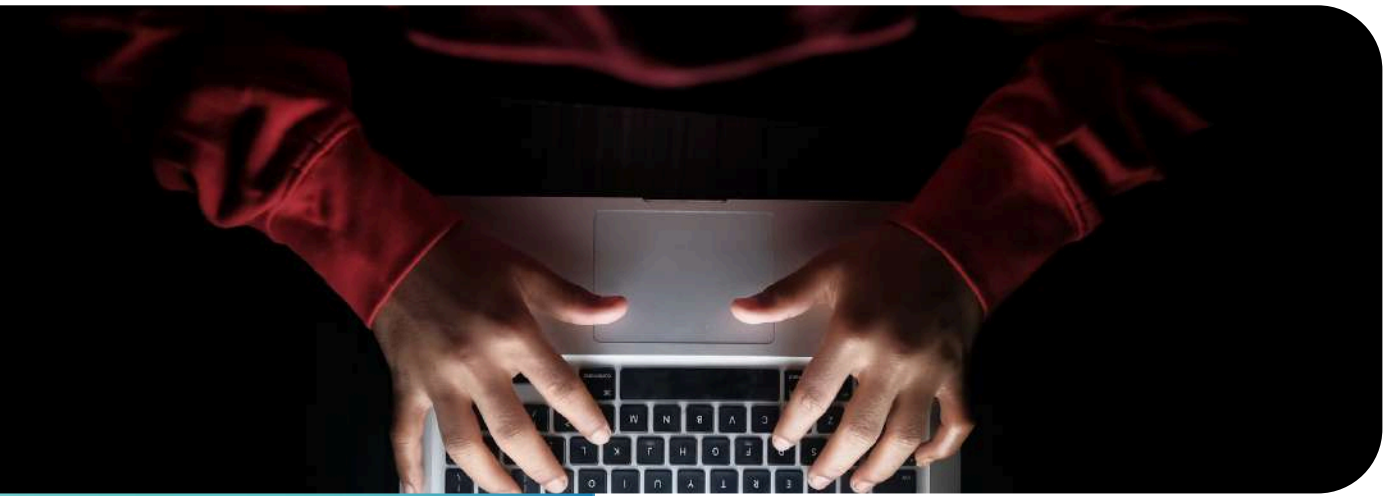
Se recomendó verificar comunicaciones solo por canales oficiales, no compartir datos bancarios ni OTP, contactar al banco si se interactuó con enlaces maliciosos y reportar mensajes sospechosos.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.002 – Phishing: SMS	Envío de mensajes SMS fraudulentos que simulan procesos de "reembolso" oficiales del evento para engañar a los asistentes.
TA0001: Acceso Inicial	T1566.003 – Phishing: Spearphishing via Service	Uso de WhatsApp para distribuir mensajes dirigidos a participantes registrados, aprovechando la temática del evento.
TA0043: Reconocimiento	T1598 – Phishing for Information	Recolección de datos financieros y personales (número de tarjeta, CVV, OTP, contactos) mediante ingeniería social.
TA0006: Acceso a Credenciales	T1056 – Input Capture	Obtención de códigos OTP y credenciales bancarias ingresadas por la víctima tras interactuar con enlaces fraudulentos.
TA0005: Evasión de Defensa	T1036 – Masquerading	Suplantación de identidad de los organizadores del evento y uso de narrativa legítima de reembolsos para aparentar autenticidad.
TA0007: Descubrimiento	T1087 – Account Discovery	Validación indirecta de números activos y datos financieros al confirmar qué víctimas responden o completan formularios.
TA0040: Impacto	T1648 – Account Access Removal / Financial Theft (Contextual)	Potencial uso de la información robada para realizar transacciones no autorizadas o fraude financiero.

