



GS PERÚ

Software - Security & Services

Empresas

BOLETÍN CIBERSEGURIDAD

Julio - 2026





EL ABUSO DE HERRAMIENTAS LEGÍTIMAS COMO NUEVA ESTRATEGIA DE ATAQUE

Julio de 2026: malware adaptable, robo de sesiones y explotación de plataformas empresariales amplían el riesgo operativo

Durante julio de 2026, el panorama de ciberseguridad evidenció una evolución en las tácticas utilizadas por los actores de amenaza. Los ataques actuales ya no dependen únicamente de archivos maliciosos o métodos fácilmente reconocibles, sino que aprovechan herramientas legítimas, componentes firmados, accesos autorizados y servicios empresariales para mezclarse con la actividad normal de las organizaciones y reducir la posibilidad de ser detectados.

Esta tendencia representa un desafío importante, debido a que muchas acciones maliciosas pueden aparentar procesos habituales de usuarios, administradores o plataformas corporativas. El abuso de sesiones activas, mecanismos de autenticación, servicios remotos y funciones administrativas permite a los atacantes mantener persistencia, ampliar sus privilegios y avanzar dentro de los entornos comprometidos sin generar señales inmediatas de alerta.

El riesgo también se extiende a plataformas de gestión, sistemas de seguridad, dispositivos móviles, servicios en la nube y entornos industriales. Una configuración inadecuada, un servicio expuesto o un componente desactualizado puede convertirse en un punto de entrada hacia activos críticos. Por ello, confiar únicamente en firmas digitales, reputación, credenciales válidas o controles tradicionales ya no resulta suficiente para determinar si una actividad es legítima.

Asimismo, las campañas de ingeniería social continúan perfeccionándose mediante el uso de comunicaciones creíbles, procesos empresariales y mecanismos reales de autorización. Estas técnicas buscan manipular al usuario para obtener permisos, sesiones o accesos sin necesidad de capturar directamente una contraseña, dificultando aún más su identificación.

Frente a este escenario, las organizaciones deben fortalecer la protección de identidades, el control de aplicaciones, la gestión de privilegios, la segmentación de redes y el monitoreo basado en comportamiento. Este boletín presenta las principales amenazas, vulnerabilidades y actividades adversarias identificadas durante el mes, con el propósito de facilitar la comprensión de los riesgos y orientar medidas de prevención, detección y respuesta.

ÍNDICE



1. MALWARE 04

- 1.1 Loader basado en Lua distribuye RAT e infostealers mediante archivos TTF camuflados
- 1.2 HollowGraph utiliza Microsoft 365 como canal encubierto de comando y control
- 1.3 Ransomware en América Latina abusa de BitLocker, servicios expuestos e impresoras corporativas
- 1.4 ESET advierte sobre malware adaptable y habilidades de IA maliciosas en su informe H1 2026



2. VULNERABILIDADES 12

- 2.1 Explotación de Ivanti Sentry CVE-2026-10520 permite ejecución remota como root
- 2.2 Cisco Catalyst Center CVE-2026-20191 permite lectura arbitraria de archivos sin autenticación
- 2.3 Vulnerabilidades de ClamAV afectan conectores de Cisco Secure Endpoint y pueden interrumpir el análisis
- 2.4 Bootloaders UEFI antiguos y firmados permiten debilitar Secure Boot



3. PHISHING 20

- 3.1 Campaña de phishing abusa del flujo OAuth Device Code de Microsoft para robar tokens
- 3.2 Falsos compradores mantienen conversaciones antes de enviar enlaces de phishing a fabricantes
- 3.3 Phishing y documentos maliciosos elevan la exposición de entornos industriales en América Latina



4. ADVERSARIOS 26

- 4.1 ToddyCat aprovecha sesiones activas de Gmail mediante depuración remota de Chromium
- 4.2 GoSerpent mantiene acceso prolongado para espionaje contra entidades gubernamentales y diplomáticas
- 4.3 Storm-2603 combina explotación de vulnerabilidades, robo de credenciales y ransomware



5. INDICADORES DE COMPROMISO 32

- 5.1 Direcciones IP
- 5.2 Dominios
- 5.3 Hashes



6. FUENTES 33

1. MALWARE

ALTA

1.1 [ALTA] Loader basado en Lua distribuye RAT e infostealers mediante archivos TTF camuflados



FortiGuard Labs identificó una campaña global que utiliza loaders desarrollados en Autolt y Lua para desplegar distintas familias de malware en equipos Windows.

La cadena de infección emplea archivos altamente ofuscados y presenta el componente principal como un supuesto archivo de fuente TrueType con extensión .ttf. Sin embargo, este archivo contiene código malicioso encargado de descifrar y ejecutar las siguientes etapas del ataque.

La campaña ha distribuido amenazas como Remcos RAT, XWorm, Agent Tesla, Snake Keylogger y Best Private LOGGER, permitiendo el robo de credenciales, la captura de información y el control remoto de los sistemas comprometidos.

