



GS PERÚ

Software - Security & Services

Empresas

BOLETÍN CIBERSEGURIDAD

Junio - 2026





JUNIO 2026: AMENAZAS QUE SUPERAN EL PERÍMETRO

Junio 2026: exposición perimetral, abuso de identidades y ataques a la cadena de suministro marcan la agenda de ciberseguridad.

Junio de 2026 dejó una señal clara para las organizaciones: los atacantes están combinando explotación de vulnerabilidades, robo de credenciales y abuso de plataformas legítimas para acelerar compromisos con impacto transversal. El riesgo ya no se concentra únicamente en servidores internos; también se materializa en firewalls, VPN, herramientas SaaS, repositorios de código, navegadores, dispositivos móviles y canales de mensajería usados a diario.

A diferencia de meses anteriores, el foco principal del periodo estuvo en servicios ampliamente desplegados. La exposición de credenciales asociada a dispositivos Fortinet, la explotación de fallas en Cisco Unified Communications Manager y Cisco Catalyst SD-WAN Manager, y los intentos contra FortiSandbox muestran que los equipos de seguridad deben tratar la infraestructura perimetral como un activo crítico que requiere parcheo continuo, MFA obligatorio y revisión forense ante cualquier indicio de acceso anómalo.

En paralelo, el ecosistema de malware continuó evolucionando hacia campañas con mayor capacidad de engaño. Se observaron APKs bancarios capaces de capturar datos de tarjetas mediante NFC, paquetes npm comprometidos orientados a robar secretos de desarrollo, adjuntos enviados por WhatsApp desde cuentas secuestradas y loaders distribuidos mediante infraestructura legítima como Google DoubleClick. Estas tácticas reducen la efectividad de controles basados solo en reputación o firmas.

El mensaje central para la gestión empresarial es directo: la defensa debe priorizar identidades, accesos remotos, dependencias de software, endpoints y monitoreo de comportamiento. La rotación preventiva de credenciales, la eliminación de interfaces administrativas públicas, el bloqueo de scripts de alto riesgo, la revisión de CI/CD y la respuesta automatizada ante phishing e infostealers ya no son controles complementarios, sino medidas básicas para sostener la resiliencia operativa.

ÍNDICE



1. MALWARE 04

- 1.1 NFCShare evoluciona: malware bancario para Android roba datos de tarjetas mediante NFC y phishing móvil
- 1.2 Campaña de adware compromete más de 50 000 sitios web para distribuir contenido malicioso
- 1.3 Campaña Miasma compromete paquetes npm de Red Hat para robar secretos de desarrollo y nube
- 1.4 Malware se propaga por WhatsApp usando cuentas comprometidas y adjuntos VBScript
- 1.5 Kaspersky advierte que los infostealers se propagan principalmente mediante archivos temporales



2. VULNERABILIDADES 14

- 2.1 Explotación activa de vulnerabilidades en Fortinet FortiSandbox permite bypass de autenticación y ejecución de comandos
- 2.2 Cisco Unified CM CVE-2026-20230 es explotada activamente y permite escritura de archivos hacia el sistema
- 2.3 Cisco Catalyst SD-WAN Manager CVE-2026-20262 es explotada para escritura arbitraria de archivos



3. PHISHING 20

- 3.1 Campaña de phishing abusa de Google DoubleClick para evadir filtros y entregar un loader .NET
- 3.2 Banco de la Nación advierte campaña de phishing con correos desde dominios Gmail
- 3.3 Quishing, spoofing telefónico y clonación de voz elevan el fraude digital en Perú



4. ADVERSARIOS 26

- 4.1 ShinyHunters explota un zero-day en Oracle PeopleSoft para atacar universidades y organizaciones
- 4.2 FortiBleed expone credenciales asociadas a decenas de miles de dispositivos Fortinet
- 4.3 Operation Endgame interrumpe infraestructura de SocGhosh, Amadey y StealC



5. INDICADORES DE COMPROMISO 32

- 5.1 Direcciones IP
- 5.2 Dominios
- 5.3 Hashes



6. FUENTES 34

1. MALWARE

ALTA

1.1 [ALTA] NFCShare evoluciona: malware bancario para Android roba datos de tarjetas mediante NFC y phishing móvil



Durante junio de 2026 se reportó una nueva ola del troyano bancario para Android NFCShare, inicialmente observado en campañas que suplantaban a Deutsche Bank y luego adaptado a entidades italianas y europeas como Intesa Sanpaolo.

El ataque combina phishing, smishing y posible vishing: la víctima es guiada a una página falsa, se le solicita instalar un APK fuera de Google Play y luego se le muestra una supuesta verificación de seguridad.

En realidad, la aplicación solicita el PIN y pide acercar la tarjeta física al teléfono para capturar datos mediante el lector NFC, exfiltrándolos por WebSocket hacia infraestructura controlada por el atacante.

La campaña destaca por alojar APKs en GitHub bajo un repositorio señuelo y por usar paquetes malformados para dificultar el análisis automatizado.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Acceso inicial	El usuario es inducido a instalar una aplicación maliciosa que aparenta ser legítima	T1204
Ocultamiento	El malware utiliza técnicas para reducir la probabilidad de ser detectado.	T1027
Obtención de información	La aplicación recopila el PIN y los datos de la tarjeta mediante la función NFC del dispositivo.	T1005
Comunicación con el atacante	La información robada es transmitida a la infraestructura utilizada por los ciberdelincuentes.	T1102

Recomendaciones

- Bloqueo de instalación externa: Aplicar políticas MDM para impedir el sideloading de APKs en equipos corporativos y dispositivos BYOD con acceso a correo, VPN o aplicaciones empresariales.
- Capacitación sobre Ingeniería Social Avanzada: Advertir a los usuarios sobre ataques telefónicos en los que falsos operadores del banco solicitan instalar aplicaciones externas o escanear tarjetas físicas mediante el chip NFC del teléfono.
- Control de aplicaciones móviles: Validar que las aplicaciones financieras instaladas provengan únicamente de tiendas oficiales y que no soliciten permisos o funciones NFC fuera de contexto.
- Detección móvil avanzada: Utilizar soluciones MTD/EDR móvil capaces de alertar por WebViews sospechosas, uso anómalo de NFC y conexiones WebSocket desde aplicaciones no autorizadas.
- Bloqueo de infraestructura: Restringir dominios de phishing identificados y monitorear descargas desde repositorios públicos de GitHub no asociados a la operación normal de la organización.

