Investigadores de seguridad cibernética revelaron un malware personalizado sigiloso y previamente indocumentado llamado SockDetour, que se dirigía a contratistas de defensa con sede en Estados Unidos con el objetivo de ser utilizado como un implante secundario en hosts de Windows comprometidos.

> *«SockDetour es una backdoor que está diseñada para permanecer sigilosamente en servidores Windows comprometidos para que pueda servir como una puerta trasera de respaldo en caso de que falle la principal. Es difícil de detectar, ya que funciona sin archivos ni sockets en servidores Windows comprometidos»*, dijo Unit 42 de Palo Alto Networks.

Además, se cree que SockDetour se utilizó en ataques desde al menos julio de 2019, según una marca de tiempo de compilación en la muestra, lo que implica que la puerta trasera logró pasar con éxito la detección durante más de dos años y medio.

Los ataques se atribuyeron a un grupo de amenazas que se rastrea como TiltedTemple (también conocido como DEV-0322 de Microsoft), que es el apodo designado para un grupo de hacking que opera fuera de China y fue fundamental en la explotación de vulnerabilidades de día cero en Zoho ManageEngine ADSelfService Plus y ServiceDesk. Más implementaciones como plataforma de lanzamiento para ataques de malware el año pasado.

Los vínculos con TiltedTemple provienen de superposiciones en la infraestructura de ataque, con uno de los servidores de comando y control (C2) que se usó para facilitar la distribución de malware para las campañas de finales de 2021 que también aloja la puerta trasera SockDetour, junto con una utilidad de volcado de memoria y numerosas shells web para acceso remoto.

Unit 42 dijo que descubrió evidencia de al menos cuatro contratistas de defensa que fueron objeto de la nueva ola de ataques, lo que resultó en el compromiso de uno de ellos.

Las intrusiones también son anteriores a los ataques que ocurrieron a través de servidores

Zoho ManageEngine comprometidos en agosto de 2021 por un mes. El análisis de la campaña ha revelado que SockDetour se entregó desde un servidor FTP externo al servidor de Windows con acceso a Internet de un contratista de defensa con sede en Estados Unidos el 27 de julio de 2021.

> *«El servidor FTP que aloja a SockDetour era un servidor de almacenamiento conectado a la red (NAS) comprometido para pequeñas oficinas y oficinas domésticas (SOHO) de Quality Network Appliance Provider (QNAP). Se sabe que el servidor NAS tiene múltiples vulnerabilidades, incluida una de ejecución remota de código, CVE-2021-28799″,* dijeron los investigadores.

Además, se cree que el mismo servidor ya estaba infectado con el ransomware QLocker, lo que plantea la posibilidad de que el actor de TiltedTemple aprovechó la falla antes mencionada para obtener acceso inicial no autorizado.

SockDetour, por su parte, está diseñado como una puerta trasera que secuestra los sockets de red de los procesos legítimos para establecer su propio canal C2 encriptado, seguido de la carga de un archivo DLL de complemento no identificado recuperado del servidor.

> *«Por lo tanto, SockDetour no requiere abrir un puerto de escucha desde el cual recibir una conexión ni llamar a una red externa para establecer un canal C2 remoto. Esto hace que la backdoor sea más difícil de detectar tanto desde el host como desde la red»*, dijeron los investigadores.