La campaña demuestra cómo los atacantes combinan componentes legítimos, extensiones engañosas y ejecución fileless para ocultar la instalación de herramientas de acceso remoto e infostealers.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Ejecución de scripts	Un archivo JavaScript ofuscado inicia la cadena de ejecución y carga las siguientes etapas del malware.	T1059.007
Enmascaramiento	El loader malicioso utiliza la extensión .ttf para aparentar ser un archivo de fuente legítimo.	T1036
Ofuscación	Los scripts incorporan código basura, cifrado y múltiples capas de protección para dificultar su análisis.	T1027
Inyección de procesos	La carga útil es ejecutada dentro de la memoria de procesos legítimos para ocultar su actividad.	T1055
Ejecución en memoria	El malware utiliza técnicas fileless para cargar componentes sin escribir el payload final directamente en disco.	T1620
Robo de información	Los RAT e infostealers desplegados pueden capturar credenciales, pulsaciones de teclado y datos del sistema.	T1056.001 / T1005
Comando y control	Las amenazas instaladas se comunican con infraestructura externa para recibir instrucciones y transferir información.	T1071.001

Recomendaciones

- Restringir la ejecución de scripts: bloquear o controlar archivos .js, .jse, .vbs, .wsf y otros scripts descargados desde correo, navegadores y directorios temporales.
- Inspeccionar archivos comprimidos: analizar mediante sandbox los archivos ZIP, RAR y 7z que contengan scripts, ejecutables o archivos con extensiones inusuales.
- Detectar extensiones engañosas: generar alertas cuando archivos con extensión .ttf sean utilizados como parámetros de intérpretes, cargadores o procesos no relacionados con la administración de fuentes.
- Monitorear intérpretes legítimos: supervisar la ejecución de Autolt, PowerShell, Windows Script Host y otros intérpretes cuando sean iniciados desde Temp, Downloads, AppData o rutas públicas.
- Detectar inyección de procesos: configurar el EDR para alertar sobre asignación anómala de memoria, process hollowing, ejecución reflectiva y carga de código dentro de procesos legítimos.
- Controlar conexiones salientes: identificar comunicaciones desde procesos inusuales hacia dominios o direcciones IP no reconocidas, especialmente después de ejecutar scripts o archivos comprimidos.

ALTA

1.2 [ALTA] HollowGraph utiliza Microsoft 365 como canal encubierto de comando y control



Investigadores de Group-IB identificaron HollowGraph, un implante malicioso desarrollado como una biblioteca .NET que utiliza Microsoft Graph y el calendario de una cuenta comprometida de Microsoft 365 como canal de comando y control.

Este tipo de técnicas representa un desafío para la ciberseguridad, ya que requiere mayor monitoreo sobre identidades, accesos y comportamientos anómalos dentro de los entornos digitales.

En lugar de conectarse directamente con servidores controlados por los atacantes, el malware intercambia instrucciones y archivos mediante operaciones legítimas dentro de la plataforma cloud, lo que dificulta su identificación mediante controles tradicionales basados en reputación de dominios o inspección del tráfico de red.

El malware permite ejecutar acciones remotas y facilitar la extracción de información desde los equipos afectados, demostrando una tendencia creciente en la que los atacantes utilizan herramientas y servicios legítimos para mezclarse con la actividad normal de las organizaciones.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Uso de servicios legítimos	HollowGraph utiliza Microsoft Graph y el calendario de Microsoft 365 para intercambiar instrucciones y resultados con sus operadores.	T1102.002
Comando y control	El malware consulta eventos de calendario para obtener nuevas tareas y recibir instrucciones del atacante.	T1071.001
Exfiltración mediante servicio web	Los archivos sustraídos son cifrados y enviados como adjuntos dentro de eventos de Microsoft 365.	T1567.002
Canal alternativo por DNS	La amenaza utiliza consultas DNS y registros IPv6 AAAA para actualizar información de configuración y credenciales.	T1071.004
Información cifrada	Las instrucciones y los archivos exfiltrados se protegen mediante cifrado RSA y AES-256.	T1027
Enmascaramiento	La configuración se almacena como logAzure.txt para aparentar ser un archivo de registro legítimo.	T1036
Ocultamiento de información	Los eventos maliciosos son programados para el año 2050 con el objetivo de reducir su visibilidad para el propietario del buzón.	T1564
Recopilación y exfiltración	El implante puede recibir instrucciones para recopilar archivos y transferirlos mediante el calendario comprometido.	T1005 / T1041

Recomendaciones

- Examinar archivos adjuntos de calendario: identificar eventos que contengan archivos con nombres similares a File1.txt, File2.txt u otras secuencias no relacionadas con la actividad normal del usuario.
- Revisar aplicaciones OAuth: auditar las aplicaciones registradas en Microsoft Entra ID, sus permisos sobre correo y calendarios, los secretos de cliente creados y las identidades que utilizan el flujo de credenciales de aplicación.
- Aplicar mínimo privilegio: limitar los permisos de Microsoft Graph exclusivamente a los buzones y funciones requeridas, evitando permisos globales sobre correo, calendarios o archivos.
- Rotar credenciales comprometidas: revocar secretos de cliente, tokens y credenciales de las aplicaciones sospechosas, además de cerrar las sesiones asociadas a los buzones afectados.
- Monitorear consultas DNS: generar alertas ante consultas frecuentes de registros AAAA, subdominios de alta entropía y comunicaciones con el dominio cloudlanecd[.]com.

CRÍTICA**1.3 [CRÍTICA] Ransomware en América Latina abusa de BitLocker, servicios expuestos e impresoras corporativas**

El 21 de julio de 2026, Kaspersky divulgó resultados de incidentes investigados en Colombia y México entre mayo y junio. Los atacantes no dependieron de un cifrador desarrollado a medida: utilizaron BitLocker para bloquear información, modificaron credenciales y aprovecharon impresoras corporativas para emitir las notas de rescate.

En Colombia, el acceso se obtuvo mediante un servicio remoto expuesto a Internet asociado a un almacenamiento de 8 TB con información financiera.

En México, los investigadores identificaron un servidor Microsoft SQL configurado de forma insegura y credenciales expuestas en código público; los intrusos debilitaron controles del servidor web y conservaron persistencia durante meses.

