Discovery of Trojan scattering steals virtual money through YouTube

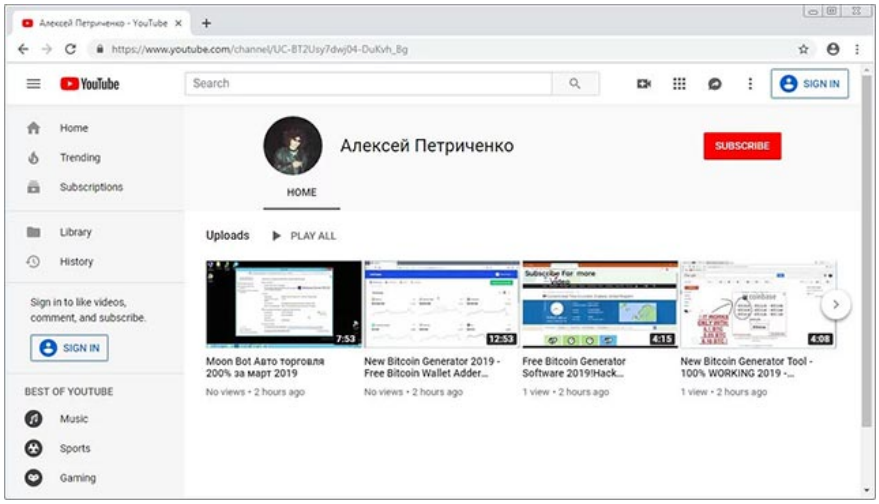
A phishing campaign and malware transmission are being conducted through YouTube.

A phishing campaign and malware transmission are being conducted through YouTube. This form of attack may sound new, but if considered carefully, this is just a method to trick victims into providing personal information or accessing malicious links. Specifically, crooks will post videos to promote the "bitcoin creation" tool, promising to make bitcoin free for users. In fact, this scam is pushing the release of information-stealing Trojan (spyware) hijacking called Qulab.

1. Hacker attacks a US city demanding $ 100,000 ransom with Bitcoin

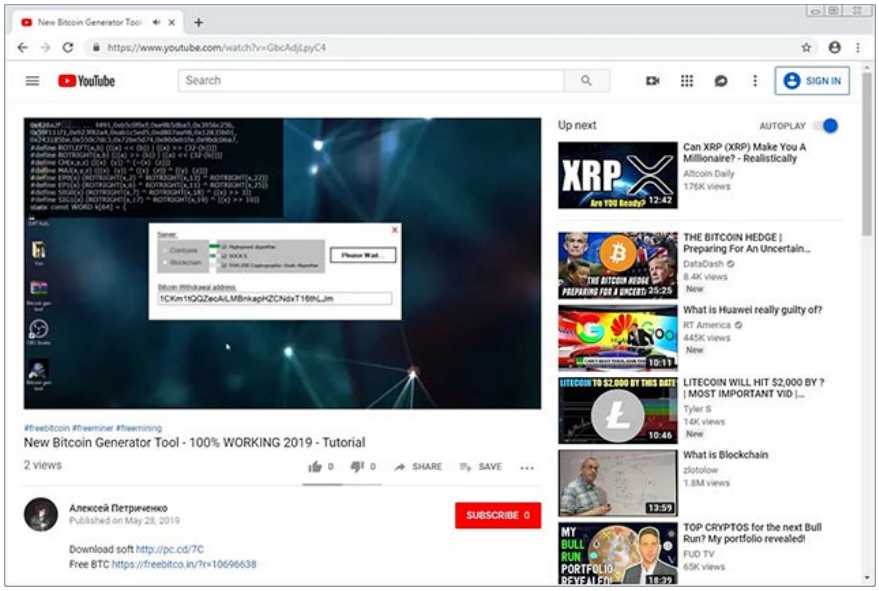
In a recent interview with the technology website BleepingComputer, Frost security researchers, who discovered a phishing campaign, said they tracked all of the campaign's activities over the past 15 days. Every time the Frost team reports a mistake against phishing videos and video upload accounts, YouTube will quickly remove them. However, this approach seems a bit passive and not very effective because the guys constantly create new accounts and reup and upload new malicious videos.

More clearly about how this phishing campaign works: First, the crook posted a series of promotional videos for the tool called "bitcoin creator tool" for free on YouTube, hitting psychology. curious of users who do not have much knowledge about virtual money market and security.

