Investigadores de seguridad cibernética de ESET dijeron el jueves que derribaron una parte de una botnet de malware de al menos 35000 sistemas Windows comprometidos, que los atacantes estaban usando en secreto para extraer la criptomoneda Monero.

La botnet, denominada *«VictoryGate»,* ha estado activa desde mayo de 2019, con infecciones reportadas principalmente en América Latina, especialmente en Perú, que representan el 90% de los dispositivos comprometidos.

> *«La actividad principal de la botnet es extraer la criptomoneda Monero. Las víctimas incluyen organizaciones de los sectores público y privado, incluidas las instituciones financieras»,* dijo ESET.

ESET también mencionó que trabajó con el proveedor de DNS dinámico No-IP para eliminar los servidores maliciosos de comando y control (C2) y que configuró dominios falsos (también conocidos como sumideros) para monitorear la actividad de la botnet.

Los datos del sumidero muestran que entre 2000 y 3500 computadoras infectadas se conectaron diariamente a los servidores C2 durante febrero y marzo de este año.

Según los investigadores de ESET, VictoryGate se propaga por medio de dispositivos extraíbles como unidades USB, que al conectarse a las máquinas de las víctimas, instalan una carga maliciosa en el sistema.

Además, el módulo también comunica con el servidor C2 para recibir una carga secundaria que inyecta código arbitrario en procesos legítimos de Windows, como la introducción del software de minería XMRig en el proceso ucsvc.exe (o la utilidad de mantenimiento de archivos de arranque), lo que facilita la minería de Monero.

> *«A partir de los datos recopilados durante nuestras actividades de hundimiento, podemos determinar que, en promedio, se extraen 2000 dispositivos durante todo*

> *el día. Si estimamos una tasa de hash promedio de 150H/s, podríamos decir que los autores de la campaña recolectaron al menos 80 XMR (aproximadamente 6000 dólares), solo de esta botnet».*

Con las unidades USB que se utilizan como vector de propagación, ESET advirtió sobre nuevas infecciones que podrían ocurrir en el futuro. Pero con una gran parte de la infraestructura C2 enredada, los bots ya no recibirían cargas secundarias. Sin embargo, aquellos que se vieron comprometidos antes de que los servidores C2 fueran retirados, seguirían minando Monero.

> *«Una de las características interesantes de VictoryGate, es que muestra un mayor esfuerzo para evitar la detección que las campañas anteriores similares en la región»*, dijo el equipo de investigación.
>
> *«Y debido a que el botmaster puede actualizar la funcionalidad de las cargas útiles que se descargan y ejecutan en los dispositivos infectados desde la minería criptográfica a cualquier otra actividad maliciosa en cualquier momento dado, esto plantea un riesgo considerable».*