University of Texas at Austin Cyber Security Bootcamp

Kenyetta Ipyana and Megan Wilson

Taught by Professor’s: Dan Schmidt and Matt Hales

Zbot/Zeus Malware Analysis

Zbot/Zeus Malware Analysis

This essay will discuss the overview of Zbot/Zeus, the threat exposes, containment practices, and awareness training to prevent those from spreading the virus.

**Overview of Zbot/Zeus**

Zbot/Zeus is a banking trojan that affects Windows operating systems “to steal confidential information from the compromised computer” (Symantec, 2016) and utilize the stolen information to exploit personal data. It was first discovered in 2008 by security researchers but was created in 2006 allegedly by Evgeniy Mikhailovich Bogachev (AKA Slavik, lucky12345). Born on October 28, 1983, Bogachev is wanted by the FBI for allegedly for creating and selling Zeus and “participating in a major cyber racketeering enterprise” (U.S. Department of State, n.d.). He started off by selling Zeus on the black market and would consistently update the software. However, in late 2009 he constructed a cybercriminal group with the program named Jabber Zeus (Graff, 2017). This program would come with a form of Zeus toolkit alongside a messenger allowing members to communicate and plan attacks. From there, Bogachev started narrowing his business to cyber-crime organizations before retiring unexpectedly in 2010. He placed a modern version of Zeus on the market that sold for $10,000 per download and to this day, he has been uncaptured. He is mentioned to be on the run in a boat along the Black Sea, and his program, however, affects many users and companies today. This program is extremely complex but maintains a standard way of infecting the computer.

**Threat Expose**

Zbot/Zeus is a builder and it created malware for hackers to exploit their victims. The highly customizable malware does a variety of tasks to help the attacker gain information and holds some exceedingly established trends in Zbot/Zeus. For example, most of the file types for the Zbot/Zeus virus are .exe and the file sizes can range anywhere from 113.5 kb to 244.00 kb. While the program started in 2006, the usage of the program spiked in 2009 when rapid releases of the updates trojan began populating almost monthly. When the builder is installed, it can generate a bot executable and web server files like PHP images, and SQL templates to use as the C&C server. When the trojan has corrupted the system, the bot will send a GET request to the C&C server to retrieve the configuration file and from there change the file %system32%\sdra64.exe. When the trojan sends a DNS request, the attacker will change the IP address of the target to whatever the attacker has in mind. However, because of these changes, Zbot/Zeus can be detected in antivirus software as a Generic Trojan, Backdoor, Win32 Trojan, or Zbot but with encryption, or it could be overlooked by the antivirus.

Another back-end change to the system files is in the registry. The Zbot/Zeus trojan will change the registry files including winlogon.exe, increase privileges, inject code and a string table into the processes, and produce a thread to execute the code. This will allow the attacker to include a web page injector on a target webpage and steal other data.

**Containment**

The Zbot/Zeus threat is “comprised of three parts: a toolkit, the authentic Trojan, and the C&C server” (Middleton, 2017), all play a role in how the trojan successfully compromises a system. The toolkit allows the user to edit the rules and configure the attack it performs, the trojan compromises the system, and the C&C server will monitor and control the configured trojan.

When Zbot/Zeus infects the system, it will show very little signs of infection because it implements fast flux. Fast flux allows the botnet “to hide the domains used to download malware or host phishing websites” (Albors, 2017). The concept of fast flux is to have multiple IP addresses designated for a domain and then quickly and constantly altering them. However, to the impact of damage to the system, there is almost no damage; the purpose of the trojan is to allow the attacker to spy on a system not necessarily destroy its contents. Due to the trojan hiding in common Windows files, “only 23% of cases of AV programs” can detect the trojan. Therefore, it is extremely challenging to remove Zbot/Zeus when you are infected. However, once the computer is infected, the attacker can see all data relevant to the target webpages they have set up. For example, if the attackers build the Zbot/Zeus trojan to only attack https://mail.google.com/mail/ and https://www.bankofamerica.com/, the trojan would only activate once the user visits one of those websites. The best solution to preventing this virus from spreading is through common practices and awareness training.

**Awareness Training**

While Zbot/Zeus is a remarkably difficult trojan to identify and remove, to prevent users from getting infected by the trojan, it is significant that the standard practices are followed. All businesses and typical users should consider a firewall that blocks all incoming connections and only allow services that the user or company wants open. Enforce strong password policies to make it difficult for attackers to exploit and ensure there are privilege settings. Check the URL or user safeweb.norton.com to verify if the webpage is safe. Patch the operating system and antivirus to make sure it is up to date with the latest virus trends and removes any bugs or possibilities of exploits. The support team or individual user should schedule regular scans on the system to verify the integrity of the system and search for any possible unauthorized changes to system files. Lastly, employees and users should be trained to not open attachments unless they are expecting them, scan a file before loading the executable, and verify the webpage before clicking it.

**Conclusion**

Zbot/Zeus is a very well designed trojan that has affected users from 2006 up to now and has been constantly updated to make it difficult to track and remove off systems. This trojan can steal any confidential data and connect the system to a botnet without the user knowing. The best way to identify or remove the trojan is through an antivirus scan. Unluckily, this is an extremely smart trojan and it will hide in common windows files and in some cases, people have no idea they are infected. The most reliable form of protection is to follow the basic security steps to prevent users from spreading or infecting their system with the virus. Update the operating system and reimage your system yearly.

# References

Admin. (2016, October 18). *Guide to Zeus Infenctions*. Retrieved December 12, 2019, from iweb: https://kb.iweb.com/hc/en-us/articles/230268468-Guide-to-Zeus-Infections#:~:targetText=In%20June%202009%20security%20company,Cisco%2C%20Amazon%2C%20and%20BusinessWeek.

Albors, J. (2017, January 12). *Fast Flux networks: What are they and how do they work?* Retrieved December 12, 2019, from welivesecurity: https://www.welivesecurity.com/2017/01/12/fast-flux-networks-work/

Graff, G. M. (2017, March 21). *Inside the Hunt for Russia's Most Notorious Hacker*. Retrieved December 12, 2019, from WIRED: https://www.wired.com/2017/03/russian-hacker-spy-botnet/

Middleton, B. (2017). Zeus-2007. In B. Middleton, & T. &. Group (Ed.), *A History of Cyber Security Attacks: 1980 to Present* (1 ed.). Bica Raton, Florida, United States of America: CRC Press. Retrieved December 12, 2019, from https://books.google.com/books?id=AJkuDwAAQBAJ&pg=PT90&lpg=PT90&dq=The+Zeus+threat+is+actually+comprised+of+three+parts&source=bl&ots=whdRfdSFEw&sig=ACfU3U3CJRlDKbwE6CapzZrOAksqAoikAA&hl=en&ppis=\_e&sa=X&ved=2ahUKEwjEhOLww7HmAhUJRa0KHUwFCJAQ6AEwAHoECAsQAQ#

Symantec. (2016, August 16). *Trojan.Zbot*. Retrieved December 12, 2019, from Symantec: https://www.symantec.com/security-center/writeup/:~:targetText=Zbot,-Download%20Removal%20Tool&targetText=Trojan.,and%20updates%20from%20the%20Internet.

U.S. Department of State. (n.d.). *Evgeniy Mikhailovich Bogachev*. Retrieved December 12, 2019, from U.S Department of State: https://www.state.gov/inl-rewards-program/transnational-organized-crime-rewards-program/evgeniy-mikhailovich-bogachev/