



GS PERÚ

Software - Security & Services

Empresas

BOLETÍN CIBERSEGURIDAD

Marzo - 2026





ESCALAR EL NEGOCIO SIN ESCALAR EL RIESGO

Marzo 2026: La seguridad ya no se limita a tu empresa, se extiende al ecosistema.

Marzo de 2026 confirma un hecho que toda organización debe asumir: el riesgo ya no está solo dentro de la empresa, sino en toda la cadena de suministro digital. Los últimos incidentes muestran un patrón claro: los atacantes no golpean la infraestructura directamente, sino que comprometen proveedores, librerías y servicios externos para llegar a sus objetivos, afectando a múltiples empresas a la vez.

En un mundo donde cada integración externa y cada servicio SaaS forman parte del negocio, los enfoques tradicionales de seguridad ya no bastan. La verdadera ventaja competitiva hoy no es tener más controles, sino gestionar el riesgo del ecosistema en tiempo real, sin frenar la innovación ni la operación.

Las organizaciones que lograron contener incidentes recientes lo hicieron gracias a tres factores clave: visibilidad total de sus dependencias, monitoreo continuo y automatización de respuesta. La seguridad deja de ser reactiva y se convierte en un motor que protege y acelera el negocio al mismo tiempo.

El mercado ya responde a esta exigencia. Soluciones de Software Supply Chain Security, análisis de composición de software (SCA) y monitoreo proactivo de proveedores ya no son opcionales: se están convirtiendo en estándares para operar con confianza. La seguridad pasa de ser un control a ser un habilitador estratégico.

ÍNDICE

	1. Malware	4
	1.1 Ataque cibernético e interrupción global en los sistemas de Stryker.	
	1.2 Alerta de Red Hat: Malware incrustado en la popular herramienta de compresión de Linux.	
	1.3 Despliegue masivo de la infraestructura del virus "StealC".	
	1.4 Alerta de espionaje sigiloso mediante la puerta trasera "GRIDTIDE"	
	1.5 El virus "Silver Dragon" y su espionaje informático en varias etapas	
	1.6 Campaña de virus enfocada en refinerías de petróleo en Libia.	
	1.7 Extracción de 1.3 Terabytes de datos en corporaciones petroleras.	
	2. Vulnerabilidades	18
	2.1 CVE-2026-21536: Agujero de seguridad de máxima gravedad en Microsoft	
	2.2 CVE-2026-1731: Falla "Día Cero" en el soporte remoto de BeyondTrust	
	2.3 CVE-2026-3055: Falla crítica por exposición de memoria del sistema	
	3. Phishing	24
	3.1 Plataforma cibercriminal logró evadir los sistemas de Autenticación de Múltiples Factores a escala global	
	3.2 Estafas financieras en Medio Oriente imitan marcas empresariales	
	4. Adversarios	28
	4.1 El grupo "APT Iran" ataca ferozmente a Lockheed Martin	
	4.2 Espías de Seedworm infiltran infraestructura crítica en EE. UU	
	5. Indicadores de compromiso	32
	5.1 Direcciones IP	
	5.2 Dominios	
	5.3 Hashes	
	6. Fuentes	

 ALTA

1. Malware

1.1 Ataque cibernético e interrupción global en los sistemas de Stryker.

El 11 de marzo de 2026, la reconocida empresa tecnológica y médica Stryker experimentó un ciberataque significativo que provocó una interrupción a nivel mundial de todas sus operaciones. Este incidente paralizó severamente el entorno de sistemas de Microsoft de la compañía, afectando su red de manera generalizada.

Al detectar esta intrusión masiva, la corporación activó de inmediato sus planes de respuesta ante emergencias y procedió a iniciar una investigación exhaustiva. Para garantizar la contención del ataque, Stryker solicitó la ayuda inmediata de asesores externos y especialistas internacionales en ciberseguridad.

Aunque la red sufrió graves cortes, la empresa informó oficialmente a sus clientes y socios que no encontraron indicios de secuestro de datos (Ransomware) o instalación de programas maliciosos tradicionales, afirmando que lograron aislar el ataque a tiempo.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Posible explotación de servicios expuestos o vulnerabilidades en la infraestructura de Microsoft para obtener acceso inicial a la red global.
TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Uso de scripts o comandos del sistema para paralizar el entorno operativo y propagar la interrupción en la red corporativa.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Ejecución de acciones que evadieron la detección de malware tradicional, sugiriendo el uso de técnicas de "Living off the Land" o manipulación de configuraciones
TA0007: Descubrimiento	T1082 – System Information Discovery	Identificación y mapeo de la red de Microsoft de la compañía para asegurar una afectación generalizada y masiva.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Establecimiento de canales de comunicación para coordinar la intrusión masiva y la interrupción de las operaciones mundiales.
TA0040: Impacto	T1499 – Endpoint Denial of Service	Provocación de una interrupción a nivel mundial y parálisis de los sistemas operativos críticos sin el uso de cifrado por Ransomware.

Recomendaciones

- Implementar monitoreo mediante soluciones SIEM/EDR para detectar ejecuciones anómalas y cambios sospechosos en el entorno operativo.
- Mantener copias de seguridad inmutables y aisladas para garantizar la restauración rápida ante incidentes masivos que paralicen la red.
- Aplicar políticas de endurecimiento (hardening) de sistemas operativos y gestionar parches de seguridad de forma prioritaria.
- Desplegar autenticación de multifactor en todos los accesos críticos y administrativos.
- Segmentar la red corporativa para limitar el impacto de intrusiones de alcance global.
- Realizar ejercicios periódicos de respuesta a incidentes enfocados en escenarios de interrupción operativa masiva.

CRÍTICA



1.2 Alerta de Red Hat: Malware incrustado en la popular herramienta de compresión de Linux.

A finales de marzo, se descubrió un ataque histórico a la cadena de suministro que resultó en la inyección de código malicioso dentro de XZ Utils, una herramienta de compresión de datos fundamental en distribuciones de Linux, afectando ecosistemas empresariales como Red Hat.

