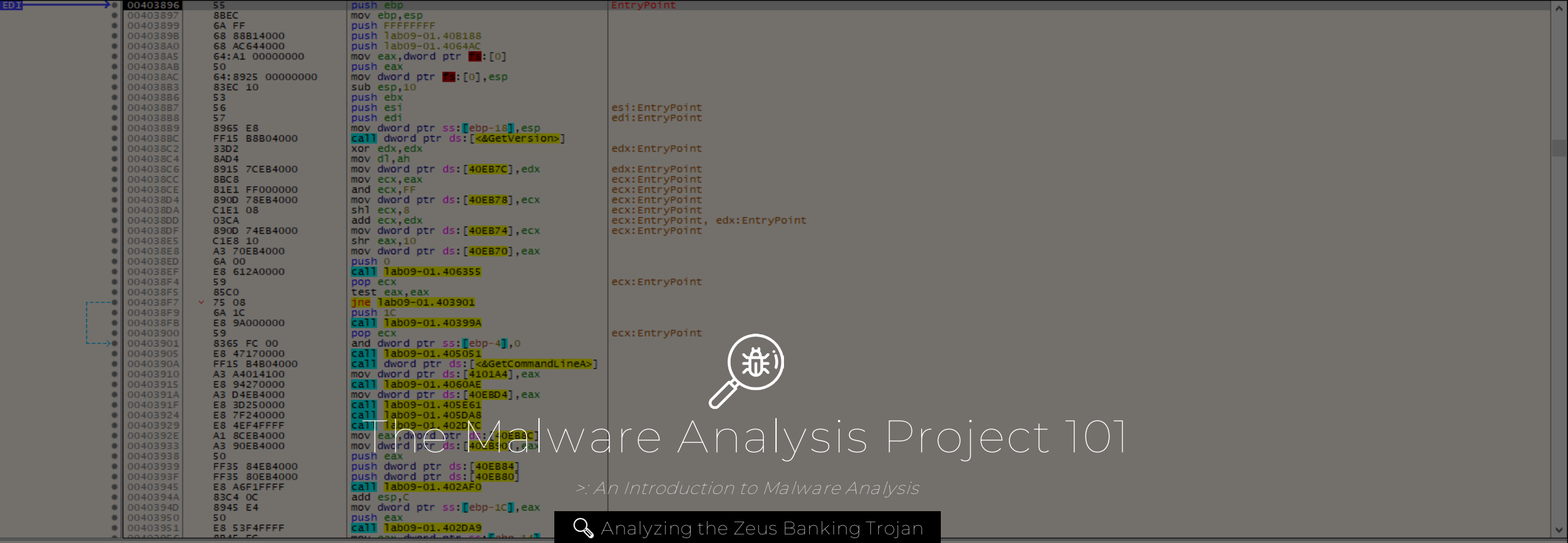


The Malware Analysis Project 101

>: An Introduction to Malware Analysis

Analyzing the Zeus Banking Trojan

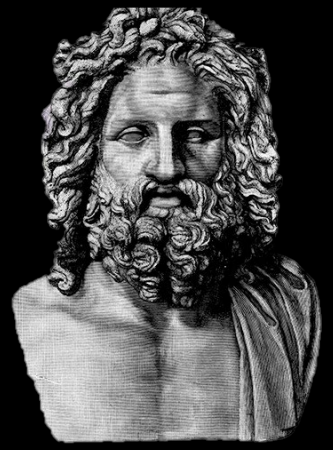
Overview

- Background Information
  - History
  - (Suspected) Author
- Overview of Analysis Tools
- Provision Lab
- Conduct Analysis
  - Download Zeus Banking Trojan ***(ZeusBankingVersion_26Nov2013)***
  - Label Malware (hashes) & VirusTotal
  - Basic Static Analysis
    - Host-based indicators
  - Basic Dynamic Analysis
    - Network-based indicators
  - Report & IOCs
    - Write a YARA rule

▶ Pre-requisites

- Malware Analysis Lab Built
  - Self-hosted
  - Cloud-hosted
- Snapshot of Base Image
- Established Internet Connection
  - https://github.com/ytisf/theZoo/tree/master/malware/Binaries/ZeusBankingVersion_26Nov2013

History

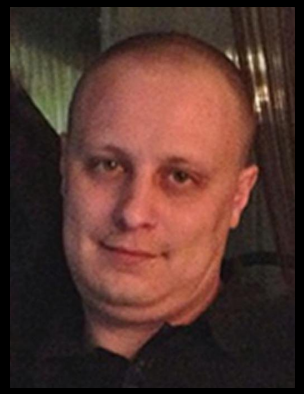


ZeuS

The prolific banking trojan.

Background Information

- Primarily created to be a financial banking trojan.
- First spotted in the wild in 2007 when Zeus Trojan was caught stealing sensitive information from systems owned by the US Department of Transportation. Since then, there have been 573+ known versions with 36 known families of the Zeus Trojan. *(according to website https://zeusmuseum.com/)*
- Malicious code become public in 2011 after a leak.



