Se ha descubierto un nuevo malware llamado Mystic Stealer, diseñado para robar información. Este malware es capaz de extraer datos de alrededor de 40 navegadores web distintos y más de 70 extensiones de navegadores.

Fue anunciado por primera vez el 25 de abril de 2023, a un precio de $150 al mes. Además de atacar navegadores web, Mystic Stealer también tiene como objetivo billeteras de criptomonedas, plataformas como Steam y Telegram, y cuenta con mecanismos sofisticados para evitar su análisis.

> *«El código está altamente oculto mediante la utilización de técnicas como la ofuscación de cadenas de caracteres, la resolución de importación basada en hash y el cálculo de constantes en tiempo de ejecución»,* señalaron los investigadores de InQuest y Zscaler en un análisis publicado la semana pasada.

Al igual que otras soluciones criminales disponibles en el mercado, Mystic Stealer se enfoca en el robo de datos y está programado en lenguaje C. El panel de control ha sido desarrollado utilizando Python.

Las actualizaciones lanzadas en mayo de 2023 incluyen un componente de carga que permite al malware obtener y ejecutar cargas útiles adicionales desde un servidor de comando y control (C2), lo que aumenta su peligrosidad.

Las comunicaciones entre el malware y los servidores C2 se realizan a través de un protocolo binario personalizado que utiliza TCP. Hasta la fecha, se han identificado al menos 50 servidores C2 en funcionamiento. Por su parte, el panel de control sirve como interfaz para que los compradores del malware accedan a registros de datos y realicen configuraciones.

La firma de ciberseguridad Cyfirma, que realizó un análisis concurrente de Mystic Stealer, informó que *«el autor del producto invita abiertamente a recibir sugerencias para mejorar el malware»* a través de un canal dedicado en Telegram, lo que indica que están activamente interesados en colaborar con la comunidad de ciberdelincuentes.

> *«Queda claro que el desarrollador de Mystic Stealer busca crear un malware a la altura de las últimas tendencias en el espacio del malware, enfocándose en técnicas anti-análisis y evasión de defensas»,* afirmaron los investigadores.

Estos hallazgos coinciden con el auge de los programas de robo de información, que se han convertido en un artículo muy solicitado en el mercado clandestino, ya que son utilizados como base por otros ciberdelincuentes para lanzar campañas de ransomware y extorsión de datos.

A pesar de su creciente popularidad, los malware de robo de información no solo se están comercializando a precios asequibles para atraer a un público más amplio, sino que también están evolucionando para volverse más peligrosos, incorporando técnicas avanzadas para pasar desapercibidos.

La naturaleza en constante evolución y volátil del mundo de los robadores de información se demuestra mejor con la continua aparición de nuevas variantes como Album Stealer, Bandit Stealer, Devopt, Fractureiser y Rhadamanthys en los últimos meses.

Como evidencia adicional de los esfuerzos de los actores de amenazas por evitar la detección, se ha observado que los robadores de información y los troyanos de acceso remoto se encuentran empaquetados dentro de crypters como AceCryptor, ScrubCrypt (también conocido como BatCloak) y Snip3.

Este desarrollo también se produce mientras HP Wolf Security detalla una campaña de ChromeLoader en marzo de 2023, llamada Shampoo, que está diseñada para instalar una extensión maliciosa en Google Chrome y robar datos confidenciales, redirigir búsquedas e insertar anuncios en la sesión del navegador de la víctima.

> *«Los usuarios se encontraron con el malware principalmente al descargar contenido ilegal, como películas (Cocaine Bear.vbs), videojuegos u otros. Estos sitios web engañan a las víctimas para que ejecuten un malicioso VBScript en sus*

> *computadoras, desencadenando así la cadena de infección»,* mencionó el investigador de seguridad Jack Royer.

A continuación, el VBScript procede a ejecutar código de PowerShell capaz de cerrar todas las ventanas abiertas de Chrome y abrir una nueva sesión con la extensión corrupta desempaquetada utilizando el argumento de línea de comandos «–load-extension».

Además, se ha descubierto un nuevo troyano modular de malware llamado Pikabot que tiene la capacidad de ejecutar comandos arbitrarios e inyectar cargas útiles proporcionadas por un servidor C2, como Cobalt Strike.

El implante, activo desde principios de 2023, se ha encontrado que comparte similitudes con QBot en cuanto a métodos de distribución, campañas y comportamiento del malware, aunque no existen pruebas concluyentes que relacionen a ambas familias.

> *«Pikabot es una nueva familia de malware que implementa un amplio conjunto de técnicas anti-análisis y ofrece capacidades habituales de puerta trasera para cargar shellcode y ejecutar binarios arbitrarios en la segunda etapa»,* afirmó Zscaler.