Un actor de amenazas logró infiltrarse como mantenedor del proyecto de código abierto durante años para introducir esta puerta trasera de manera sigilosa. Este código malicioso es extremadamente peligroso porque intercepta y modifica el proceso de autenticación del servicio SSH, permitiendo a los atacantes eludir los controles de seguridad y ejecutar código de forma remota en los servidores afectados.

El descubrimiento fortuito por parte de un ingeniero de software evitó que esta vulnerabilidad comprometiera de manera silenciosa a cientos de miles de infraestructuras críticas a nivel global.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1195 – Supply Chain Compromise	Insertión metódica de código malicioso en el código fuente legítimo de la biblioteca de compresión XZ Utils a lo largo de varios meses.
TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Ejecución de secuencias de comandos ofuscadas durante el proceso de compilación del software para inyectar la puerta trasera en el sistema operativo.
TA0003: Persistencia	T1543.002 – Systemd Services	Integración del componente malicioso en el proceso de inicio del servicio SSHD a través de los administradores de servicios como systemd.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Alteración de las funciones de validación de claves RSA en el demonio SSH para eludir las alertas de intrusión sin dejar rastros en los registros habituales.
TA0008: Movimiento Lateral	T1021.004 – SSH	Abuso del túnel SSH comprometido para enviar cargas útiles adicionales, sortear el perímetro y tomar el control total de la infraestructura del servidor.

Recomendaciones:

- Auditar inmediatamente la infraestructura de servidores para identificar la presencia de las versiones comprometidas de XZ Utils, específicamente las versiones 5.6.0 y 5.6.1.
- Revertir o degradar los paquetes de software afectados a versiones previas seguras y comprobadas, como la 5.4.6, siguiendo las directrices oficiales de mitigación del proveedor.
- Monitorear activamente los registros del servicio SSH en busca de conexiones entrantes anómalas, uso de recursos inusual o picos de procesamiento del CPU durante los intentos de inicio de sesión.
- Implementar una estricta segmentación de red para aislar los servidores críticos expuestos a Internet y limitar el impacto de posibles ejecuciones remotas de código.
- Restringir el acceso SSH únicamente a direcciones IP de confianza mediante listas de control de acceso perimetrales y firewalls a nivel de host.

 ALTA

1.3 Despliegue masivo de la infraestructura del virus "StealC".

Los investigadores de la división de ciberseguridad Unit 42 de Palo Alto Networks detectaron una agresiva campaña en marzo de 2026 centrada en el despliegue del virus "StealC", diseñado para robar información personal y bancaria.

Los ciberdelincuentes registraron miles de nuevos dominios en internet relacionados con el actual conflicto en Medio Oriente para utilizarlos como un disfraz perfecto. A través de estos dominios falsos, los atacantes crearon portales fraudulentos y tiendas ficticias que infectan de manera invisible a los usuarios que navegan por ellos.

Una vez que el virus "StealC" se instala en el equipo de la víctima, procede a extraer silenciosamente todas las contraseñas, documentos financieros y datos almacenados en el navegador, enviándolos directamente a los servidores controlados por los criminales.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1189 – Drive-by Compromise	Uso de miles de dominios falsos, portales fraudulentos y tiendas ficticias relacionadas con el conflicto en Medio Oriente para infectar a usuarios que navegan por ellos.
TA0005: Evasión de Defensa	T1036 – Masquerading	Registro de dominios temáticos actuales para utilizarlos como camuflaje y evitar sospechas durante la infección inicial.
TA0009: Recolección	T1555 – Credentials from Password Stores	Extracción silente de contraseñas, documentos financieros y datos almacenados directamente en el navegador de la víctima.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Establecimiento de comunicación con servidores controlados por los criminales para coordinar el robo de información.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Envío de todas las contraseñas y documentos financieros recolectados directamente hacia los servidores de los atacantes.

Recomendaciones:

- Desplegar soluciones de protección de endpoints (EDR/XDR) capaces de identificar comportamientos de recolección de datos previos a la exfiltración.
- Implementar filtros DNS para bloquear el acceso a dominios maliciosos o sospechosos recientemente registrados.
- Monitorear el tráfico de red saliente para detectar transferencias de datos inusuales hacia servidores externos.
- Aplicar el principio de mínimo privilegio y robustecer la gestión de credenciales corporativas.
- Mantener el sistema operativo y las aplicaciones críticas actualizadas para reducir los vectores de infección inicial.

 ALTA

1.4 Alerta de espionaje sigiloso mediante la puerta trasera "GRIDTIDE".

A inicios de marzo de 2026, las agencias de inteligencia emitieron un reporte detallado sobre el descubrimiento de una sofisticada herramienta de espionaje digital denominada "GRIDTIDE". Este programa malicioso, catalogado como una puerta trasera (backdoor), ha sido utilizado intensamente por el grupo de hackers identificado como UNC2814 para llevar a cabo infiltraciones sumamente silenciosas.

La principal amenaza de este virus radica en su capacidad para establecer un acceso oculto y permanente dentro de las redes corporativas, permitiendo a los atacantes observar las operaciones internas de la empresa durante meses sin ser detectados por los antivirus convencionales.

El objetivo central de esta operación de espionaje es extraer secretos industriales y comerciales de alto valor antes de que los equipos de seguridad informática se percaten de la intrusión.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0003: Persistencia	T1547 – Boot or Logon Autostart Execution	Capacidad de establecer un acceso oculto y permanente dentro de las redes corporativas para mantener la presencia durante meses.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Infiltración silenciosa diseñada para evitar la detección por parte de soluciones de antivirus convencionales.
TA0007: Descubrimiento	T1083 – File and Directory Discovery	Observación continua de las operaciones internas de la empresa para identificar activos y secretos de alto valor.
TA0009: Recolección	T1005 – Data from Local System	Monitoreo de actividades internas para la obtención de secretos industriales y comerciales estratégicos.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Uso de la sofisticada herramienta de espionaje GRIDTIDE para gestionar la comunicación remota del grupo UNC2814.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Extracción de secretos industriales y comerciales de alto valor antes de que los equipos de seguridad detecten la intrusión.