Los casos demuestran que las herramientas administrativas legítimas pueden convertirse en mecanismos de impacto cuando existen errores de configuración y baja visibilidad.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Acceso remoto	Los atacantes aprovechan servicios externos expuestos o configurados de forma insegura.	T1133
Credenciales expuestas	Se utilizan credenciales encontradas en código o recursos accesibles públicamente.	T1552.001
Evasión de defensas	Se deshabilitan o debilitan mecanismos de protección para mantener el acceso.	T1562.001
Cifrado de datos	BitLocker es utilizado para impedir el acceso a unidades y archivos corporativos.	T1486
Bloqueo de cuentas	La modificación de credenciales impide que usuarios legítimos ingresen a los sistemas.	T1531

Recomendaciones

- Reducción de exposición: eliminar RDP, SQL y consolas administrativas públicas; utilizar VPN, bastión y listas de acceso restrictivas.
- Gestión de secretos: retirar credenciales de repositorios y código, aplicar escaneo de secretos y rotar cualquier valor expuesto.
- Protección de BitLocker: controlar quién puede habilitar cifrado, custodiar claves de recuperación y alertar por activación masiva o cambios no planificados.
- Centralización de logs: conservar registros fuera de los equipos afectados y correlacionar cambios de cuentas, sesiones remotas, uso de RMM e impresión masiva.
- Recuperación: mantener copias inmutables, probar restauraciones y segmentar respaldos para impedir que credenciales comprometidas alcancen el repositorio de backup.

ALTA

1.4 [ALTA] ESET advierte sobre malware adaptable y habilidades de IA maliciosas en su informe H1 2026



El ESET Threat Report H1 2026, publicado el 8 de julio, destaca que los atacantes están adaptando técnicas conocidas a nuevos ecosistemas.

ESET analizó cerca de 900 000 habilidades utilizadas por agentes de inteligencia artificial e identificó decenas de miles de componentes sospechosos y miles clasificados como maliciosos.

El informe también resalta PromptSpy, el primer malware Android conocido que incorpora IA generativa dentro de su flujo de ejecución.

PromptSpy utiliza Gemini para interpretar elementos de la interfaz y adaptar gestos entre dispositivos, complementando capacidades de captura de pantalla, control remoto y recopilación de información.

El hallazgo no implica que el uso de IA sea todavía generalizado en malware, pero evidencia una evolución hacia amenazas más flexibles y menos dependientes de secuencias codificadas de forma rígida.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Instalación maliciosa	El usuario instala una aplicación Android que contiene funciones de vigilancia y control.	T1204.002
Captura de pantalla	La amenaza puede registrar visualmente la actividad mostrada en el dispositivo.	T1113
Captura de entradas	El malware busca obtener información introducida o mostrada durante el uso del equipo.	T1056
Control remoto	El componente VNC permite operar el dispositivo afectado de manera remota.	T1219
Recopilación local	La información almacenada o accesible en el dispositivo puede ser recolectada.	T1005

Recomendaciones

- Gobierno de aplicaciones móviles: autorizar únicamente tiendas oficiales y bloquear sideloading en dispositivos corporativos o con acceso a información empresarial.
- Seguridad de agentes de IA: evaluar habilidades, plugins y herramientas antes de integrarlas; aplicar repositorios confiables, revisión de código y mínimos privilegios.
- Protección móvil: usar MDM/MTD para detectar permisos excesivos, accesibilidad abusiva, VNC no autorizado y aplicaciones que bloqueen su desinstalación.
- Acceso condicional: impedir que dispositivos no administrados o con señales de compromiso accedan a correo, VPN y aplicaciones SaaS.
- Monitoreo de comportamiento: priorizar detecciones por acciones y secuencias anómalas, no solo por firmas estáticas del archivo.

2. VULNERABILIDADES

CRÍTICA

2.1 [CRÍTICA] Explotación de Ivanti Sentry CVE-2026-10520 permite ejecución remota como root



FortiGuard Labs reportó el 2 de julio de 2026 que continúa observando intentos de explotación contra CVE-2026-10520, después de la publicación de detalles técnicos y código de prueba de concepto.

La vulnerabilidad afecta Ivanti Sentry y permite que un atacante remoto no autenticado ejecute comandos del sistema operativo con privilegios root mediante una API expuesta.

Las versiones 10.5.1 y anteriores, 10.6.1 y anteriores, y 10.7.0 y anteriores se encuentran afectadas; las ramas corregidas son 10.5.2, 10.6.2 y 10.7.1. Debido a que Sentry funciona como gateway de acceso móvil a correo, aplicaciones y contenido corporativo, un compromiso puede facilitar robo de credenciales, persistencia y acceso hacia servicios internos.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Explotación externa	El atacante aprovecha una API accesible sin autenticación para comprometer el dispositivo.	T1190
Ejecución de comandos	La falla permite ejecutar órdenes del sistema operativo en el appliance.	T1059.004
Creación de persistencia	Tras el acceso, podrían crearse usuarios, web shells u otros mecanismos permanentes.	T1136.001 / T1505.003
Transferencia de herramientas	El sistema comprometido puede descargar cargas o utilidades adicionales.	T1105
Acceso a credenciales	Tokens y credenciales gestionados por el gateway pueden quedar expuestos.	T1552

Recomendaciones

- Actualización de emergencia: migrar inmediatamente a Ivanti Sentry 10.5.2, 10.6.2 o 10.7.1, según la rama instalada.
- Suposición de compromiso: tratar appliances expuestos y sin parche como potencialmente comprometidos hasta concluir una revisión técnica.
- Búsqueda forense: revisar cuentas administrativas nuevas, web shells, procesos con privilegios root, tareas persistentes y conexiones salientes inusuales.
- Rotación de secretos: invalidar tokens y renovar credenciales asociadas al gateway si existió una ventana de exposición.
- Contención perimetral: restringir la administración a redes autorizadas y aplicar IPS o virtual patching mientras se completa la actualización.

