Malware Analysis Report:

ZEUS

By:

Anthony Nathan

Denish Gandhi

TJ Livermore

Wayne Badan

Table of Contents

Introduction

At present, technology is changing rapidly and everything with technology is connected to the Internet. With companies inclining more towards technology to provide a seamless customer experience, it opens them up to fraudsters who are looking for that one opportunity to break in. The Banking industry worldwide has seen a recent increase in online attacks due to the digital push around banking.

One such malware that was created is the Zeus trojan also known as Zbot. Zeus is a malware package that is readily available for sale and also traded in underground forums. The package contains a builder that can generate a bot executable and Web Server files (PHP, image files, SQL templates amongst others) for use as the command and control server.

While Zbot is a generic back door that allows full control by an unauthorized remote user, the primary function is financial gain, accomplished by stealing online credentials such as FTP, email, online banking and other passwords.

Once the Zeus trojan is executed, it downloads the configuration file from a predetermined location, then waits for the victim to log in to a particular target that was defined by it's *config*file, which usually comprises a selection of websites, such as banks, and the login URLs.

History

Zeus was first seen in 2007 and was used to steal information from the United States ministry of Transportation, since then Zeus has had a major impact worldwide causing close to USD $100 million in damages.

The Zeus source code was released by its user in 2011 to the public on several website, which attracted other perpetrators to download and modify the code to create several other and complex variants of Zeus. The information stolen on Zeus was traded in the black market for a steep price and since there was a demand for such information it encouraged more perpetrators to use the source code.

The Zeus virus used spam messages and drive-by downloads methods to spread the infection. The virus primarily impacted only windows-based systems. Later there were other variants release that affected android based mobile devices. Even though the Zeus virus has been identified and most security software are able to detect and eliminate the threat from Zeus, it is believed that perpetrators are still developing newer variants based on the Zeus model.

Functionality

There's a reason why Zeus is considered the largest botnet on the internet. It is difficult even for up-to-date security software to detect. Zeus has no problem remaining undetected by smaller security programs which is why a lot of internet security software specifically advertises that they can catch Zeus.

Generally, Zeus functions as a keystroke logger in order to steal banking information, although different variants have specific purposes as well. Zeus is a very versatile malware that can infect computers through man-in-the-browser attacks, form grabbing, malicious spam emails and ads, specifically ones that state your computer has a virus, when in reality your computer is virus-free.

Once infected, Zeus lies dormant until you visit a targeted site. Then Zeus will add additional fields for the user input, stealing personal information. Then the information is often sent to the dark web where it is sold to interested buyers.

Ways to detect Zeus include but isn't limited to pop-up ads showing up on your browser despite being on secure sites, random search engine replaces your home page, web page and system slowdowns, crashes, and other abnormal system behavior.

Variants

1. Game-Over Zeus (GOZ)
    - GOZ was used to distribute Cyptolocker which is a ransomware that stole your personal data then demanded payment for its release.
    - It's a P2P (peer-to-peer) malware extension that connects to a C&C server to send out botnet attacks.
    - GOZ activity was suspended in June 2014 when the FBI intercepted the communication between the C&C servers and Zeus.

2. Zeus-in-the-mobile (ZITMO)
    - ZITMO is the mobile version of Zeus.
    - Initially was created to target Android and Blackberry users.
    - Its main functionality is to use social engineering techniques to steal mobile transaction authorization number (mTan) codes as quick as possible without the user noticing.
    - To attempt cash transactions from a user's bank account, the hacker still needs an mTan code.
    - The mTan code is sent by the bank to the user as a transaction is being made which is intercepted by ZITMO, which then poses as the bank to steal the user's banking information.

3. Terdot
    - One of the newest versions of Zeus. First emerged in 2016.
    - Specifically, was designed to target first-world countries (CAN, USA, UK, GER, AUS).