Recomendaciones:

- Establecer un monitoreo continuo de movimiento lateral y uso indebido de credenciales dentro del Active Directory.
- Utilizar soluciones SIEM/EDR avanzadas para identificar la presencia de backdoors persistentes.
- Segmentar estrictamente las redes críticas y restringir el acceso remoto únicamente a usuarios verificados.
- Realizar auditorías periódicas de accesos y permisos para detectar persistencias no autorizadas ocultas.
- Implementar MFA robusta en todas las cuentas de servicio y administrativas de la organización.

MEDIA



1.5 El virus "Silver Dragon" y su espionaje informático en varias etapas.

El 10 de marzo de 2026, especialistas en inteligencia de amenazas documentaron la existencia de un complejo programa informático malicioso bautizado como "Silver Dragon". Este virus se caracteriza por llevar a cabo sus tareas de espionaje encubierto a través de múltiples etapas, lo que significa que el ataque no ocurre de golpe, sino de manera gradual para no levantar sospechas.

Inicialmente, el virus implanta una versión muy ligera en el sistema que apenas consume recursos. Posteriormente, descarga componentes adicionales para rastrear los movimientos del usuario, capturar las pulsaciones de teclado y enviar información confidencial hacia servidores extranjeros.

Este enfoque estructurado permite a los delincuentes garantizar una persistencia a largo plazo en las computadoras de sus víctimas corporativas.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Uso de un programa inicial ligero para ejecutar la primera fase de la infección sin alertar al sistema.
TA0003: Persistencia	T1547 – Boot or Logon Autostart Execution	Implementación de un enfoque estructurado por etapas para asegurar una permanencia a largo plazo en equipos corporativos.
TA0005: Evasión de Defensa	T1027 – Obfuscated Files or Information	Ejecución de tareas de manera gradual y con bajo consumo de recursos para evitar levantar sospechas de los sistemas de seguridad.
TA0007: Descubrimiento	T1016 – System Network Configuration Discovery	Rastreo de los movimientos y actividades del usuario dentro del sistema comprometido.
TA0009: Recolección	T1056.001 – Input Capture: Keylogging	Captura de las pulsaciones de teclado para obtener información confidencial y credenciales.
TA0011: Comando y Control	T1105 – Ingress Tool Transfer	Descarga de componentes adicionales y herramientas de espionaje una vez establecida la conexión inicial.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Envío de la información confidencial recolectada hacia servidores extranjeros controlados por los atacantes.

Recomendaciones:

- Implementar sistemas de detección basados en comportamiento para identificar actividades maliciosas que operan de forma gradual.
- Monitorear el uso de herramientas nativas del sistema (Living off the Land) e intérpretes de comandos sospechosos.
- Adoptar un modelo de Confianza Cero (Zero Trust) para validar de forma continua cada acceso a la red.
- Mantener respaldos aislados y probados para asegurar la recuperación tras periodos de espionaje prolongado.
- Capacitar al personal en la detección de comportamientos anómalos en sus estaciones de trabajo.



1.6 Campaña de virus enfocada en refinerías de petróleo en Libia

A finales de marzo de 2026, un preocupante reporte de seguridad expuso los detalles de una campaña de espionaje cibernético de larga duración que tenía como blanco principal a una refinería de petróleo en Libia.

Los piratas informáticos lograron infiltrar y mantener su presencia dentro de las redes operativas de estas instalaciones críticas, utilizando programas maliciosos altamente especializados en la recolección de datos.

El objetivo de este ataque no fue paralizar la producción de combustible, sino ejecutar un robo silencioso y continuo de información estratégica relacionada con la industria petrolera.

Estas acciones de espionaje industrial demuestran el interés de grupos organizados en comprometer la infraestructura de energía nacional para obtener ventajas económicas y secretos corporativos a nivel internacional.

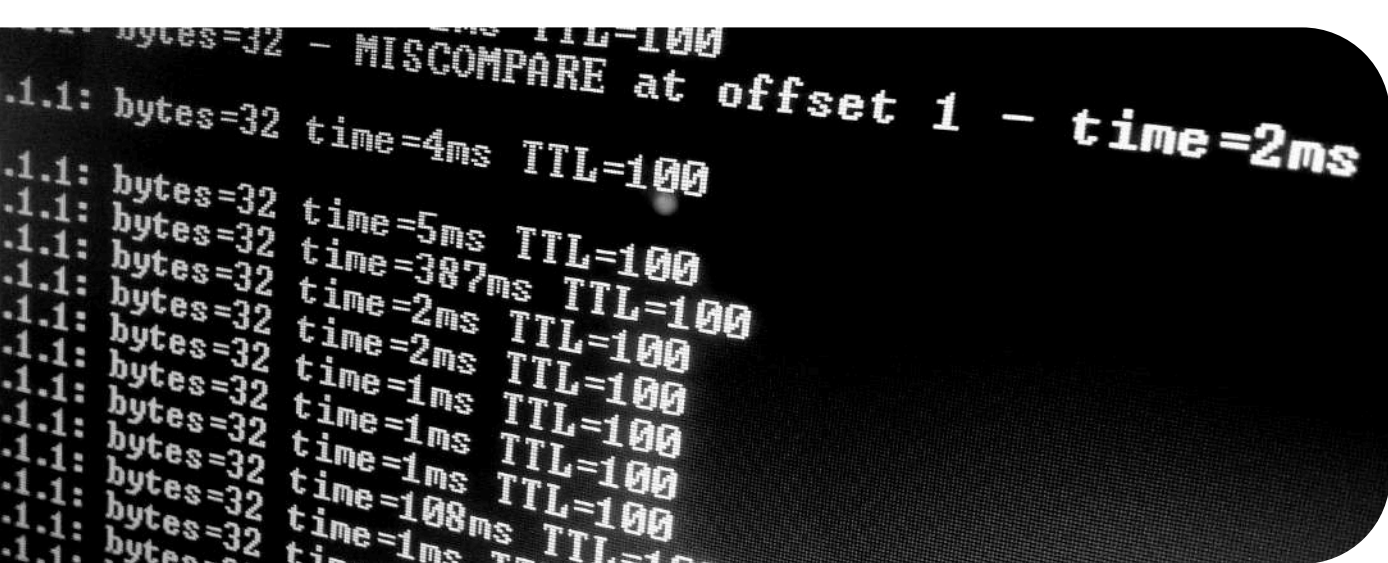
Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Tático	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Infiltración inicial en las redes de la refinería mediante la explotación de servicios o aplicaciones expuestas en la infraestructura de la instalación.
TA0003: Persistencia	T1106 – Native API	Uso de malware especializado para mantener una presencia de larga duración y acceso estable dentro de las redes operativas críticas.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Ejecución de una infiltración sigilosa diseñada para evitar la detección y permitir el espionaje prolongado sin ser advertido.
TA0007: Descubrimiento	T1083 – File and Directory Discovery	Exploración de las redes operativas para identificar y localizar información estratégica y secretos corporativos de la industria petrolera.
TA0009: Recolección	T1005 – Data from Local System	Empleo de programas maliciosos altamente especializados en la recolección de datos estratégicos y documentos industriales.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Establecimiento de canales de comunicación para la gestión remota de la campaña de espionaje y la recepción de instrucciones.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Ejecución de un robo silente y continuo de información estratégica y secretos corporativos hacia servidores externos.

