Avalanche (crimeware-as-a-service infrastructure)

us-cert.gov/ncas/alerts/TA16-336A

Systems Affected

Microsoft Windows

Overview

“Avalanche” refers to a large global network hosting infrastructure used by cyber criminals to conduct phishing and malware distribution campaigns and money mule schemes. The United States Department of Homeland Security (DHS), in collaboration with the Federal Bureau of Investigation (FBI), is releasing this Technical Alert to provide further information about Avalanche.

Description

Cyber criminals utilized Avalanche botnet infrastructure to host and distribute a variety of malware variants to victims, including the targeting of over 40 major financial institutions. Victims may have had their sensitive personal information stolen (e.g., user account credentials). Victims’ compromised 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’ computers.

In addition, Avalanche infrastructure was used to run money mule schemes where criminals recruited people to commit fraud involving transporting and laundering stolen money or merchandise.

Avalanche used fast-flux DNS, a technique to hide the criminal servers, behind a constantly changing network of compromised systems acting as proxies.

The following malware families were hosted on the infrastructure:

- 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
- iBanking Trusteer App Trojan
- 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)

Impact

A system infected with Avalanche-associated malware may be subject to malicious activity including the theft of user credentials and other sensitive data, such as banking and credit card information. Some of the malware had the capability to encrypt user files and demand a ransom be paid by the victim to regain access to those files. In addition, the malware may have allowed criminals unauthorized remote access to the infected computer. Infected systems could have been used to conduct distributed denial-of-service (DDoS) attacks.

Solution

Users are advised to take the following actions to remediate malware infections associated with Avalanche:

- *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. (See Understanding Anti-Virus Software for more information.)
- *Avoid clicking links in email* – Attackers have become very skilled at making phishing emails look legitimate. Users should ensure the link is legitimate by typing the link into a new browser (see Avoiding Social Engineering and Phishing Attacks for more information).

- *Change your passwords* – Your original passwords may have been compromised during the infection, so you should change them. (See Choosing and Protecting Passwords for more information.)
- *Keep your operating system and application software up-to-date* – Install software patches so that attackers cannot take advantage of known problems or vulnerabilities. You should enable automatic updates of the operating system if this option is available. (See Understanding Patches for more information.)
- *Use anti-malware tools* – Using a legitimate program that identifies and removes malware can help eliminate an infection. Users can consider employing a remediation tool. A non-exhaustive list of examples is provided below. The U.S. Government does not endorse or support any particular product or vendor.

ESET Online Scanner

https://www.eset.com/us/online-scanner/

F-Secure

https://www.f-secure.com/en/web/home_global/online-scanner

McAfee Stinger

http://www.mcafee.com/us/downloads/free-tools/index.aspx

Microsoft Safety Scanner

https://www.microsoft.com/security/scanner/en-us/default.aspx

Norton Power Eraser

https://norton.com/npe

Trend Micro HouseCall

http://housecall.trendmicro.com/

References

Revisions

December 1, 2016: Initial release

December 2, 2016: Added TrendMicro Scanner

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.