CASHING IN ON CYBERCRIME

New Malware Target *Bitcoin*

Cybercriminals are cashing in on Bitcoin, a digital currency that is slowly gaining acceptance as payment for various items bought online. This is probably why creating malware that cause victims to generate money for cybercriminals—akin to the pay-per-click (PPC) schemes of the past and these days' Bitcoin mining—is seemingly becoming a trend.

Eyeing Bitcoins

Most types of cybercrime involve stealing users' money though some cybercriminals also use their victims to make money for them. TrendLabs℠ engineers recently came across a malware that leverages Bitcoin—a digital currency that can be generated or mined with the use of a computer.

In a recent malware attack, cybercriminals unleashed a Bitcoin miner detected by Trend Micro as BKDR_BTMINE.MNR, which installs three different Bitcoin-mining programs in infected systems. The processing speed and installed hardware of the infected system will dictate which of the three programs will run. To help speed up the processing and creation of Bitcoins, the malware downloads the necessary drivers, depending on the infected system's graphics processing unit (GPU), aka video card, and CPU. These drivers make the process more efficient compared with a stock *Windows* installation. The cybercriminals also gain ownership of any Bitcoin generated by this process.

Figure 1. *BKDR_BTMINE.MNR's infection diagram*

Bitcoin miners can also be packaged with other malware to perform functions apart from mining. One such variant, detected by Trend Micro as BKDR_BTMINE.DDOS, can perform distributed denial-of-service (DDoS) attacks against targets. It may be part of a package, along with BKDR_BTMINE.MNR, and has the capability to obtain a list of targets from remote sites. BKDR_BTMINE.DDOS tries to communicate with a list of 2,000 IP addresses, which has been hard-coded into its body and is constantly updated upon execution, for various malicious purposes.

From *Twitter* Links to Bitcoin Miner

Apart from accessing malicious sites, Bitcoin miners also spread via social networking sites. TrendLabs engineers encountered malicious shortened URLs spammed on *Twitter* that ultimately led to Bitcoin mining. Clicking the shortened links leads to a malicious site under a domain that appears to belong to *Facebook.* The said site hosts a .JPEG file that is actually an executable file Trend Micro now detects as WORM_KOLAB.SMQX. The file creates a directory of files that includes an executable file that we detect as HKTL_BITCOINMINE—a Bitcoin miner that cybercriminals can use for various malicious schemes.

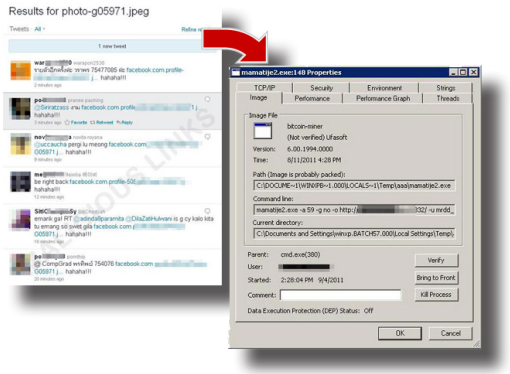

Figure 2. *Malicious links found on* Twitter *that led to the download of HKTL_BITCOINMINE*

Searching for the image file using *Twitter's* search function reveals a list of users who Tweeted or re-Tweeted the malicious link, most of whom were from Indonesia. Apart from the Tweets, WORM_KOLAB.SMQX also accesses malicious sites that play host to other malicious files. Note that these sites use the names of famous personalities like Robert Pattinson and John Lennon to lure more users into clicking them.

Bitcoin Mining

As the *Bitcoin* system's unit of currency, Bitcoin was conceptualized as a form of electronic currency that uses peer-to-peer (P2P) networks to track and verify transactions without going through a financial institution. Even though Bitcoin has been in existence since 2008, only now has it been slowly gaining traction. The use of Bitcoins is not governed by a central authority that can manipulate its value or that can issue more of it. Unlike regular currencies, a finite number of Bitcoins—21 million—can be generated.

A Bitcoin is generated after a "block" of data has been processed. A Bitcoin block is a cryptographic problem; processing such a block is called mining. Cryptographic problems, on the other hand, are mathematically complex problems, solving which requires brute forcing that eats up computing power.

Unlike most online transactions or services, Bitcoin usage does not require setting up any kind of online account, giving out an email address, or coming up with a user name or a password. Bitcoin trading involves the use of randomly generated public-private key pairs; whoever has the private key for a Bitcoin can sign for transactions with it. Every public-private key pair has a Bitcoin address. A user can have as many addresses, each with its own Bitcoin balance, as possible, which makes it difficult to determine who owns what amount.

Bitcoin mining may seem like a good way to earn money without doing hard work but the process takes its toll on one's system. Mining Bitcoin blocks can be tricky, as the cryptographic problems these involve become more difficult to solve each time. Regular CPUs used to be able to handle Bitcoin mining. Now, however, miners have to use GPUs with higher processing capabilities to process blocks, which can cost them dearly.

