Malware Forces Your Computer Into The Bitcoin Mines – The Blogs at HowStuffWorks

Wednesday, April 10 2013, 11:33 AM

Malware Forces Your Computer Into The Bitcoin Mines

by **Jonathan Strickland** | April 8, 2013

If Spielberg and Lucas were to remake *Indiana Jones and the Temple of Doom* and set it in the present, our intrepid hero might be attempting to free thousands of computers rather than children from enslavement. According to **ZDNet**, Internet security firm Kaspersky Labs discovered some malicious code — aka malware — out in the wild that forces computers to mine for bitcoins. So what does that actually mean?

Bitcoin is a digital currency, meaning it has no physical form. Instead, it's bits of code, just like any other piece of software. The code is encrypted and contains within it a hash. A hash is the end product of some sort of mathematical process (it varies from hash to hash). Basically, the way bitcoins enter circulation is through "mining." In this case, mining doesn't involve taking a pickax to a rock wall. Instead, a computer mines a bitcoin by figuring out which numbers combined to create the hash in a block of code. This involves performing millions of calculations as the computer goes through every possible combination of numbers that could have produced the hash.

Bitcoin's design is clever in that the difficulty of the mining process depends entirely upon how much computing power is being directed at mining. If a lot of processors are trying to find that next bitcoin, the difficulty ramps up. If people get discouraged and quit, the difficulty decreases. This way, the flow of bitcoins into circulation remains steady. There's also a cap on how many bitcoins will ever be in circulation, which I suppose is to prevent the currency from becoming worthless due to an endless supply.

The value of bitcoins — the **Washington Post** reported a couple of days ago that the currency hit an all-time high exchange rate of $147 per bitcoin — means that a lot of people are interested in mining them. But how do you have a chance of mining a digital currency that gets harder to find the more people look for it? A single computer — even one with a decent **GPU** parallel processor — doesn't stand a chance against the more powerful mining rigs out there. Enter the malware.

The malicious code Kaspersky Labs detected pulls computers into a botnet, also known as a **zombie computer army**. The code allows hackers to repurpose a compromised computer's processor to mining for bitcoins. Corrupt enough computers and you've got a huge amount of processing power you can use to find new bitcoins out there. Meanwhile, the victim sees his or her computer performing under par. It may also leave the computer vulnerable to future attacks or manipulation.

The ZDNet story mentions that hackers are distributing the malware with file names that tempt people into opening them. An example might be "is this you in this video." The hackers are counting on our curiosity to trick us into installing malicious code. The best advice is to always be suspicious of any files you come across online. Verify that the file is legitimate before opening it.

While all this is interesting, I still wonder if bitcoins are ever going to be a widely-accepted currency. At the moment, I'd say they're more of a commodity. People want bitcoins because they're worth a lot of "real" money. There's not a large enough marketplace to spend bitcoins to make them worthwhile as an actual currency. I'm skeptical that there ever will be.

Tags: bitcoins, botnet, currency, hackers, malware, mining, virus, zombie computers