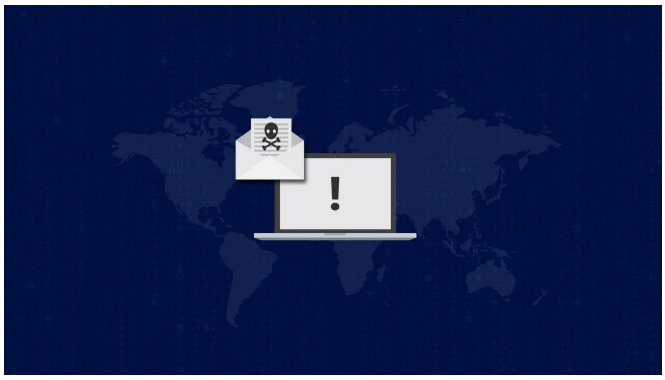
Virobot: How to say your PC is toast, in French?

24 September 2018, by Nancy Owano



Credit: CC0 Public Domain

A ransomware-flavored Virobot with keylogger capabilities was found to be capable of enslaving personal computers in a botnet, reported a number of sites including *HotHardware*. It was affecting targets in the United States.

It not only locks up the computers it infects but enlists them as part of a botnet. Brandon Hill's report on Friday described victimized computers placed in a kind of zombie botnet with a ransomware component, no less.

An infected user's computer sees the ransom note displayed, said Hill, "but even though Virobot has primarily affected users the United States, it's written in French."

How much does it ask for? Alfred Ng in CNET said the note demanded "around $520 in bitcoin."

Hill in *HotHardware* said a "multipronged" attack vector was at work. Ng in CNET also said the malware certainly was not "letting any part of an infected computer go to waste." CNET said the Virobot infects devices and then forces them to spread malware via email.

Mischief with your e-mail? Hill said the Virobot "can also take full control over Microsoft Outlook to join in on an email spamming campaign." Ng said the email has a copy of Virobot in hopes to spread the malware.

Sergiu Gatlan discussed this in *Softpedia*: The infected e-mails are sent to the victim's Outlook contact list, containing a copy of the malware or a link to a payload file downloaded on the target machine when the spam message is opened.

Who spotted it? Reports said researchers at Trend Micro did, earlier this month. The Trend Micro blog stepped readers through what happens and how. Not that it came as a shock to spot ransomware still rearing its head in 2018.

"We've predicted that ransomware attacks will plateau in 2017 but will diversify in terms of attack methods as time progresses," the company wrote in its blog of September 21. "Ransomware activity in the first half of 2018 proved this to be true, with more innovative methods to raise the ante."

They said Virobot detected by Trend Micro was a case in point, observed with both ransomware and botnet capabilities.

"Once Virobot is downloaded to a machine, it will check the presence of registry keys (machine GUID and product key) to determine if the system should be encrypted. The ransomware then generates an encryption and decryption key via a cryptographic Random Number Generator. Together with the generated key, Virobot will then send the machine-gathered data to its C&C server via POST."

Virobot starts the encryption process and after that comes the display of a ransom note ("Vos fichiers personnels ont été chiffré.").

The good news: Virobot's C&C server has been taken offline, wrote Hill. The ransomware is no

longer able to encrypt files. At the moment, Virobot's command-and-control (C&C) server has been shut down," said Gatlan in *Softpedia*, "and the malware will not be able to successfully encrypt infected systems until the threat actors who designed it will switch to a new one."

Hah. That brings us to the bad news: Gatlan said that "the malware will not be able to successfully encrypt infected systems until the threat actors who designed it will switch to a new one." Until the actors switch to a new...worth repeating?

Hill had a similar remark to make in his article, saying "there's no way of knowing if other Virobot mutations will start propagating in the coming days and weeks."

More information:
blog.trendmicro.com/trendlabs- … lity-breaks-through/

APA citation: Virobot: How to say your PC is toast, in French? (2018, September 24) retrieved 3 December 2021 from https://techxplore.com/news/2018-09-virobot-pc-toast-french.html