Name: Dhruva Kapadia
MIS: 111903142

Assignment 3

MALWARE REVERSE ENGINEERING

What Is Reverse Engineering Malware?

Reverse engineering malware is the process of analyzing malware to understand its functionality and purpose. This process can determine how to remove the malware from a system or create defenses against it.

Reverse engineering malware is challenging, as malware is often designed to be difficult to analyze. Typically, a malware reverse engineering program would be necessary to become proficient at it. Threat actors may use obfuscation techniques, encryption, and other tricks to make the programs more complex. In addition, malware authors may change the code frequently to make it harder to reverse engineer.

Malware used: Zeus Variant Panda

The original Zeus banking trojan's source code was leaked in 2011 and since then several independent threat actors have used the source code as a basis for new variants of the malware. One of the most prolific and advanced of these variants is the Zeus.Panda banking trojan which we will analyze in this white paper. Zeus.Panda targets Windows operating systems from WinXP through Windows 10 and is typically spread through phishing mail campaigns, but proliferation through drive-by exploits has been seen.

Tools Required

- Oracle VM Virtualbox - For safe Sandbox Environment
- Regshot - what registry malware changes
- InetSim - Faking Sane Network Environment
- Procmon - Clear all events, filter on malware executable name, Run Malware, Analyze Capture Logs
- Radare2 - Static Analysis (Hashing, String matching, File Information, Imports)
- VirusTotal - For matching hashes of Malware

Malware Behavior

The most common ways Zeus infects compromised machines are:

- *Drive-by-downloads*: Zeus operators compromise legitimate websites, and leverage browser and operating system vulnerabilities to install the Zeus malware when users access the site.
- *Spam messages*: Zeus spreads via phishing emails and malicious social media campaigns. Because the malware has the ability to gain illicit access to credentials, it can be used to infiltrate social media accounts on compromised machines and use them to publish phishing messages. This is one of the factors that allowed Zeus to spread fast and infect millions of devices around the world.

Since Zeus is available as open-source malware, its effects can vary widely. Historically, it’s had two consistent roles:

1. *Steal sensitive information*: Zeus is known as a banking Trojan, but it can steal anything its operator wants it to steal: system information, stored passwords, online account credentials, and more.
2. *Build a botnet*: Zeus maintains contact with its operator through a command-and-control (C&C) server so that it can remotely receive additional instructions. The operator can hijack the victim’s computer and install more malware.

Zeus originally stole passwords via Internet Explorer’s Password Store feature: Zeus simply helped itself to any passwords stored in the browser. If Zeus detected that the victim was visiting a banking site, it would use keylogging or form-grabbing methods from within the browser to capture usernames and passwords.

Keylogging records your keystrokes as you type, while form-grabbing captures content you enter into website form fields before the info is sent to a website’s server. That way, Zeus’s creators never had to overcome the security features on the banking sites themselves.

Zeus can also intercept legitimate websites and add additional forms to provide the operators with even more personal information.

Detection / Identification of Malware Using Basic Static Analysis

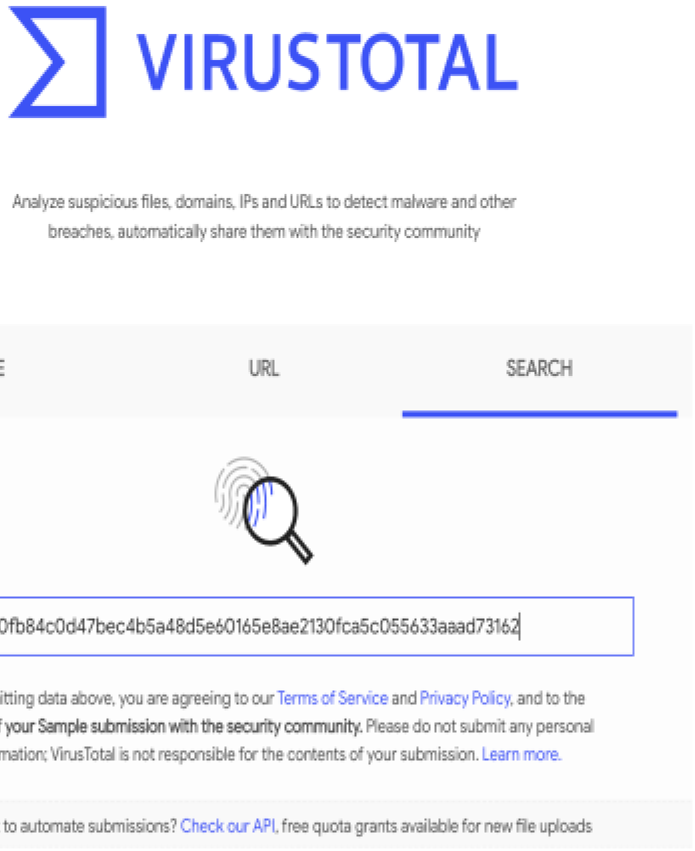
1. **Hashing:** It is used for identifying unique malware.The malicious software is run through a hashing program that produces a unique hash that identifies that malware. Hashes of the current file are:

   MD5
   Packed: e005c4009c22e0f73fcdaeba99bd0075
   Unpacked: 655f65b1b08621dfcb2603b59fca05bc

   SHA1
   Packed: 6f5c186baa0d69799c250769052236b8bcfb13a1
   Unpacked: 88782d3b74067d405e56f0a5e9b92e3fdb77dcd8