ALTA

1.2 [ALTA] Campaña de adware compromete más de 50 000 sitios web para distribuir contenido malicioso



Durante junio de 2026, investigadores de seguridad identificaron una campaña de adware a gran escala que comprometió más de 50 000 sitios web, principalmente portales de contenido no oficial, streaming y descargas.

La infraestructura maliciosa utilizaba scripts de JavaScript incrustados para perfilar a las víctimas, recopilar información del navegador y redirigir automáticamente a sitios de phishing, descargas de malware o campañas de publicidad fraudulenta.

La operación incorporaba técnicas de ofuscación y rotación dinámica de dominios para dificultar su detección, permitiendo mantener activa la infraestructura durante largos periodos.

Aunque la campaña se orientó principalmente a usuarios finales, representa un riesgo para las organizaciones cuando dispositivos corporativos acceden a sitios comprometidos o cuando las credenciales obtenidas son reutilizadas en servicios empresariales.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Compromiso inicial	El usuario accede a un sitio web comprometido, donde se ejecuta contenido malicioso sin requerir una acción adicional.	T1189
Ocultamiento	La infraestructura del ataque emplea técnicas para dificultar su detección, como la ofuscación del código y el cambio constante de dominios	T1027
Obtención de información	Se recopila información del navegador, del sistema operativo y del dispositivo para identificar a la víctima y adaptar el ataque	T1082
Transmisión de información	Los datos obtenidos son enviados a servidores controlados por los atacantes mediante conexiones web.	T1041
Entrega de contenido malicioso	El usuario es redirigido a sitios de phishing, descargas de malware o campañas de publicidad fraudulenta para continuar el ataque.	T1071.001

Recomendaciones

- Fortalecer el filtrado web: Implementar soluciones DNS Security o Secure Web Gateway que bloqueen el acceso a dominios maliciosos y sitios de alto riesgo.
- Restringir la navegación no autorizada: Aplicar políticas que limiten el acceso a plataformas de streaming, descargas no oficiales y sitios con baja reputación desde equipos corporativos.
- Mantener navegadores actualizados: Garantizar que los navegadores y sus extensiones permanezcan actualizados para reducir el riesgo de explotación mediante scripts maliciosos.
- Higiene de credenciales: Prohibir reutilización de contraseñas entre servicios personales y corporativos, reforzando MFA y gestores de contraseñas aprobados.
- Capacitar a los usuarios: Sensibilizar al personal sobre los riesgos asociados al acceso a sitios no confiables y la descarga de contenido desde fuentes no verificadas.

CRÍTICA

1.3 [CRÍTICA] Campaña Miasma compromete paquetes npm de Red Hat para robar secretos de desarrollo y nube



El 1 de junio de 2026 se reportó la campaña Miasma, un ataque de cadena de suministro que afectó paquetes npm asociados a @redhat-cloud-services.

El malware se ejecutaba durante la instalación y buscaba credenciales de GitHub, tokens npm, secretos de CI/CD, llaves SSH, credenciales cloud, datos de Kubernetes, Vault y material sensible de entornos DevOps.

La operación también incorporaba mecanismos de persistencia en herramientas usadas por desarrolladores, como configuraciones de Claude Code y tareas automáticas de Visual Studio Code, además de técnicas de exfiltración cifrada hacia GitHub.

El caso es relevante porque demuestra que una dependencia aparentemente legítima puede transformarse en un vector de robo de credenciales y propagación hacia pipelines de construcción y despliegue.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Compromiso de la cadena de suministro	El atacante compromete paquetes de software legítimos para que el malware se ejecute automáticamente cuando los desarrolladores los instalan.	T1195.001
Obtención de credenciales	El malware busca y recopila credenciales, claves de acceso y otros secretos utilizados en plataformas de desarrollo y servicios en la nube.	T1552
Persistencia	Se realizan modificaciones en el entorno de desarrollo para que el malware permanezca activo y vuelva a ejecutarse automáticamente.	T1053 / T1546
Extracción de información	Las credenciales y datos sensibles recopilados son enviados de forma cifrada a la infraestructura controlada por el atacante utilizando servicios legítimos.	T1567.001

Recomendaciones

- Aislamiento de hosts de desarrollo: Separar inmediatamente estaciones o runners que hayan instalado versiones afectadas y evitar que sigan publicando artefactos, imágenes o paquetes.
- Rotación de secretos DevOps: Revocar y regenerar tokens de GitHub, npm, llaves SSH, credenciales cloud, secretos de CI/CD y credenciales de Kubernetes o Vault expuestas.
- Revisión de persistencia: Auditar archivos como .vscode/tasks.json, configuraciones de Claude Code, workflows de GitHub Actions y scripts añadidos fuera del proceso normal de cambio.
- Control de dependencias: Exigir revisión de versiones, bloqueo de paquetes vulnerables y validación de scripts preinstall/postinstall antes de construir proyectos críticos.
- Monitoreo de actividad anómala: Alertar por commits firmados inesperados, creación de repositorios públicos desconocidos, cambios en pipelines y llamadas inusuales a APIs de GitHub o proveedores cloud.