Recomendaciones:

- Segmentar de forma estricta las redes de TI (tecnología de información) y OT (tecnología operativa).
- Desplegar soluciones de detección especializadas para entornos industriales (ICS/SCADA) que identifiquen anomalías en los controladores.
- Aplicar parches de seguridad de forma prioritaria en todos los dispositivos perimetrales y gateways.
- Limitar los accesos bidireccionales entre redes siguiendo el principio de mínimo privilegio.
- Ejecutar ejercicios de respuesta a incidentes específicos para infraestructuras críticas de energía.

● CRÍTICA



1.7 Extracción de 1.3 Terabytes de datos en corporaciones petroleras.

El sector energético sufrió un golpe devastador, el 3 de marzo de 2026, cuando atacantes informáticos lograron vulnerar a la Sharjah National Oil Corporation y a la empresa Israel Opportunity Energy. Utilizando herramientas maliciosas para la extracción de información, los ciberdelincuentes lograron robar más de 1.3 Terabytes de datos sumamente confidenciales.

El paquete de información secuestrada incluye detalles críticos sobre proyectos en desarrollo, contratos petroleros privados y bases de datos financieras exclusivas de ambas corporaciones.

Este masivo robo de información confidencial representa un riesgo incalculable, ya que la publicación de estos contratos y datos financieros en internet puede tener severas consecuencias económicas y políticas en toda la región afectada.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Vulneración de las redes corporativas de Sharjah National Oil Corporation e Israel Opportunity Energy para obtener acceso inicial a sus sistemas.
TA0003: TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Empleo de herramientas maliciosas especializadas para ejecutar procesos de extracción de información dentro de los entornos vulnerados.
TA0007: Descubrimiento	T1083 – File and Directory Discovery	Identificación y localización de proyectos en desarrollo, contratos petroleros privados y bases de datos financieras exclusivas.
TA0009: Recolección	T1005 – Data from Local System	Recopilación de un paquete masivo de información de 1.3 Terabytes con detalles críticos sobre las operaciones de ambas corporaciones.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Uso de canales de comunicación para gestionar las herramientas maliciosas encargadas de la extracción de datos.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Robo y transferencia exitosa de más de 1.3 Terabytes de datos sumamente confidenciales hacia servidores externos controlados por los atacantes.
TA0040: Impacto	T1560 – Archive Collected Data	Generación de un riesgo incalculable con potenciales consecuencias económicas y políticas severas debido a la posible publicación de la información secuestrada.

Recomendaciones:

- Implementar soluciones de Prevención de Pérdida de Datos (DLP) para monitorear el movimiento de información sensible.
- Restringir y auditar el acceso a bases de datos financieras y documentos estratégicos de proyectos.
- Monitorear el tráfico de red en busca de transferencias masivas de datos hacia destinos inusuales.
- Fortalecer la gestión de cuentas privilegiadas (PAM) y monitorear sus actividades de forma continua.
- Mantener copias de seguridad cifradas y fuera de línea para proteger la integridad de los datos ante posibles filtraciones.

 CRÍTICA

2. Vulnerabilidades

2.1 CVE-2026-21536: Agujero de seguridad de máxima gravedad en Microsoft.

Los investigadores publicaron los detalles de la vulnerabilidad CVE-2026-21536, calificada con un nivel de peligro de 9.8 sobre 10, la cual afecta al programa de fijación de precios de dispositivos de Microsoft (Microsoft Devices Pricing Program).

Lo más alarmante es que el ataque no requiere que ningún empleado interactúe con el archivo ni que el pirata tenga contraseñas o permisos especiales, otorgándole el control inmediato del servidor afectado.