ALTA**2.2 [ALTA] Cisco Catalyst Center CVE-2026-20191 permite lectura arbitraria de archivos sin autenticación**

Cisco publicó el 1 de julio de 2026 una corrección para CVE-2026-20191, vulnerabilidad de severidad alta y puntuación CVSS 7.5 en Cisco Catalyst Center.

La falla se debe a una validación insuficiente de entradas y permite que un atacante remoto no autenticado envíe una solicitud HTTP especialmente diseñada para leer archivos arbitrarios dentro de un contenedor restringido.

No existen soluciones alternativas que eliminen el riesgo; Cisco recomienda actualizar a una versión corregida. Al momento del aviso, PSIRT indicó que no tenía conocimiento de explotación maliciosa.

Sin embargo, la plataforma centraliza inventario, automatización y operación de red, por lo que la exposición de archivos de configuración, registros o secretos puede facilitar acciones posteriores.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Explotación de servicio	Una solicitud HTTP manipulada permite acceder al componente vulnerable sin autenticación.	T1190
Lectura de archivos	El atacante puede obtener archivos accesibles desde el contenedor restringido.	T1005
Búsqueda de secretos	Archivos de configuración pueden contener tokens, credenciales o información operativa.	T1552.001
Preparación de acceso posterior	La información obtenida puede utilizarse para identificar sistemas, cuentas y rutas de administración.	T1018 / T1087

Recomendaciones

- Aplicación de la corrección: actualizar Catalyst Center y Catalyst Center Global Manager a las versiones señaladas por Cisco.
- Restricción administrativa: permitir la interfaz únicamente desde redes de gestión, VPN o bastiones controlados.
- Revisión de registros: buscar solicitudes HTTP inusuales, accesos a rutas no esperadas y lecturas repetitivas de archivos.
- Protección de secretos: evitar credenciales en texto plano, rotar secretos si se detecta explotación y reducir privilegios de integraciones.
- Segmentación: limitar la comunicación desde la plataforma de gestión hacia segmentos que no sean necesarios para su función.

ALTA**2.3 [ALTA] Vulnerabilidades de ClamAV afectan conectores de Cisco Secure Endpoint y pueden interrumpir el análisis**

Cisco publicó en julio de 2026 un aviso que agrupa siete vulnerabilidades de ClamAV: CVE-2026-20213, CVE-2026-20214, CVE-2026-20215, CVE-2026-20216, CVE-2026-20217, CVE-2026-20243 y CVE-2026-20244.

Archivos especialmente manipulados en formatos PE, FSG, 7z, InstallShield, PESpin, ALZ o DMG pueden provocar corrupción de memoria, terminación del proceso de análisis o consumo temporal de recursos.

El impacto es alto en Cisco Secure Endpoint Connector para Windows, donde el motor trabaja en un contexto privilegiado, y medio en Linux y macOS.

Cisco no publicó workarounds y recomienda actualizar los conectores a las versiones corregidas: Windows 8.6.2, Linux 1.29.0 y macOS 1.27.2. PSIRT indicó que no conocía explotación activa al momento del aviso.

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

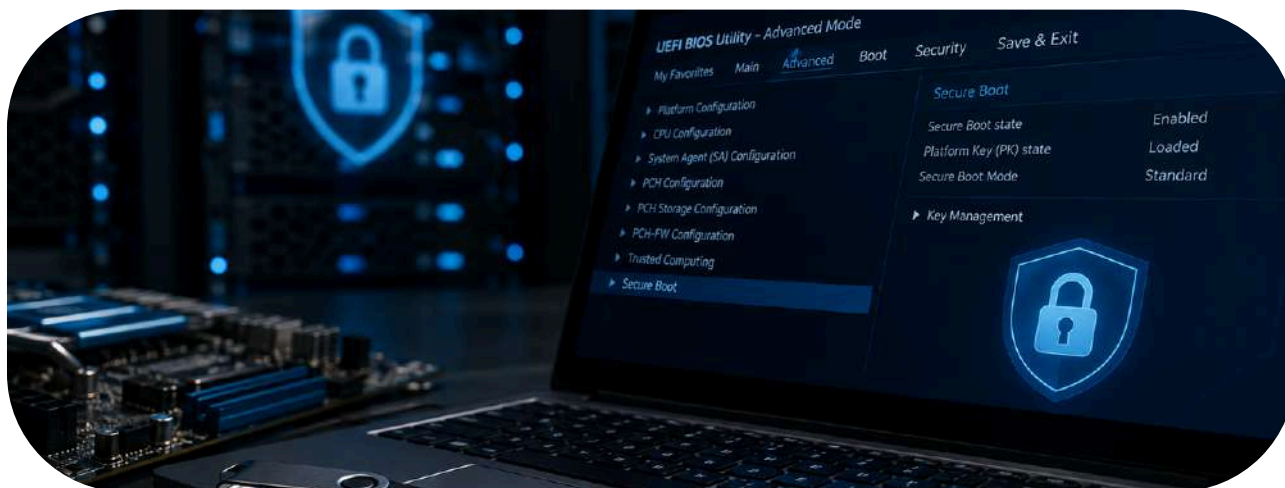
Fase del ataque	Descripción	Referencia Mitre Att&Ck
Entrega de archivo	El atacante presenta al motor antimalware un archivo diseñado para activar la vulnerabilidad.	T1204 / T1105
Explotación de software	El procesamiento del formato manipulado desencadena corrupción de memoria o agotamiento de recursos.	T1203
Denegación de servicio	La explotación puede finalizar el proceso de escaneo o dejar el endpoint sin análisis temporal.	T1499.004
Debilitamiento de defensas	La interrupción del motor reduce la capacidad de inspeccionar archivos posteriores.	T1562.001

