How malware operators use infected computers to mine cryptocoins

February 26 2014, by Ioana Patringenaru

A team of computer scientists at the University of California, San Diego, has taken an unprecedented, in-depth look at how malware operators use the computers they infect to mine Bitcoin, a virtual currency whose value is highly volatile.

Researchers examined more than 2,000 pieces of malware used by Bitcoin mining operations in 2012 and 2013. They were able to estimate

how much money operators made off their operations and which countries were most affected. The computer scientists report that the revenue of 10 of the mining operations they studied reached at least 4,500 Bitcoin over two years. This may not seem like much, but Bitcoin's value increased from about $10 to about $1,000 during that time, with a peak of $1,100 in November 2013. One Bitcoin is currently worth about $618.

Bitcoin mining is particularly attractive for malware operators because of its low cost and because it requires little to no investment in any kind of infrastructure. "At the current stratospheric value of Bitcoin, miners with access to significant computational horsepower are literally printing money," said Danny Huang, a Ph.D. student in computer science and the first author on the study.

This has the potential to change the game in malware, explained Alex Snoeren, a professor of computer science at the Jacobs School of Engineering at UC San Diego, and one of the paper's co-authors. "If it ever becomes very profitable, it could reinvigorate the malware industry," he said.

The study is part of a larger effort by computer scientists at UC San Diego to better understand how malware operators make money, from sending spam to stealing personal information, such as credit card numbers. "These transactions show how society and technology shape each other," said Huang. Researchers will present their paper, "Botcoin: Monetizing Stolen Cycles," at the Network Distributed System Security conference Feb. 26 in San Diego. To track down transactions, researchers used techniques developed by their colleague and co-author, Sarah Meiklejohn, a Ph.D. student at the Jacobs School of Engineering.

The study was conducted in partnership with George Mason University, UC Berkeley and the International Computer Science Institute.

Following the money

Most of the infected computers were located in Europe. But the malware could be found in Asia and Latin America as well. The United States was not immune either. For example, ZeroAccess, a well-known malware operation, conducted mining via at least 2,600 computers it controlled in this country. In all, PCs were infected in more than 60 countries, from Brazil, to Mexico, Vietnam, France, Turkey and Bulgaria.

Most of the major players were well-known malware operators. They collected anywhere from a few hundred to a few thousand Bitcoin over the period researchers surveyed, from December 2011 to November 2013.

Most botnet managers moved the Bitcoin they mined into exchanges where they could be converted into dollars within a few days, suggesting that they planned to cash in their profits quickly. "We wanted to know if these were Bitcoin enthusiasts who turned to the dark side," said Kirill Levchenko, a research scientist and one of the paper's lead authors. "This behavior suggests they're not."

Bitcoin mining by malware operators took off in 2011 and was fairly widespread last year. It's less common now, due to ever-increasing computational requirements to mine Bitcoin. Evidence suggests that some operations have moved on to Litecoin, another online currency.

At the height of the Bitcoin rush, botnet operators with 10,000 PCs in their network could make about $100 dollars a day. But as the currency's popularity increased, the computational resources required to mine it grew exponentially. As a result, that 10,000 PC-botnet would only make less than $10 a day today.

Snoeren and colleagues believe that at this point, malware operators are

not building botnets to exclusively mine Bitcoin. But botnet operators likely added mining to their portfolio of malware operations, such as spam and denial of service attacks. Mining is complimentary to other malware activities such as sending SPAM and conducting click fraud, and has low overhead costs, Snoeren explained. "It's easy money," he said.

Botnets and Bitcoin mining: how it works

Malware operators take over computers by exploiting vulnerabilities in browsers or browser plug-ins, such as Java and Flash. The malware infects computers with a series of programs that make the machines perform illegal activities. The computers are connected as a network, known as a botnet. Operators can then combine the computers' computational power to perform the complex calculations required to mine Bitcoin.

Mining Bitcoin is much like taking part in a lottery, Snoeren explains. It's the computational equivalent of having to pick six numbers at random out of a hat and see if they are a match with a number that will earn Bitcoins. A user mining on an individual PC is unlikely to win, just as someone buying a single lottery ticket is unlikely to win the jackpot. The best way to acquire Bitcoin is to join a mining pool that shares its proceeds, much like co-workers pool their resources to buy a large number of lottery tickets, dividing any potential winnings.

To find illicit Bitcoin mining operations, researchers consulted public repositories of malware providers. They also contacted several people who run Bitcoin mining pools. Computer scientists expected malware operators to hide their mining activities behind proxies. Instead, they found that operators often were mining in the open and joining public mining pools.

Mining in public pools makes malware operators more visible, where their large computational resources stand out. But pool operators rarely call them out, fearing reprisals, mostly in the form of denial of service attacks. Law enforcement would be less hesitant, Snoeren pointed out.

"This could be the equivalent of tax evasion for Al Capone," he said.

Provided by University of California - San Diego