OnionPoison: Infected Tor Browser distribution via YouTube gives new meaning to "going viral"

Kaspersky researchers have recently uncovered an ongoing malicious campaign, which they have dubbed 'OnionPoison', that is being distributed via a YouTube channel with more than 180,000 subscribers. Cybercriminals spread malware to collect users' personal data and obtain full control over the victim's computer by placing a link to an infected version of Tor Browser in the description bar of a video about Darknet.

Kaspersky researchers identified multiple cases of infections via malicious Tor Browser installers spread through an explanatory video about Darknet on YouTube. This channel has more than 180,000 subscribers, while the view count on the video with the malicious link exceeds 64,000.

Supplied image: Screenshot of the video with a link to the malicious Tor Browser installer in the description section

Most of the affected users were from China. As the Tor Browser website is blocked in China, individuals from this country often resort to downloading Tor from third-party websites. And cybercriminals are keen on spreading their malicious activity via such resources.

The analysed version Tor Browser is configured to be less private than the original Tor - it stores browsing history and all the data users enter into website forms. Additionally, it distributes spyware to collect various personal data and send it to the attackers' server. Curiously, unlike many other stealers, OnionPoison does not seem to show a particular interest in collecting users' passwords or wallets. Instead, it tends to be more interested in gathering victims' identifying information which can be used to track down the victims' identities, such as browsing histories, social network account IDs and Wi-Fi networks.

This fact is concerning since the risks are moving from digital to real life. The attackers can gather information on the victim's personal life, family or home address. Additionally, there are cases when the attacker used the obtained information to blackmail the victim.

The spyware also provides the functionality to execute shell commands on the victim's device.

YouTube comments become new tool for scammers

6 Jul 2022

"Today we witness how video content is replacing texts, while video platforms are more often used as search engines. Cybercriminals are well aware of the current web consumption trends, hence they started to distribute malware on popular video platforms. This trend will stay with us for some time, that is why we highly recommend installing a reliable security solution to stay protected against all potential threats," comments Georgy Kucherin, a security expert at Kaspersky.

To reduce the risks of becoming a victim of a similar malicious campaign, do not download software from suspicious third-party websites. If using official websites is not an option for you, it is possible to verify the authenticity of installers downloaded from third-party sources by examining their digital signatures. A legitimate installer should have a valid signature, and the company name specified in its certificate should match the name of the software developer.

Learn more about OnionPoison on Securelist.com.