Dos años después de que se robaran y publicaran las explotaciones altamente clasificadas creadas por la Agencia de Seguridad Nacional, los piratas informáticos siguen utilizando las herramientas para cometer crímenes.

Los investigadores de seguridad de Symantec afirman que está aumentando el uso de un nuevo malware, denominado como Beapy, que utiliza las herramientas de piratería filtradas por la NSA para propagarse con el fin de ejecutar un código minero y generar criptomonedas.

Beapy fue visto por primera vez en enero, pero se disparó a más de 12 mil infecciones únicas en 732 organizaciones desde marzo, según dijo Alan Neville, investigador principal de Symantec. El malware se dirige casi únicamente a empresas, aloja una gran cantidad de computadoras, que cuando se infectan con malware de minería de criptomonedas puede generar sumas grandes de dinero.

El malware se basa en alguien de la empresa que abre un correo electrónico malicioso. Una vez abierto, el malware elimina la herramienta DoublePulsar, desarrollado por la NSA para crear una puerta trasera persistente en la computadora infectada, y utiliza el exploit EternalBlue de la NSA para propagarse lateralmente por medio de la red.

Estos son los mismos ataques que ayudaron a difundir el ransomware WannaCry en 2017. Una vez que las computadoras de la red están en la puerta trasera, el malware Beapy se extrae del servidor de control y comando del pirata informático para infectar cada computadora con el software de minería.

Beapy no solo utiliza las vulnerabilidades de la NSA para propagarse, sino que también utiliza Mimikatz, un ladrón de credenciales de código abierto, para recopilar y usar las contraseñas de las computadoras infectadas para navegar por medio de la red.

Según los investigadores, más del 80% de las infecciones de Beapy están en China.

El secuestro de computadoras para explotar criptomonedas, conocido como cryptojacking, ha estado en declive en los últimos meses, parcialmente luego del cierre de Coinhive, una

herramienta popular para la minería. Los hackers están descubriendo que las recompensas fluctúan en gran medida según el valor de la criptomoneda. Pero el cryptojacking sigue siendo una fuente de ingresos más estable que los resultados impredecibles del ransomware.

En septiembre, unas 919 mil computadoras fueron vulnerables a los ataques de EternalBliue, muchas de las cuales fueron explotadas por la minería de criptomonedas. Hoy, dicha cifra a subido a más de un millón.

Por lo general, los cryptojackers explotan vulnerabilidades en sitios web que, cuando se abren en el navegador de un usuario, utilizan la capacidad de procesamiento de la computadora para generar criptomonedas. Pero el cryptojacking basado en archivos es mucho más eficiente y rápido, lo que permite a los hackers ganar más dinero.

En un solo mes, la minería basada en archivos puede generar hasta 750 mil dólares, estiman los investigadores de Symantec, en comparación con solo 30,000 dólares de una operación de minería basada en el navegador.

El cryptojacking puede parecer un delito sin víctimas: no se roban datos y los archivos no están encriptados, pero Symantec dice que las campañas de minería pueden ralentizar las computadoras y causar la degradación del dispositivo.