Microsoft ha alertado sobre una campaña activa de malvertising (publicidad maliciosa) que utiliza Node.js para distribuir cargas maliciosas diseñadas para robar información y exfiltrar datos.

Esta actividad, detectada por primera vez en octubre de 2024, se basa en temas relacionados con el comercio de criptomonedas para engañar a los usuarios y hacer que descarguen un instalador falso desde sitios web fraudulentos, los cuales simulan ser plataformas legítimas como Binance o TradingView.

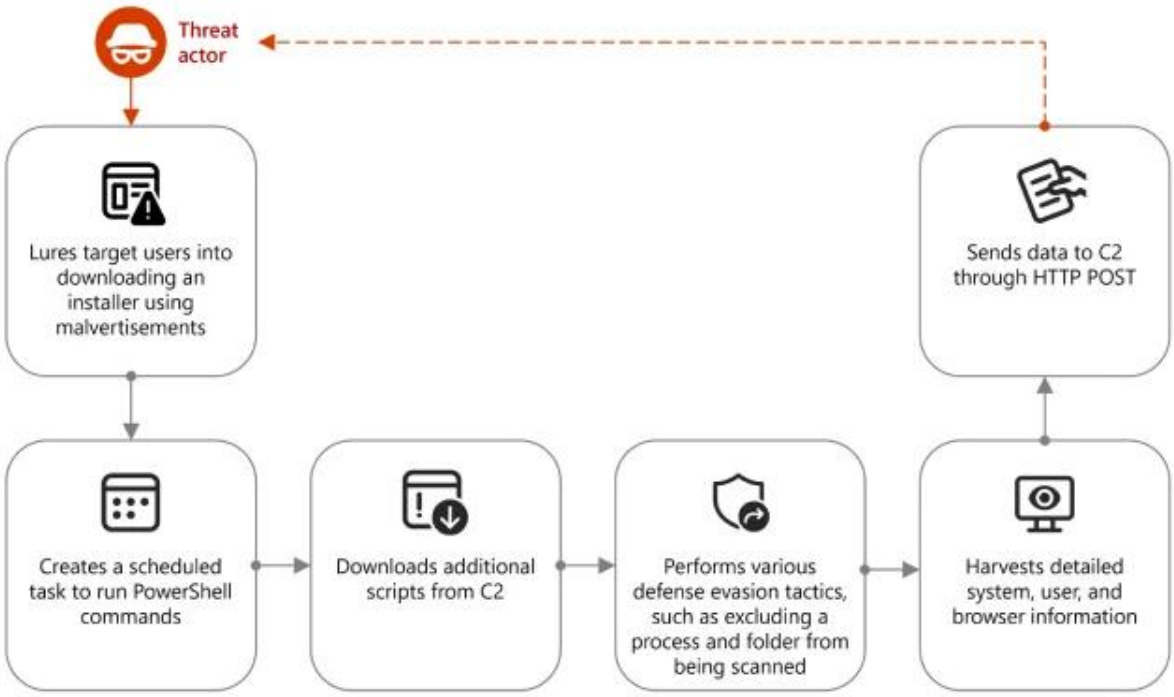
El instalador descargado contiene una biblioteca dinámica («CustomActions.dll») que se encarga de recopilar información básica del sistema mediante WMI (Windows Management Instrumentation) y establecer persistencia en el equipo creando una tarea programada.

Para mantener el engaño, esta DLL abre una ventana del navegador usando «msedge_proxy.exe«, mostrando la página real del sitio de criptomonedas. Este ejecutable puede utilizarse para presentar cualquier sitio web como si fuera una aplicación nativa.

Mientras tanto, la tarea programada ejecuta comandos PowerShell que descargan desde un servidor remoto otros scripts. Estos scripts excluyen tanto el proceso actual de PowerShell como el directorio en uso de los análisis de Microsoft Defender for Endpoint, evitando así ser detectados.

Luego de estas exclusiones, se lanza un comando PowerShell ofuscado que descarga y ejecuta scripts desde URLs remotas. Estos scripts recopilan información detallada sobre el sistema operativo, BIOS, hardware y software instalado, y convierten los datos a formato JSON, que es enviado al servidor de comando y control (C2) a través de una petición HTTPS POST.

Posteriormente, otro script PowerShell se encarga de descargar un archivo comprimido desde el C2, el cual contiene el ejecutable de Node.js junto con un archivo JavaScript compilado (JSC). Este ejecutable inicia el archivo JSC, que establece conexiones de red y probablemente roba información sensible del navegador.



Microsoft también ha observado otra variante del ataque, en la cual se usa una técnica llamada ClickFix. En este caso, se ejecuta JavaScript malicioso en línea mediante PowerShell, sin necesidad de archivos externos. Este código realiza exploración de red para identificar objetivos valiosos, oculta el tráfico del C2 como si fuera legítimo tráfico de Cloudflare, y logra persistencia modificando claves del Registro de Windows.

> *"Node.js es un entorno de ejecución de JavaScript de código abierto y multiplataforma, que permite ejecutar código fuera del navegador. Es ampliamente utilizado y confiable por los desarrolladores para crear aplicaciones frontend y backend,"* explicó Microsoft.

Sin embargo, también advirtieron que los ciberdelincuentes están aprovechando estas características de Node.js para ocultar malware entre aplicaciones legítimas, eludir controles de seguridad convencionales y mantenerse activos dentro de los sistemas infectados.

Este informe coincide con una revelación de CloudSEK, que identificó un sitio falso de conversión PDF a DOCX (como *candyxpdf[.]com* o *candyconverterpdf[.]com*), el cual también usa la técnica ClickFix para inducir a los usuarios a ejecutar comandos PowerShell codificados que instalan el malware SectopRAT (también conocido como ArechClient2).

> *"Los atacantes replicaron cuidadosamente la interfaz del sitio legítimo y registraron dominios con nombres similares para engañar a los usuarios,"* comentó Varun Ajmera, investigador de seguridad.

Este malware es un potente ladrón de información, diseñado para recolectar datos sensibles de los sistemas comprometidos.

Además, se han detectado campañas de phishing que usan kits desarrollados en PHP para atacar a empleados de empresas con engaños relacionados con recursos humanos (RR. HH.). El objetivo es obtener acceso no autorizado a portales de nómina y modificar los datos bancarios de las víctimas, redirigiendo así los fondos a cuentas controladas por los atacantes.

Algunas de estas actividades se han atribuido a un grupo de cibercriminales conocido como Payroll Pirates, quienes emplean publicidad engañosa en buscadores como Google y sitios falsos de recursos humanos para engañar a las víctimas y robar sus credenciales y códigos de autenticación de dos factores (2FA).