Investigadores de seguridad cibernética trazaron la evolución de Jupyter, un infostealer .NET conocido por destacar los sectores de la salud y la educación, lo que lo hace excepcional para evadir a la mayoría de las soluciones de escaneo de seguridad de endpoints.

La nueva cadena de entrega, detectada por Morphisec el 8 de septiembre, subraya que el malware no solo ha seguido activo, sino que también muestra *«cómo los actores de amenazas siguen desarrollando sus ataques para volverse más eficientes y evasivos»*. La compañía israelí dijo que en la actualidad, está investigando la escala y alcance de los ataques.

Documentado por primera vez en noviembre de 2020, Jupyter (también conocido como Solarmarker), es probablemente de origen ruso y se dirige principalmente a los datos del navegador Chromium, Firefox y Chrome, con capacidades adicionales que permiten una funcionalidad de puerta trasera completa, incluidas funciones para desviar información y cargar los detalles a un servidor de control remoto y descargar y ejecutar cargas útiles adicionales. La evidencia forense recopilada por Morphisec muestra que distintas versiones de Jupyter comenzaron a surgir a partir de mayo de 2020.

En agosto de 2021, Cisco Talos atribuyó las intrusiones a un *«actor bastante sofisticado que se centró en gran medida en el robo de credenciales y de información residual».* La compañía de seguridad cibernética Crowdstrike, a inicios de febrero, describió el malware como un cargador de PowerShell de múltiples etapas, muy ofuscado, que conduce a la ejecución de una puerta trasera compilada .NET.

Aunque los ataques anteriores incorporaron binarios legítimos de software bien conocido como Docx2Rtf y Expert PDF, la última cadena de entrega utiliza otra aplicación PDF llamada Nitro Pro. Los ataques comienzan con la implementación de una carga útil del instalador MSI que tiene más de 100 MB de tamaño, lo que les permite eludir los motores anti-malware y ofuscarlos mediante un asistente de empaquetado de aplicaciones de terceros llamado Advanced Installer.

La ejecución de la carga útil de MSI conduce a la ejecución de un cargador PowerShell

incrustado dentro de un binario legítimo de Nitro Pro 13, dos variantes de las cuales se han observado firmadas con un certificado válido que pertenece a una empresa real en Polonia, lo que sugiere una posible suplantación o robo del certificado. El cargador, en la etapa final, decodifica y ejecuta el módulo .NET de Jupyter en la memoria.

> *«La evolución del ladrón de información/puerta trasera de Jupyter desde que lo identificamos por primera vez en 2020 demuestra la verdad de la afirmación de que los actores de amenazas siempre están innovando. El hecho de que este ataque siga teniendo detecciones bajas o nulas en VirusTotal indica además la facilidad con la que los actores de amenazas evaden las soluciones basadas en la detección»*, dijo Naddav Lorber, investigador de Morphisec.