Systems Affected

Microsoft Windows

Overview

The Simda botnet – a network of computers infected with self-propagating malware – has compromised more than 770,000 computers worldwide [1(link is external)].

The United States Department of Homeland Security (DHS), in collaboration with Interpol and the Federal Bureau of Investigation (FBI), has released this Technical Alert to provide further information about the Simda botnet, along with prevention and mitigation recommendations.

Description

Since 2009, cyber criminals have been targeting computers with unpatched software and compromising them with Simda malware [2(link is external)]. This malware may re-route a user's Internet traffic to websites under criminal control or can be used to install additional malware.

The malicious actors control the network of compromised systems (botnet) through backdoors, giving them remote access to carry out additional attacks or to "sell" control of the botnet to other criminals [1(link is external)]. The backdoors also morph their presence every few hours, allowing low anti-virus detection rates and the means for stealthy operation [3(link is external)].

Impact

A system infected with Simda may allow cyber criminals to harvest user credentials, including banking information; install additional malware; or cause other malicious attacks. The breadth of infected systems allows Simda operators flexibility to load custom features tailored to individual targets.

Solution

Users are recommended to take the following actions to remediate Simda infections:

- *Use and maintain anti-virus software* - Anti-virus software recognizes and protects your computer against most known viruses. It is important to keep your anti-virus software up-to-date (see Understanding Anti-Virus Software 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. Many operating systems offer automatic updates. If this option is available, you should enable it (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 (examples below) that will help with the removal of Simda from your system.
  Kaspersky Lab : http://www.kaspersky.com/security-scan(link is external)
  Microsoft: http://www.microsoft.com/security/scanner/en-us/default.aspx(link is external)
  Trend Micro: http://housecall.trendmicro.com/(link is external)
- *Check to see if your system is infected* – The link below offers a simplified check for beginners and a manual check for experts.
  Cyber Defense Institute: http://www.cyberdefense.jp/simda/(link is external)

The above are examples only and do not constitute an exhaustive list. The U.S. government does not endorse or support any particular product or vendor.

References

- [1] INTERPOL Coordinates Global Operation to Take Down Simda Botnet(link is external)
- [2] Microsoft partners with Interpol, industry to disrupt global malware attack affecting more than 770,000 PCs in past six mo(link is external)
- [3] Botnet that Enslaved 770,000 PCs Worldwide Comes Crashing Down(link is external)

Revisions

- April 15, 2015: Initial Release