Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ Instituto Nacional de Ciberseguridad

TBQ Técnicas Básicas iBERSEGURIDAD Quantum

Diego Domínguez Martínez
presenta el resumen del trabajo

Informe sobre ciberataques a empresas en la Unión Europea

10 de marzo de 2025

SERIE DE RESÚMENES EN ESPAÑOL

Palabras clave: Ataques de día cero, Ataques dirigidos, puerta trasera (backdoor), ciberseguridad, cadena de suministro, ejecución remota de código (RCE), GDPR, Hackers, Inteligencia Artificial, ofuscación, phising, ransomware.

Introducción

Este informe analiza en profundidad varios ciberataques recientes de gran relevancia, centrándose especialmente en aquellos que han tenido impacto en la Unión Europea. En ellos se analizan las vulnerabilidades aprovechadas por los ciberdelincuentes para infiltrarse así como los parches y medidas de seguridad adoptados por las empresas. Además de examinar incidentes significativos y sus consecuencias, se abordará cómo las empresas manejan y protegen los datos personales de los ciudadanos en cumplimiento de regulaciones como el GDPR.

Kaseya VSA

Un Caso de Ransomware a Gran Escala

El ataque dirigido a Kaseya VSA en julio de 2021 fue uno de los incidentes de ransomware más sofisticados y dañinos de los últimos años. Kaseya es una empresa de software que proporciona soluciones de administración remota y automatización a proveedores de servicios gestionados (MSP), como la gestión de dispositivos de forma centralizada.

El ataque fue llevado a cabo por el grupo de ciberdelincuentes REvil, una organización de **ransomware-as-a-service** (RaaS) con vínculos a Rusia. Según el informe técnico publicado por CISA y Sophos, los atacantes utilizaron una **vulnerabilidad de día cero** en la autenticación del servidor Kaseya VSA, lo que les permitió ejecutar código malicioso sin necesidad de credenciales válidas [1, 2].

Una vez dentro, se desplegó el ransomware en todos los sistemas conectados aprovechándose de la infraestructura centralizada de VSA. Afectó a más de 1.500 empresas en todo el mundo, incluyendo tiendas minoristas, colegios, bancos y entidades gubernamentales debido a la naturaleza de la cadena de suministro digital.

La respuesta de Kaseya incluyó la desconexión inmediata de los servidores VSA afectados y la colaboración con **agencias de ciberseguridad como FBI y CISA** para contener el ataque [2]. Eventualmente, las autoridades estadounidenses lograron recuperar una clave de descifrado universal, permitiendo a muchas empresas restaurar sus datos sin pagar el rescate. Sin embargo, el incidente puso en evidencia la fragilidad de las infraestructuras de administración remota y la creciente tendencia de los cibercriminales a atacar proveedores de servicios para maximizar el daño.

MOVEit Transfer

Explotación de una Vulnerabilidad Crítica en la Transferencia de Datos

El ataque contra MOVEit Transfer en 2023 representó una de las mayores brechas de seguridad relacionadas con la **exfiltración masiva de datos**. MOVEit Transfer, desarrollado por la empresa Progress Software, es una solución ampliamente utilizada para la transferencia segura de archivos entre empresas, instituciones financieras y organismos gubernamentales. Su diseño tiene como objetivo proteger la información crítica mediante cifrado, autenticación avanzada y auditorías de acceso. Sin embargo, en mayo de 2023, investigadores de ciberseguridad descubrieron que atacantes habían explotado una vulnerabilidad de **inyección SQL** previamente desconocida, permitiéndoles comprometer servidores que utilizaban este software.

El grupo de ciberdelincuentes Cl0p, con presuntos vínculos en Rusia, se atribuyó el ataque. Utilizaron la vulnerabilidad CVE-2023-34362 para ejecutar comandos SQL maliciosos en los servidores afectados sin necesidad de credenciales legítimas. Según informes publicados por Progress Software y Akamai Security Intelligence Group [3, 4], los atacantes automatizaron el proceso de explotación, lo que les permitió comprometer múltiples organizaciones de forma simultánea. Entre las víctimas se encontraban gobiernos, bancos, universidades y grandes corporaciones, por lo que se expusieron datos personales de millones de personas.

