GS PERÚ

Software - Security & Services

Empresas

BOLETÍN CIBERSEGURIDAD

Agosto - 2026

EL RIESGO DIGITAL SE DESPLAZA HACIA IDENTIDADES, SERVICIOS Y HERRAMIENTAS DE CONFIANZA

Agosto 2026: phishing avanzado, herramientas legítimas y vulnerabilidades críticas amplían las oportunidades de intrusión.

Durante las primeras semanas de agosto de 2026, el panorama de ciberseguridad mostró una evolución hacia ataques que combinan ingeniería social, abuso de herramientas legítimas, explotación de servicios expuestos y robo de sesiones o credenciales. Los adversarios buscan integrarse dentro de actividades aparentemente normales, utilizando navegadores, aplicaciones de acceso remoto, servicios cloud, clientes VPN y componentes firmados para reducir su visibilidad y mantener acceso prolongado a los entornos comprometidos.

En malware, las campañas observadas abarcaron distintos sistemas y objetivos. Instaladores falsos de Zoom distribuyeron Overlord RAT en macOS; Head Mare comprometió servidores TrueConf para desplegar PhantomCore y PhantomGraph; Evooo1Bot amplió las capacidades tradicionales de las botnets Linux mediante funciones de proxy, fuerza bruta y DDoS; mientras que HoneyMyte incorporó capacidades de rootkit a CoolClient para ocultar procesos, archivos y actividad maliciosa directamente desde el kernel.

En vulnerabilidades, la prioridad se concentró en sistemas empresariales y servicios con capacidad de administración remota. Se reportó explotación de una falla de Screen Sharing en macOS, un zero-day de Windows utilizado para elevar privilegios hasta SYSTEM, una vulnerabilidad crítica en SAP Commerce Cloud con posibilidad de ejecución remota y fallas en Veeam Service Provider Console capaces de exponer credenciales y permitir ejecución de código. Estos casos refuerzan la necesidad de priorizar la actualización de plataformas expuestas y revisar posibles indicadores de compromiso cuando los sistemas permanecieron vulnerables.

El phishing y la actividad de adversarios continúan enfocándose en el robo de identidades y accesos corporativos mediante técnicas AiTM, ClickFix, falsas auditorías y abuso de herramientas RMM. Actores como Sandworm, Armored Likho y Laundry Bear mantienen campañas dirigidas, por lo que resulta prioritario reforzar MFA resistente al phishing, control de acceso remoto, protección de sesiones y monitoreo de identidades, endpoints y servicios cloud.

ÍNDICE

1. MALWARE

ALTA

1.1 [ALTA] Falso instalador de Zoom despliega Overlord RAT en equipos macOS

Jamf Threat Labs informó el 6 de agosto de 2026 sobre una campaña que utiliza un instalador falso de Zoom para desplegar Overlord RAT en sistemas macOS.

El archivo malicioso, denominado ZoomMeetings, está desarrollado como una aplicación .NET 10 autocontenida y puede identificar el sistema operativo y la arquitectura del equipo para descargar la carga correspondiente.

Mientras instala el malware en segundo plano, también descarga el instalador legítimo de Zoom para reducir las sospechas del usuario.

La segunda etapa despliega Overlord, un framework de acceso remoto que establece comunicaciones mediante WebSockets cifrados y permite mantener el control sobre el sistema comprometido.

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

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Enmascaramiento	El ejecutable malicioso utiliza nombres y metadatos asociados con Zoom para aparentar ser un instalador legítimo.	T1036
Descubrimiento del sistema	El downloader identifica el sistema operativo y la arquitectura para seleccionar la carga adecuada.	T1082
Transferencia de herramientas	El malware descarga desde infraestructura externa la versión de Overlord correspondiente al equipo.	T1105
Ofuscación	El downloader utiliza cadenas codificadas y el agente Overlord emplea técnicas de ofuscación para dificultar el análisis.	T1027
Comando y control	Overlord mantiene comunicación remota mediante conexiones WebSocket cifradas.	T1071.001

Recomendaciones

- Software autorizado: permitir la instalación de Zoom únicamente desde repositorios corporativos o desde el dominio oficial del fabricante.
- Control de aplicaciones: restringir la ejecución de binarios no firmados o procedentes de directorios temporales.
- Monitoreo de procesos: detectar ejecutables que se presenten como instaladores legítimos y posteriormente descarguen cargas adicionales.
- Supervisión de /tmp: alertar ante binarios ejecutables creados y lanzados desde directorios temporales en macOS.
- Inspección de C2: identificar conexiones WebSocket persistentes hacia dominios o infraestructura de baja reputación.

ALTA

1.2 [ALTA] Head Mare compromete servidores TrueConf para distribuir PhantomCore y PhantomGraph

Kaspersky informó el 11 de agosto de 2026 sobre una campaña del grupo APT Head Mare que explota servidores TrueConf sin actualizar para desplegar los backdoors PhantomCore y PhantomGraph.

Los atacantes aprovechan una vulnerabilidad que permite la ejecución de código con privilegios elevados, instalan un web shell y posteriormente reemplazan el instalador legítimo de TrueConf por una versión comprometida.

Los equipos que descargan este instalador pueden recibir PhantomCore, mientras que PhantomGraph incorpora funciones adicionales como extracción de credenciales desde LSASS, reconocimiento del sistema y comunicaciones mediante servicios legítimos como Microsoft OneDrive.