Recomendaciones

- Actualizar conectores: verificar que Secure Endpoint Connector ejecute Windows 8.6.2, Linux 1.29.0, macOS 1.27.2 o una versión posterior corregida.
- Validar despliegue: confirmar desde la consola que los endpoints recibieron el nuevo conector y que no existen equipos rezagados.
- Monitorear el servicio: alertar por caídas repetidas del motor, reinicios inesperados, consumo anómalo de recursos o pérdida de telemetría.
- Aislar archivos sospechosos: analizar formatos de alto riesgo en sandbox y limitar su entrega directa a endpoints sensibles.
- Defensa en profundidad: mantener filtrado de correo, proxy y controles EDR adicionales para evitar depender de un único motor de análisis.

CRÍTICA

2.4 [CRÍTICA] Bootloaders UEFI antiguos y firmados permiten debilitar Secure Boot



ESET Research publicó el 14 de julio de 2026 el hallazgo de 11 bootloaders UEFI shim antiguos, firmados por Microsoft, que pueden utilizarse para eludir UEFI Secure Boot en sistemas que confían en el certificado Microsoft Corporation UEFI CA 2011.

Las aplicaciones afectadas, basadas en versiones 0.9 o anteriores, permiten ejecutar código no confiable durante el arranque y podrían facilitar la instalación de bootkits UEFI.

El riesgo no se limita a equipos que tengan instalado el software original: un atacante con acceso suficiente puede llevar una copia del binario vulnerable a otro sistema que mantenga esa cadena de confianza.

Los hallazgos se relacionan con CVE-2026-8863 y CVE-2026-10797. Microsoft incluyó las revocaciones correspondientes en su actualización del 9 de junio de 2026, por lo que la protección depende de que la base dbx se encuentre actualizada.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Modificación de arranque	El atacante introduce un componente UEFI vulnerable dentro de la cadena de inicio.	T1542.001
Evasión de confianza	Un binario firmado pero antiguo es usado para eludir validaciones de Secure Boot.	T1553.006
Bootkit	La ejecución previa al sistema operativo puede permitir desplegar código persistente de arranque.	T1542.003
Debilitamiento de defensas	La manipulación de la cadena de confianza reduce la eficacia de controles del sistema operativo.	T1562.001

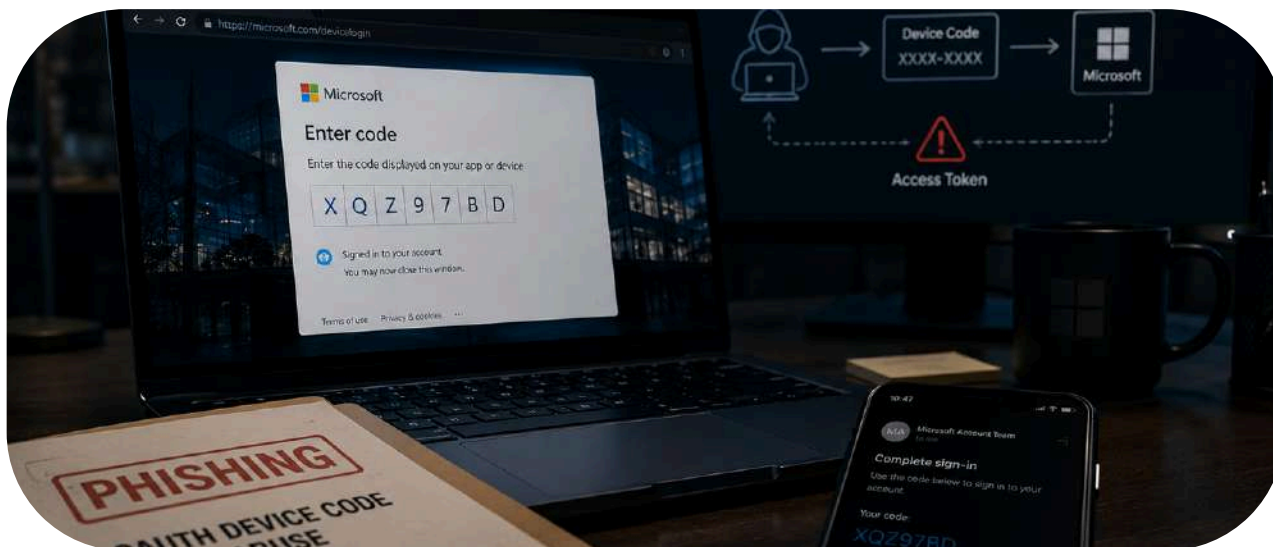
Recomendaciones

- Actualizar revocaciones UEFI: aplicar las actualizaciones de Windows que incorporan la dbx más reciente; en Linux, utilizar las actualizaciones distribuidas mediante LVFS.
- Verificar Secure Boot: auditar que Secure Boot permanezca habilitado y que las revocaciones necesarias estén presentes en equipos críticos.
- Proteger privilegios locales: reducir administradores, controlar acceso físico y monitorear cambios en la partición EFI y variables UEFI.
- Detección de bootkits: utilizar capacidades EDR o de integridad que supervisen la cadena de arranque y cambios en firmware o bootloaders.
- Inventario de hardware: identificar equipos fuera de soporte o incapaces de recibir actualizaciones de firmware y planificar su reemplazo.