En lugar de desplegar ransomware como en ataques tradicionales, los atacantes optaron por un modelo de extorsión basado en la filtración de datos, amenazando con hacer públicos los archivos robados si las víctimas no pagaban un rescate.

La respuesta de Progress Software incluyó la publicación de parches de seguridad urgentes y recomendaciones para que las empresas revisaran sus sistemas en busca de accesos no autorizados [5].

3CX

Compromiso de la Cadena de Suministro

3CX, una empresa con sede en Chipre, es conocida por su software de telefonía basado en VoIP (Voice over IP), que permite a las organizaciones gestionar llamadas, conferencias y sistemas de atención al cliente de manera eficiente. En 2023 sufrió un ataque a su cadena de suministro, afectando así a su aplicación 3CX Desktop App.

El ataque fue atribuido a un grupo de amenazas persistentes avanzadas (APT) con vínculos a Corea del Norte, identificado por Mandiant [6] y Microsoft Threat Intelligence como UNC4736. Los atacantes lograron comprometer la cadena de suministro de 3CX inyectando un ejecutable troyanizado en las versiones legítimas del software. Según un análisis de The Hacker News [7], la infección se originó en una dependencia de software utilizada en el proceso de compilación, haciendo que la versión oficial de la aplicación se convirtiera en un vector de ataque.

Una vez instalado, el software malicioso desplegó un malware de robo de información, diseñado para recolectar credenciales almacenadas en navegadores web como Google Chrome, Microsoft Edge y Mozilla Firefox. Posteriormente, los atacantes utilizaron estas credenciales para acceder a información confidencial y filtrar datos críticos.

Empresas del sector financiero, tecnológico y gubernamental se vieron comprometidas al ejecutar una versión aparentemente legítima del software. La respuesta de 3CX incluyó la retirada de la versión comprometida de su aplicación, la recomendación a los clientes de desinstalar el software afectado y la colaboración con firmas de ciberseguridad para mitigar el impacto del incidente.

Este incidente reforzó la necesidad de mejorar la seguridad en la cadena de suministro, promoviendo prácticas como la firma digital de código, auditorías de seguridad en el proceso de desarrollo y la implementación de herramientas de detección de amenazas avanzadas para prevenir ataques similares en el futuro.

Microsoft Exchange
Por Hafnium (2021)

El ataque a Microsoft Exchange en 2021 fue ejecutado por el grupo de amenazas conocido como Hafnium, una entidad con vínculos con China, según informes de Microsoft [8]. Este incidente expuso una serie de vulnerabilidades críticas en los servidores de Exchange, permitiendo que los atacantes accedieran de forma remota a los sistemas afectados y extrajeran información sensible. Las organizaciones más afectadas fueron empresas del sector tecnológico, contratistas de defensa, instituciones de investigación y entidades gubernamentales en Estados Unidos y Europa.

Las vulnerabilidades explotadas por Hafnium consistían en fallos de seguridad de día cero en los servidores locales de Microsoft Exchange, concretamente, las identificadas como CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 y CVE-2021-27065. La primera vulnerabilidad, CVE-2021-26855, permitía a los atacantes autenticarse como el servidor Exchange sin necesidad de credenciales, utilizando solicitudes de acceso falsificadas. Una vez dentro, empleaban CVE-2021-26857, que permitía la ejecución remota de código con privilegios de SYSTEM en el servidor comprometido. Posteriormente, las otras dos vulnerabilidades, CVE-2021-26858 y CVE-2021-27065, se usaban para escribir archivos arbitrarios en el sistema y obtener un control total sobre el servidor.

El vector de ataque comenzó con el escaneo masivo de servidores Exchange vulnerables expuestos a internet. Una vez identificado un servidor susceptible, los atacantes enviaban una solicitud especialmente diseñada para explotar CVE-2021-26855, logrando acceso inicial. Luego, desplegaban un web shell, una herramienta maliciosa que permitía a Hafnium ejecutar comandos arbitrarios en los sistemas comprometidos y mantener acceso persistente. Este web shell, generalmente alojado en rutas accesibles de los servidores web de Exchange, facilitaba el control remoto incluso después de que la vulnerabilidad inicial fuera parcheada.