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

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Explotación	Se aprovechan vulnerabilidades en servidores TrueConf expuestos y sin actualizar.	T1190
Persistencia	Los atacantes instalan un web shell sobre el servidor comprometido.	T1505.003
Cadena de suministro	El instalador legítimo del cliente TrueConf es sustituido por una versión que contiene PhantomCore.	T1195.002
Acceso a credenciales	PhantomGraph puede realizar volcados de memoria del proceso LSASS para recuperar credenciales.	T1003.001
Comando y control	Componentes de la operación utilizan Microsoft OneDrive como infraestructura para intercambiar información con los atacantes.	T1102.002

Recomendaciones

- Actualización de TrueConf: instalar las versiones corregidas 5.3.9, 5.4.9, 5.5.5 o posteriores según la rama utilizada.
- Validación de instaladores: comprobar firma digital e integridad de los clientes distribuidos desde servidores internos.
- Monitoreo de servidores: identificar creación o modificación inesperada de archivos web y scripts en directorios de TrueConf.
- Protección de credenciales: detectar accesos anómalos a lsass.exe y habilitar protecciones contra credential dumping.
- Control de servicios cloud: supervisar comunicaciones de procesos no autorizados hacia Microsoft Graph y OneDrive.

ALTA

1.3 [ALTA] Evooo1Bot convierte routers y dispositivos Linux en proxies controlados por atacantes

FortiGuard Labs publicó el 13 de agosto de 2026 el análisis de Evooo1Bot, una nueva botnet Linux basada en Mirai que amplía significativamente las funciones tradicionales de este malware.

La amenaza explota múltiples vulnerabilidades conocidas en routers y dispositivos perimetrales expuestos a Internet, descarga binarios adaptados a la arquitectura del dispositivo y establece comunicaciones cifradas con su infraestructura C2.

Además de realizar ataques DDoS, incorpora fuerza bruta SSH, captura de credenciales, ejecución remota de comandos y un módulo SOCKS que convierte los dispositivos comprometidos en nodos proxy para ocultar o reenviar actividad maliciosa.

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

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Acceso inicial	La botnet explota vulnerabilidades conocidas presentes en dispositivos expuestos a Internet.	T1190
Fuerza bruta	Evooo1Bot incorpora un escáner SSH para intentar autenticaciones con diferentes credenciales.	T1110.001
Transferencia de herramientas	Después de la explotación se ejecuta un loader que descarga el binario adecuado para la arquitectura del dispositivo.	T1105
Captura de tráfico	El malware puede interceptar información como encabezados HTTP de autenticación y cookies.	T1040
Comando y control	Las comunicaciones entre el dispositivo infectado y el servidor C2 utilizan canales cifrados.	T1573
Impacto	Incorpora capacidades para ejecutar ataques distribuidos de denegación de servicio.	T1498

Recomendaciones

- Gestión de vulnerabilidades: actualizar routers, gateways, cámaras, dispositivos IoT y otros equipos perimetrales expuestos.
- Reducción de superficie: deshabilitar servicios administrativos innecesarios accesibles desde Internet.
- Protección SSH: impedir autenticación mediante contraseñas débiles y restringir SSH mediante ACL o VPN.
- Segmentación: separar dispositivos IoT y equipos perimetrales de redes corporativas y segmentos críticos.
- Monitoreo de red: detectar dispositivos que generen conexiones C2 inesperadas, escaneos SSH o funcionamiento como proxy SOCKS.

ALTA

1.4 [ALTA] HoneyMyte incorpora un rootkit de kernel a la nueva versión del backdoor CoolClient

Kaspersky reveló el 14 de agosto de 2026 una nueva evolución del backdoor CoolClient, asociado con el grupo APT HoneyMyte, también conocido como Mustang Panda.

La variante observada en campañas de ciberespionaje utiliza un driver firmado en modo kernel para aumentar su capacidad de evasión, ocultando procesos, archivos, módulos y entradas del registro relacionadas con el malware.

El backdoor incorpora además funciones de keylogging, robo del portapapeles, recopilación de credenciales, reconocimiento del sistema y ejecución mediante plugins.

En las intrusiones analizadas, PlugX fue utilizado para desplegar componentes de CoolClient en los sistemas comprometidos.

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

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Transferencia de herramientas	PlugX es utilizado para introducir componentes adicionales de CoolClient en los sistemas comprometidos.	T1105
Inyección de procesos	El malware inyecta componentes en procesos legítimos para ejecutar su código de forma encubierta.	T1055
Escalada de privilegios	La cadena contempla técnicas de bypass de UAC para ejecutar componentes con mayores privilegios.	T1548.002
Evasión de defensas	Un driver en modo kernel permite ocultar procesos y artefactos asociados con CoolClient.	T1014
Captura de entradas	CoolClient incorpora funciones para registrar las pulsaciones realizadas por el usuario.	T1056.001
Recolección	El malware puede capturar información almacenada temporalmente en el portapapeles.	T1115

Recomendaciones

- Control de drivers: restringir la instalación de controladores no autorizados y utilizar mecanismos de bloqueo de drivers vulnerables o sospechosos.
- Protección del kernel: habilitar VBS, HVCI y las funciones de integridad de memoria disponibles en Windows cuando sean compatibles.
- Monitoreo de servicios: detectar creación de servicios de kernel y carga de drivers desde ubicaciones no habituales.
- Detección de inyección: supervisar procesos legítimos que carguen memoria ejecutable o módulos no reconocidos.
- Respuesta ante rootkits: ante evidencia de manipulación del kernel, aislar el endpoint y realizar análisis desde un entorno confiable debido a la capacidad del malware para ocultar artefactos.

