Investigadores en ciberseguridad han dado a conocer detalles de una campaña de malware activa llamada Stealit, que ha aprovechado la función Single Executable Application (SEA) de Node.js como método para distribuir sus cargas maliciosas.

Según Fortinet FortiGuard Labs, algunas variantes también han utilizado el framework de código abierto Electron para entregar el malware. Se estima que la propagación se realiza mediante instaladores falsos de juegos y aplicaciones VPN subidos a plataformas de intercambio de archivos como Mediafire y Discord.

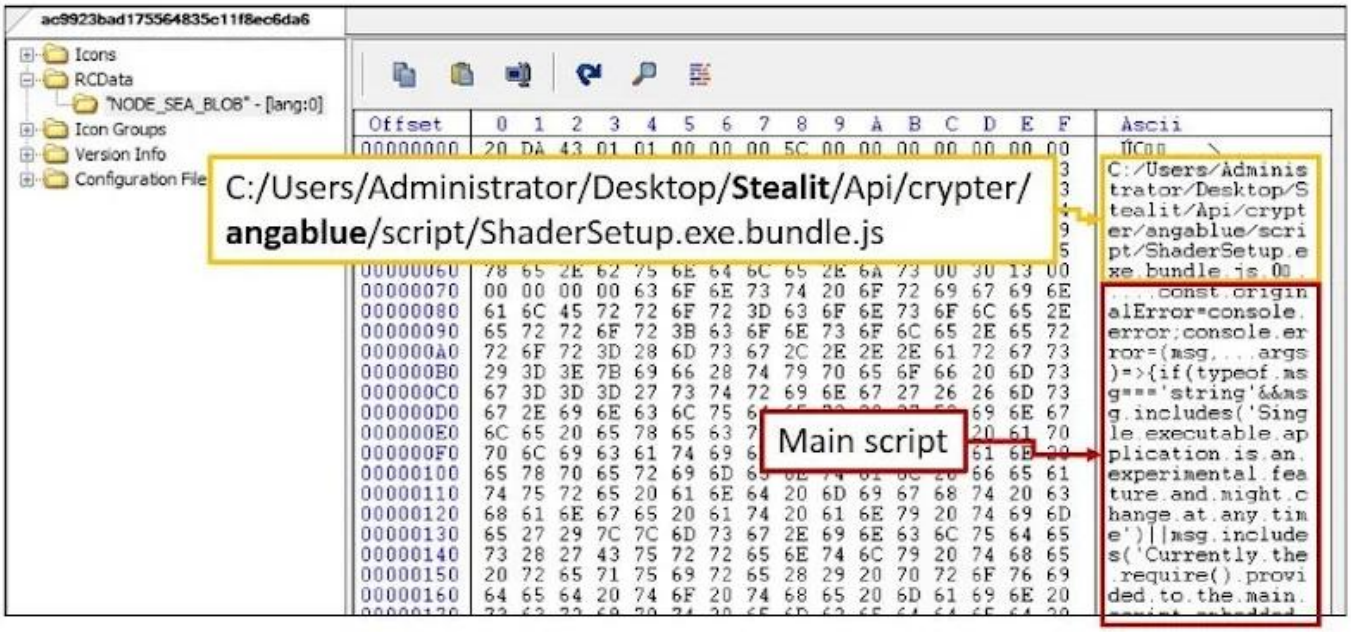
SEA es una característica que permite empaquetar aplicaciones Node.js en un único ejecutable independiente, de modo que puedan ejecutarse incluso en equipos donde Node.js no esté instalado.

Los actores detrás de la campaña mantienen un sitio web donde promocionan *«soluciones profesionales de extracción de datos»* con distintos planes de suscripción. Entre las herramientas que ofertan figura un troyano de acceso remoto (RAT) con funciones de extracción de archivos, control de cámara, monitorización de pantalla en vivo y desplegado de ransomware para Android y Windows.

Los precios anunciados para el «Windows Stealer» van desde 29,99 USD por una suscripción semanal hasta 499,99 USD por una licencia de por vida. En el caso del RAT para Android, las tarifas oscilan entre 99,99 USD y 1.999,99 USD.

Los ejecutables falsos incluyen un instalador diseñado para descargar los componentes principales del malware desde un servidor de comando y control (C2) y proceder a su instalación, pero antes ejecutan varias comprobaciones anti-análisis para determinar si se están ejecutando en un entorno virtualizado o en un sandbox.

Un punto clave de este proceso es escribir una clave de autenticación codificada en Base64 —una cadena alfanumérica de 12 caracteres— en el archivo %temp%\cache.json. Esa clave sirve para autenticar la comunicación con el servidor C2 y también permite a los suscriptores acceder al panel de control para, presumiblemente, supervisar y gestionar a sus víctimas.



El malware está programado además para añadir exclusiones en Microsoft Defender Antivirus, de modo que la carpeta que aloja los componentes descargados no sea detectada. Las funciones de los tres ejecutables son las siguientes:

- save_data.exe: se descarga y ejecuta únicamente si el malware cuenta con privilegios elevados. Su propósito es desplegar una herramienta llamada *cache.exe* —parte del proyecto de código abierto ChromElevator— para extraer datos de navegadores basados en Chromium.
- stats_db.exe: orientado a extraer información de mensajerías (Telegram, WhatsApp), billeteras de criptomonedas y extensiones de monederos (Atomic y Exodus), además de datos de aplicaciones relacionadas con juegos (Steam, Minecraft, GrowTopia y Epic Games Launcher).
- game_cache.exe: diseñado para lograr persistencia en el equipo creando un script de Visual Basic que se ejecuta al reiniciar el sistema; se comunica con el C2 para retransmitir la pantalla de la víctima en tiempo real, ejecutar comandos arbitrarios, subir/descargar archivos y cambiar el fondo de escritorio.

“Esta nueva campaña de Stealit explota la característica experimental Single Executable Application (SEA) de Node.js —todavía en desarrollo activo— para distribuir cómodamente scripts maliciosos en sistemas que no disponen de Node.js instalado”, señaló Fortinet. *“Los actores maliciosos podrían estar aprovechando la novedad de la función, confiando en el factor sorpresa y en la posibilidad de tomar desprevenidas a las soluciones de seguridad y a los analistas de malware.”*