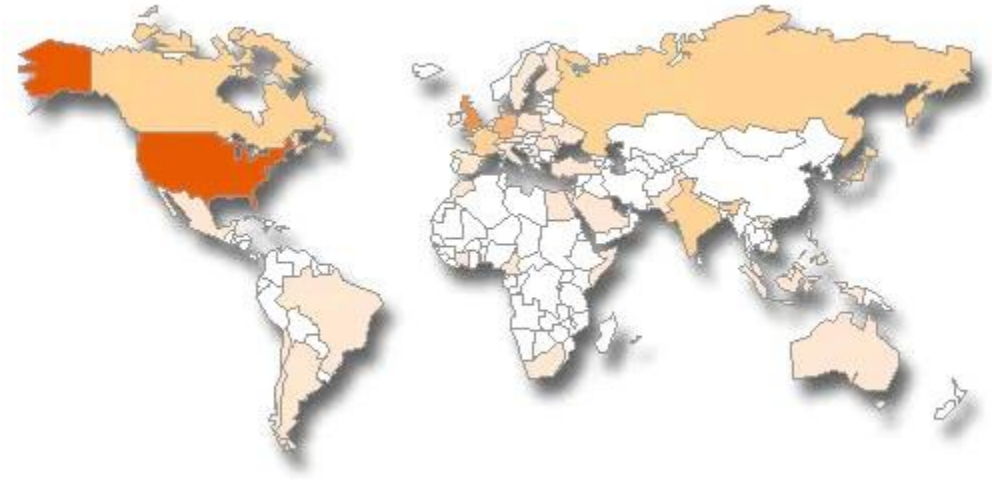
- Terdot affects users through spam emails containing seemingly harmless looking PDF files but once it is clicked on, Zeus starts installing on your computer.
- It injects HTML code into web pages to carry out MITM attacks.
- What makes Terdot so dangerous is that it has automatic update capabilities which means it can evolve constantly with new features.

4. Panda Banker (Zeus Panda)
    - One of, if not the most dangerous variant of Zeus.
    - Panda's primary objective is to steal as many passwords and login credentials as possible in a short amount of time.
    - It is also a relatively newer variant of Zeus.
    - Uses a variety of strategies such as man-in-the-browser attack, keystroke logging, and form grabbing attacks.
    - Zeus Panda launches attack campaigns with a variety of exploits such as drive-by downloads and phishing emails.
    - Most recently, fraudsters were caught trying to inject malicious code to links in Google's top search results' positions.

Impacts

"It is not possible either to trick or escape the mind of Zeus".

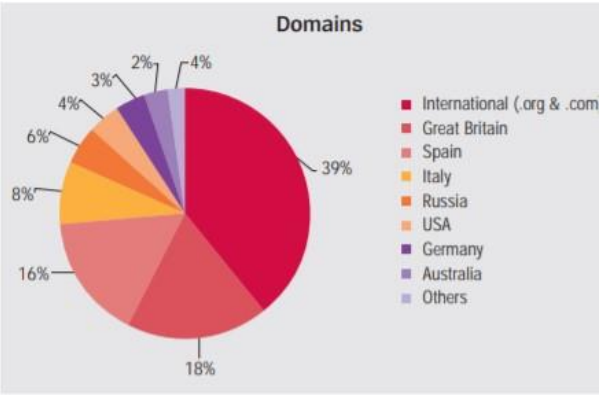
While the Zeus Hesiod is referring to is one mythical legend, it is not a far cry from the undeniable impact of its malware counterpart. As 2010 Zeus still is responsible for 44% of BMI's (Banker Malware Infections) and has infected 90% of fortune 500 companies. The malware's malicious effects have been felt across the globe with its higher concentration areas being the U.S, Canada, Europe, Russia and India.



To date the creator of the Zeus malware Evgeniy Mikhailovich Bogachev still remains at large with a 3 million dollar reward leading to his arrest. An amount that pales in comparison to the damage his God-

like malware has accomplished. According to Jeremy Kirk in 2008 there was a 200 million attempted loss and 70 million actual loss to banking corps. In 2008 the "Rock Phishing Gang" who used Zeus in its attacks cost the banks 100 million. Later in 2010 by means of fraudulent wire transfers $164,000 lost was given to Little & King LLC. These attacks are not limited to big corporations as smaller business and dental practices have also suffered a loss due to this malware. An example of this is when it was used in social media platforms to send out phishing messages infecting the device upon opening the message.