2. VULNERABILIDADES

CRÍTICA

2.1 [CRÍTICA] Vulnerabilidad en Screen Sharing de macOS permite acceso remoto sin credenciales válidas

Apple corrigió en agosto de 2026 la vulnerabilidad CVE-2026-65400, asociada al servicio Screen Sharing de macOS.

El fallo de autenticación permite a un atacante con acceso de red al servicio autenticarse sin disponer de credenciales válidas.

La vulnerabilidad afecta versiones anteriores a macOS Tahoe 26.6.1, Sequoia 15.7.9 y Sonoma 14.8.9.

Posteriormente, el NCSC de Países Bajos reportó explotación activa contra sistemas con el puerto TCP/5900 expuesto a Internet; en los incidentes observados, los atacantes consiguieron acceso root e instalaron software para minería de Monero.

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

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Explotación de servicio remoto	El atacante aprovecha el fallo de autenticación en Screen Sharing accesible desde la red.	T1210
Acceso remoto	El servicio basado en VNC permite interactuar remotamente con el sistema comprometido.	T1021.005
Ejecución	Una vez obtenido el acceso, el atacante puede ejecutar aplicaciones o comandos sobre el equipo.	T1059
Impacto	En ataques observados se utilizaron los recursos del sistema para realizar minería de criptomonedas.	T1496

Recomendaciones

- Actualizar macOS: instalar Tahoe 26.6.1, Sequoia 15.7.9, Sonoma 14.8.9 o versiones posteriores.
- Deshabilitar Screen Sharing: mantener el servicio desactivado cuando no exista una necesidad operacional.
- Restringir TCP/5900: impedir que el servicio VNC sea accesible directamente desde Internet.
- Controlar acceso remoto: permitir administración remota únicamente mediante VPN y segmentos de gestión autorizados.
- Buscar indicadores de compromiso: revisar procesos de minería, consumo anómalo de CPU, conexiones externas persistentes y cambios inesperados en cuentas o servicios.

ALTA

2.2 [ALTA] Zero-day de Windows permite elevar privilegios a SYSTEM y fue explotado por Lazarus

Microsoft corrigió el 11 de agosto de 2026 la vulnerabilidad CVE-2026-68820 en Windows Ancillary Function Driver for WinSock, afd.sys.

El fallo de tipo use-after-free permite que un atacante autenticado localmente ejecute una aplicación especialmente manipulada y eleve sus privilegios hasta SYSTEM, sin interacción adicional del usuario.

Microsoft confirmó explotación activa antes de disponer de la actualización.

Check Point vinculó su utilización a una operación de Lazarus basada en falsas ofertas laborales, en la que el exploit se empleó para desplegar una nueva versión del rootkit de kernel FudModule.

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

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Acceso inicial	La campaña observada utiliza señuelos relacionados con oportunidades laborales para comprometer a las víctimas.	T1566
Ejecución del usuario	La víctima es inducida a interactuar con archivos o componentes maliciosos utilizados durante la intrusión.	T1204.002
Elevación de privilegios	CVE-2026-68820 es explotada para pasar de privilegios limitados a SYSTEM.	T1068
Evasión de defensas	Tras la explotación se observó el despliegue de FudModule para dificultar la visibilidad de las soluciones de seguridad.	T1562.001
Rootkit	FudModule opera en modo kernel para ocultar actividad maliciosa y mantener capacidades avanzadas sobre el endpoint.	T1014

Recomendaciones

- Aplicar Patch Tuesday: desplegar las actualizaciones de seguridad de Windows publicadas el 11 de agosto de 2026.
- Priorizar endpoints sensibles: actualizar inmediatamente estaciones de administradores, desarrolladores y usuarios con acceso privilegiado.
- Monitorear elevaciones: investigar procesos que pasen inesperadamente de un contexto de usuario a NT AUTHORITY\SYSTEM.
- Supervisar drivers: detectar carga de controladores de kernel desconocidos, modificados o procedentes de ubicaciones no habituales.
- Fortalecer EDR: mantener habilitadas las capacidades de protección contra manipulación y telemetría de kernel.

CRÍTICA

2.3 [CRÍTICA] CVE-2026-58231 permite ejecución remota sin autenticación en SAP Commerce Cloud

SAP publicó en su Security Patch Day de agosto de 2026 la corrección para CVE-2026-58231, una vulnerabilidad crítica con CVSS 10.0 que afecta al Data Hub Adapter de SAP Commerce Cloud en las versiones COM_CLOUD 2211 y 2211-JDK21.

Un atacante no autenticado puede abusar de un cliente de autenticación predeterminado y enviar entradas especialmente manipuladas a determinadas funciones, posibilitando la ejecución de código arbitrario y el compromiso de componentes internos.