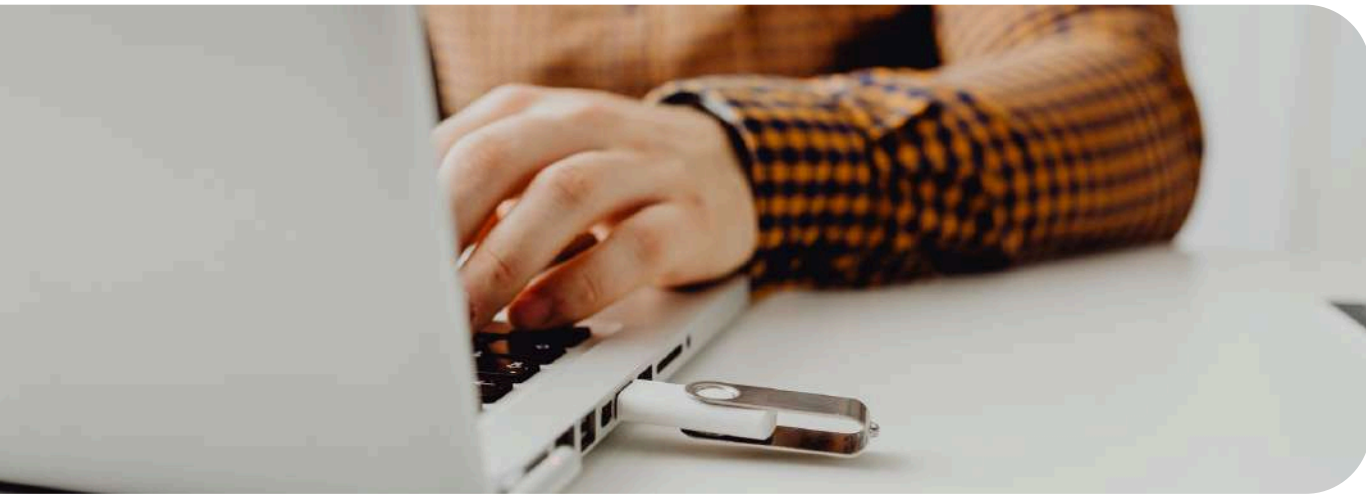
El gravísimo problema radica en que este sistema permite subir archivos desde internet sin comprobar correctamente de qué tipo de archivo se trata. Gracias a esto, un cibercriminal ubicado en cualquier lugar del planeta puede enviar un archivo contaminado y ejecutar códigos maliciosos de manera remota.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Explotación del sistema de carga de archivos en el programa de fijación de precios de dispositivos de Microsoft expuesto a internet.
TA0003: TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Ejecución de códigos maliciosos de manera remota mediante la carga de un archivo contaminado en el servidor.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Omisión de la validación del tipo de archivo y de los mecanismos de control de acceso o permisos especiales del sistema.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Establecimiento de comunicación remota para obtener el control inmediato del servidor sin requerir interacción del usuario.
TA0040: Impacto	T1499 – Endpoint Denial of Service	Compromiso total de la integridad del servidor afectado mediante la ejecución de código no autorizado con privilegios elevados.

Recomendaciones

- Aplicar de forma inmediata los parches oficiales proporcionados por el fabricante.
- Restringir la capacidad de carga de archivos desde fuentes externas no confiables.
- Implementar validaciones de integridad y comprobaciones de firmas para cualquier archivo procesado por el servidor.
- Aislar los servidores afectados en segmentos de red seguros y sin exposición directa a internet.
- Monitorear los registros del sistema en busca de intentos de ejecución de código remoto o inyección de archivos.

 CRÍTICA

2.2 CVE-2026-1731: Falla "Día Cero" en el soporte remoto de BeyondTrust:

Una peligrosa vulnerabilidad identificada como CVE-2026-1731 fue descubierta en el popular programa de asistencia técnica a distancia BeyondTrust Remote Support. Este defecto fue catalogado como una falla de "Día Cero" porque las bandas de ciberdelincuentes comenzaron a utilizarla activamente para lanzar virus de secuestro de datos antes de que existiera una solución disponible.

El error permite que un atacante envíe órdenes maliciosas a la red corporativa sin necesidad de introducir un nombre de usuario ni una contraseña.

Debido a que los delincuentes estaban infectando rápidamente las redes de las empresas que confían en esta herramienta, la agencia gubernamental de ciberseguridad CISA emitió una orden de emergencia obligando a instalar el parche correctivo en un plazo máximo de tres días.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Explotación del software BeyondTrust Remote Support expuesto para obtener acceso inicial a la red corporativa.
TA0003: TA0002: Ejecución	T1059 – Command and Scripting Interpreter	Envío de órdenes maliciosas a la infraestructura interna aprovechando el error de seguridad del programa.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Evasión de controles de seguridad al permitir la intrusión sin requerir el ingreso de nombre de usuario ni contraseña.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Establecimiento de comunicación remota maliciosa utilizando la propia herramienta de asistencia técnica como canal.
TA0040: Impacto	T1486 – Data Encrypted for Impact	Despliegue de ransomware para comprometer la disponibilidad e integridad de la información en las redes afectadas.

Recomendaciones:

- Instalar el parche correctivo de emergencia en el plazo perentorio de tres días establecido por CISA.
- Restringir el uso de herramientas de acceso remoto no autorizadas mediante políticas de control de aplicaciones.
- Monitorear estrechamente las sesiones de soporte remoto y alertar ante comportamientos no aprobados.
- Validar el uso de herramientas de asistencia técnica mediante autenticación multifactor (MFA).
- Ejecutar escaneos de integridad para detectar ejecutables no firmados o cambios anómalos en los servicios.

 CRÍTICA

2.3 CVE-2026-3055: Falla crítica por exposición de memoria del sistema.

A finales de marzo de 2026, los equipos de ciberseguridad tuvieron que priorizar la corrección del defecto técnico CVE-2026-3055, clasificado con nivel crítico y considerado de muy alto riesgo.

Esta falla ocurre cuando el sistema lee áreas de la memoria de la computadora que no debería poder ver, exponiendo accidentalmente información íntima de la máquina.

Al explotar esta ventana abierta, un atacante puede robar claves de seguridad secretas y obtener acceso a componentes vitales de la aplicación afectada. Este tipo de exposición de memoria suele ser el primer paso que utilizan los piratas informáticos para ejecutar ataques mucho más complejos que terminan en el control remoto total del equipo, siendo muy difíciles de detectar sin herramientas de monitoreo avanzado.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Explotación del defecto técnico crítico CVE-2026-3055 en aplicaciones vulnerables para iniciar la intrusión.
TA0007: Descubrimiento	T1082 – System Information Discovery	Lectura no autorizada de áreas de la memoria de la computadora para exponer información íntima y configuraciones de la máquina.
TA0006: Acceso a Credenciales	T1555 – Credentials from Password Stores	Robo de claves de seguridad secretas mediante la explotación de la ventana de memoria abierta.
TA0004: Escalada de Privilegios	T1068 – Exploitation for Privilege Escalation	Obtención de acceso no autorizado a componentes vitales de la aplicación afectada aprovechando la falla de memoria.
TA0011: Comando y Control	T1219 – Remote Access Software	Uso del compromiso inicial como primer paso para establecer el control remoto total del equipo afectado.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Ejecución de ataques complejos diseñados para ser difíciles de detectar sin el uso de herramientas de monitoreo avanzado.

