Una vulnerabilidad de seguridad ya corregida en Google Chrome fue explotada como un zero-day por un actor de amenazas identificado como TaxOff, con el objetivo de instalar una puerta trasera con el nombre en clave Trinper.

El ataque, detectado a mediados de marzo de 2025 por Positive Technologies, implicó el uso de una vulnerabilidad de escape de sandbox registrada como CVE-2025-2783 (puntaje CVSS: 8.3).

Google solucionó la falla más adelante ese mismo mes, luego de que Kaspersky reportara su explotación activa en una campaña bautizada como Operación ForumTroll, que tenía como blanco a diversas organizaciones rusas.

> *«El vector inicial del ataque fue un correo electrónico de phishing que contenía un enlace malicioso. Cuando la víctima hacía clic en el enlace, se activaba un exploit de un solo clic (CVE-2025-2783), lo que llevaba a la instalación de la puerta trasera Trinper utilizada por TaxOff»,* explicaron los investigadores en seguridad Stanislav Pyzhov y Vladislav Lunin.

Se indica que el correo de phishing simulaba ser una invitación al foro Lecturas Primakov, el mismo señuelo descrito por Kaspersky, instando a los usuarios a hacer clic en un enlace que dirigía a un sitio web falso que alojaba el exploit.

TaxOff es el nombre asignado a un grupo de hackers identificado por primera vez por la firma rusa de ciberseguridad a finales de noviembre de 2024, el cual atacaba agencias gubernamentales locales mediante correos fraudulentos relacionados con temas legales y financieros para distribuir Trinper.

Escrita en C++, la puerta trasera utiliza multihilo para recolectar información del sistema comprometido, registrar pulsaciones de teclas, buscar archivos con extensiones específicas (.doc, .xls, .ppt, .rtf y .pdf), y establecer conexión con un servidor remoto desde el que recibe instrucciones y al que exfiltra los resultados.

Las instrucciones enviadas desde el servidor C2 amplían las capacidades del implante, permitiéndole leer y escribir archivos, ejecutar comandos mediante `cmd.exe`, lanzar una shell inversa, cambiar de directorio e incluso autodesactivarse.

> *«El uso de múltiples hilos proporciona un alto grado de paralelismo, lo que ayuda a ocultar la puerta trasera mientras conserva la capacidad de recolectar y extraer datos, instalar módulos adicionales y mantener la comunicación con el C2*«, señaló Lunin en ese momento.

Positive Technologies afirmó que su análisis del ataque de marzo de 2025 llevó al descubrimiento de otra intrusión ocurrida en octubre de 2024, la cual también comenzó con un correo de phishing, esta vez disfrazado de invitación a una conferencia internacional titulada 'Seguridad del Estado de la Unión en el mundo moderno'.

Ese correo contenía un enlace que descargaba un archivo ZIP, el cual incluía un acceso directo de Windows que a su vez ejecutaba un comando PowerShell, con el fin de mostrar un documento señuelo y desplegar un loader encargado de lanzar la puerta trasera Trinper mediante el cargador de código abierto Donut. Se detectó una variante de este ataque que sustituía Donut por Cobalt Strike.

Según la compañía, esta cadena de ataque comparte varias tácticas similares con las empleadas por otro grupo de amenazas conocido como Team46, lo que sugiere la posibilidad de que ambas agrupaciones sean en realidad la misma.

Curiosamente, otro conjunto de correos maliciosos enviados por Team46 un mes antes afirmaba provenir de la operadora de telecomunicaciones moscovita Rostelecom, advirtiendo a los destinatarios sobre supuestas interrupciones por mantenimiento ocurridas el año anterior.

Estos mensajes incluían un archivo ZIP que contenía un acceso directo capaz de ejecutar un comando PowerShell, con el fin de desplegar un loader previamente utilizado en un ataque

contra una empresa rusa del sector ferroviario de carga.

La intrusión de marzo de 2024, descrita por Doctor Web, destaca por el hecho de que uno de los componentes maliciosos aprovechó una vulnerabilidad de DLL hijacking en el navegador Yandex (CVE-2024-6473, puntaje CVSS: 8.4) como zero-day para descargar y ejecutar un malware no especificado. Esta falla fue corregida en la versión 24.7.1.380, publicada en septiembre de 2024.

> *«Este grupo se vale de exploits de día cero, lo que le permite infiltrarse en infraestructuras seguras con mayor eficacia. Además, desarrolla y utiliza malware sofisticado, lo que indica una estrategia de largo plazo y un claro objetivo de persistencia dentro de los sistemas comprometidos»,* comentaron los investigadores.