Se ha observado que una nueva versión del malware MyloBot está implementando cargas maliciosas que se utilizan para enviar correos electrónicos de sextorsión que exigen a las víctimas que paguen $2372 dólares en criptomonedas.

Se sabe que MyloBot, detectado por primera vez en 2018, presenta una serie de sofisticadas capacidades anti-depuración y técnicas de propagación para conectar las máquinas infectadas a una red de bots, sin mencionar la eliminación de rastros de otro malware de la competencia de los sistemas.

El principal de sus métodos para evadir la detección y permanecer bajo el radar incluye una demora de 14 días antes de acceder a sus servidores de comando y control y la instalación para ejecutar archivos binarios maliciosos directamente desde la memoria.

MyloBot también aprovecha una técnica llamada vaciado de procesos, en la que el código de ataque se inyecta en un proceso suspendido y vaciado para eludir las defensas basadas en procesos. Esto se logra al desasignar la memoria asignada al proceso en vivo y reemplazarla con el código arbitrario que se ejecutará, en este caso, un archivo de recursos decodificado.

> *«El ejecutable de la segunda etapa crea una nueva carpeta en C:\ProgramData. Busca svchost.exe en un directorio del sistema y lo ejecuta en estado suspendido. Usando una técnica de inyección de APC, se inyecta en el proceso svchost.exe generado»,* dijo la investigadora de Minerva Labs, Natalie Zargarov.

La inyección de APC, similar al vaciado de procesos, también es una técnica de inyección de procesos que permite la inserción de código malicioso en un proceso víctima existente por medio de la cola de llamada de procedimiento asíncrono (APC).

La siguiente fase de la infección consiste en establecer la persistencia en el host comprometido, utilizando el punto de apoyo como trampolín para establecer comunicaciones con un servidor remoto para obtener y ejecutar una carga útil que, a su vez, decodifica y ejecuta el malware de etapa final.

Este malware está diseñado para abusar del punto final para enviar mensajes de extorsión que aluden a los comportamientos en línea de los destinatarios, como visitar sitios pornográficos y amenazar con filtrar un video que supuestamente se grabó al irrumpir en la cámara web de sus computadoras.

El análisis de Minerva Labs sobre el malware, también revela su capacidad para descargar archivos adicionales, lo que sugiere que el atacante dejó una puerta trasera para llevar a cabo más ataques.

> *«Este actor de amenazas pasó por muchos problemas para colocar el malware y mantenerlo sin ser detectado, solo para usarlo como un remitente de correo de extorsión. Las redes de bots son peligrosas precisamente por esta próxima amenaza desconocida. Podría fácilmente colocar y ejecutar ransomware, spyware, gusanos u otras amenazas en todos los puntos finales infectados»,* dijo Zargarov.