CRÍTICA**1.4 [CRÍTICA] Malware se propaga por WhatsApp usando cuentas comprometidas y adjuntos VBScript**

Kaspersky reveló una campaña masiva que utiliza cuentas de WhatsApp previamente comprometidas para enviar archivos maliciosos a contactos de confianza. Los atacantes emplean nombres de documentos comerciales rutinarios, como facturas, estados de cuenta o avisos de deuda, localizados en varios idiomas para elevar la tasa de apertura.

Al ejecutar el archivo VBScript, la víctima inicia una cadena por etapas que descarga herramientas de administración remota y otorga control del equipo Windows al atacante.

El abuso de relaciones de confianza convierte esta campaña en un riesgo relevante para organizaciones que permiten WhatsApp Web o Desktop como canal informal de coordinación con clientes, proveedores o equipos internos.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Distribución del malware	El atacante utiliza cuentas de WhatsApp previamente comprometidas para enviar archivos maliciosos a contactos de confianza, aumentando la probabilidad de que sean abiertos.	T1566.003
Ejecución del archivo	La víctima ejecuta un archivo que aparenta ser un documento legítimo, iniciando la instalación del malware en el equipo	T1059.005
Ocultamiento	El malware utiliza nombres y características similares a documentos o archivos legítimos para reducir las sospechas del usuario y dificultar su identificación.	T1036
Control del equipo	El malware descarga herramientas de acceso remoto que permiten al atacante tomar el control del equipo afectado y realizar acciones no autorizadas.	T1219 / T1105

Recomendaciones

- Bloqueo de extensiones de riesgo: Impedir la ejecución por defecto de archivos .vbs, .vbe, .js, .hta, .bat, .cmd, .ps1 y ejecutables no firmados desde mensajería o descargas.
- Política de uso de mensajería: Definir cuándo WhatsApp Web/Desktop puede utilizarse en equipos corporativos y prohibir la recepción de adjuntos ejecutables por este canal.
- Monitoreo de rutas públicas: Generar alertas ante ejecución de scripts o binarios desde C:\Users\Public\Documents, AppData, Temp u otras rutas típicas de staging.
- Detección de RMM no autorizado: Bloquear o alertar por instalación de herramientas de administración remota que no estén inventariadas o aprobadas por TI.

ALTA

1.5 [ALTA] Kaspersky advierte que los infostealers se propagan principalmente mediante archivos temporales



Kaspersky Digital Footprint Intelligence informó que más de un tercio de las infecciones por infostealer comienzan cuando el usuario ejecuta archivos directamente desde carpetas temporales del navegador o del sistema.

La investigación refuerza una conclusión práctica: gran parte del robo de credenciales no depende de exploits complejos, sino de descargas de software no autorizado, cracks, instaladores falsos, mods de videojuegos o herramientas de origen dudoso.

Los infostealers extraen contraseñas, cookies, tokens, datos de navegador y, en algunos casos, información de correo o wallets.

En un entorno empresarial, una infección en un equipo personal o corporativo puede terminar en acceso válido a VPN, correo, SSO o aplicaciones SaaS.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Infección inicial	El usuario ejecuta un archivo descargado desde una fuente no confiable, como un instalador falso, software pirata o herramientas no autorizadas.	T1204.002
Ejecución del malware	El programa malicioso se ejecuta desde carpetas temporales del sistema o del navegador, iniciando la infección del equipo.	T1059
Evasión de controles de seguridad	El malware intenta evitar su detección aprovechando configuraciones inseguras o induciendo al usuario a desactivar las protecciones del equipo.	T1562.001
Robo de credenciales	Se recopilan contraseñas, cookies de sesión, tokens y otra información confidencial almacenada en el dispositivo y las aplicaciones utilizadas por el usuario.	T1555
Envío de la información robada	La información obtenida es transmitida a la infraestructura controlada por los atacantes para su posterior utilización o comercialización.	T1041

Recomendaciones

- Restricción de descargas: Bloquear software pirata, activadores, instaladores de terceros y utilidades no aprobadas mediante proxy, EDR y control de aplicaciones.
- Protección del endpoint: Impedir que usuarios deshabiliten antivirus o EDR, y alertar por ejecuciones desde Temp, Downloads o AppData con reputación desconocida.
- Gestión segura de credenciales: Prohibir contraseñas guardadas en texto plano, notas, navegadores sin control corporativo o capturas de pantalla; promover gestores aprobados.
- Monitoreo de exposición: Implementar inteligencia de credenciales filtradas para detectar cuentas corporativas en logs de infostealers y forzar rotación inmediata.
- MFA y sesiones: Aplicar MFA resistente al phishing donde sea posible y revocar sesiones activas ante evidencia de robo de cookies o tokens.

2. VULNERABILIDADES

CRÍTICA

2.1 [CRÍTICA] Explotación activa de vulnerabilidades en Fortinet FortiSandbox permite bypass de autenticación y ejecución de comandos



Durante junio de 2026 se reportó explotación activa contra tres vulnerabilidades de Fortinet FortiSandbox: CVE-2026-39813, CVE-2026-39808 y CVE-2026-25089.

La cadena de riesgo combina bypass de autenticación, path traversal, inyección de comandos y escalamiento de privilegios, lo que puede permitir a un atacante no autenticado ejecutar acciones no autorizadas sobre un componente diseñado justamente para analizar archivos sospechosos.