Pocos días después de la publicación del parche se detectaron intentos de explotación contra sistemas expuestos.

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

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Acceso inicial	Un atacante remoto puede dirigir solicitudes especialmente manipuladas contra una instancia vulnerable del Data Hub Adapter expuesta a la red, sin requerir autenticación ni interacción del usuario.	T1190
Abuso de autenticación predeterminada	La explotación aprovecha un cliente de autenticación predeterminado de SAP Commerce Cloud para acceder a funciones que presentan controles de autorización insuficientes.	T1078.001
Ejecución de código	Las entradas manipuladas pueden alcanzar funciones con validación insuficiente y provocar ejecución arbitraria de código dentro del contexto de la aplicación.	T1059

Recomendaciones

- Aplicar la corrección: implementar con prioridad la actualización asociada con SAP Security Note 3771065.
- Validar versiones: identificar implementaciones COM_CLOUD 2211 y 2211-JDK21 afectadas.
- Restringir exposición: impedir que el Data Hub Adapter sea directamente accesible desde redes no confiables.
- Revisar registros: buscar peticiones anómalas, errores de ejecución, procesos secundarios inesperados y conexiones salientes desde componentes SAP.
- Realizar threat hunting: debido a los intentos de explotación reportados, los sistemas expuestos antes de actualizarse deben revisarse para descartar compromiso.

CRÍTICA

2.4 [CRÍTICA] Vulnerabilidades en Veeam Service Provider Console permiten robo de credenciales y ejecución remota

Veeam publicó el 4 de agosto de 2026 varias vulnerabilidades en Veeam Service Provider Console, incluyendo dos fallos críticos.

CVE-2026-58073, con CVSS 9.5, permite que un atacante no autenticado suplante a un agente administrado y obtenga sus credenciales.

Por su parte, CVE-2026-58072, con CVSS 9.0, permite la escritura arbitraria de archivos en el servidor de administración y puede conducir a la ejecución remota de código.

También se corrigieron vulnerabilidades de denegación de servicio y acceso no autorizado a la API.

Los fallos afectan a VSPC 9.2.1.33875 y versiones anteriores de la rama 9 y fueron solucionados en 9.3.0.35057.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Acceso inicial	Servicios expuestos de VSPC pueden convertirse en objetivo para explotar las vulnerabilidades identificadas.	T1190
Acceso a credenciales	CVE-2026-58073 permite obtener credenciales pertenecientes a un agente administrado.	T1552
Uso de credenciales	Las credenciales obtenidas podrían utilizarse posteriormente para suplantar sistemas o cuentas legítimas.	T1078
Transferencia de archivos	CVE-2026-58072 permite la escritura arbitraria de archivos en el servidor de administración.	T1105
Ejecución	La escritura de archivos puede encadenarse hasta conseguir ejecución remota de código.	T1059

Recomendaciones

- Actualizar VSPC: migrar a Veeam Service Provider Console 9.3.0.35057 o una versión posterior corregida.
- Priorizar servidores expuestos: actualizar primero consolas accesibles desde Internet o redes de clientes.
- Rotar credenciales: si existió exposición durante el periodo vulnerable, considerar la renovación de credenciales utilizadas por agentes administrados.
- Revisar integridad: identificar archivos inesperados o modificados recientemente dentro del servidor de gestión.
- Monitorear autenticaciones: detectar agentes desconocidos, conexiones desde direcciones IP atípicas y accesos administrativos anómalos.

3. PHISHING

ALTA

3.1 [ALTA] Greatness PhaaS suplanta a RingCentral para robar cuentas y sesiones de Microsoft 365

ZeroBEC publicó el 4 de agosto de 2026 una investigación sobre la evolución de Greatness, una plataforma de Phishing-as-a-Service distribuida mediante Telegram que incorpora técnicas Adversary-in-the-Middle, phishing mediante códigos de dispositivo y abuso de OAuth.

En la campaña analizada, los atacantes enviaron correos que suplantaban a RingCentral con notificaciones falsas de mensajes de voz y evaluaciones de desempeño.

Los mensajes lograron evadir controles de correo debido a configuraciones de remitentes confiables, aun cuando fallaban SPF, DKIM y DMARC.

La víctima era posteriormente redirigida hacia infraestructura que intermediaba el inicio de sesión real de Microsoft 365, permitiendo capturar credenciales y tokens de autenticación ya validados mediante MFA.

ZeroBEC también observó actividad posterior al compromiso durante agosto, incluyendo reutilización de tokens para acceder a Outlook, Teams, SharePoint y OneDrive.

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

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Phishing	Correos que suplantan a RingCentral contienen enlaces hacia la infraestructura de Greatness.	T1566.002
Ejecución del usuario	La víctima interactúa con el enlace presentado como mensaje de voz o evaluación empresarial.	T1204.001
Captura de credenciales	Las páginas AiTM interceptan las credenciales introducidas durante el proceso de autenticación.	T1056.003
Robo de sesión	Greatness captura tokens o cookies de una autenticación completada, incluso después de MFA.	T1539
Uso de cuentas válidas	Los tokens obtenidos permiten acceder posteriormente a servicios de Microsoft 365 como usuario legítimo.	T1078.004

Recomendaciones

- Revisar remitentes confiables: eliminar excepciones basadas únicamente en dominios y exigir validaciones SPF, DKIM y DMARC antes de aplicar confianza.
- MFA resistente al phishing: priorizar FIDO2, passkeys o llaves de seguridad frente a mecanismos MFA susceptibles a intermediación.
- Monitorear tokens: identificar reutilización de sesiones desde geografías, proveedores VPN o direcciones IP no habituales.
- Control de Device Code: bloquear o restringir el flujo de autenticación por código de dispositivo cuando no sea requerido.
- Monitoreo de Microsoft 365: alertar ante accesos inusuales y correlacionados en Outlook, Teams, SharePoint, OneDrive y Microsoft Graph después de una autenticación sospechosa.