Evgeniy Mikhailovich Bogachev
Is the suspected author of the original Zeus trojan. Has a $3 million dollar bounty from the FBI. Continues to be one of the most wanted hackers.

FBI Listing

Goal & Delivery Methods

Goal

- Steal people's financial information to exfiltrate financial information.
- Add machines to a globally distributed P2P botnet (depends on the variant).

Delivery Method

Drive-by downloads: Require a user to visit a website that has the backdoor trojan code on it.

- Modern web browsers block these downloads by default.
- Attack vector is mostly obsolete.

Phishing & Spam Campaigns: Main infection method.

Crackdown & Impact

Crackdown

- FBI cracked down on Gameover Zeus (which was a prolific variant of the Zeus Trojan) in 2014.
- An estimated 1 million computers were infected. 25% in United States.
- $100+ million in financial damages due to Gameover Zeus.
- Evgeniy Mikhailovich Bogachev had a $3 million dollar bounty from the FBI. Continues to be one of the most wanted hackers.

Source: CrowdStrike

Impact

- Inspired hundreds of additional variants which use parts of source code.
- Millions of infected machines with associated costs in damages in the millions.

Overview of Analysis Tools

c:\users\admin\desktop\267.exe

- indicators (wait...)
- virustotal (warning)
- dos-header (64 bytes)
- dos-stub (176 bytes)
- file-header (Oct.2019)
- optional-header (GUI)
- directories (6)
- sections (98.96 %)
- libraries (wait...)
- imports (wait...)
- exports (Run)
- tls-callbacks (n/a)
- resources (4)
- strings (wait...)
- debug (path)
- manifest (trust-info-missing)
- version (n/a)
- certificate (n/a)
- overlay (wait...)

property	value
md5	F3F48C57C38BFF2DDD220F20569E1EE6
sha1	0421127F1BCCA91A6AB2A570A47F8159101B751A
sha256	B1CAD1540ECB290088252635F8E130022EED7486EB128C0CA3D676945D60A9FC
md5-without-overlay	wait...
sha1-without-overlay	wait...
sha256-without-overlay	wait...
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
size	393216 (bytes)
size-without-overlay	wait...
entropy	5.983
imphash	EFE1C3568D573BCCB1E9D2B521C47CEA
signature	Microsoft Visual C++ 8
entry-point-hex	E8 59 9C 00 00 E9 16 FE FF FF CC CC CC CC 8B 4C 24 04 F7 C1 03 00 00 00 74 24 8A 01 83 C1 01 84
file-version	n/a
description	n/a
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x5D9A34BC (Sun Oct 06 19:38:52 2019)
debugger-stamp	0x5D9A34BC (Sun Oct 06 19:38:52 2019)
resources-stamp	empty
exports-stamp	0x5D9A34BC (Sun Oct 06 19:38:52 2019)
version-stamp	n/a

VirusTotal

- Analysis tool used to assess malicious files, domains, IP addresses, and URLs to detect malware.
- Works by aggregating the results of antivirus products and online security scan engines. Outputs which engines have flagged a file as malicious or known threat.
- Used to fingerprint a malicious sample and measure its functionality against established security engines.

Static Tool

PeStudio

- Program used to statically analyze malware and identify artifacts of interest.
- Collects static information:
  - Hashes
  - File Header
  - File Properties
  - Strings
  - Libraries Used
  - Imports
- Easy-to-use program.

“FLOSS” Floss

- Extracts strings from executables.
- Uses advanced static analysis technique to automatically deobfuscate strings from malware binaries.

```
$> floss malicious.exe
```

Strings: Extracting strings from compiled programs provides possible information about URLs, imports, IP addresses, and functions hidden within the program.

Packing: Authors will use “packing” or compression techniques to obfuscate valuable information contained within the binary and make it harder to analyze.

Capa

- Automatically detects capabilities of program and outputs what it thinks it can the program can do.
- Rules are matched against known API calls identified, strings of interest and more (for example a rule may be "connect to URL").
- Behavior is mapped to the MITRE ATT&CK framework.

```
$> capa [-v] [-v] malicious.exe
```

Cutter

- Reverse-engineering platform.
- Used to view assembly-level instructions of programs.
- View decompiled code.

INetSim

- Software suite used for simulating common internet services.
- Can be used to analyze the network behavior for malware samples.
- Supports simulation for many services
  - HTTP, SMTP, POP3, DNS, FTP, NTP, TFTP, IRC, Ident, Finger, Syslog, ‘Small servers’ (Daytime, Time, Echo, Chargen, Discard, Quotd)

```
$> inetsim
```

Wireshark

- Network packet sniffer and analyzer. Used for network troubleshooting and packet analysis.
- Malware Analysis Use Cases:
  - View ingress / egress network traffic from malicious programs.
  - Flag domains or IP addresses being reached out to within the program.

