GameOver Zeus P2P Malware | CISA

Published: 2016-09-30 · Archived: 2026-04-05 20:12:54 UTC

Systems Affected

- Microsoft Windows 95, 98, Me, 2000, XP, Vista, 7, and 8
- Microsoft Server 2003, Server 2008, Server 2008 R2, and Server 2012

Overview

GameOver Zeus (GOZ), a peer-to-peer (P2P) variant of the Zeus family of bank credential-stealing malware identified in September 2011, [1] uses a decentralized network infrastructure of compromised personal computers and web servers to execute command-and-control. The United States Department of Homeland Security (DHS), in collaboration with the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ), is releasing this Technical Alert to provide further information about the GameOver Zeus botnet.

GOZ, which is often propagated through spam and phishing messages, is primarily used by cybercriminals to harvest banking information, such as login credentials, from a victim's computer. [2] Infected systems can also be used to engage in other malicious activities, such as sending spam or participating in distributed denial-of-service (DDoS) attacks.

Prior variants of the Zeus malware utilized a centralized command and control (C2) botnet infrastructure to execute commands. Centralized C2 servers are routinely tracked and blocked by the security community. [1] GOZ, however, utilizes a P2P network of infected hosts to communicate and distribute data, and employs encryption to evade detection. These peers act as a massive proxy network that is used to propagate binary updates, distribute configuration files, and to send stolen data. [3] Without a single point of failure, the resiliency of GOZ's P2P infrastructure makes takedown efforts more difficult. [1]

Impact

A system infected with GOZ may be employed to send spam, participate in DDoS attacks, and harvest users' credentials for online services, including banking services.

Solution

Users are recommended to take the following actions to remediate GOZ 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 can't 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 GOZ from your system.

F-Secure

https://www.f-secure.com/en/web/home_global/online-scanner (Windows Vista, 7 and 8)

https://www.f-secure.com/en/web/labs_global/removal-tools/-/carousel/view/142 (Windows XP)

Heimdal

http://goz.heimdalsecurity.com/ (Microsoft Windows XP, Vista, 7, 8 and 8.1)

McAfee

www.mcafee.com/stinger (Windows XP SP2, 2003 SP2, Vista SP1, 2008, 7 and 8)

Microsoft

https://www.microsoft.com/security/scanner/en-us/default.aspx (Windows 8.1, Windows 8, Windows 7, Windows Vista, and Windows XP)

Sophos

https://www.sophos.com/VirusRemoval (Windows XP (SP2) and above)

Symantec

https://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network (Windows XP, Windows Vista and Windows 7)

Trend Micro

https://www.trendmicro.com/threatdetector (Windows XP, Windows Vista, Windows 7, Windows 8/8.1, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2)

FireEye and Fox-IT

www.decryptcryptolocker.com

FireEye and Fox-IT have created a web portal claiming to restore/decrypt files of CryptoLocker victims. US-CERT has performed no evaluation of this claim, but is providing a link to enable individuals to make their own

determination of suitability for their needs. At present, US-CERT is not aware of any other product that claims similar functionality.

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.

- GOZ has been associated with the CryptoLocker malware. For more information on this malware, please visit the CryptoLocker Ransomware Infections page.been associated with the Cryptolocker malware, for more information on that malware, please visit https://www.us-cert.gov/ncas/alerts/TA13-309A.

References

[1] Highly Resilient Peer-to-Peer Botnets Are Here: An Analysis of Gameover Zeus

[3] The Lifecycle of Peer-to-Peer (Gameover) ZeuS

Revisions

Initial Publication - June 2, 2014|Added McAfee - June 6, 2014|Added FireEye and Fox-IT web portal to Solutions section - August 15, 2014