El caso es crítico porque FortiSandbox suele estar integrado con correo, firewall, endpoints o flujos de análisis de malware; por tanto, su compromiso puede afectar controles de detección y abrir una ruta hacia datos sensibles o infraestructura interna.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Explotación de la vulnerabilidad	El atacante aprovecha una falla en FortiSandbox para acceder al sistema sin necesidad de una autenticación válida.	T1190
Ejecución de acciones maliciosas	Una vez explotada la vulnerabilidad, puede ejecutar comandos no autorizados y comprometer el funcionamiento del equipo afectado	T1059
Escalamiento de privilegios	El atacante puede obtener un mayor nivel de acceso al sistema, ampliando su capacidad para modificar configuraciones, acceder a información sensible o afectar otros componentes de la infraestructura.	T1068

Recomendaciones

- Actualización prioritaria: Aplicar las versiones corregidas indicadas por Fortinet para FortiSandbox 4.4, 5.0 y ramas afectadas, sin esperar al ciclo regular de parchado.
- Restricción de exposición: Aislar interfaces administrativas y APIs de FortiSandbox para que no sean accesibles desde Internet o redes no confiables.
- Revisión de logs e IoCs: Buscar solicitudes HTTP anómalas, intentos de path traversal, comandos inesperados y cambios no autorizados en configuración o usuarios.
- Segmentación de integración: Validar que FortiSandbox no tenga permisos excesivos sobre correo, firewalls, EDR o repositorios de muestras que puedan amplificar el impacto.

ALTA

2.2 [ALTA] Cisco Unified CM CVE-2026-20230 es explotada activamente y permite escritura de archivos hacia el sistema



Cisco publicó actualizaciones para CVE-2026-20230, una vulnerabilidad SSRF en Cisco Unified Communications Manager y Unified CM SME.

El fallo permite a un atacante remoto no autenticado enviar solicitudes especialmente diseñadas y provocar escritura de archivos en el sistema subyacente, con posibilidad de ser usada como paso previo para elevar privilegios a root.

CISA añadió la vulnerabilidad al catálogo KEV el 25 de junio de 2026 tras confirmarse explotación activa.

Dado que estas plataformas suelen soportar telefonía corporativa, extensiones, WebDialer y comunicaciones críticas, el riesgo va más allá de la indisponibilidad: puede comprometer infraestructura de voz y facilitar movimiento hacia otros sistemas internos.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Explotación de la vulnerabilidad	El atacante aprovecha una falla en Cisco Unified CM para enviar solicitudes especialmente diseñadas que explotan el sistema sin requerir autenticación.	T1190
Modificación del sistema	La vulnerabilidad permite escribir archivos en el servidor afectado, lo que puede utilizarse para alterar su funcionamiento o preparar acciones posteriores.	T1203
Escalamiento de privilegios	El atacante puede utilizar los archivos creados para obtener un mayor nivel de acceso al sistema y comprometer componentes críticos de la infraestructura de telefonía.	T1068

Recomendaciones

- Aplicación de parches: Actualizar Cisco Unified CM y Unified CM SME a las versiones corregidas por Cisco; no existen workarounds equivalentes para eliminar el riesgo.
- Revisión de exposición: Restringir el acceso a interfaces web de administración y componentes asociados como WebDialer a redes internas o VPN administrativa.
- Búsqueda de compromiso: Revisar escritura de archivos inesperada, procesos anómalos, errores de aplicación y solicitudes HTTP inusuales en servidores Unified CM.
- Control de segmentación: Limitar la comunicación desde servidores de telefonía hacia otros segmentos críticos, evitando que una explotación se convierta en pivote lateral.

CRÍTICA

2.3 [CRÍTICA] Cisco Catalyst SD-WAN Manager CVE-2026-20262 es explotada para escritura arbitraria de archivos



El 15 de junio de 2026, Cisco publicó actualizaciones para CVE-2026-20262, una vulnerabilidad de escritura arbitraria de archivos en la interfaz web de Cisco Catalyst SD-WAN Manager, anteriormente vManage.

Aunque requiere un usuario autenticado con privilegios, CISA la incorporó al catálogo KEV por evidencia de explotación activa.

La criticidad práctica es alta porque SD-WAN Manager centraliza políticas, configuración y operación de componentes de red distribuidos; un actor con credenciales comprometidas podría alterar archivos locales, preparar persistencia o afectar la administración de conectividad entre sedes.

Cisco también publicó una guía de remediación para recolectar admin-tech y revisar indicadores en logs.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Uso de credenciales válidas	El atacante utiliza credenciales legítimas o previamente comprometidas para acceder a la interfaz de administración de Cisco SD-WAN Manager.	T1078
Modificación del sistema	Una vez dentro de la plataforma, puede crear o modificar archivos en el sistema, alterando configuraciones o preparando acciones posteriores.	T1059
Ocultamiento	Los cambios realizados pueden mezclarse con actividades administrativas legítimas, dificultando su identificación temprana.	T1036
Impacto operativo	La explotación puede afectar la administración centralizada de la red SD-WAN, comprometiendo políticas, conectividad entre sedes y la estabilidad de servicios críticos.	T1565