Recomendaciones

- Priorizar la aplicación de las actualizaciones de seguridad para corregir el defecto técnico de lectura de memoria.
- Utilizar soluciones EDR/XDR capaces de detectar el acceso a áreas de memoria fuera de los límites permitidos.
- Segmentar entornos críticos para evitar que una falla de memoria local facilite el movimiento lateral.
- Aplicar el principio de mínimo privilegio para restringir el acceso de las aplicaciones a recursos sensibles del sistema.
- Implementar controles de integridad que impidan la carga de componentes no autorizados en el kernel o la memoria.

 ALTA

3 . Phishing

3.1 Plataforma cibercriminal logró evadir los sistemas de Autenticación de Múltiples Factores a escala global.

El sofisticado servicio de fraudes conocido como Tycoon 2FA orquestó campañas de engaño masivo que enviaron correos fraudulentos, enlaces maliciosos e incluso códigos QR falsos a millones de usuarios. Esta plataforma introdujo un nivel de peligro extraordinario al utilizar la técnica de "adversario en el medio" (AiTM), la cual crea una página falsa idéntica a la original que intercepta en vivo la conexión de la víctima.

Gracias a este método avanzado, los criminales lograron robar no solo las contraseñas, sino que también capturaron los códigos numéricos de seguridad que llegan al teléfono móvil de los usuarios. Los reportes demostraron que en el 59% de las cuentas vulneradas con éxito, las víctimas tenían activadas todas las protecciones de autenticación de doble factor, lo cual afectó a escuelas, hospitales y agencias gubernamentales.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566 – Phishing	Orquestación de campañas de engaño masivo mediante el envío de correos fraudulentos, enlaces maliciosos y códigos QR falsos.
TA0007: TA0002: Ejecución	T1204 – User Execution	Los usuarios interactúan con los elementos maliciosos (clics en enlaces o escaneo de QR), iniciando la conexión con la infraestructura del atacante.
TA0006: Acceso a Credenciales	T1557.001 – Adversary-in-the-Middle	Uso de la técnica AiTM para crear una página falsa idéntica a la original que intercepta en vivo la sesión de la víctima.
TA0006: Acceso a Credenciales	T1056 – Input Capture	Captura de contraseñas y códigos numéricos de seguridad (OTP/MFA) que llegan al dispositivo móvil del usuario durante el proceso de autenticación.
TA0005: Evasión de Defensa	T1553 – Subvert Trust Controls	Elusión de los sistemas de autenticación de múltiples factores (MFA), logrando comprometer el 59% de las cuentas atacadas exitosamente.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Establecimiento de un canal de comunicación para retransmitir la conexión entre la víctima y el sitio auténtico de manera transparente.

Recomendaciones

- Implementar claves de seguridad físicas (FIDO2) como método de autenticación resistente a técnicas de interceptación.
- Monitorear anomalías en los tokens de sesión y detectar cambios repentinos de ubicación geográfica o dirección IP.
- Usar gateways de correo con análisis en tiempo real para bloquear redirecciones hacia portales clonados.
- Aplicar políticas de acceso condicional que revaliden la identidad ante comportamientos sospechosos.
- Capacitar a los usuarios sobre las técnicas de "adversario en el medio" y la importancia de verificar la URL del sitio.



3.2 Estafas financieras en Medio Oriente imitan marcas empresariales

Los expertos en seguridad reportaron una agresiva ola de ataques de correo electrónico falso (phishing) dirigida estratégicamente contra empresas líderes y organizaciones comerciales en Arabia Saudita durante el mes de marzo de 2026.

Los atacantes implementaron una estrategia dual sumamente refinada: por un lado, enviaban correos altamente personalizados a los empleados, falsificando de manera idéntica los logotipos y el formato visual de los sistemas de contabilidad y recursos humanos (ERP) más famosos del mercado.

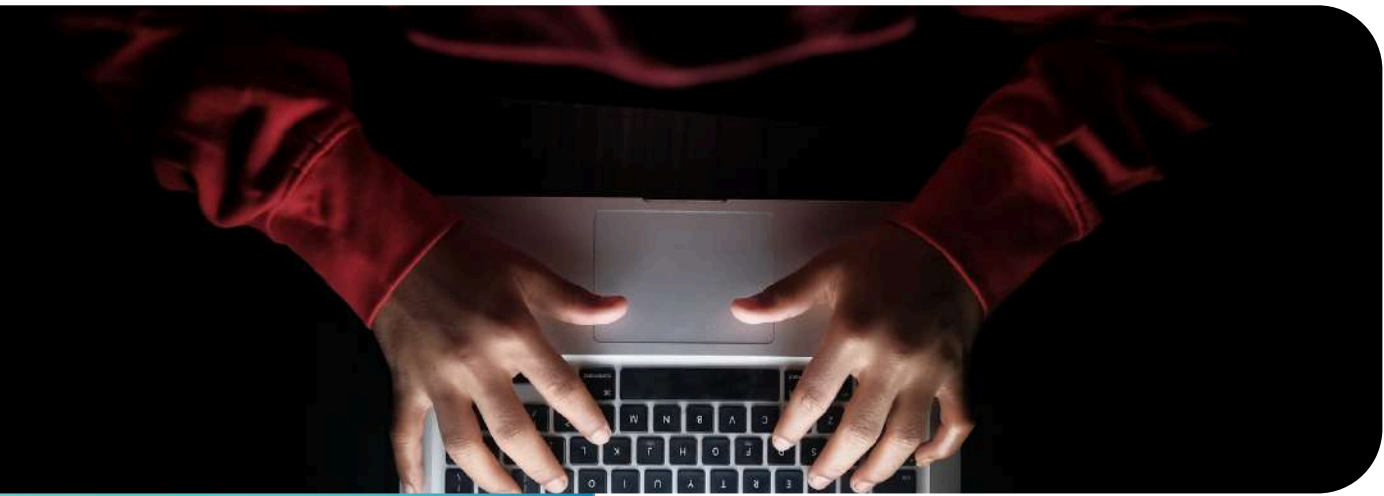
Por otro lado, utilizaban estas identidades corporativas falsas para engañar a los trabajadores y manipularlos psicológicamente. El objetivo final de estos engaños perfectos no era instalar un virus, sino ejecutar fraudes financieros a gran escala, convenciendo al personal de finanzas de que realizaran grandes transferencias de dinero a las cuentas de los delincuentes.