Digital Currency with Real-World Value

Unlike some digital currencies, Bitcoin use is not tied to a particular product or service. Bitcoins can be used to pay for various online services like Web hosting, mobile app development, and cloud file storage. These can also buy products like games, music, gift cards, and books. Unlike most digital currencies, too, Bitcoins have real world value, as some brick-and-mortar establishments accept them as payment for various goods. These can also be traded for traditional currency. In fact, several sites offer most international currencies in exchange for Bitcoins, each of which is currently worth around US$5.

The growing awareness and recognition of Bitcoin as a legitimate currency, not to mention having real-world value, are seemingly spurring cybercriminal interest.

Like any other activity, Bitcoin mining, however rewarding, can take its toll on one's computing hardware. Cybercriminals, crafty as they usually are, have thus decided to remedy this setback by delegating the hard work—the mining process—to unsuspecting users. They have taken to creating Bitcoin miners in order to mine blocks without their victims' knowledge. Once processed, they then take the Bitcoins generated from their unwitting miners' systems. All that's left for cybercriminals to do is to harvest what the users have sown.

Left with Nothing but Loss

What's the worst that can happen to Bitcoin-mining victims? Users of Bitcoin-miner-infected systems suffer most from computing resource abuse. Their systems sustain increased wear and tear. Since Bitcoin mining uses up a lot of processing power, an infected system can become abnormally sluggish, particularly if the victim uses graphics-intensive applications.

While the cybercriminals do not currently target specific individuals, gamers may especially feel the brunt of involuntary Bitcoin mining, as they are the most common users of computers with highly capable GPUs.

What Can Users Do?

All is not lost, however, as adhering to sound safe computing habits like the following can keep Bitcoin miners at bay:

- Never download and install applications from unknown sites.
- Think twice about clicking shortened links on *Twitter* or any other site for that matter, regardless of source. Remember that URL shortening makes it hard to determine a link's legitimacy.
- If your system suddenly slows down, check it for clues of Bitcoin mining such as an unexplained increase in processing power usage.

Over and above every ounce of online safety practice, however, investing in a security solution that can detect and prevent all kinds of malware from infecting your system is still best. It is also crucial to stay abreast of the latest threats and threat trends so as not to become cybercriminal prey.

References

- Bitcoin. (September 30, 2011). *The Bitcoin Wiki.* https://en.bitcoin.it/wiki/ (Retrieved October 2011).
- Karl Dominguez. (September 4, 2011). *TrendLabs Malware Blog.* "Bitcoin Mining Botnet Found with DDoS Capabilities." http://blog.trendmicro.com/bitcoin-mining-botnet-found-with-ddos-capabilities/ (Retrieved October 2011).
- Natasha Lomas. (September 16, 2011). *silicon.com.* "Bitcoin: Cheat Sheet." http://www.silicon.com/management/finance/2011/09/16/bitcoin-cheat-sheet-39747938/ (Retrieved October 2011).
- Paul Pajares. (September 4, 2011). *TrendLabs Malware Blog.* "Malicious Links on *Twitter* Lead to Bitcoin Mining." http://blog.trendmicro.com/malicious-links-on-twitter-lead-to-bitcoin-mining/ (Retrieved October 2011).
- Ryan Shrout. (July 13, 2011). *PC Perspective.* "Bitcoin Mining Update: Power Usage Costs Across the United States." http://www.pcper.com/reviews/Graphics-Cards/Bitcoin-Mining-Update-Power-Usage-Costs-Across-United-States (Retrieved October 2011).
- Satoshi Nakamoto. *Bitcoin. "Bitcoin:* A Peer-to-Peer Electronic Cash System." http://bitcoin.org/bitcoin.pdf (Retrieved October 2011).
- Trend Micro, Incorporated. (September 8, 2011). *Threat Encyclopedia.* "HKTL_BITCOINMINE." http://about-threats.trendmicro.com/malware.aspx?language=us&name=HKTL_BITCOINMINE (Retrieved October 2011).
- Trend Micro, Incorporated. (September 2, 2011). *Threat Encyclopedia.* "BKDR_BTMINE.MNR." http://about-threats.trendmicro.com/malware.aspx?language=us&name=BKDR_BTMINE.MNR (Retrieved October 2011).
- Trend Micro, Incorporated. (September 1, 2011). *Threat Encyclopedia.* "BKDR_BTMINE.DDOS." http://about-threats.trendmicro.com/Malware.aspx?language=us&name=BKDR_BTMINE.DDOS (Retrieved October 2011).
- Trend Micro, Incorporated. (July 26, 2011). *Threat Encyclopedia.* "WORM_KOLAB.SMQX." http://about-threats.trendmicro.com/malware.aspx?language=us&name=WORM_KOLAB.SMQX (Retrieved October 2011).