CIBERCRIMINALES UTILIZAN PHANTOMLOADER PARA DISTRIBUIR EL POTENTE MALWARE SSLOAD

Introducción

En los últimos años, la ciberdelincuencia ha aumentado de manera significativa, y los ciberdelincuentes están utilizando cada vez más técnicas sofisticadas para llevar a cabo sus ataques. Recientemente, se ha descubierto que están utilizando un nuevo método para distribuir el malware SSLoad, empleando un cargador llamado PhantomLoader. Este cargador se inserta en archivos de programas legítimos para evadir la detección y se entrega a través de correos electrónicos de phishing. Una vez dentro del sistema, SSLoad puede recopilar información, realizar tareas de reconocimiento y descargar más malware. Esta sofisticada técnica subraya la adaptabilidad y complejidad del malware, que también se ha relacionado con la distribución de herramientas peligrosas como Cobalt Strike.

Funcionamiento

El funcionamiento de esta nueva técnica de distribución de malware es bastante complejo y demuestra la habilidad de los ciberdelincuentes para evadir la detección. El cargador utilizado, PhantomLoader, es un programa previamente no documentado que se inserta en una DLL legítima, generalmente de productos de seguridad EDR o AV. Utiliza técnicas de automodificación y parcheo binario para integrarse en el archivo y evitar ser detectado. Este proceso se inicia a través de un instalador MSI, que al ejecutarse, inicia la secuencia de infección. Una vez dentro del sistema, PhantomLoader se hace pasar por un módulo DLL para el software antivirus 360 Total Security y su función principal es extraer y ejecutar una carga útil primaria, una DLL de descarga escrita en Rust. Esta carga útil descarga la carga principal de SSLoad desde un servidor remoto controlado por los atacantes a través de un canal de Telegram. La carga útil final, también escrita en Rust, realiza huellas digitales del sistema comprometido y envía esta información al servidor de comando y control (C2). El servidor responde con comandos para descargar y ejecutar más malware. Se ha relacionado a SSLoad con la implementación de Cobalto Strike, una herramienta utilizada para actividades post-explotación.

Impacto y consecuencias

La utilización de PhantomLoader y SSLoad por parte de los ciberdelincuentes tiene múltiples impactos y consecuencias técnicas significativas. En primer lugar, su capacidad de evadir la detección dificulta la seguridad del sistema, ya que puede pasar desapercibido para soluciones de seguridad tradicionales como antivirus y herramientas de detección y respuesta de endpoint. Además, su uso como cargador persistente asegura que SSLoad pueda reinstalarse y ejecutar cargas útiles adicionales incluso después de intentos de eliminación, lo que complica la limpieza del sistema comprometido. En términos operativos, SSLoad puede recopilar información del sistema y descargar y ejecutar más malware, lo que puede comprometer la confidencialidad y disponibilidad de los datos y servicios del sistema afectado. Por último, su complejidad y capacidad de evasión aumentan la superficie de ataque, permitiendo la infiltración de otros actores maliciosos o la instalación de diferentes tipos de malware destructivo. En resumen, el uso de PhantomLoader y SSLoad por parte de los ciberdelincuentes tiene graves

consecuencias tanto técnicas como administrativas, y es importante estar al tanto de estas amenazas y tomar medidas de seguridad adecuadas para proteger nuestros sistemas.

Impacto de la actividad maliciosa

La presencia de malware en una organización puede tener un impacto significativo en sus operaciones y finanzas. En el caso de las familias de malware SSLoad y PhantomLoader, la remediación de las infecciones puede ser costosa y laboriosa, ya que requiere recursos importantes para la detección, análisis forense y recuperación completa del sistema. Además, las organizaciones afectadas pueden experimentar interrupciones en sus operaciones debido a la necesidad de desinfectar sistemas, restaurar datos y restablecer servicios comprometidos. Un ejemplo de flujo de ataque común para estas familias de malware comienza con el envío de un correo electrónico de phishing con un instalador malicioso, lo que demuestra la importancia de la concienciación y formación de los usuarios para prevenir este tipo de ataques.

Categorización Mitre

La categorización Mitre es una herramienta útil para comprender las técnicas utilizadas por los atacantes en una actividad maliciosa. En el caso de SSLoad y PhantomLoader, se han identificado varias técnicas relevantes, como la ofuscación de archivos o información (T1027), el enmascaramiento (T1036) y la exfiltración de datos a través de canales de comando y control (T1041). Estas técnicas permiten a los atacantes evadir la detección y mantener el control sobre los sistemas comprometidos, lo que demuestra la sofisticación de estas familias de malware.

Razones técnicas de relevancia

Las razones técnicas por las que cada técnica es relevante en la actividad maliciosa de SSLoad y PhantomLoader son fundamentales para comprender cómo estos malware operan y cómo pueden ser detectados y mitigados. Por ejemplo, la inyección de procesos (T1055) es una técnica utilizada por PhantomLoader para evadir la detección y ejecutar código malicioso dentro de procesos legítimos. El descubrimiento de información del sistema (T1082) es una función de SSLoad que recopila datos del sistema comprometido y los envía al servidor de comando y control para facilitar actividades maliciosas posteriores. Y, por supuesto, el phishing (T1566) es el vector de entrada principal para la infección inicial de estos malware, lo que demuestra la importancia de la formación de los usuarios en la prevención de ataques.

Mitigaciones Mitre

Para mitigar el riesgo de infección por SSLoad y PhantomLoader, es importante implementar las mitigaciones recomendadas por Mitre. Estas incluyen el uso de software antivirus y antimalware (M1049) con firmas y heurísticas actualizadas para detectar y bloquear estos malware antes de que puedan ejecutarse. También es importante bloquear la ejecución de código en un sistema (M1038) mediante el control de aplicaciones o el bloqueo de scripts, lo que puede prevenir la ejecución de PhantomLoader y SSLoad en primer lugar. Establecer y hacer cumplir políticas de contraseñas seguras (M1027) también es esencial para prevenir el acceso no autorizado que podría ser aprovechado por estos malware. Configurar el Control de Cuentas de Usuario de Windows (M1052) puede dificultar que SSLoad realice cambios críticos en el sistema, y la formación de los usuarios (M1017) puede reducir el riesgo de éxito del phishing. Por último, realizar auditorías y escaneos de sistemas (M1047) puede

ayudar a identificar posibles debilidades y actividades inusuales asociadas con la presencia de SSLoad y PhantomLoader.

Fernando Vargas Hincapié
https://alertas-y-seguridad.jimdosite.com/