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

Táctica	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1566.002 – Phishing: Spearphishing Link	Envío de correos altamente personalizados a empleados, falsificando logotipos y formatos visuales de sistemas ERP conocidos para dirigir a las víctimas hacia portales falsos.
TA0043: Reconocimiento (Ingeniería Social)	T1566 – Phishing	Uso de identidades corporativas falsas para manipular psicológicamente a los trabajadores y ganar su confianza mediante una estrategia dual refinada.
TA0002: Ejecución	T1204 – User Execution	Interacción del personal de finanzas con el contenido fraudulento, motivada por la apariencia legítima y profesional de los mensajes.
TA0005: Evasión de Defensa	T1036 – Masquerading	Suplantación de la identidad visual y del formato de sistemas de contabilidad y recursos humanos famosos para evitar sospechas y detecciones.
TA0040: Impacto	T1496 – Robo Financiero (Contextual)	Ejecución de fraudes financieros a gran escala mediante la transferencia de grandes sumas de dinero a cuentas controladas por los criminales.

Recomendaciones

- Establecer canales de verificación fuera de banda (out-of-band) antes de autorizar transferencias financieras de alto valor.
- Capacitar específicamente al personal de finanzas y recursos humanos sobre tácticas de phishing asistido por IA.
- Activar alertas de transacciones en tiempo real y establecer límites preventivos en cuentas corporativas.
- Implementar filtros avanzados que realicen sandboxing de archivos adjuntos sospechosos antes de que lleguen al usuario final.
- Monitorear la aparición de dominios similares a los corporativos que puedan ser usados para suplantación de identidad.

 CRÍTICA

4. Adversarios

4.1 El grupo "APT Iran" ataca ferozmente a Lockheed Martin:

El 23 de marzo de 2026, el mundo de la defensa aeroespacial entró en alerta máxima luego de que la organización ciberactivista denominada "APT Iran" anunciara haber vulnerado las redes informáticas del gigante militar Lockheed Martin.

Este agresivo grupo de hackers, que cuenta con antecedentes previos de ataques contra infraestructuras en Jordania, se caracteriza por utilizar la aplicación de mensajería Telegram para amenazar a sus víctimas y exigir enormes rescates económicos.

En este incidente de proporciones colosales, los delincuentes cibernéticos afirmaron haber extraído y robado 375 Terabytes de información confidencial. Según sus propias declaraciones públicas, los datos secuestrados contienen documentos corporativos clasificados y planos técnicos extremadamente secretos de los modernos aviones de combate F-35, representando una amenaza crítica a la seguridad nacional.

Objetivos principales:

- **Infiltración de Redes de Alta Seguridad:** Vulnerar los sistemas informáticos de una de las corporaciones militares más importantes del mundo.
- **Extorsión y Rescate Económico:** Utilizar plataformas como Telegram para lanzar amenazas directas y exigir pagos millonarios a cambio de no filtrar la información.
- **Exfiltración Masiva de Propiedad Intelectual:** Robar un volumen colosal de datos (375 Terabytes) para obtener ventajas tecnológicas o políticas.
- **Espionaje Militar Estratégico:** Obtener planos técnicos secretos de armamento avanzado, específicamente de los aviones de combate F-35.
- **Desestabilización de la Seguridad Nacional:** Comprometer documentos clasificados que ponen en riesgo la integridad de la defensa de un país.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Vulneración de las redes informáticas del gigante militar Lockheed Martin para obtener acceso inicial a su infraestructura.
TA0009: Recolección	T1005 – Data from Local System	Identificación y recopilación de 375 Terabytes de información confidencial, incluyendo documentos corporativos y planos técnicos del F-35.
TA0011: Comando y Control	T1102.002 – Web Service: Bidirectional Communication	Uso de la aplicación de mensajería Telegram para la comunicación con las víctimas, emisión de amenazas y exigencia de rescates económicos.
TA0010: Exfiltración	T1041 – Exfiltration Over C2 Channel	Extracción masiva de datos secuestrados, que incluyen planos técnicos extremadamente secretos, hacia servidores externos controlados por el grupo.
TA0040: Impacto	T1496 – Data Destruction / Exfiltration Impact	Generación de una amenaza crítica a la seguridad nacional mediante el robo y potencial publicación de tecnología de defensa de última generación.

Recomendaciones:

- Gestionar y aplicar parches de forma prioritaria en todos los dispositivos perimetrales y de borde expuestos.
- Segmentar estrictamente las redes de defensa y proteger los activos estratégicos en entornos aislados.
- Realizar Threat Hunting (cacería de amenazas) proactivo para identificar intrusiones de largo plazo de actores estatales.
- Mantener copias de seguridad inmutables y fuera de línea para proteger la propiedad intelectual estratégica.
- Implementar autenticación multifactor robusta en todos los puntos de acceso a información clasificada.

 ALTA

4.2 Espías de Seedworm infiltran infraestructura crítica en EE. UU.

Las agencias de inteligencia cibernética lograron rastrear e identificar la prolongada presencia oculta del grupo de espionaje iraní conocido como "Seedworm" (también llamado MuddyWater o Static Kitten) dentro de las redes corporativas de Estados Unidos. Las actividades invasivas de estos piratas informáticos comenzaron a registrarse desde febrero de 2026 y han continuado de manera ininterrumpida a lo largo del mes de marzo, coincidiendo con la reciente escalada del conflicto militar internacional.

Las agencias de inteligencia cibernética lograron rastrear e identificar la prolongada presencia oculta del grupo de espionaje iraní conocido como "Seedworm" (también llamado MuddyWater o Static Kitten) dentro de las redes corporativas de Estados Unidos. Las actividades invasivas de estos piratas informáticos comenzaron a registrarse desde febrero de 2026 y han continuado de manera ininterrumpida a lo largo del mes de marzo, coincidiendo con la reciente escalada del conflicto militar internacional.