3. PHISHING

ALTA

3.1 [ALTA] Campaña de phishing abusa del flujo OAuth Device Code de Microsoft para robar tokens



Kaspersky publicó el 22 de julio de 2026 el análisis de una campaña observada entre abril y mediados de mayo que simulaba comunicaciones de un estudio jurídico.

El mensaje incluía un PDF protegido con contraseña y conducía a una página con múltiples CAPTCHA.

Después, el usuario recibía un código de un solo uso y era redirigido a la página legítima de autorización de Microsoft para pegarlo. El código había sido solicitado previamente por el atacante mediante OAuth 2.0 Device Authorization Grant.

Al completar la autorización y el MFA en el sitio real, la víctima entregaba al atacante los tokens de sesión y actualización, permitiéndole leer o enviar correo, extraer archivos de OneDrive y acceder a conversaciones de Teams sin capturar directamente la contraseña.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Spearphishing	El correo utiliza un PDF protegido para generar confianza y conducir a la víctima al flujo fraudulento.	T1566.001
Interacción del usuario	La víctima copia un código y completa la autorización en una página legítima.	T1204.001
Robo de token	El atacante obtiene tokens OAuth y de actualización vinculados a la sesión autorizada.	T1528
Uso de token	Los tokens permiten acceder a servicios en nombre del usuario sin reutilizar su contraseña.	T1550.001
Acceso a nube	La sesión autorizada puede utilizarse para correo, archivos y colaboración empresarial.	T1114.002 / T1530

Recomendaciones

- Deshabilitar Device Code Flow: bloquear este mecanismo en Microsoft Entra ID cuando no sea requerido por procesos empresariales.
- Acceso condicional: limitar la autorización de dispositivos, exigir equipos administrados y aplicar políticas basadas en riesgo.
- MFA resistente al phishing: priorizar FIDO2, passkeys o certificados, recordando que MFA tradicional no evita una autorización engañosa.
- Monitoreo de OAuth: alertar por device_code, consentimientos inusuales, nuevas aplicaciones y uso de refresh tokens desde ubicaciones no esperadas.
- Respuesta: revocar sesiones y tokens, revisar reglas de buzón, aplicaciones consentidas, actividad de OneDrive y conversaciones accesibles si se confirma exposición.

ALTA

3.2 [ALTA] Falsos compradores mantienen conversaciones antes de enviar enlaces de phishing a fabricantes



Kaspersky informó el 15 de julio de 2026 sobre una campaña activa desde abril contra empresas manufactureras de Europa, Asia y Medio Oriente.

Los atacantes se presentan como compradores potenciales y envían consultas en inglés sobre precios, disponibilidad o características de productos.

Si el destinatario responde, los criminales continúan la conversación y posteriormente entregan un enlace que supuestamente contiene especificaciones técnicas.

El sitio de destino imita un servicio popular para trabajar con documentos PDF y busca obtener datos corporativos. Esta técnica eleva la credibilidad porque el enlace no aparece necesariamente en el primer mensaje y el atacante construye previamente un contexto comercial.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Spearphishing por enlace	El atacante utiliza una conversación comercial para entregar posteriormente un enlace malicioso.	T1566.002
Confianza progresiva	La interacción previa reduce las sospechas y aumenta la probabilidad de apertura.	T1204.001
Captura en portal falso	La página imita un servicio de documentos para solicitar información empresarial.	T1056.003
Suplantación	El actor se presenta como comprador o cliente interesado en productos reales de la víctima.	T1036

Recomendaciones

- Validación comercial: confirmar identidad, dominio, empresa y datos de contacto de nuevos compradores antes de descargar documentación.
- Reescritura y análisis de URLs: inspeccionar enlaces enviados en hilos ya iniciados y no limitar controles al primer correo.
- Aislamiento del navegador: abrir enlaces externos de alto riesgo en entornos protegidos o navegadores remotos.
- Protección de credenciales: evitar ingresar cuentas corporativas en servicios documentales no aprobados y utilizar SSO solo en dominios verificados.
- Capacitación dirigida: incluir a ventas, compras, logística y personal de atención comercial en simulaciones de phishing contextual.

ALTA

3.3 [ALTA] Phishing y documentos maliciosos elevan la exposición de entornos industriales en América Latina



Kaspersky ICS CERT señaló el 6 de julio de 2026 que América Latina fue la segunda región con mayor proporción de equipos industriales afectados durante el periodo analizado: 20,4 % de las computadoras ICS registraron amenazas.

El correo electrónico representó 5,30 % de los vectores observados, los documentos maliciosos 3,08 % y los scripts maliciosos o páginas de phishing 9,65 %.

Entre los segmentos más impactados se encontraron biometría, automatización de edificios, construcción, energía, ingeniería ICS y manufactura.

La relevancia empresarial radica en que una cuenta de correo o estación de ingeniería comprometida puede convertirse en punto de entrada hacia redes OT si no existe segmentación, control de medios y monitoreo especializado.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Phishing	Correos, enlaces y documentos son utilizados para inducir interacción del personal industrial.	T1566.001 / T1566.002
Ejecución del usuario	El operador abre un archivo o sitio que inicia la cadena de compromiso.	T1204
Captura de credenciales	Portales falsos pueden obtener cuentas utilizadas en servicios IT u OT.	T1056.003
Uso de cuentas válidas	Credenciales robadas facilitan acceso a sistemas y servicios permitidos.	T1078
Movimiento hacia OT	La falta de separación puede permitir acceso remoto o lateral a activos industriales.	T1021

Recomendaciones

- Seguridad de correo industrial: aplicar sandboxing, CDR y bloqueo de macros, scripts y adjuntos no requeridos para usuarios OT.
- Segmentación IT/OT: implementar zonas, firewalls y conduits con reglas mínimas; impedir acceso directo desde correo o navegación a redes de control.
- Estaciones de ingeniería: restringir navegación, correo y software no autorizado en equipos que administran PLC, HMI o sistemas de automatización.
- Medios removibles: controlar USB mediante estaciones de transferencia, análisis previo y registro de uso.
- Monitoreo especializado: correlacionar eventos IT y OT, vigilar accesos remotos, cuentas compartidas y cambios de configuración fuera de ventana.