ALTA

3.2 [ALTA] Falsa auditoría de seguridad de COLDCARD instala ScreenConnect para obtener acceso remoto

El 5 de agosto de 2026 se informó sobre una campaña de phishing identificada por Proofpoint que aprovecha la preocupación generada por recientes problemas de seguridad relacionados con billeteras COLDCARD.

Los atacantes envían correos desde un dominio que suplanta a la compañía e informan sobre una supuesta auditoría obligatoria de hardware. El enlace dirige a un portal falso donde se solicita descargar una herramienta de diagnóstico.

En sistemas Windows, el archivo ejecutado despliega un paquete MSI correspondiente a ConnectWise ScreenConnect, mientras que una aplicación legítima relacionada con DocuSign funciona como señuelo.

Una vez establecida la conexión, los atacantes pueden controlar remotamente el equipo, acceder a información o criptomonedas y desplegar cargas maliciosas adicionales.

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

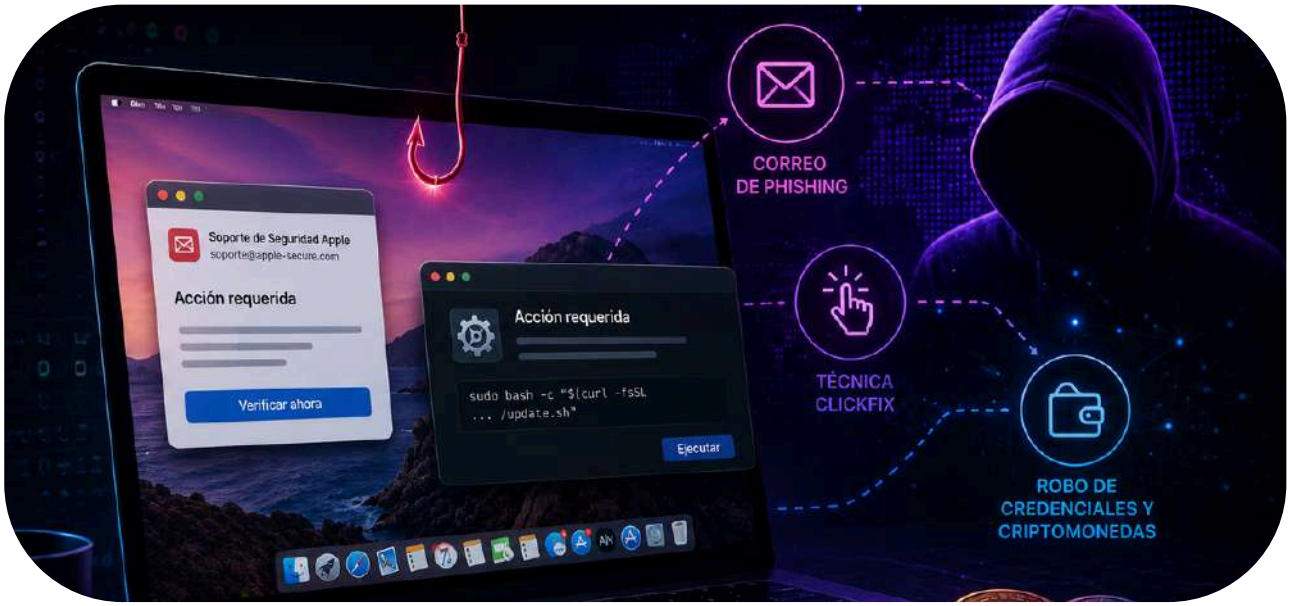
Fase del ataque	Descripción	Referencia MITRE ATT&CK
Phishing	El atacante envía una falsa notificación de auditoría de seguridad que suplanta a COLDCARD.	T1566.002
Ejecución del usuario	La víctima accede al enlace y descarga la supuesta herramienta de diagnóstico.	T1204.001
Archivo malicioso	El usuario ejecuta un archivo BAT que aparenta realizar verificaciones sobre el dispositivo.	T1204.002
Ejecución de comandos	El script utiliza PowerShell y otras herramientas de Windows durante la instalación.	T1059.001
Acceso remoto	ScreenConnect proporciona al atacante control interactivo y persistente sobre el endpoint.	T1219.002

Recomendaciones

- Verificación de comunicaciones: validar alertas o auditorías de fabricantes directamente mediante sus portales oficiales, sin utilizar enlaces recibidos por correo.
- Control de RMM: inventariar las herramientas de administración remota permitidas y bloquear instalaciones de ScreenConnect no gestionadas por TI.
- Filtrado de dominios: detectar dominios recién registrados o similares a fabricantes de hardware, servicios financieros y criptomonedas.
- Restricción de scripts: controlar la ejecución de archivos BAT, VBS y PowerShell descargados desde Internet.
- Concientización: advertir sobre campañas que explotan vulnerabilidades, brechas o incidentes reales para generar urgencia y obtener interacción inmediata.

ALTA

3.3 [ALTA] Campaña ClickFix contra macOS utiliza correos de phishing para robar credenciales y criptomonedas



Huntress publicó el 6 de agosto de 2026 el análisis de una infección en macOS originada a partir de un correo de phishing con un enlace hacia una página ClickFix.

El sitio presentaba una falsa verificación que indicaba al usuario que copiara y ejecutara manualmente un comando en Terminal.

La instrucción descargaba un script Bash encargado de identificar la arquitectura del sistema y desplegar un malware Mach-O escrito en Go.

La carga buscaba contraseñas almacenadas en navegadores, información de Apple Keychain y cookies, además de incorporar funciones para desviar parcial o totalmente fondos de distintas criptomonedas hacia billeteras controladas por los atacantes.

El malware también establecía persistencia mediante LaunchAgents y utilizaba ventanas falsas de macOS para solicitar la contraseña del usuario.

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

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Phishing	La víctima recibe un correo electrónico que contiene un enlace hacia la infraestructura maliciosa.	T1566.002
Ejecución del usuario	El usuario accede voluntariamente al enlace incluido en el mensaje.	T1204.001
ClickFix	La página engaña al usuario para que copie y pegue un comando directamente en Terminal.	T1204.004
Intérprete de comandos	El comando ejecuta scripts Bash responsables de perfilar el sistema y descargar la carga.	T1059.004
Acceso a credenciales	El malware intenta obtener contraseñas almacenadas en Apple Keychain y navegadores.	T1555.001 / T1555.003

Recomendaciones

- Concientización sobre ClickFix: indicar expresamente que ninguna verificación CAPTCHA legítima requiere copiar comandos en Terminal, PowerShell o CMD.
- Protección de macOS: supervisar scripts y binarios ejecutados desde /tmp, directorios de caché y otras ubicaciones de usuario.
- Monitoreo de Terminal: alertar cuando curl, Bash u otros intérpretes descarguen y ejecuten contenido inmediatamente después de la navegación web.
- Protección de credenciales: restringir el acceso no autorizado a Apple Keychain y revisar solicitudes inesperadas de contraseñas mediante ventanas del sistema.
- Monitoreo de persistencia: detectar creación o modificación no autorizada de LaunchAgents y aplicaciones que imiten componentes de Apple.

4. ADVERSARIOS

CRÍTICA

4.1 [CRÍTICA] Sandworm utiliza falsas entrevistas laborales para comprometer a profesionales de TI

El 11 de agosto de 2026 se informó sobre una campaña atribuida a UAC-0145, clúster relacionado con Sandworm/APT44, dirigida principalmente contra administradores de sistemas y profesionales de TI.

Los atacantes revisan perfiles publicados en plataformas laborales, se presentan como reclutadores de empresas tecnológicas y trasladan posteriormente la conversación a Telegram y Zoom para realizar una aparente entrevista.

Durante una prueba técnica, la víctima recibe configuraciones de WireGuard y es inducida a descargar SopraVPN, una versión modificada del cliente VPN.

El programa incorpora una opción denominada SymmetricKey capaz de descifrar y ejecutar código PowerShell, crear tareas programadas y descargar cargas adicionales.

El interés específico en personal técnico aumenta el riesgo de acceso posterior a credenciales, VPN, infraestructura administrativa y otros recursos corporativos.

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

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Ingeniería social	El actor contacta a profesionales mediante plataformas laborales y posteriormente continúa la interacción mediante Telegram y videollamadas.	T1566.003
Ejecución del usuario	La víctima descarga y ejecuta SopraVPN creyendo que forma parte de una prueba técnica legítima.	T1204.002
Ejecución de PowerShell	El cliente modificado descifra y ejecuta instrucciones PowerShell almacenadas en su configuración.	T1059.001
Persistencia	En sistemas Windows, la cadena maliciosa puede crear una tarea programada para ejecutar componentes adicionales.	T1053.005
Descarga de herramientas	El código ejecutado recupera nuevas cargas desde infraestructura externa controlada por el atacante.	T1105
Ofuscación	El actor modifica el mecanismo Base64 para dificultar la lectura y el análisis del código PowerShell incrustado.	T1027

Recomendaciones

- Validación de procesos de selección: confirmar entrevistas, pruebas técnicas y descargas de software directamente con los dominios y canales oficiales de la empresa.
- Control de software VPN: permitir únicamente clientes VPN aprobados y distribuidos mediante repositorios corporativos.
- Monitoreo de PowerShell: alertar cuando aplicaciones recién descargadas generen procesos PowerShell o ejecuten comandos codificados.
- Control de tareas programadas: detectar tareas creadas por aplicaciones no autorizadas o desde perfiles de usuario.
- Protección de personal técnico: aplicar controles reforzados sobre estaciones utilizadas por administradores y restringir el acceso corporativo desde dispositivos personales.

ALTA

4.2 [ALTA] Armored Likho amplía sus capacidades de espionaje para robar sesiones de Telegram y grabar conversaciones

Kaspersky reveló el 13 de agosto de 2026 una nueva campaña de ciberespionaje atribuida con alta confianza a Armored Likho, también conocido como Eagle Werewolf.