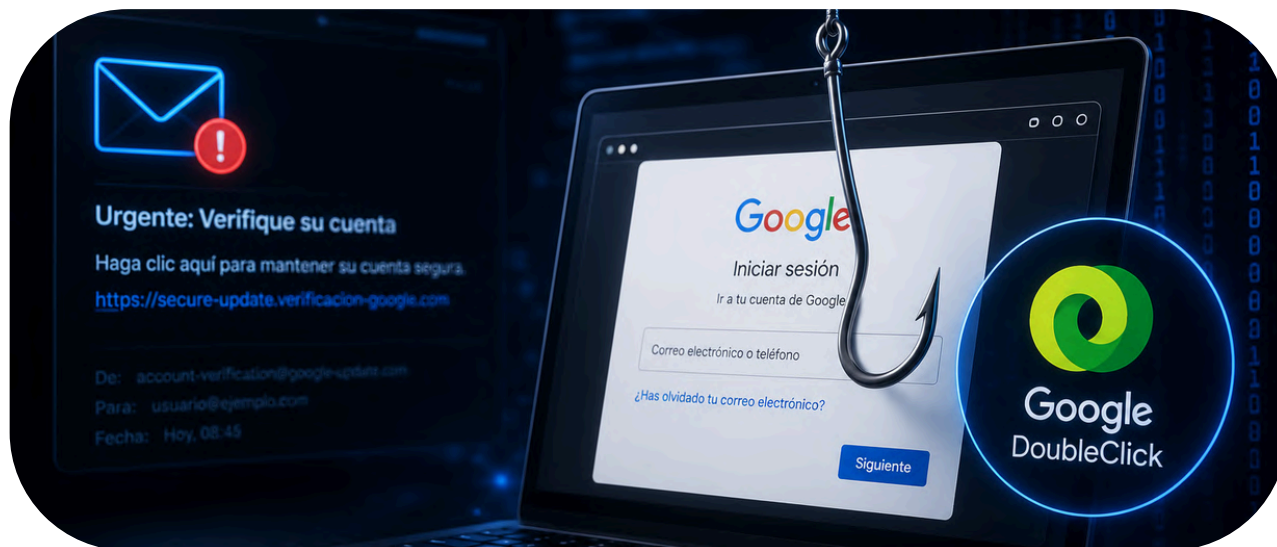
Recomendaciones

- Instalación de versiones corregidas: Aplicar las actualizaciones de Cisco para Catalyst SD-WAN Manager y validar compatibilidad con controladores y componentes edge.
- Auditoría de usuarios privilegiados: Revisar cuentas netadmin/admin, sesiones recientes, cambios de permisos y autenticaciones desde ubicaciones o horarios inusuales.
- Recolección de admin-tech: Generar paquetes admin-tech de los componentes de control y abrir caso TAC si se identifican señales de compromiso o escritura de archivos.
- Revisión de logs: Buscar entradas relacionadas con carga o modificación de archivos, especialmente en SD-WAN Manager, scripts.log y registros recomendados por Cisco.
- Fortalecimiento de acceso: Exigir MFA, segmentación administrativa y acceso por VPN/bastion para consolas SD-WAN; eliminar exposición innecesaria de la interfaz web.
- Plan de contención: Preparar procedimientos para rotar credenciales, respaldar configuración y aislar componentes de control si se confirma actividad maliciosa.

3. PHISHING

ALTA

3.1 [ALTA] Campaña de phishing abusa de Google DoubleClick para evadir filtros y entregar un loader .NET



Huntress documentó una campaña de malspam que utiliza el dominio legítimo de Google DoubleClick como etapa intermedia de redirección.

El correo inicial contiene un HTML adjunto que lleva al usuario a una supuesta descarga de PDF, con páginas que pueden personalizarse usando información de la organización objetivo.

Si la víctima descarga el ZIP, se ejecuta una cadena con JavaScript y PowerShell que instala un loader .NET, intenta deshabilitar controles como AMSI y ETW, configura persistencia y puede inyectar código en procesos firmados por Microsoft.

El uso de infraestructura confiable incrementa la probabilidad de que los filtros tradicionales permitan la navegación inicial.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Distribución del ataque	El usuario recibe un correo con un archivo adjunto que lo dirige a descargar contenido malicioso.	T1566.001
Ejecución del malware	Al abrir el archivo, se ejecutan scripts que instalan el malware en el equipo.	T1059.007 / T1059.001
Persistencia	Al abrir el archivo, se ejecutan scripts que instalan el malware en el equipo.	T1547.001
Evasión de controles de seguridad	El malware intenta evitar su detección deshabilitando o eludiendo mecanismos de protección.	T1562.001 / T1055.012
Comunicación con el atacante	El malware se comunica con la infraestructura del atacante para recibir instrucciones o enviar información.	T1095

Recomendaciones

- Restricción por GPO: Configurar .js, .vbs y .hta para abrirse por defecto con Notepad o Notepad++, evitando ejecución automática por doble clic.
- Autenticación de correo: Mantener DMARC, DKIM y SPF correctamente configurados y monitoreados para reducir suplantación y entrega de malspam.
- Sandboxing de adjuntos: Analizar HTML, ZIP, scripts y enlaces en un entorno seguro antes de permitir su entrega al usuario final.
- Telemetría EDR: Alertar por wscript.exe, powershell.exe o msbuild/installutil ejecutándose desde rutas de usuario, así como por intentos de evasión de AMSI/ETW.

ALTA

3.2 [ALTA] Banco de la Nación advierte campaña de phishing con correos desde dominios Gmail



El Banco de la Nación emitió una advertencia sobre correos fraudulentos que intentan suplantar comunicaciones institucionales usando dominios públicos como Gmail.

Los mensajes buscan generar urgencia, inducir a la descarga de archivos o dirigir a páginas falsas para capturar credenciales bancarias.

El caso es importante para el contexto local porque combina una marca de alta confianza con tácticas simples pero efectivas: remitentes no oficiales, lenguaje de emergencia, enlaces o adjuntos inesperados y solicitudes indirectas de información sensible.

