Advanced Notification of Avalanche (crimeware-as-a-service infrastructure)

Security Advisory AE-Advisory 16-044

Criticality High

Advisory Released On 5 December 2016

Impact

- Theft of user credentials and other sensitive data such as credit card information
- Encrypt user files and demand a ransom be paid for regaining access to those files
- Creates a botnet from infected systems that will conduct DDoS attacks

Solution

Refer to the “Solution” section below

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about Avalanche. “Avalanche” refers to a large global network hosting infrastructure used by cyber criminals to conduct phishing and malware distribution campaigns and money mule schemes. It is said that the Avalanche botnet was destroyed on the 30th of November 2016 at the end of a four year project. However, there might be systems that are still infected and so, further information is explained in the “Threat Details” section below.

Threat Details

Attackers utilized Avalanche botnet infrastructure to host and distribute a variety of malware variants to victims. These victims may have had their personal information stolen (user credentials, banking credit card information and so on). These victims' systems may also have been used to conduct other malicious activity, such as launching denial-of-service (DoS) attacks or distributing malware variants to other victims' systems. Avalanche used fast-flux DNS (a technique to hide the attacker servers, behind a constantly changing network of compromised systems acting as proxies). Avalanche was found to use the following malware families:

- Windows-encryption Trojan horse (WVT) (aka Matsnu, Injector,Rannoh,Ransomlock.P)
- URLzone (aka Bebloh)
- Citadel
- VM-ZeuS (aka KINS)
- Bugat (aka Feodo, Geodo, Cridex, Dridex, Emotet)
- newGOZ (aka GameOverZeuS)
- Tinba (aka TinyBanker)
- Nymaim/GozNym
- Vawtrak (aka Neverquest)
- Marcher
- Pandabanker
- Ranbyus
- Smart App
- TeslaCrypt
- Trusteer App
- Xswkit

Avalanche was also used as a fast flux botnet which provides communication infrastructure for other botnets including the following:

- TeslaCrypt
- Nymaim
- Corebot
- GetTiny
- Matsnu
- Rovnix
- Urlzone
- QakBot (aka Qbot, PinkSlip Bot)

Refer to the "Solution" section below if you believe you have been infected and also, prevent your system from being infected with malware.

Solution

- Use and maintain anti-virus software - Anti-virus software recognizes and protects your computer against most known viruses. Even though parts of Avalanche are designed to evade detection, security companies are continuously updating their software to counter these advanced threats. Therefore, it is important to keep your anti-virus software up-to-date. If you suspect you may be a victim of an Avalanche malware, update your anti-virus software definitions and run a full-system scan.

- Avoid clicking links in emails – You may be a victim of a phishing website claiming to be a legitimate one, make sure that you see the hyperlink before you are obliged to click on a link in an email.

- Change your passwords – Your original passwords may have been compromised during the infection, it is recommended that you change the passwords.

- Keep your operating system and application software up-to-date – Install software patches so that attackers cannot take advantage of known vulnerabilities. Enable automatic updates of the operating system if this option is available for you.

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae