Los piratas informáticos han comenzado a explotar un esquema más rentable que los ataques cibernéticos comunes, ahora las botnets no solo lanzan DDoS o spam, sino que también extraen criptomonedas.

Smominru, una botnet de minería de criptomonedas y robo de credenciales, se convirtió en uno de los virus informáticos de rápida propagación que ahora infecta a más de 90 mil máquinas cada mes en todo el mundo.

Aunque las campañas que están pirateando computadoras con la botnet Smominru no han sido diseñadas para perseguir objetivos con ningún interés específico, el último informe de los investigadores de Guardicore Labs arroja luz sobre la naturaleza de las víctimas y la infraestructura del ataque.

Según los investigadores, el mes pasado, más de 4,900 redes fueron infectadas por el gusano sin discriminación alguna, y muchas de estas redes tenías muchas máquinas internas infectadas.

Las redes infectadas incluyen instituciones de educación superior con sede en Estados Unidos, empresas médicas e incluso compañías de ciberseguridad, con la red más grande perteneciente a un proveedor de atención médica en Italia, con un total de 65 hosts infectados.

Activo desde 2017, la botnet Smominru compromete las máquinas de Windows que utilizan principalmente EternalBlue, un exploit creado por la Agencia de Seguridad Nacional de Estados Unidos, pero que luego fue filtrado al público por el grupo de hackers Shadow Brokers y luego el más utilizado por el ataque del ransomware WannaCry en 2016.

La botnet también se ha diseñado para obtener acceso inicial en sistemas vulnerables simplemente al forzar credenciales débiles para diferentes servicios de Windows, incluyendo MS-SQL, RDP y Telnet.

Una vez con acceso inicial a los sistemas específicos, Smominru instala un módulo troyano y un minero de criptomonedas, luego se propaga dentro de la red para aprovechar la potencia de la CPU de las PC de las víctimas para extraer la cripto divisa Monero y enviarla a una billetera del operador del malware.

Hace un mes, también se reveló que los operadores detrás de la botnet actualizaron Smominru para agregar un módulo de recolección de datos y un troyano de acceso remoto (RAT) al código de minería de criptomonedas de su botnet.

La última variante de Smominru descarga y ejecuta al menos 20 scripts maliciosos distintos y cargas binarias, incluido un descargador de gusanos, un troyano y un rootkit MBR.

> *«Los atacantes crean muchas puertas traseras en la máquina en diferentes fases del ataque. Estos incluyen usuarios recién creados, tareas programadas, objetos WMI y servicios configurados para ejecutarse en el momento del arranque»,* dijeron los investigadores.

Según el nuevo informe, los investigadores de Guardicore Labs dijeron que lograron obtener acceso a uno de los servidores centrales de los atacantes, que almacena información de las víctimas y sus credenciales robadas, y observaron de cerca la naturaleza de las víctimas.

> *«Los registros de los atacantes describen cada host infectado; incluyen sus direcciones IP externas e internas, el sistema operativo que ejecuta e incluso la carga en las CPU del sistema. Además, los atacantes intentan recopilar los procesos en ejecución y robar credenciales utilizando Mimikatz»,* agregaron.
>
> *«Guardicore Labs informó a las víctimas identificables y les proporcionó los detalles de sus máquinas infectadas».*

La botnet está infectando máquinas vulnerables, la mayoría de las cuales ejecutan Windows 7 y Windows Server 2008, a una velocidad de 4,700 máquinas por día con miles de infecciones detectadas en países como China, Taiwán, Rusia, Brasil y Estados Unidos.

La mayoría de las máquinas infectadas descubiertas eran principalmente servidores pequeños, con 1 a 4 núcleos de CPU, dejando la mayoría de ellos inutilizables debido a la sobrecarga de trabajo con el proceso de minería.

El análisis de los investigadores también reveló que una cuarta parte de las víctimas de Smominru fue reinfectada por el gusano, lo que sugiere que *«intentaron limpiar sus sistemas sin solucionar el problema de la causa raíz que los dejó vulnerables en primer lugar».*

A diferencia de las variantes anteriores de Smominru, la nueva variante también elimina las infecciones de los sistemas comprometidos, si existen, que son agregadas por otros grupos de piratas informáticos, junto con el bloqueo de los puertos TCP (SMB, RPC) en un intento por evitar que otros atacantes infecten sus máquinas.

Los investigadores de Guardicore también publicaron una lista completa de IoC (Indicadores de Compromiso) y un script Powershell gratuito en GitHub, que se puede ejecutar desde la interfaz de línea de comandos de Windows para verificar si el sistema está infectado con el gusano Smominru.

Debido a que el gusano Smominru aprovecha el exploit EternalBlue y las contraseñas débiles, se recomienda a los usuarios que mantengan sus sistemas y software actualizados y se adhieran a contraseñas fuertes, complejas y únicas para evitar ser víctimas de este tipo de amenazas.