Aunque la campaña está orientada a clientes, el mismo patrón puede afectar cuentas corporativas cuando los usuarios mezclan correo personal y laboral.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Distribución del ataque	Los atacantes envían correos que aparentan provenir del Banco de la Nación para inducir a los usuarios a abrir archivos o acceder a enlaces maliciosos.	T1566.001 / T1566.002
Suplantación de identidad	Los mensajes utilizan logotipos, lenguaje institucional y remitentes similares a los oficiales para generar confianza y reducir las sospechas de la víctima.	T1036
Robo de credenciales	El usuario es dirigido a formularios o sitios web fraudulentos donde se solicita el ingreso de credenciales y otra información confidencial.	T1056
Impacto	Las credenciales comprometidas pueden ser utilizadas para realizar operaciones fraudulentas, acceder a cuentas bancarias o afectar otros servicios asociados al usuario.	T1657

Recomendaciones

- Verificación de remitentes: Desconfiar de cualquier comunicación bancaria enviada desde dominios públicos o gratuitos, aun cuando use logos o nombres institucionales.
- Acceso directo al portal: Ingresar al banco escribiendo la URL oficial en el navegador; no usar enlaces recibidos por correo, SMS o mensajería.
- Protección de credenciales: Recordar que ninguna entidad bancaria debe solicitar contraseñas, token, CVV, PIN o códigos de verificación por correo.
- Validación de urgencia: Tratar como sospechosos los mensajes con amenazas de bloqueo, actualización inmediata o beneficios condicionados a abrir adjuntos.
- Reporte oportuno: Canalizar correos sospechosos al área de seguridad o a los canales oficiales antifraude para facilitar bloqueo y prevención de nuevas víctimas

ALTA

3.3 [ALTA] Quishing, spoofing telefónico y clonación de voz elevan el fraude digital en Perú



Durante junio de 2026 se advirtió en Perú un crecimiento de estafas digitales más sofisticadas, entre ellas códigos QR falsos, llamadas con Caller ID Spoofing, wangiri y uso de inteligencia artificial para clonar voces o generar engaños más creíbles.

Estas modalidades explotan hábitos cotidianos: escanear QR sin validar la URL, devolver llamadas internacionales perdidas, confiar en el número que aparece en pantalla o reaccionar ante supuestas emergencias familiares.

Para empresas, el riesgo no se limita al fraude personal; también puede derivar en entrega de credenciales, pagos no autorizados, suplantación de proveedores o aprobación de transferencias mediante ingeniería social.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Contacto con la víctima	Los atacantes utilizan códigos QR, enlaces, llamadas telefónicas o mensajes fraudulentos para dirigir a la víctima hacia sitios falsos o iniciar el engaño.	T1566
Suplantación de identidad	Se hacen pasar por bancos, proveedores, familiares u otras entidades de confianza mediante números telefónicos falsificados o tecnologías de clonación de voz para generar credibilidad.	T1036
Obtención de información	Mediante técnicas de ingeniería social, inducen a la víctima a proporcionar credenciales, códigos de verificación, información bancaria u otros datos confidenciales.	T1056.002
Fraude financiero	La información obtenida es utilizada para realizar transferencias, pagos no autorizados u otras operaciones fraudulentas que generan pérdidas económicas.	T1657
Manipulación mediante ingeniería social	Los atacantes ejercen presión para que la víctima tome decisiones rápidas sin verificar la autenticidad de la solicitud, aumentando la probabilidad de éxito del fraude.	N/A (Ingeniería Social Avanzada)

Recomendaciones

- Validación de QR: Confirmar que el código no esté sobrepuesto físicamente y revisar la URL antes de abrirla; no instalar aplicaciones desde códigos QR no verificados.
- Bloqueo de wangiri: No devolver llamadas internacionales desconocidas y solicitar a la operadora restricciones para números premium o destinos de riesgo.
- Mitigación de spoofing: Si una llamada aparenta venir del banco o de un proveedor, colgar y devolver la comunicación usando un número oficial previamente validado.
- Defensa contra IA: Usar palabras de seguridad o doble validación por canal alternativo ante solicitudes urgentes de dinero, cambios de cuenta bancaria o aprobación de pagos.
- Controles empresariales: Capacitar a usuarios de finanzas, compras y mesa de ayuda para verificar solicitudes sensibles mediante procesos formales y no solo por voz o mensajería.

4. ADVERSARIOS

CRÍTICA

4.1 [CRÍTICA] ShinyHunters explota un zero-day en Oracle PeopleSoft para atacar universidades y organizaciones



En junio de 2026 se reportó una campaña de extorsión atribuida a ShinyHunters que explotó una vulnerabilidad zero-day en Oracle PeopleSoft (CVE-2026-35273) para comprometer entornos empresariales, con fuerte impacto en universidades.

La operación habría permitido acceso a sistemas ERP, robo de información interna y presión extorsiva para evitar filtraciones públicas.

Este tipo de incidente es especialmente sensible porque PeopleSoft suele concentrar información académica, financiera, laboral y de identidad, por lo que una intrusión puede derivar en exposición de datos personales, interrupción administrativa y ataques posteriores contra estudiantes, docentes o proveedores mediante ingeniería social.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Explotación de la vulnerabilidad	El atacante aprovecha una vulnerabilidad en Oracle PeopleSoft para obtener acceso no autorizado a los sistemas empresariales expuestos.	T1190
Acceso a información sensible	Una vez dentro del sistema, busca credenciales y datos confidenciales relacionados con las operaciones de la organización	T1552
Extracción de información	La información recopilada es enviada a la infraestructura controlada por los atacantes con fines de robo o extorsión.	T1041 / T1567
Extorsión e impacto operativo	Los atacantes utilizan la información sustraída para exigir pagos, amenazar con su divulgación y generar afectaciones operativas y reputacionales para la organización	T1657 / T1491.002

Recomendaciones

- Parchado de emergencia: Aplicar actualizaciones y mitigaciones de Oracle PeopleSoft, priorizando instancias expuestas o integradas con portales públicos.
- Revisión de accesos ERP: Auditar cuentas administrativas, integraciones, sesiones anómalas y cambios recientes en roles, flujos y objetos del sistema.
- Búsqueda de exfiltración: Analizar logs de transferencia, consultas masivas, descargas inusuales y accesos desde IPs no habituales durante la ventana de exposición.
- Protección de usuarios afectados: Preparar comunicaciones, rotación de credenciales y monitoreo de phishing dirigido si se confirma exposición de datos.