SHA256
Packed:
d037723b90acb9d5a283d54b833e171e913f6fa7f44dd6d996d0cecae9595d0b
Unpacked:
bd956b2e81731874995b9b92e20f75dbf67ac5f12f9daa194525e1b673c7f83c

2. **Antivirus scanning:** For performing static analysis, the malicious files are scanned using anti-virus but one AV solution cannot detect all malware pieces. Hence, it is important to scan the file using different AV products. VirusTotal is an online platform for scanning files using different AV solutions. The file can be directly uploaded or one can type the md5 hash of that file as given below:

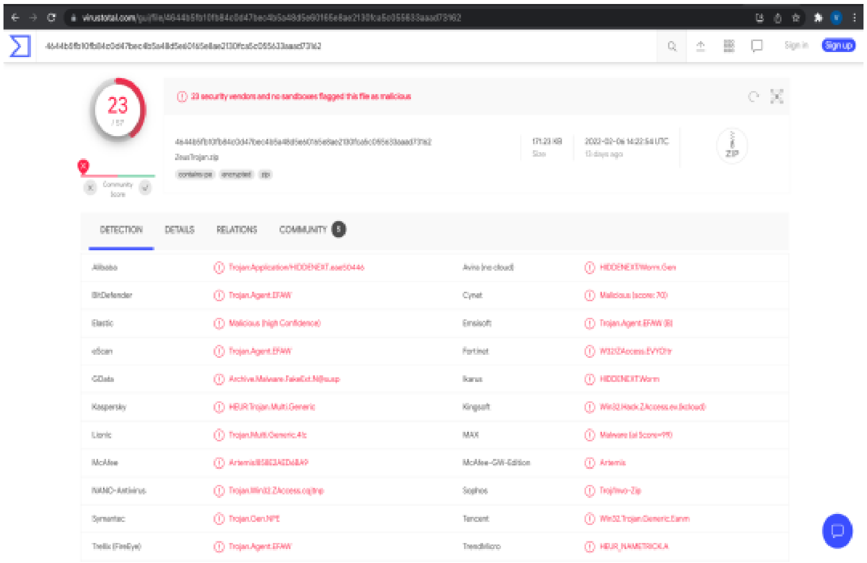


Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community

4644b5fb10fb84c0d47bec4b5a48d5e60165e8ae2130fca5c055633aaad73162

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, free quota grants available for new file uploads



virustotal.com/gui/file/4644b5fb10fb84c0d47bec4b5a48d5e60f65e8ae2130fca5c055633aaad73162
4644b5fb10fb84c0d47bec4b5a48d5e60f65e8ae2130fca5c055633aaad73162
Sign in
Sign up
23
/ 57
Community Score

23 security vendors and no sandboxes flagged this file as malicious

4644b5fb10fb84c0d47bec4b5a48d5e60f65e8ae2130fca5c055633aaad73162
ZeusTrojan.zip
contains-pe encrypted zip

171.23 KB
Size

2022-02-06 14:22:54 UTC
13 days ago

ZIP
DETECTION
DETAILS
RELATIONS
COMMUNITY 5

Alibaba	Trojan:Application/HIDDENEXT.aae50446	Avira (no cloud)	HIDDENEXT/Worm.Gen
BitDefender	Trojan.Agent.EFAW	Cynet	Malicious (score: 70)
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.Agent.EFAW (B)
eScan	Trojan.Agent.EFAW	Fortinet	W32/ZAccess.EVYO!tr
GData	Archive.Malware.FakeExt.M@susp	Ikarus	HIDDENEXT.Worm
Kaspersky	HEUR:Trojan.Multi.Generic	Kingsoft	Win32.Hack.ZAccess.ev.(kcloud)
Lionic	Trojan.Multi.Generic.4!c	MAX	Malware (ai Score=99)
McAfee	Artemis!B5B23AEDA8A9	McAfee-GW-Edition	Artemis
NANO-Antivirus	Trojan.Win32.ZAccess.cqjtnp	Sophos	Troj/Inva-Zip
Symantec	Trojan.Gen.NPE	Tencent	Win32.Trojan.Generic.Eanm
Trellix (FireEye)	Trojan.Agent.EFAW	TrendMicro	HEUR_NAMETRICK.A

23 AV engines could detect the ZeusTrojan virus.

3. **String Matching:** A string in a program is a sequence of characters .A program contains strings if it prints a message, connects to a URL, or copies a file to a specific location.

Dynamic Analysis

- *File System Changes:* Panda tries to find a directory underneath %APPDATA%\Roaming that is empty. Panda ended up in %APPDATA%\Roaming\Sun\Java. In the directory, Panda creates four files with random file extensions.

  Files created- Desktop (create shortcut).exe (malware executable), Control Panel.cyd, Desktop.ysq, and Notepad.kix.
- *Registry Changes:* Aside from writing some files to disk, Panda also uses some registry keys to store data. All the registry keys used by Panda are located in the HKCU\Software\Microsoft key.

  The names of the keys are- Ivoc (regDynamicConfig), Kounhu (regLocalConfig), and Useglugy (regLocalSettings). Additionally, Panda creates a new entry within the HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry key

Removal

If your computer becomes infected, the best way to remove Zeus Trojan malware is to use a Trojan removal tool. Download the anti-malware software, and then clear out the Trojan infection like you would remove a computer virus.

1. Download strong antivirus software from a reputable provider.
2. After installation, restart your computer in Safe Mode to prevent any malware from connecting to the internet.
3. Scan your computer for malware with your newly installed antivirus software to detect Trojans or any other malware.
4. If any malware is found, follow the instructions to remove it.