It seems like something out of science fiction that even the likes of NASA also had breaches involving this very malware. Even as technology advances this malware refuses to be left behind.



Consider the lesson learned by IT firm Cynxsure LLC who lost $100,000. While making the transition to two-step authentication by means of fingerprints, Zeus stole the fingerprint data before it was even encrypted. Despite malware detection advancements Zeus damage count sits over 100 million and is climbing.

Endpoint Protection Against Zeus Malware Attack

As the old saying goes – "prevention is better than cure," it is best to stay protected through safe internet practices. Avoid visiting websites that are unknown or suspicious, websites that deal with adult content, illegal downloads or illegal free software. The owners of these websites have no issues letting malware owners host their software on the site.

On the other hand, by simply not clicking on social media messages or links in email, you can stay safe. Treat all messages equally and if the message arrives from a source affiliated with Zeus, chances are the message could pose a possible threat.

Make use of the two-factor authentication, whereby the financial website triggers a confirmation code to be sent to your mobile device and confirm the login is legit. Recently, a few offshoots from Zeus infected smart devices, too. Below are a few tips for individuals and businesses:

For Individual Users:

- Never visit suspicious websites
- Be careful when opening e-mails or attachments from unknown sources.
- Back up your files regularly
- Have the popup blockers always enabled
- Keep your computer OS and antivirus software up-to-date

For Businesses (Corporates):

- Implement stringent controls on privileged accounts
- Have a proper data backup and recovery plan
- Make sure all the corporate-connected devices are up to date

Since the advent of Bring Your Own Device (BYOD), users have been accessing corporate data from outside of the office and through preferred networks. This makes it all the more vulnerable for hackers to infiltrate through the defense systems to steal potential banking details from websites that deal with a lot of online fund transactions, e.g., e-commerce sites, banking sites, online ticket booking sites and so on. A powerful, updated antivirus solution is a must to stay away from such vulnerabilities.

When it comes to the business safety, antivirus products are not a viable option. The ideal way to disarm Zeus malware is to have an advanced endpoint protection system in place.

Advanced Endpoint Protection (AEP) isolates malware (including ransomware) from penetrating your company's local area network at the device layer and executes them in an isolated or restricted system environment. It is the most intelligent endpoint protection solution that offers multiple layers of protection against both known and unknown threats. Basically, the Advanced Endpoint Protection can easily scan the endpoints and remove the malware if it already exists on the device.

AEP offers complete 360-degree protection for the endpoints connected to the corporate network both locally and virtually. It combines numerous security techniques to defend the corporate network and endpoints with complete protection. Some of the robust features include:

Host Intrusion Prevention System (HIPS) – blocks malicious activities by monitoring the behavior of the code.

Containment Technology – This works on Artificial Intelligence and moves the unknown files in a virtual isolated container. This file is later analyzed and the intention of the file is known. It ensures that the users can run programs and applications on their enterprise endpoints; however, the known good applications run as usual while the unknown suspicious files run in the virtual environment.

IT and Security Manager – It is a single console to ensure efficient IT security and device management. It provides a complete report on the status of each device and its level of security.

The Zeus Trojan has infected millions of computers across the globe in a relatively short time. The original creator is no longer running Zeus Malware however, the code is still very much available online to customize per hacker needs.

Conclusion

Zeus is the most significant financial malware created so far and there is little evidence that its impact is fading. Because of its wide distribution, Zeus threatens a broader number of organizations, even outside the financial sector. Zeus attacks are still occurring and may increase as cybercriminals develop more sophisticated concealment and evasion techniques in order to widen infection to many more users across the globe. Already, the transition to hybrid centralized or hybrid decentralized botnets poses obstacles to takedown. We may also anticipate a move to Cloud-based malware. On the positive side, with recent improvements in anti-malware techniques, the impact of Zeus functions may be limited. Of course, we should expect more advanced Zeus versions in due course.