CRÍTICA

4.2 [CRÍTICA] FortiBleed expone credenciales asociadas a decenas de miles de dispositivos Fortinet



CISA alertó en junio de 2026 sobre reportes globales de actividad maliciosa contra dispositivos Fortinet accesibles desde Internet, asociada a credenciales comprometidas de aproximadamente 74.000 firewalls y gateways VPN. La campaña, conocida como FortiBleed, no debe interpretarse solo como una filtración de contraseñas:

el verdadero riesgo es que credenciales válidas permitan acceso administrativo o VPN, cambios de configuración, creación de cuentas persistentes y movimiento hacia Active Directory u otros segmentos internos.

Fortinet indicó que está contactando a clientes potencialmente afectados y recomendó terminar sesiones activas, rotar credenciales, aplicar MFA y actualizar versiones soportadas.

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

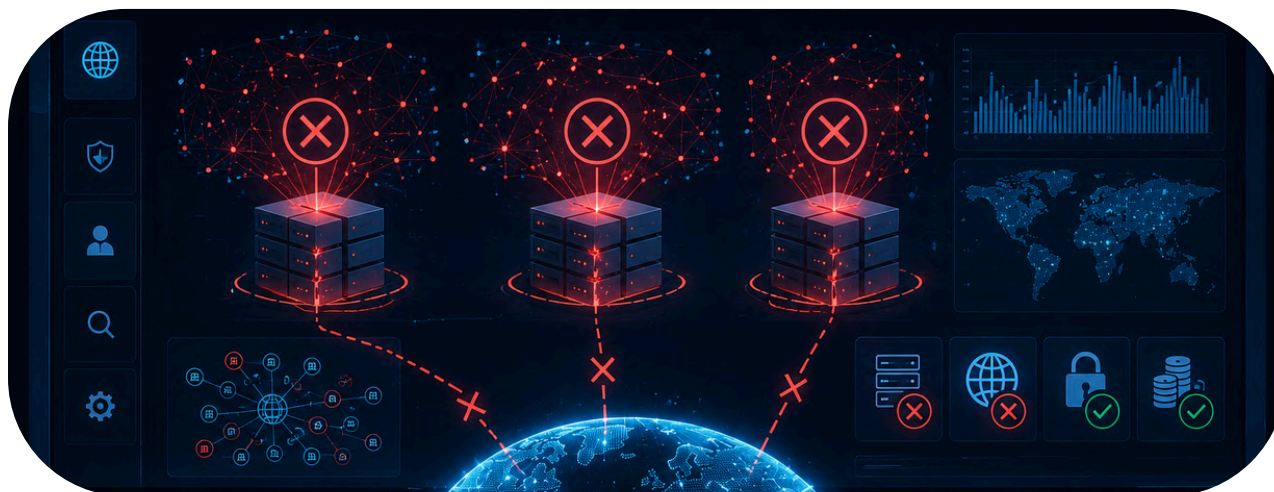
Fase del ataque	Descripción	Referencia Mitre Att&Ck
Acceso mediante credenciales comprometidas	El atacante utiliza credenciales administrativas o de acceso remoto previamente comprometidas para ingresar a dispositivos Fortinet expuestos a Internet.	T1078
Compromiso de credenciales	Las credenciales filtradas pueden ser reutilizadas o validadas para obtener acceso no autorizado a la infraestructura de la organización.	T1110.002 / T1552
Establecimiento de acceso persistente	Una vez dentro del dispositivo, el atacante puede crear nuevas cuentas o modificar configuraciones para mantener el acceso incluso después de un cambio de contraseña.	T1136 / T1098
Propagación hacia otros sistemas	El acceso al dispositivo comprometido puede utilizarse como punto de entrada para alcanzar servidores internos, servicios corporativos o el directorio activo de la organización.	T1021

Recomendaciones

- Eliminar exposición pública: Retirar interfaces de administración FortiGate/FortiOS de Internet y permitir acceso solo desde VPN, bastión o redes internas autorizadas.
- Rotación y cierre de sesiones: Terminar sesiones administrativas y VPN activas, restablecer contraseñas de administradores y usuarios VPN, y revocar credenciales antiguas.
- MFA obligatorio: Habilitar MFA resistente al phishing para administradores, VPN y cuentas con acceso privilegiado al perímetro.
- Auditoría de compromiso: Revisar usuarios nuevos, cambios de política, objetos VPN, rutas, scripts, logs borrados y autenticaciones históricas desde ubicaciones no esperadas.
- Actualización de firmware: Migrar a versiones soportadas de FortiOS y validar que las mejores prácticas de hardening se mantengan aplicadas después del upgrade.

ALTA

4.3 [ALTA] Operation Endgame interrumpe infraestructura de SocGhosh, Amadey y StealC



Europol, Microsoft y socios internacionales anunciaron una nueva fase de Operation Endgame contra infraestructura usada por SocGhosh, Amadey y StealC. La operación buscó afectar la fase inicial de la cadena criminal: loaders, infostealers, dominios y servidores C2 que alimentan accesos para fraude, ransomware y robo de credenciales

Según los reportes, se interrumpieron cientos de servidores y dominios, se recuperaron millones de credenciales robadas y se identificaron activos de criptomonedas vinculados a la operación.