4. ADVERSARIOS

CRÍTICA

4.1 [CRÍTICA] ToddyCat aprovecha sesiones activas de Gmail mediante depuración remota de Chromium



Kaspersky reveló el 14 de julio de 2026 una técnica atribuida al grupo APT ToddyCat denominada Shadow Token via Remote Debug (STRD).

En lugar de robar directamente la contraseña, el actor utiliza el malware Umbrij para abrir de forma encubierta la capacidad de depuración remota de un navegador basado en Chromium que mantiene una sesión corporativa de Gmail activa.

Desde esa sesión, el malware envía solicitudes como usuario autenticado, solicita permisos amplios sobre Gmail, Google Drive y contactos, y puede aprobar automáticamente la ventana de consentimiento.

El resultado es la obtención de un token OAuth con acceso a recursos corporativos, lo que demuestra que una sesión abierta y un navegador comprometido pueden anular la protección práctica de una contraseña robusta.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Abuso de sesión	El actor opera dentro de una sesión de navegador que ya se encuentra autenticada.	T1539
Obtención de token	El malware solicita y obtiene permisos OAuth sobre recursos de Google Workspace.	T1528
Uso de token	El token se utiliza para acceder a servicios corporativos en nombre de la víctima.	T1550.001
Correo en la nube	El actor puede consultar comunicaciones alojadas en Gmail mediante la API.	T1114.002
Datos en nube	Los permisos pueden extenderse a archivos de Drive y contactos empresariales.	T1530

Recomendaciones

- Bloquear depuración remota: aplicar políticas de navegador que restrinjan remote debugging y parámetros de inicio no autorizados.
- Control de extensiones y procesos: permitir únicamente extensiones aprobadas y alertar por Chromium iniciado con puertos o flags de depuración.
- Gobierno OAuth: limitar aplicaciones y scopes, requerir aprobación administrativa y revisar consentimientos de alto privilegio.
- Sesiones de navegador: reducir duración, exigir reautenticación para acciones sensibles y revocar sesiones ante señales de malware.
- Respuesta en Google Workspace: revisar tokens, aplicaciones autorizadas, actividad de API, Gmail, Drive y contactos desde endpoints afectados.

ALTA

4.2 [ALTA] GoSerpent mantiene acceso prolongado para espionaje contra entidades gubernamentales y diplomáticas



Kaspersky GReAT informó el 16 de julio de 2026 sobre una campaña de ciberespionaje denominada GoSerpent, dirigida a entidades gubernamentales y diplomáticas del Sudeste Asiático.

La operación utiliza un conjunto de herramientas personalizadas que incluye el troyano de acceso remoto GoSerpent, Stowaway y TmcLoader.

El backdoor, desarrollado en Go y activo al menos desde 2021, emplea nombres que imitan procesos legítimos y mecanismos de persistencia.

Los investigadores destacan una permanencia deliberada: después del acceso inicial, el actor puede esperar semanas antes de desplegar herramientas secundarias de recopilación y exfiltración, dificultando la correlación cuando la retención de registros es insuficiente.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Enmascaramiento	Los archivos utilizan nombres similares a procesos legítimos para reducir sospechas.	T1036
Persistencia	El backdoor mantiene ejecución a largo plazo mediante mecanismos persistentes.	T1547 / T1053
Transferencia de herramientas	El actor despliega componentes adicionales después de consolidar el acceso.	T1105
Recopilación	Las herramientas buscan información sensible en los sistemas comprometidos.	T1005
Exfiltración	Los datos recopilados son transferidos mediante la infraestructura de control.	T1041

Recomendaciones

- Retención de telemetría: conservar logs de endpoint, autenticación y red durante periodos suficientes para detectar despliegues separados por semanas.
- Threat hunting: buscar binarios Go no inventariados, nombres que imiten procesos del sistema y conexiones periódicas de baja frecuencia.
- Segmentación de usuarios sensibles: aislar puestos diplomáticos, ejecutivos y administrativos; limitar privilegios y acceso a repositorios de información.
- Control de herramientas: detectar túneles, loaders y utilidades no autorizadas como Stowaway o equivalentes.
- Respuesta coordinada: ante un hallazgo, investigar el periodo completo de permanencia y no limitar el análisis al último payload observado.

CRÍTICA

4.3 [CRÍTICA] storm-2603 combina explotación de vulnerabilidades, robo de credenciales y ransomware



FortiGuard Labs actualizó el 2 de julio de 2026 el perfil de Storm-2603, actor de origen chino con motivación financiera y actividad contra infraestructura crítica, educación y gobierno.

El grupo ha sido asociado con ataques a sistemas Windows y Microsoft SharePoint mediante vulnerabilidades zero-day o fallas ya explotadas públicamente. Su conjunto de herramientas incluye backdoors AK47, ransomware AK47 y LockBit Black, utilidades de escaneo, extracción de credenciales y movimiento lateral como masscan, nxc, PsExec y PyPyKatz.