Recomendaciones

- Verificación por canales oficiales: Confirmar reembolsos o cambios solo vía sitio web o redes oficiales, evitando enlaces por SMS o WhatsApp.
- Bloqueo de SMS maliciosos: Implementar MTD/EDR móvil para detectar enlaces sospechosos, dominios nuevos y acortadores de URL.
- Protección financiera: Activar alertas en tiempo real, límites preventivos y autenticación basada en riesgo para reducir impacto de filtraciones.
- Capacitación en eventos masivos: Advertir sobre phishing temático y enfatizar que nunca se solicitarán CVV, OTP o credenciales por mensajería.
- Procedimiento de respuesta inmediata: Establecer protocolo para víctimas: contactar al banco, bloquear tarjetas, monitorear transacciones y reportar a organizadores y autoridades.



4. Adversarios

4.1 Actor de amenazas en foco – DRAGONFLY (TA17-293A): Operaciones cibernéticas contra infraestructura crítica

DRAGONFLY, también conocido como Energetic Bear o Crouching Yeti, es un actor de amenazas vinculado a intereses rusos, activo desde al menos 2011 y enfocado en el sector energético y otras infraestructuras críticas. El grupo ha resurgido con campañas dirigidas a organizaciones en Europa, Asia y América del Norte, priorizando entornos industriales ICS y SCADA. Su operación TA17-293A emplea fases múltiples, usando compromisos iniciales en entidades de menor perfil como pivote hacia objetivos estratégicos de mayor valor.

El actor ha explotado vulnerabilidades críticas en productos ampliamente usados, incluyendo Confluence (CVE-2023-22518), servicios de Windows y Netlogon (CVE-2023-36884), NetScaler, Exchange y dispositivos perimetrales expuestos. Recientemente, se reportaron intentos de intrusión en más de 30 organizaciones energéticas y manufactureras en Europa, usando FortiGate vulnerables para obtener acceso persistente.

DRAGONFLY prioriza espionaje, posicionamiento preoperacional y capacidad de interrupción sobre ganancias financieras inmediatas. Su metodología incluye reconocimiento interno, abuso de credenciales, movimiento lateral y consolidación en redes IT-OT. La actividad reciente muestra interés en manipulación de controladores industriales, borrado selectivo y preparación de interrupciones coordinadas alineadas con objetivos geopolíticos.

Objetivos principales:

- Organizaciones del sector energético y servicios públicos con integración IT-OT.
- Entornos ICS/SCADA vinculados a generación, distribución y control industrial.
- Dispositivos perimetrales expuestos (firewalls, VPN, gateways) vulnerables.
- Servidores empresariales críticos (Exchange, Confluence, NetScaler).
- Redes de manufactura e infraestructura estratégica en Europa y Norteamérica.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Explotación de dispositivos perimetrales vulnerables (VPN, firewalls, gateways) para obtener acceso inicial a redes corporativas y entornos OT.
TA0003: Persistencia	T1078 – Valid Accounts	Uso y mantenimiento de credenciales comprometidas para conservar acceso prolongado en Active Directory y sistemas críticos.
TA0004: Escalada de Privilegios	T1068 – Exploitation for Privilege Escalation	Abuso de vulnerabilidades en servidores empresariales para obtener privilegios elevados dentro del dominio.
TA0007: Descubrimiento	T1087 – Account Discovery	Enumeración de cuentas, servicios y relaciones de confianza entre entornos IT–OT para identificar activos estratégicos.
TA0008: Movimiento Lateral	T1021 – Remote Services	Desplazamiento lateral mediante RDP, SMB o servicios administrativos hacia servidores críticos y segmentos industriales.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Comunicación cifrada a través de HTTPS desde sistemas comprometidos para mantener control remoto encubierto.
TA0040: Impacto	T1485 – Data Destruction	Eliminación selectiva de archivos y manipulación de sistemas industriales para generar interrupciones operativas.