Aunque este tipo de acciones reduce la capacidad temporal de los actores, las organizaciones no deben asumir que el riesgo desaparece: los infostealers suelen reconstruir infraestructura y monetizar credenciales ya robadas.

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

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Preparación de la infraestructura	Los atacantes establecen dominios, servidores y otros recursos para distribuir malware y mantener la comunicación con los equipos comprometidos.	T1583.001 / T1583.004
Infección inicial	Las víctimas son comprometidas mediante sitios web infectados, campañas de phishing o descargas engañosas que instalan el malware.	T1189 / T1566
Robo de credenciales	El malware recopila contraseñas, cookies y otros datos de autenticación que pueden utilizarse para acceder a sistemas corporativos.	T1555
Uso de la información comprometida	Las credenciales robadas pueden emplearse para cometer fraude, acceder a redes empresariales o facilitar ataques posteriores, como ransomware.	T1657 / T1486

Recomendaciones

- Revisión de credenciales expuestas: Buscar cuentas corporativas en logs de StealC, Amadey y otros infostealers, y forzar rotación cuando exista coincidencia.
- Detección de loaders: Alertar por Amadey, SocGholish, StealC, descargas desde sitios comprometidos y ejecución de binarios con baja reputación.
- Controles de identidad: Revocar sesiones, exigir MFA y aplicar políticas de riesgo ante inicios de sesión desde dispositivos no administrados o ubicaciones anómalas.
- Monitoreo continuo: Mantener inteligencia de amenazas activa, ya que las campañas desmanteladas pueden reaparecer con nuevos dominios, servidores o marcas de malware.

5. INDICADORES DE COMPROMISO

5.1 Direcciones IP

200[.]105[.]172[.]184	204[.]48[.]28[.]177	45[.]78[.]235[.]96
107[.]150[.]112[.]48	193[.]124[.]20[.]233	141[.]11[.]187[.]237
176[.]65[.]139[.]246	83[.]235[.]16[.]111	45[.]227[.]254[.]170
1[.]168[.]64[.]152	185[.]55[.]229[.]75	90[.]230[.]226[.]175

5.2 Dominios

dfgjhklkhuuk[.]info	eventsyouwant[.]com
increvalor[.]com	plasteredplayn[.]com
baileyemas[.]com	autobaenasl[.]com
sixmexicos[.]com	postelnini[.]mk
solar-sanat[.]net	co-emas[.]com
vanta[.]st	n[.]vs108[.]com

5.3 Hashes

488eca83789084f7cea7388507507ae2d7baf5822f8f8fb5d7897eced88e3d24
33c17d8894c2312e9be34fe364f9825abbb619cfc58575b6c9852f5f759cefa8
a1d44b0831a84664bb04019cb8e71a09e4a43adddedb55bfcd99c9f745058f06
7fad51a51214124a5c92adfc455c91c596a6d3d51812b587d7cdb5935245422f
e0075a69558494c5e5fe7f44ccad33a787c956fa460384d5f412b79db3273504
27392ed3727242da298176dde9ee699a2d20a61a403d330bb2390c600299ef20
40a803463027ee84e64ef511b40ca9a4fbc3681a689787e3bfd38fd50ac0ef01
6f55ef2c93b5c5b1f773b9e6a1e1f34394ae86a00eb62d27f79b5a630aba47cc
3ca71c5ddf3941a72345bd86e0913a384050e1a5e66a77ae984690dbe0b63a06
b10a49e2587b457bd05f1f3096d5be22cea340496bc7ab0bb83f25adab173f1a
7c04d762bfb2322a5e4c6ca8c238a7209aae00217a7242077224c668c39f3f25
f83bd5cf65fe7405e6f827d33a29841d7a84865750734e2e507d1850152ade6b

6. FUENTES

- 6.1 <https://www.d3lab.net/nfcshare-evolves-from-a-banking-phishing-apk-to-a-github-hosted-android-nfc-fraud-campaign/>
- 6.2 <https://www.techradar.com/vpn/vpn-privacy-security/hundreds-of-thousands-at-risk-as-nordvpn-uncovers-sophisticated-adware-campaign-hidden-in-50-000-pirate-sites?>
- 6.3 <https://thehackernews.com/2026/06/miasma-supply-chain-attack-compromises.html>
- 6.4 <https://www.kaspersky.com/about/press-releases/kaspersky-uncovers-a-new-massive-campaign-spreading-malware-via-whatsapp>
- 6.5 <https://www.kaspersky.com/about/press-releases/kaspersky-35-of-infostealer-infections-begin-with-users-running-files-directly-from-temporary-folders>
- 6.6 <https://thehackernews.com/2026/06/attackers-exploit-three-fortinet.html>
- 6.7 <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW>
- 6.8 <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/226014-remediate-catalyst-sd-wan-security.html>
- 6.9 <https://www.huntress.com/blog/malspam-to-loader-delivery-chain-analysis>
- 6.10 <https://www.bn.com.pe/noticias/2026/09062026-comunicado-correo-fraudulento.asp>
- 6.11 <https://www.infobae.com/peru/2026/06/17/suplantando-bancos-clonando-vozes-y-creando-qr-falsos-las-estafas-digitales-que-crecen-en-peru/>
- 6.12 <https://thehackernews.com/2026/06/shinyhunters-exploits-oracle-peoplesoft.html>
- 6.13 <https://www.cisa.gov/news-events/alerts/2026/06/18/cisa-urges-hardening-fortinet-devices-after-reports-credential-exposure>
- 6.14 <https://www.europol.europa.eu/media-press/newsroom/news/global-cyber-strike-disrupts-socgholish-amadey-and-steal-malware-networks>