Special delivery: Cybercriminals use pirated software to secretly infect PCs for cryptocurrency mining

Kaspersky Lab researchers have identified a fraud scheme where mining software was distributed and secretly installed on users' PCs through pirated software commonly used for work and entertainment, such as photo and text editors, etc. The PCs were then exploited for the creation of cryptocurrencies, with all profits going to the criminals involved.

While the cryptocurrency market continues to burst with enormous increases in the number and value of investments, more and more criminals are also keeping an eye on its development. The fact that this excitement has captured so many people plays into their hands, making it easier to cheat general users who are not IT-savvy individuals. For instance, cryptocurrency miners became one of the major trends in 2017, according to the annual Kaspersky Security Bulletin. This trend was predicted last year by Kaspersky Lab researchers who spotted a comeback of mining software amid the growing popularity of Zcash. Just a year later, miners are everywhere. Criminals are using different tools and techniques, such as social engineering campaigns or by exploiting cracked software, in order to affect as many PCs as possible.

As an example of the latter fraud method, Kaspersky Lab experts have recently discovered a number of similar websites offering ways for users to download free pirated software – popular computer programs and applications. To inspire confidence, criminals have been using domain names similar to the real ones. After downloading a piece of software, the user receives an archive that also contains a mining program. This is then installed automatically, together with the desired software. The installation archive includes text files containing initialization information – wallet and mining pool addresses. A mining pool is a server that unites several participants and distributes the mining task among their computers. In exchange, participants receive their share of the cryptocurrency that is being mined much faster than they would if mining through only their own PC. Because of architectural particularities, mining Bitcoins and other cryptocurrencies is currently a very resource-heavy and time-consuming operation, so such pools significantly increase the productivity and speed of cryptocurrency generation.

After being installed, miners start to silently operate on the victim's PC, generating crypto-coins for criminals. According to Kaspersky Lab research, in all cases they used the NiceHash project software, which recently suffered a major cybersecurity breach resulting in the theft of millions of dollars' worth of cryptocurrency. Some of the victims were connected to a mining pool of the same name.

In addition, experts have found that some miners contained a special feature that allowed the user to remotely change a wallet number, pool or miner. This means criminals could set another destination for the cryptocurrency at any time and thus manage their earnings by distributing mining flows between wallets, or even make the victim's computer work for another mining pool.

"Although not considered malicious, mining software reduces the device's system performance, which inevitably affects the user experience in general. Plus, it increases the victim's electricity bill – not a major outcome of being a victim of this fraud scheme, but still an unpleasant one. Of course, some people might be OK with the knowledge that an anonymous person is becoming richer at their expense, but we advise users to resist these attempts as even though it is not being conducted with standard malicious software, it is still a fraudulent activity," says Alexander Kolesnikov, Malware

Analyst at Kaspersky Lab.
In order to prevent your PC from becoming part of a mining network, Kaspersky Lab advises the following:
• Download only legal software from proven sources,
• Install a reliable security solution such as Kaspersky Internet Security or Kaspersky Free that protects you from all possible threats, including malicious mining software.