Recomendaciones:

- Aplicar parches de seguridad de forma prioritaria en dispositivos perimetrales y sistemas expuestos a Internet, especialmente firewalls y gateways VPN.
- Segmentar estrictamente redes IT y OT, limitando accesos bidireccionales y aplicando principios de mínimo privilegio.
- Implementar monitoreo continuo de movimiento lateral, abuso de credenciales y escalada de privilegios en Active Directory.
- Desplegar soluciones de detección en entornos industriales capaces de identificar manipulación de controladores y anomalías en SCADA.
- Realizar ejercicios periódicos de respuesta a incidentes enfocados en escenarios de interrupción operativa en infraestructura crítica

 ALTA

4.2 Google desmantela grupo de hackers vinculado a China que atacó 53 organizaciones

El 25 de febrero de 2026, Google anunció que interrumpió a UNC2814, también conocido como “Gallium”, un grupo de hackers vinculado a China que comprometió al menos 53 organizaciones en 42 países, principalmente gobiernos y empresas de telecomunicaciones.

Google y sus socios cancelaron proyectos de Google Cloud controlados por el grupo, deshabilitaron su infraestructura de Internet y cerraron cuentas usadas para exfiltrar datos mediante Google Sheets, mezclando actividad maliciosa con tráfico normal para evadir detección.

El grupo tuvo acceso confirmado a 53 entidades y potencial en otros 22 países. En un caso, se implantó la puerta trasera “GRIDTIDE” en sistemas con datos sensibles como nombres, fechas de nacimiento, números de identificación y de votante.

Gallium utilizó estas técnicas para espionaje, monitoreo de mensajes SMS y seguimiento de objetivos específicos, demostrando un enfoque sofisticado de ciberespionaje global.

China declaró que combate sistemáticamente la piratería informática conforme a la ley y rechazó acusaciones de difamación. Google aclaró que esta actividad es diferente de la campaña “Salt Typhoon”, centrada en objetivos estadounidenses.

Objetivos principales:

- Organizaciones gubernamentales y empresas de telecomunicaciones de alto valor estratégico.
- Sistemas que manejan información sensible de ciudadanos, clientes o empleados.
- Plataformas en la nube y servicios colaborativos (Google Cloud, Google Sheets).
- Redes y servidores críticos que permiten exfiltración de datos o espionaje.
- Entidades internacionales con comunicación transfronteriza y datos confidenciales.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1078 – Valid Accounts	Uso de credenciales comprometidas para acceder a cuentas de Google Cloud y Google Sheets utilizadas por objetivos estratégicos.
TA0002: Ejecución	T1203 – Exploitation for Client Execution	Ejecución de operaciones de segmentación y extracción de datos a través de scripts en Google Sheets sin comprometer productos de Google.
TA0003: Persistencia	T1547 – Boot or Logon Autostart Execution	Mantener acceso indirecto a través de cuentas en la nube y documentos compartidos, asegurando persistencia en la infraestructura del objetivo.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Mezcla de actividad con tráfico normal de red para evitar detección de sistemas de monitoreo y soluciones EDR.
TA0007: Descubrimiento	T1083 – File and Directory Discovery	Identificación de archivos sensibles y registros en sistemas de telecomunicaciones y organizaciones gubernamentales.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Comunicación y control encubiertos mediante Google Sheets y servicios en la nube para coordinar exfiltración de datos.
TA0040: Impacto	T1486 – Data Encrypted for Impact	Acceso a información personal sensible (números de identificación, datos de votantes) para espionaje y vigilancia estratégica.

Recomendaciones

- Aplicar autenticación multifactor robusta en todas las cuentas administrativas y de servicio.
- Monitorear tráfico saliente y actividad inusual en plataformas de colaboración en la nube.
- Segmentar redes críticas y limitar el acceso remoto a usuarios verificados.
- Implementar alertas de comportamiento anómalo y auditorías periódicas de accesos y permisos.
- Capacitar al personal en ciberseguridad, reforzando detección de accesos no autorizados y ataques dirigidos.

