Investigadores de seguridad cibernética descubrieron una nueva variante del ransomware Snatch, que primero reinicia las computadoras infectadas con Windows en modo seguro y luego encripta los archivos de las víctimas para evitar la detección antivirus.

A diferencia del malware tradicional, el nuevo ransomware Snatch elige ejecutarse en modo seguro porque en el modo de diagnóstico, el sistema operativo Windows comienza con un conjunto mínimo de controladores y servicios sin cargar la mayoría de los programas de inicio de terceros, incluido el software antivirus.

Snatch ha estado activo desde al menos el verano de 2018, pero los investigadores de Sophos Labs detectaron la mejora del modo seguro para esta cepa de ransomware solo en los recientes ataques cibernéticos contra distintas entidades investigadas.

> *«Los investigadores de Sophos Labs han estado investigando una serie continua de ataques de ransomware en los que el ejecutable del ransomware obliga a la máquina de Windows a reiniciarse en modo seguro antes de comenzar el proceso de cifrado»,* dijeron los investigadores.
>
> *«El ransomware, que se llama a sí mismo Snatch, se configura como un servicio denominado SuperBackupMan con la ayuda del registro de Windows, que se ejecutará durante un arranque en modo seguro. Cuando la computadora vuelve a funcionar después del reinicio, esta vez en modo seguro, el malware usa el componente net.exe de Windows para detener el servicio SuperBackupMan, y luego usa el componente vssadmin.exe de Windows para eliminar todas las instantáneas de volumen en el sistema, que impide la recuperación forense de los archivos cifrados por el ransomware»*, agregaron.

Lo que hace más peligroso a Snatch, es que también es un ladrón de datos. Snatch incluye un sofisticado módulo de robo de datos, que permite a los atacantes robar grandes cantidades de información de las organizaciones objetivo.

Aunque Snatch está desarrollado en Go, un lenguaje de programación conocido para el desarrollo de aplicaciones multiplataforma, los autores diseñaron este ransomware para ejecutarse solo en la plataforma Windows.

> *«Snatch puede ejecutarse en las versiones más comunes de Windows, de 7 a 10, en versiones de 32 y 64 bits. Las muestras que hemos visto también están empaquetadas con el paquete de código abierto UPX para ofuscar sus contenidos»,* dijeron los investigadores.

Además, los atacantes detrás de Snatch también ofrecen oportunidades de asociación a otros ciberdelincuentes y empleados corruptos que poseen credenciales y puertas traseras en grandes organizaciones y pueden explotarlo para implementar el ransomware.

Utilizando credenciales forzadas robadas, los atacantes primero obtienen acceso a la red interna de la compañía y luego ejecutan varios administradores legítimos y herramientas de prueba de penetración para comprometer los dispositivos dentro de la misma red sin levantar ninguna bandera roja.

> *«También encontramos una gama de herramientas legítimas que han sido adoptadas por delincuentes instalados en máquinas dentro de la red del objetivo, incluyendo Process Hackers, IObit Uninstaller, PowerTool y PsExec. Los atacantes generalmente las usan para tratar de desactivar los productos AV»*, agregaron.

Coveware, una compañía que se especializa en negociaciones de extorsión entre atacantes y víctimas de ransomware, informó a Sophos que negociaron con los piratas informáticos de Snatch *«en 12 ocasiones entre julio y octubre de 2019 en nombre de sus clientes»*, con pagos de rescate que oscilan entre 2000 y 35000 dólares en Bitcoin.