In conjunction with such malware developments, we can expect to see new forms of aggressive attacks, such as water-holing and spear-phishing. As cybercriminals continue to evolve such tactics, security firms must maintain vigilance and strive to combat such attacks through advances in anti-malware software. More directed development of Zeus-based botnets may be linked to state-sponsored attacks, with associated loss of international trust.

Indications are that anonymous and untrustworthy app stores will increase as a source of mobile malware. Ransomware is expected to spread across a wider range of mobile devices, using more sophisticated measures to avoid early detection and a move to new ransom payment methods with the rise in crypto-currencies.

The ready availability of source code and malware kits has helped cybercrooks target mobile platforms but many cybercriminal groups will continue to target traditional platforms, such as PCs. The prevalence of legacy systems, including MS-Windows, Apple Macintosh and Linux, means that vulnerabilities in operating systems will continue to offer opportunities for malware infection.

The Zeus Trojan has come a long way in just a few years, coming out of nowhere to infect millions of computers around the world in a relatively short amount of time. Even though the original creator may not be running the malware any longer, the fact that its code is online and constantly being talked about, updated and improved upon within hacker circles means that it will continue to be a threat for years to come. Understanding that it's out there and taking steps to keep yourself, your finances and your family safe is imperative for anyone who wants to avoid the headache and financial pain of identity theft.

References

Counter Threat Unit™ Research Team. “ZeuS Banking Trojan Report.”

Secureworks, www.secureworks.com/research/zeus.

Usa.kaspersky.com, usa.kaspersky.com/resource-center/threats/zeus-virus.

Kiguolis, Linas. “Remove Zeus Panda Virus (Virus Removal Guide) - Updated Nov 2019.”

Security and Spyware News, www.2-spyware.com/remove-zeus-panda-virus.html.

KnowBe4. “Gameover Zeus (GOZ).” KnowBe4, www.knowbe4.com/gameover-zeus.

BOTEZATU, Bogdan. “Terdot: Zeus-Based Malware Strikes Back with a Blast from thePast.”
Bitdefender Labs, 20 Nov. 2017, labs.bitdefender.com/2017/11/terdot-zeus-based-malware-strikes-back-with-a-blast-from-the-past/.

Seals, Tara, and US/North America News. “Zeus Spawn 'Terdot' Is a Banking Trojan with a Twist.”

Infosecurity Magazine, 16 Nov. 2017, www.infosecurity-magazine.com/news/zeus-spawn-terdot-is-a-banking/.
“Zitmo (Zeus-in-the-Mobile) Trojan Attacks Android and Blackberry Smartphones.”

Remove Spyware & Malware with SpyHunter - EnigmaSoft Ltd, 17 Aug. 2012, www.enigmasoftware.com/zitmo-zeus-in-the-mobile-trojan-attacks-android-blackberry-smartphones/.

Maslennikov, Denis. “ZeuS-in-the-Mobile for Android.”

Securelist English, securelist.com/zeus-in-the-mobile-for-android/29258/

SC Magazine, (2014). Two new GameoverZeuS variants in the wild. Available at:
http://www.scmagazine.com/two-new-gameover-ZeuS-variants-in-the-wild/article/365647/

Soltani, S., Seno, S. A. H., Nezhadkamali, M., & Budiarto, R. (2014). A survey on real world botnets and detection mechanisms. International Journal of Information and Network Security (IJINS), 3(2)

OpenDNS SecurityLabs (2014). GameoverZeuS Switches From P2P to DGA. Available at:
http://labs.opendns.com/2014/07/11/gameover-ZeuS-switches-p2p-dga/

Hesiod Quotes. (n.d.). BrainyQuote.com. Retrieved November 19, 2019, from BrainyQuote.com Web site:
https://www.brainyquote.com/quotes/hesiod_397216

Zeus Malware: Threat Banking Industry Unisys Stealth Solution Team May 2010

Symantec Security Center: https://www.symantec.com/security-center Trojan.Zbot