

CYBER BITS

Sefnit and Click Fraud

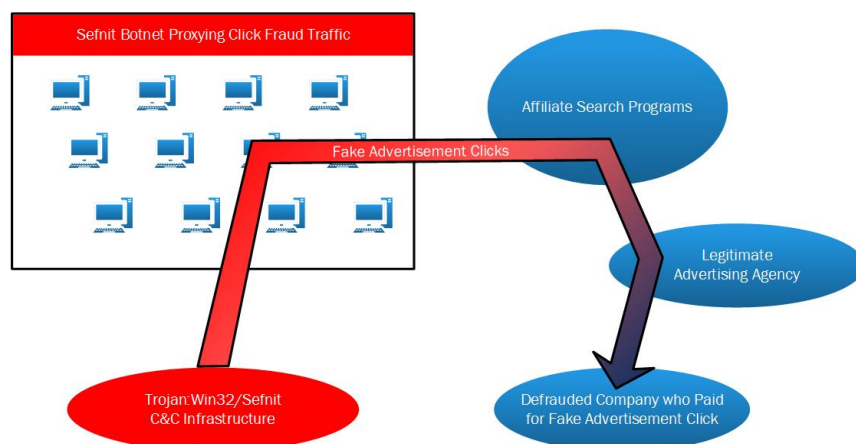
What happened?

Sefnit is a Trojan malware also known as **Mevade**. It was spotted for the first time in 2010 but since mid-2013 a new version appeared, different from the previous ones. The malware is used mainly for click-fraud and to a lesser extent for bitcoin mining; as a backdoor and for downloading other files.

Sefnit malware is considered one of the most active Trojans, targeting Microsoft computers. According to Microsoft's Security Intelligence Report the Sefnit malware relies on two other pieces of software which appeared legitimate ("Rotbrow" and "Brantall") in order to infect the victim's computers¹.

How does it work?

The malware gets installed on the victim's computer through different methods such as eMule peer-to-peer file network, installation of apparently legitimate software such as Rotbrow, Brantall, File Vault.



Once installed the infected computer becomes part of the Sefnit Botnet and starts sending HTTP traffic containing fake advertisement clicks. What follows is called "pay-per-click". The clicks are counted and paid by the company who requested the advertisement to the legitimate advertisement agency.

¹ <http://www.microsoft.com/security/sir/default.aspx>

CYBER BITS

The advertisement agency relies on a system of affiliates. The actors behind Sefnit are part of this affiliate system and get paid for the fake clicks through the advertisement agency.

Why do you need to know?

- The Sefnit Botnet caused a sudden spike on Tor network in August - September 2013 because its C&C server was configured as a Tor's hidden service. According to Facebook researchers, in April 2014 the Botnet switched from Tor C&C to using a SSH (Secure Shell) connection with it's C&C².
- According to a blog.trendmicro.com article from September 2013 the actors behind Sefnit are from Kharkov, Ukraine and Israel and are known using the monikers "Scorpion" and "Dekadent".
- Click fraud is a method used by botnet herders to make profits with less visibility and risk. The fact that the victim is a company which pays for advertising (practically pays to have persons accessing their websites) reduces the risk of the suspects of becoming the subject of a complaint. Usually, the company doesn't find out that the computer is actually infected and acts based on a command received from the Command and Control server. Use of a botnet bypasses traditional countermeasures which detect overactive IP addresses.
- Other examples of Click Fraud Botnets are ZeroAccess or Chameleon.

2

EC3 would welcome reactions on this note. Please mail to O31@europol.europa.eu.

(note that the "O" is a letter and not a number)

²<http://www.pcworld.com/article/2149220/sefnit-click-fraud-malware-drops-tor-for-ssh-facebook-researchers-say.html>