Millions of PCs Targeted by Cryptocurrency-Mining Malware

This story originally appeared on PCMag

Malware is increasingly developing an appetite for cryptocurrency mining. One newly discovered strain has tried to infect millions of Windows machines, all in an effort to siphon their computing power and possibly sell it for mining purposes.

The operation has been going on for over four months, and may have targeted around 15 million machines or more, security firm Palo Alto Networks said Wednesday.

To spread the malware, the hackers have been disguising the code as EXE files made to look like file-sharing downloads with names such as “File4org,” “RapidFiles” and “Dropmefiles.” Those EXE files have then been circulated online via shortened URL links through services like Bitly and possibly Adfly. It isn’t clear where the hackers have been posting the links, but they’ve generated at least 15 million clicks, according to Palo Alto Networks.

Once the malware infects, it will secretly run an open-source utility called XMRig, which mines Monero, a digital currency now worth about $310 per coin.

“In this case the attackers set it to never use more than 20 percent of (CPU) resources,” said Josh Grunzweig, a malware researcher with Palo Alto Networks, in an email. As a result, most victims probably won’t notice that the mining is taking place.

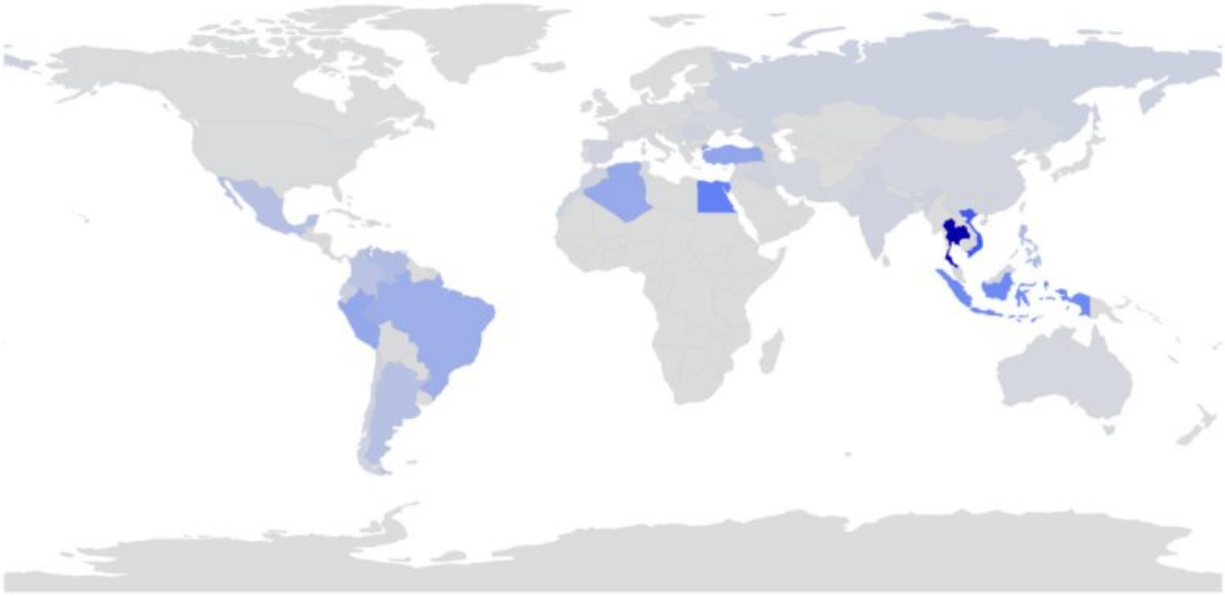

Figure 11 Malicious bitly downloads by country

However, the hackers may be less interested in generating the Monero for themselves than helping others mine it. The malware's code actually contains a reference to NiceHash, an online marketplace for people to buy and sell computing power to mine cryptocurrencies.

"In our research, we've seen that the attackers using it as the marketplace where they 'sell' the hash processing power of the systems they've loaded XMRig on," Grunzweig said.

Palo Alto Networks doesn't know how much Monero the hackers have mined with their malware, but it's been targeting computers mainly in Southeast Asia, North Africa and South America.

The scheme is among the latest hacking threats to capitalize on the rising value of Monero, which was worth only $13 a year ago. Last month, F5 Networks reported that hackers were using leaked NSA cyberweapons to take over Windows and Linux systems, and download malware to mine Monero.

Meanwhile, other cybercriminals have been hijacking websites to run Monero mining scripts over internet browsers. Victims may notice a hit in their computer's processing power

when they load the affected websites. Fortunately, antivirus software and browser add-ons can block the activity.

https://www.entrepreneur.com/article/308125