35 mil computadores foram infectados na América Latina por malware que minerava Monero

criptonizando.com/35-mil-computadores-foram-infectados-na-america-latina-por-malware-que-minerava-monero/

April 26, 2020

Mais de 35 mil computadores na América Latina estavam infectados com um malware que minerava Monero, conforme reportou o Livecoins.

O malware denominado como VictoryGate, é uma botnet (uma conexão de rede entre computadores) que usava o poder computacional combinado de diferentes máquinas ligadas à um servidor para minerar criptomoedas.

Segundo a equipe de pesquisa da ESET, essa botnet é composta principalmente de dispositivos na América Latina, especificamente no Peru, onde mais de 90% dos dispositivos comprometidos estão localizados.

O malware era especializado em mineração de Monero (XMR) e estava ativo desde maio de 2019. Mais de 35 mil computadores com sistema operacional Windows foram infectados.

Durante fevereiro e março de 2020, entre 2.000 e 3.000 sistemas infectados se conectaram aos servidores diariamente.

Com o poder de mineração adquirido, foram minerados cerca de 80 XMR, na cotação atual cerca de US$6 mil.

A botnet já foi derrubada e eliminada pelos pesquisadores, contudo, a equipe alertou que novos ataques podem acontecer.

O golpe é conhecido como cryptojacking, que está ficando cada vez mais comum. Esse tipo de ataque acontece quando um vírus infecta um computador e passa a roubar o poder computacional para minerar as criptomoedas.

A criptomoeda Monero (XMR) está se tornando uma das favoritas dos ataques de cryptojacking, pois é focada em privacidade e evita que os hackers sejam descobertos.

A Monero está sendo utilizada por ataques de cryptojacking por conta do algoritmo de mineração que é resistente às mineradoras ASIC. A mineração por CPU e GPU são efetivas, tornando o ataque mais lucrativos em diferentes tipos de máquinas.

Os pesquisadores da ESET, informaram que para se proteger desses golpes, é preciso ter cuidado com os sites que acessa e programas instalados.

Se possível, nunca utilizar dispositivos USB desconhecidos ou sem a certeza de que estão livre de vírus.

Assim que os dispositivos móveis com conexão USB é inserido e reconhecido pelo sistema, um pacote malicioso é enviado e instalado no computador.

O Cryptojacking costuma atacar o processador de computadores, deixando o sistema bem lento. Utilize programas anti-malware para tentar identificar o problema assim que notar a lentidão, ou procure uma assistência especializada.

Devido ao foco em privacidade da Monero ser muitas vezes usado para atividades ilícitas, o ativo tem sido retirado de exchanges de criptomoedas.

Receba artigos sobre Bitcoin e Criptomoedas no seu email

*Obrigatório
Tudo sobre: criptomoedas