El actor utiliza como señuelo una aplicación falsa que imita un servicio para realizar donaciones y, mientras la víctima interactúa con su interfaz, ejecuta de forma encubierta el nuevo Still Toolkit, desarrollado principalmente en Rust.

Su componente Still Sync busca archivos de sesión tdata de Telegram y los utiliza para acceder a la cuenta, recopilar conversaciones, contactos y archivos multimedia mediante la API.

Un segundo componente, Still Audio, activa el micrófono, detecta automáticamente la presencia de voz y registra conversaciones para enviarlas al servidor de comando y control.

La campaña muestra una evolución hacia capacidades de vigilancia persistente y recolección simultánea de diferentes fuentes de información.

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

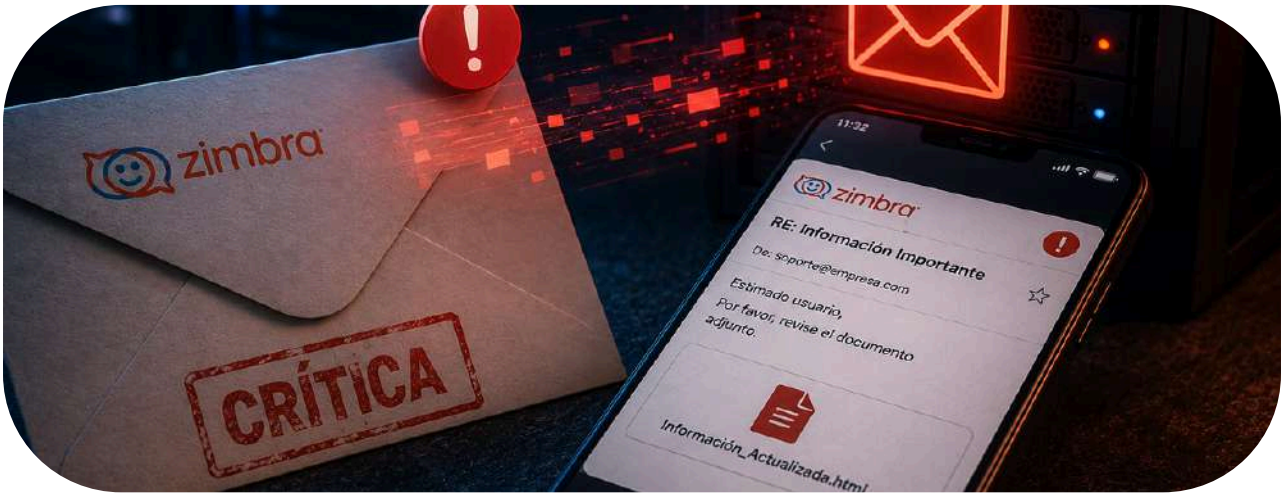
Fase del ataque	Descripción	Referencia MITRE ATT&CK
Enmascaramiento	El dropper se presenta como una aplicación legítima relacionada con donaciones para engañar a la víctima.	T1036
Ejecución del usuario	La víctima ejecuta la aplicación falsa e interactúa con su interfaz, activando la siguiente etapa de la infección.	T1204.002
Descubrimiento del sistema	Still Sync recopila identificadores de hardware, dominio del equipo y otros datos para identificar el endpoint comprometido.	T1082
Recolección de datos	El malware localiza y extrae archivos de sesión de Telegram almacenados en el sistema.	T1005
Captura de audio	Still Audio utiliza dispositivos de entrada para detectar voz y registrar conversaciones.	T1123
Resolución de C2	El malware puede utilizar un repositorio de GitHub como Dead Drop Resolver para recuperar una dirección C2 alternativa.	T1102.001

Recomendaciones

- Control de aplicaciones: impedir la ejecución de software desconocido o no firmado que simule servicios corporativos, gubernamentales o benéficos.
- Protección de Telegram: restringir el uso de Telegram Desktop en equipos sensibles y proteger el acceso local a sus archivos de sesión.
- Monitoreo del micrófono: detectar procesos desconocidos que accedan de manera persistente a dispositivos de captura de audio.
- Supervisión de datos locales: alertar por procesos ajenos a Telegram que accedan masivamente al directorio tdata.
- Control de servicios legítimos: monitorear aplicaciones desconocidas que consulten GitHub u otros servicios públicos para obtener configuraciones o infraestructura C2.

CRÍTICA

4.3 [CRÍTICA] Laundry Bear explota correos de Zimbra para realizar espionaje sin interacción adicional del usuario



NÚKIB informó el 10 de agosto de 2026 sobre una campaña de espionaje atribuida al actor Laundry Bear, vinculado con intereses de la Federación Rusa, dirigida contra usuarios de Zimbra Collaboration Suite.

El grupo aprovecha CVE-2025-66376 mediante correos especialmente manipulados capaces de ejecutar código cuando son visualizados desde una versión vulnerable del webmail.

Tras conseguir acceso, los atacantes buscan obtener comunicaciones de correo electrónico, listas de contactos, credenciales, códigos de respaldo de MFA y otra información sensible, además de intentar conservar acceso prolongado a las cuentas comprometidas.

