WIKIPEDIA

Form grabbing

Form grabbing is a form of malware that works by retrieving authorization and log-in credentials from a web data form before it is passed over the Internet to a secure server. This allows the malware to avoid HTTPS encryption. This method is more effective than keylogger software because it will acquire the user's credentials even if they are input using virtual keyboard, auto-fill, or copy and paste.[1] It can then sort the information based on its variable names, such as email, account name, and password. Additionally, the form grabber will log the URL and title of the website the data was gathered from.[2]

Contents

History

The method was invented in 2003 by the developer of a variant of a trojan horse called Downloader.Barbew, which attempts to download Backdoor.Barbew from the Internet and bring it over to the local system for execution. However, it was not popularized as a well known type of malware attack until the emergence of the infamous banking trojan Zeus in 2007.[3] Zeus was used to steal banking information by man-in-the-browser keystroke logging and form grabbing. Like Zeus, the Barbew trojan was initially spammed to large numbers of individuals through e-mails masquerading as big-name banking companies.[4] Form grabbing as a method first advanced through iterations of Zeus that allowed the module to not only detect the grabbed form data but to also determine how useful the information taken was. In later versions, the form grabber was also privy to the website where the actual data was submitted, leaving sensitive information more vulnerable than before.[5]

Known occurrences

A trojan known as Tinba (Tiny Banker Trojan) has been built with form grabbing and is able to steal online banking credentials and was first discovered in 2012. Another program called Weyland-Yutani BOT was the first software designed to attack the macOS platform and can work on Firefox. The web injects templates in Weyland-Yutani BOT were different from existing ones such as Zeus and SpyEye.[6]

Countermeasures

Due to the recent increase in keylogging and form grabbing, antivirus companies are adding additional protection to counter the efforts of key-loggers and prevent collecting passwords. These efforts have taken different forms varying from antivirus companies, such as safepay, password manager, and others.[1] To further counter form grabbing, users' privileges can become limited which would prevent them from installing Browser Helper Objects (BHOs) and other form grabbing software. Administrators should create a list of malicious servers to their firewalls.[2]

See also

- Keystroke logging
- Malware
- Trojan horse
- Web security exploits
- Computer insecurity
- Internet privacy
- Tiny Banker Trojan

References

1. "Capturing Online Passwords and Antivirus." (http://blogs.secure-bits.com/?cat=22) Web log post. Business Information Technology Services, 24 July 2013.
2. Graham, James, Richard Howard, and Ryan Olson. Cyber Security Essentials. Auerbach Publications, 2011. Print.
3. *Shevchenko, Sergei. "Downloader.Berbew." (http://www.symantec.com/security_response/writeup.jsp?docid=2003-071612-0251-99) Symantec, 13 Feb. 2007.
4. *Abrams, Lawrence. "CryptoLocker Ransomware Information Guide and FAQ." (http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information) Bleeding Computers. 20 Dec. 2013.
5. *"Form Grabbing." (https://ritcyberselfdefense.wordpress.com/tag/form-grabbing/) Web log post. Rochester Institute of Technology, 10 Sept. 2011.
6. Kruse, Peter. "Crimekit for MacOSX Launched." (https://www.csis.dk/en/csis/blog/3195/) Web log post. Canadian Security Intelligence Service, 02 May 2011.