Objetivos principales:

- **Establecimiento de Presencia Persistente:** Lograr una infiltración prolongada y oculta dentro de las redes corporativas para operar sin ser detectados.
- **Alineación con Conflictos Geopolíticos:** Realizar actividades invasivas coordinadas con la escalada de tensiones militares internacionales.
- **Control de Sistemas de Comunicación Financiera:** Penetrar en los sistemas de un banco estadounidense importante para monitorear o interrumpir flujos de información.
- **Vigilancia de Redes de Transporte:** Acceder a las redes operativas de aeropuertos nacionales para obtener datos logísticos o de movimiento.
- **Capacidad de Sabotaje:** Posicionarse técnicamente para realizar actos de sabotaje en infraestructuras críticas que afecten la vida cotidiana de la sociedad.
- **Espionaje en el Sector Tecnológico:** Comprometer sucursales de empresas de software internacionales para expandir su alcance de espionaje.

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

Táctico	Técnicas / Subtécnicas	Procedimientos
TA0001: Acceso Inicial	T1190 – Exploit Public-Facing Application	Penetración de las redes corporativas de un banco estadounidense, un aeropuerto nacional y sucursales de una compañía de software.
TA0003: Persistencia	T1106 – Native API	Mantenimiento de una presencia oculta y prolongada dentro de las redes infiltradas de manera ininterrumpida desde febrero de 2026.
TA0005: Evasión de Defensa	T1562 – Impair Defenses	Ejecución de actividades invasivas diseñadas para mantenerse ocultos en los sistemas de comunicaciones y redes de operación sin ser detectados.
TA0007: Descubrimiento	T1083 – File and Directory Discovery	Identificación y reconocimiento de los sistemas de comunicaciones y redes de operación de infraestructuras críticas.
TA0009: Recolección	T1005 – Data from Local System	Uso de una altísima capacidad técnica para realizar labores de espionaje sobre información estratégica de los sectores afectados.
TA0011: Comando y Control	T1071 – Application Layer Protocol	Empleo de infraestructura de mando para coordinar el espionaje y las capacidades de sabotaje de forma remota.
TA0040: Impacto	T1496 – Resource Hijacking / Sabotaje (Contextual)	Demostración de capacidad técnica para sabotear infraestructuras críticas nacionales mediante el control de sus redes de operación.

Recomendaciones

- Implementar autenticación multifactor robusta en todas las cuentas administrativas y de servicio.
- Monitorear el tráfico de red saliente en busca de comunicaciones hacia infraestructuras de comando y control (C2).
- Segmentar las redes de operación de infraestructuras críticas para limitar el alcance de las infiltraciones.
- Activar alertas ante comportamientos anómalos detectados por herramientas de monitoreo SIEM/EDR.
- Realizar auditorías periódicas de accesos y permisos para identificar cuentas comprometidas o persistencias ocultas.

5. Indicadores de Compromiso

5.1 Direcciones IP

92[.]118[.]39[.]205
 141[.]98[.]10[.]108
 36[.]25[.]240[.]114
 140[.]245[.]47[.]69
 103[.]164[.]9[.]74
 64[.]227[.]15[.]74
 101[.]36[.]228[.]201
 65[.]49[.]1[.]129
 176[.]120[.]22[.]13
 2[.]57[.]121[.]86
 85[.]217[.]140[.]45

5.2 Dominio

- mediareleaseupdates[.]com
- carpmaxxbait[.]online
- grouperwadeseconomy[.]com
- cat-watches-site[.]xyz
- symantecsecuritycloud[.]com
- secssl[.]com
- alace5[.]com
- wellfitplan[.]ru
- galaxyswapper[.]pro
- lionsdenim[.]xyz
- upload-microsoft[.]com

5.3 Hashes

ca44ae42f5b2e789ddfd0881a97b388813
 561b3669d50bc86600602d57dc235d

 d506e1c84b50a0cdce0df35770da913f30
 ca36474075971a0f3944e595858fcl

 b8dfbc57349d1e4a0067f1bd6e5cb778b5
 98aa81190dd08cd344e77129804848

 abf546e4fea6a7e84bc66d85aa958f2cd
 42986e267837618506349d86e80de64

 938e9963d63e540a3f8922d74158996e4
 9281a7288a1bb5b4dc80da6ce6f0a48

 4f78db54f05ff4472874276da3c01833bf12
 70f90belaec4c8794545faf0874

 2c651833512a0dba3213a82bf3cfd847cf71
 bab288bbef8c8d207f8cba86c3c2

 841d03961672ef7e2a6eb1bacbe64c32ed
 bbe687d0f6ece48dc160f5473b213a

 226a723ffb4a91d9950a8b266167c5b354
 ab0db1dc225578494917fe53867ef2

 178ba564b39bd07577e974a9b677dfd86
 ffa1fld0299dfd958eb883c5ef6c3e1

 e2a24ab94f865caeacdf2c3ad015f31f23
 008ac6db8312c2cbfb32e4a5466ea2

6. Fuentes

- 6.1 <https://orthospinenews.com/2026/03/27/customer-updates-stryker-network-disruption/>
- 6.2 https://www.nwcmss.org/assets/1/news/2026-03-16_Stryker_Customer_Certification_Letter.pdf
- 6.3 <https://www.hornetsecurity.com/en/blog/monthly-threat-report/>
- 6.4 <https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/>
- 6.5 <https://www.penligent.ai/hackinglabs/es/stryker-hacked-what-the-march-2026-attack-reveals-about-medical-device-security/>
- 6.6 <https://www.upguard.com/news/lockheed-martin-data-breach-2026-03-24>
- 6.7 <https://hackread.com/dark-web-market-375tb-lockheed-martin-data/>
- 6.8 <https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-march-2026/>
- 6.9 <https://ine.com/blog/march-2026-cve-round-up-critical-and-network-vulnerabilities>
- 6.10 <https://www.hornetsecurity.com/en/blog/monthly-threat-report/>
- 6.11 <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4229506/nsa-cisa-fbi-and-dc3-warn-iranian-cy...>
- 6.12 <https://www.cloudsek.com/blog/middle-east-escalation-israel-iran-us-cyber-war-2026>
- 6.13 <https://www.euronews.com/next/2026/03/18/how-cyberattacks-are-being-used-as-weapons-in-the-iran-war>
- 6.14 <https://www.immersivelabs.com/resources/blog/defending-the-digital-front-line-cyber-readiness-in-a-period-of-high-intensity-risk>