5. Indicadores de Compromiso

5.1 Direcciones IP

80[.]94[.]92[.]165
 80[.]94[.]95[.]242
 193[.]3[.]53[.]7
 93[.]92[.]136[.]217
 198[.]11[.]177[.]57
 113[.]231[.]9[.]157
 147[.]185[.]133[.]36
 154[.]255[.]19[.]97
 198[.]12[.]122[.]25
 143[.]244[.]132[.]78
 220[.]200[.]154[.]169

5.2 Dominio

- dmzhost[.]co
- 3xktech[.]cloud
- verizon[.]com
- onyphe[.]io
- chinaunicom[.]cn
- vodafone[.]com
- rcp.net[.]pe
- ipnxxnigeria[.]net
- cosmonova[.]net
- gunabahan.my[.]id
- comcast[.]net

5.3 Hashes

831e3a373b18d57064ff610fd8d9e44488
 e92dcc1a1f057e97a87641ca78619

83e1edc4024c0ede33833ec50fe7e638e
 7b42d19193e03a0f374da983f59c4a4

f0b1072fbba2d66b1c9ca118aabaf084e45
 f778aab936ada4c30c3b9aee19092

c40ba34acffe823a341f04ba436e81395f4
 fla91ea0ec86b052dd01ea51d3d81

c1395e1eda6cd464fc67e9b128db8a7b6
 8eb0d58a11008844e5f186359d4079b

c4a365e546682c36492ed7c33b6b4292f
 27cb1cdcd358845997e2d6447832cf5

d5b7a626be9f3b30b03d655c0bbb9374
 f129d968c71d0d1f97a7d7afaa07c606

171ed1327dfb01eda9a2af58ce73c107208f
 0760d122dc38d99b81e3bf99350d

51c2cbedfc897e716f4dbbf81a9a6ca602
 c8a4386798c71b80cc84ab8f51e0ff\

bcaca556bc65be108bb3a801765c99161
 4ebab9bbbede9f31841ba4daa4cf8dcb

f6b841e69ab1222548ac910f38a792b007
 8058d092c65adb84f0a3c29887b4f2

15842707f4725b9d2c6fffb6ac7e4788374
 78920933ddf678d8465e02e4d67f2

6. Fuentes

- 6.1 <https://www.abuseipdb.com/check/>
- 6.2 <https://urlhaus.abuse.ch/browse.php?search=pinaton.ru&page=1>
- 6.3 <https://krebsonsecurity.com/2026/02/starkiller-phishing-service-proxies-real-login-pages-mfa/>
- 6.4 <https://www.cyfirma.com/news/weekly-intelligence-report-20-february-2026/>
- 6.5 <https://thehackernews.com/2026/02/clickfix-campaign-abuses-compromised.html>
- 6.6 <https://www.trendtic.cl/2026/02/mas-de-13-000-dispositivos-android-infectados-con-keenadu-un-malware-que-puede-venir-preinstalado-desde-fabrica/>
- 6.7 <https://www.infosecurity-magazine.com/news/advantest-ransomware-attack/>
- 6.8 <https://www.notebookcheck.org/El-FBI-advierte-del-aumento-de-los-ataques-de-jackpotting-en-cajeros-automaticos-con-malware.1232705.0.html>
- 6.9 <https://www.csoononline.com/article/4137527/steaelite-rat-combines-data-theft-and-ransomware-management-capability-in-one-tool.html>
- 6.10 <https://www.techradar.com/pro/the-ai-model-and-prompt-are-predefined-in-the-code-and-cannot-be-changed-experts-say-prompts-py-is-the-first-known-android-malware-to-use-gemini-to-ensure-infection>
- 6.11 <https://www.cnbctv18.com/technology/india-ai-impact-summit-2026-attendees-warned-of-targeted-phishing-scam-ws-l-19852141.htm>
- 6.12 <https://www.reuters.com/sustainability/boards-policy-regulation/google-disrupts-chinese-linked-hackers-that-attacked-53-groups-globally-2026-02-25/>
- 6.13 <https://socradar.io/blog/february-2026-patch-tuesday-zero-day>