La combinación de explotación inicial, acceso persistente y cifrado evidencia una operación capaz de pasar del compromiso de aplicaciones expuestas al impacto directo sobre la continuidad del negocio.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Explotación de aplicaciones	El actor aprovecha vulnerabilidades nuevas o conocidas en servicios expuestos.	T1190
Credenciales válidas	Las cuentas comprometidas permiten ampliar acceso y evadir controles básicos.	T1078
Obtención de credenciales	Herramientas como PyPyKatz pueden extraer material de autenticación en Windows.	T1003
Movimiento lateral	PsExec y utilidades administrativas permiten ejecutar acciones en otros sistemas.	T1569.002
Impacto por ransomware	El actor utiliza familias de ransomware para cifrar datos y presionar a la víctima.	T1486

Recomendaciones

- Parchado basado en exposición: priorizar SharePoint y otras aplicaciones accesibles desde Internet, incluso antes del ciclo regular.
- Monitoreo de herramientas duales: alertar por masscan, nxc, PsExec, volcado de LSASS y utilidades de administración fuera de procedimientos aprobados.
- Protección de identidades: aplicar MFA, cuentas administrativas separadas, rotación de secretos y detección de autenticaciones anómalas.
- Segmentación y contención: reducir comunicación lateral, especialmente desde servidores web hacia controladores de dominio, respaldos y plataformas de gestión.
- Preparación contra ransomware: mantener respaldos inmutables, EDR con protección antimanipulación y procedimientos de aislamiento rápido de activos comprometidos.

5. INDICADORES DE COMPROMISO

5.1 Direcciones IP

213[.]159[.]64[.]191	104[.]239[.]66[.]86	198[.]23[.]185[.]81
162[.]33[.]179[.]46	46[.]183[.]223[.]21	2[.]59[.]134[.]97
91[.]92[.]240[.]140	107[.]174[.]34[.]137	185[.]254[.]97[.]249
78[.]40[.]209[.]32	162[.]216[.]241[.]242	45[.]145[.]41[.]205

5.2 Dominios

faturanova[.]xyz	mail[.]teamengineersgroup[.]com
facture-in[.]pages[.]dev	mail[.]allportcargoservice[.]com
facture-arsys[.]duckdns[.]org	mail[.]trimnt[.]com
faturanova[.]duckdns[.]org	mora1987[.]work[.]gd
controlfacturas[.]site	studioobs[.]com
newremupdate[.]duckdns[.]org	servermanagemen[.]xyz

5.3 Hashes

6bc2e11b0917f47d0557288c4f0cb20bd7589185943b989a969fdc6d3704ee73
540ee1936e61d2344b5ebc93485589a351ec2f113a9b4940ae16f3baa4807392
e2f0c2d4c1552cd81fa012043e4a5ac832582b639b7b6b7eccc0c4802d7a8ad8
5a2ed557c357ba8f96f2d55a8a00695987806b5df766cd1dfdab0cbcd111774a
19ac18a50abb48dc0ea9524850acfaec49359e6b3bcc67c6193c2d56da812c71
21b24f7ee1f6bdbbb670f0394d66009ee0daa8ced57048298da715e88f7a7cdd
d4eb4ff02df659fdeec17d36b77084627469623bb3c7d16383d257404b52d1c3
ffb9eb47cc0cb2f43e04a10dc84df13d04bca1ebacbe47fad0b669728de2f59c
18fd38988d58dd930f5992d448cc09a9400c1eafba76b820b9a83239ac48cf4e
4ca2c863d740bb7022776dccabd8ae34bb9998768928042d76ebcf08984eefcb
9674da676ee226ee456d35c774715d9b58655423806f281de19dc9ef899e9532
16f9692debe0d4e35d76b48312979e5a90a85ce066e7375269ce78f43da52769

6. FUENTES

- 6.1 <https://www.fortinet.com/blog/threat-research/the-ttf-trap-a-global-campaign-of-a-low-detection-lua-loader>
- 6.2 <https://www.group-ib.com/blog/hollowgraph-microsoft-365/>
- 6.3 <https://latam.kaspersky.com/about/press-releases/kaspersky-alerta-sobre-una-creciente-tactica-de-ransomware-hackers-imprimen-demandas-de-rescate-durante-ataques-en-america-latina>
- 6.4 <https://www.welivesecurity.com/en/eset-research/eset-threat-report-h1-2026/>
- 6.5 <https://www.fortiguard.com/outbreak-alert/ivanti-sentry-os-command-injection>
- 6.6 <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catc-file-read-wLH2vf8X>
- 6.7 <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyR>
- 6.8 <https://www.welivesecurity.com/en/eset-research/forgotten-uefi-shims-undermining-secure-boot/>
- 6.9 <https://me-en.kaspersky.com/about/press-releases/kaspersky-warns-of-a-phishing-campaign-abusing-microsoft-authentication-mechanism>
- 6.10 <https://me-en.kaspersky.com/about/press-releases/kaspersky-has-detected-a-multi-stage-phishing-attack-targeting-manufacturing-facilities-in-europe-asia-and-the-middle-east>
- 6.11 <https://latam.kaspersky.com/about/press-releases/phishing-y-documentos-maliciosos-ponen-a-america-latina-como-la-segunda-region-mas-expuesta-a-ciberamenazas-industriales-kaspersky>
- 6.12 <https://www.kaspersky.com/blog/google-oauth-email-hijacking-shadow-token-remote-debug/>
- 6.13 <https://www.kaspersky.com/about/press-releases/kaspersky-uncovers-a-patient-cyber-espionage-campaign-using-new-goserpent-malware-to-harvest-diplomatic-secrets>
- 6.14 <https://www.fortiguard.com/threat-actor/6192/storm-2603>