Issued 1/29/18

Millions of PCs Targeted by Cryptocurrency-Mining Malware

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.