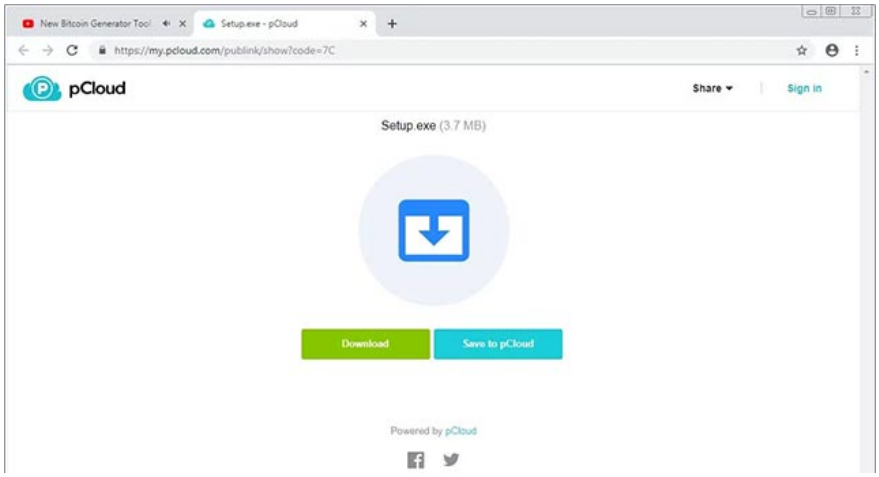


1. The cybersecurity tools that every business should know

Just below, in the video description, crooks will provide links to download this tool. However, this is actually a Trojan as well as a malicious link, directing users to the address https://freebitco.in as shown below.



When users click on the download link provided in the description of these videos, they will be taken to a website, providing the file called Setup.exe.



1. Hacker earned $ 32,000 in 7 weeks by fixing a series of gaps in e-money projects

If the victim clicks the download button and runs the Setup.exe file, it means that the Qulab Trojan will be installed on their computer.

Payload of Qulab spyware

In this phishing campaign, the distributed payload is the Trojan that hijacked information and hijacked the control named Qulab. When executed, the Trojan will copy itself to the% AppData% amd64_microsoft-windows-netio-infrastructuremsaudite.module.exe file, and launch itself from this location.

According to experts from Fumko forum, after being successfully installed on the target system, Qulab will try to steal browser history, save browser information, browser cookies, login information. saved in FileZilla, Discord login information and even Steam login information. At the same time, the Trojan also contains malicious code designed to steal .txt, .maFile and .wallet files from infected computers.

Finally, Qulab will also act as a clipboard, or clipper attacker, meaning that it will monitor Windows clipboard for certain data and when it finds the data to collect, it will proceed. Swap with different data that the attacker targets.

1. A very large black web market has just been destroyed

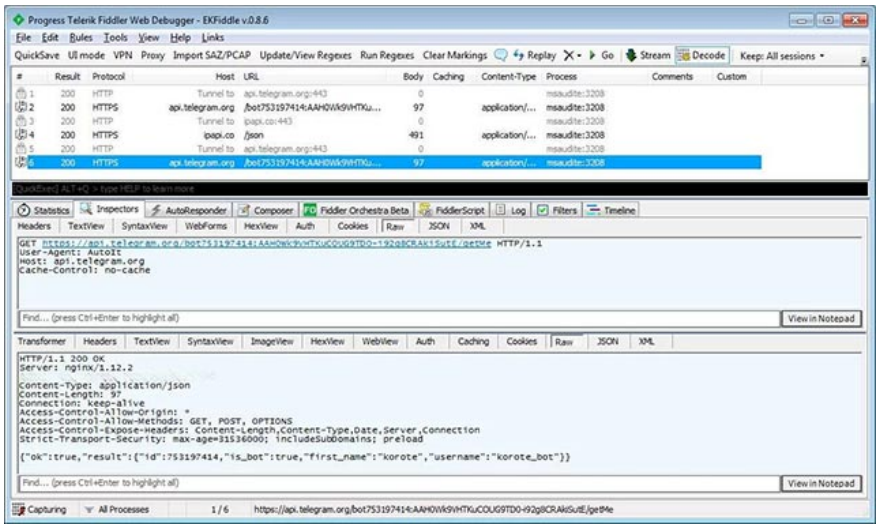
In this particular case, Qulab is searching for the electronic money addresses that have been copied into the Clipboard. In many cases, Qulab can identify the address that the user transfers money to and exchange that address with another address under the attacker's control.

In fact, electronic money addresses are extremely long and difficult to remember, so many users cannot remember how they copied the clipboard. Thus, when Qulab swapped the initial deposit address to the attacker's malicious address, the user didn't even know it. This simple but extremely effective attack method allows an attacker to steal electronic money by tricking users into sending money to their addresses quickly.

According to Fumko, Qulab will only support the following electronic currency addresses for the clipper component:

Bitcoin Bitcoin Cash Bitcoin Gold Bytecoin Cardano Lisk Dash Doge Electron Ethereum Graft Litecoin Monero Neo QIWI Qtum Steam Trade Link Stratis VIA WME WMR WMU WMX WMZ Waves Yandex Money ZCash

When compiling stolen data, the Trojan sends it to the attacker using Telegram as shown below:



1. The alarming increase in the number of attacks targeted at IoT devices

If you believe that your system has been infected with this Trojan, immediately change all passwords for any financial account and website you visit. On the other hand, you should also use more password managers to create strong and unique passwords for every important access account.