Entre las acciones llevadas a cabo por los atacantes una vez dentro del sistema, se identificó la exfiltración masiva de correos electrónicos y documentos almacenados en los servidores Exchange. Utilizaron herramientas como PowerShell y frameworks de código abierto como China Chopper, un web shell ampliamente usado por actores de amenazas chinos. Además, en algunos casos, instalaron backdoors para asegurar su presencia en los sistemas, lo que aumentó el impacto a largo plazo del ataque.

El impacto del incidente fue significativo y afectó a miles de organizaciones en todo el mundo. Microsoft y varias firmas de ciberseguridad, como Volexity y FireEye (actualmente Mandiant), detectaron que los atacantes habían comprometido múltiples sectores, incluyendo sanidad, defensa y organismos gubernamentales. Se estima que más de 30,000 organizaciones en Estados Unidos y 60,000 a nivel global fueron víctimas del ataque antes de que se lanzaran los parches de seguridad.

A medida que se hacía pública la explotación de estas vulnerabilidades, otros grupos de amenazas comenzaron a replicar el ataque, ampliando la superficie de riesgo y obligando a las empresas a reaccionar rápidamente. Microsoft lanzó parches de emergencia y trabajó con agencias de seguridad como CISA y la Agencia de Seguridad Nacional (NSA) para mitigar el impacto. Además, el FBI intervino directamente en la eliminación de web shells de servidores Exchange comprometidos en Estados Unidos, una acción inusual pero justificada por la magnitud del incidente [9].

Para mitigar futuras amenazas similares, Microsoft implementó cambios en su enfoque de seguridad para Exchange, promoviendo la migración a su plataforma en la nube y reforzando las prácticas de detección temprana. También se recomendó a las organizaciones reforzar sus controles de seguridad, aplicar segmentación de redes y monitorear constantemente la actividad en sus servidores Exchange.

Referencias

[1] Sophos Group. *Ataque de ransomware de la cadena de suministro de Kaseya VSA*. Sophos, 5 de julio de 2021. Recuperado de: https://news.sophos.com/es-419/2021/07/05/ataque-de-ransomware-de-la-cadena-de-suministro-de-kaseya-vsa/.

[2] CISA (Cybersecurity and Infrastructure Security Agency) y FBI (Federal Bureau of Investigation). *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*. CISA, 1 de julio de 2021. Recuperado de: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a.

[3] Progress Software. *MOVEit Transfer and MOVEit Cloud Vulnerability*. Progress Software, 5 de julio de 2023. Recuperado de: https://www.progress.com/trust-center/moveit-transfer-and-moveit-cloud-vulnerability.

[4] Akamai Security Intelligence Group. *El grupo de ransomware CL0P aprovecha la vulnerabilidad de día cero SQLi de MOVEit (CVE-2023-34362)*. Akamai, 8 de junio de 2023. Recuperado de: https://www.akamai.com/es/blog/security-research/moveit-sqli-zero-day-exploit-clop-ransomware.

[5] Progress Software. *MOVEit Transfer Product Security Alert Bulletin – June 2024 (CVE-2024-5806)*. Recuperado de: https://community.progress.com/s/article/MOVEit-Transfer-Product-Security-Alert-Bulletin-June-2024-CVE-2024-5806

[6] Mandiant. *3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible*. 21 de abril de 2023. Recuperado de: https://cloud.google.com/blog/topics/threat-intelligence/3cx-software-supply-chain-compromise.

[7] The Hacker News. *3CX Supply Chain Attack — Here's What We Know So Far*. 31 de marzo de 2023. Recuperado de: https://thehackernews.com/2023/03/3cx-supply-chain-attack-heres-what-we.html.

[8] Microsoft. *Hafnium Targeting Exchange Servers*. Microsoft Security Blog, 2 de marzo de 2021. Recuperado de: https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

[9] Cybersecurity and Infrastructure Security Agency (CISA). *Alert (AA21-062A): Hafnium Exploitation of Microsoft Exchange Server Vulnerabilities*. CISA, 11 de marzo de 2021. Recuperado de: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-062a.