Los sectores afectados incluyen entidades gubernamentales, defensa, energía, medios, educación, organizaciones no gubernamentales y compañías tecnológicas.

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

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Phishing	El actor utiliza correos especialmente manipulados contra usuarios de Zimbra Collaboration Suite.	T1566
Explotación del cliente	La vulnerabilidad puede activarse simplemente cuando el mensaje malicioso es visualizado en una versión vulnerable del webmail.	T1203
Recolección de correo	Tras el compromiso, el actor obtiene comunicaciones almacenadas en las cuentas afectadas.	T1114.002
Uso de cuentas válidas	Las credenciales obtenidas pueden facilitar el acceso posterior a cuentas y servicios legítimos de las víctimas.	T1078
Recolección de información	La operación busca contactos, credenciales, códigos MFA y otros datos sensibles útiles para actividades posteriores de espionaje.	T1114

Recomendaciones

- Actualizar Zimbra: confirmar que las instalaciones tengan aplicada la corrección de CVE-2025-66376 y todas las actualizaciones de seguridad posteriores.
- Revisar indicadores de compromiso: analizar registros históricos de Zimbra, actividad webmail y conexiones externas asociadas con los IoC publicados para la campaña.
- Proteger cuentas: restablecer credenciales y revocar sesiones activas cuando exista evidencia o sospecha de compromiso.
- Revisar MFA: regenerar códigos de respaldo y validar métodos de autenticación registrados en cuentas potencialmente afectadas.
- Monitorear correo: identificar accesos anómalos, exportaciones masivas de mensajes y consultas inusuales a buzones o directorios corporativos.

5. INDICADORES DE COMPROMISO

5.1 Direcciones IP

92[.]118[.]57[.]209	187[.]17[.]224[.]139	69[.]87[.]221[.]194
45[.]198[.]224[.]26	103[.]9[.]205[.]204	103[.]100[.]211[.]71
15[.]235[.]148[.]79	14[.]224[.]238[.]73	20[.]48[.]238[.]59
170[.]39[.]184[.]167	4[.]213[.]169[.]8	31[.]25[.]239[.]91

5.2 Dominios

enter-press-cdn[.]info	api-server-cdn[.]sbs
auth-code-check[.]info	lb[.]propertyfind[.]cc
authorization-code-cdn[.]info	packetmeridian[.]top
auth-clo-id[.]cc	datadock[.]info
enter-code-cdn[.]info	abcsgftr[.]cc
markol[.]pro	hostreservation-reports[.]one

5.3 Hashes

9250e9fd0d73df09d608a544d27f048089071562ceb40de3600e9b5d85fa5f50
1e3d5fe030122186af6224340deb2440165cf36a932b59ef03d8fc2ca57495b3
e0683807ac2e7ba5215d642f629745387c9ca42941c27a9dbe5eae1eb4f9c73f
b09c4b720472ee2fb724a5318cecac95cf1664b49154e63bfdbbf419a09d0758
d165c4d72c0bff469d16f73e1840cb6edcdcfcb2785d136dbd8646db668c236a
e36506611eae772d25b84fa97fba9f173f8b9b984b0906a29ebd8ac537dedce3
2e0de81a63e34de5337e31356ff87acab04f06e0280344fa93079c43ad004f8e
b871f50abbd7e06e6dbede78f499c2efc426d7f8ba08943f06e104f82d8ecc0c
b44daa31105868bafd0a0b29762e614ef238547a256577ae5671efedd3c652c1
db2c21c75dbae5bf08f157db63caf53ac28c6b57a94458e4eac78e174637f053
e026bc9a0b7ac31a86cdbbd88e2b2be5236ba81b469723007c8b3c1d9461198f
e98edce318f2ee5d241b87ca9305f8ed72cc8eb5a21757d8430c4152d0a47c87

6. FUENTES

6.1 https://www.jamf.com/blog/fake-zoom-installer-delivers-overlord-rat-macos/

6.2 https://securelist.com/tr/head-mare-targets-trueconf-server-with-phantomcore/120988/

6.3 https://www.fortinet.com/blog/threat-research/multi-functional-linux-botnet-evooo1bot

6.4 https://securelist.com/honeymyte-coolclient-driver-rootkit/121028/

6.5 https://www.bleepingcomputer.com/news/security/hackers-exploit-macos-screen-sharing-flaw-to-deploy-monero-miner/

6.6 https://blog.checkpoint.com/research/state-sponsored-hackers-use-fake-job-offers-to-deliver-new-zero-day-exploit/

6.7 https://www.veeam.com/kb4893?ad

6.8 https://zerobec.com/blog/greatness-phaas-aitm-and-device-code-phishing

6.9 https://www.bleepingcomputer.com/news/security/coldcard-security-audit-phishing-attack-installs-remote-access-tool/

6.10 https://www.huntress.com/blog/mac-crypto-draining-malware

6.11 https://www.bleepingcomputer.com/news/security/sandworm-hackers-target-it-pros-with-trojanized-wireguard-vpn-client/

6.12 https://securelist.com/armored-likho-still-toolkit/121033/

6.13 https://nukib.gov.cz/en/infoservis-en/news/2448-nukib-joins-international-advisory-on-russian-cyber-campaign-targeting-zimbra-collaboration-suite/