Dynamic Tool

Process Monitor (Procmon)

- Apart of the Sysinternals Suite.
- Monitors and displays real-time information on the Windows filesystem.
- Captures events from five different classes:
  - Registry
  - Filesystem
  - Network
  - Processes
  - Profiling Events
- Used to capture malicious activity occurring on filesystem (ex setting arbitrary registery keys, writing files to Windows Paths, etc).

Sysinternals: A suite of software programs used to manage, troubleshoot, and diagnose Windows applications. Actively maintained by Microsoft.

Dynamic Tool

YARA

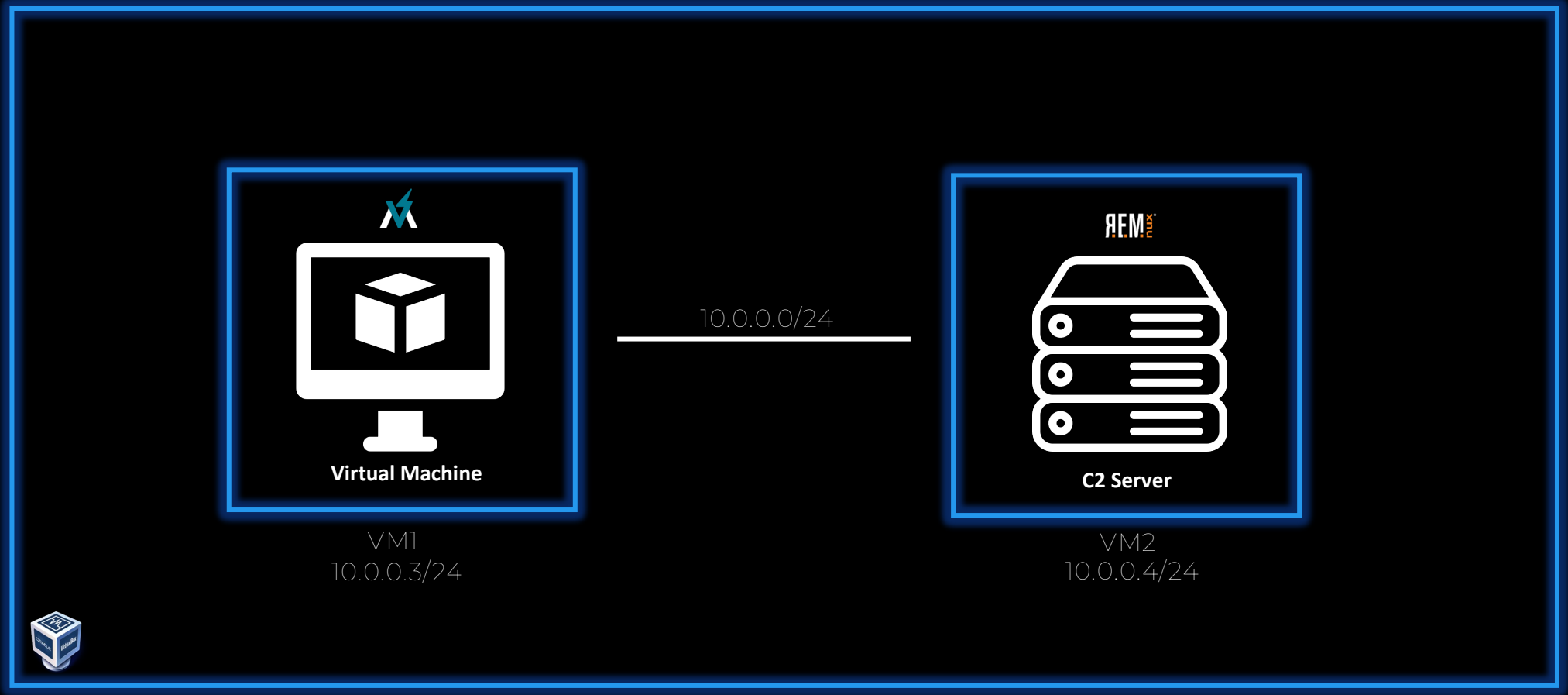
- Used to classify and identify malware samples by creating “rules” of malware families based on textual or binary patterns.
- YARA rules are written by defining variables with interesting strings and byte sequences. Variables are evaluated by the condition block, which implements the logic of where, how, or when strings or byte sequences occur.

```
rule Zeus_IOC {

        strings:
              $file_name="invoice_2318362983713_823931342io.pdf.exe" ascii
              $PE_magic_byte="MZ“

        condition:
               $PE_magic_byte at 0 and $filename
}
```

Topology



Host-only Adapter (no Internet access)

⚠Warning & Disclaimers

- Safety is key when dealing with malware. Ensure you always are following protocols when it comes to downloading and detonating a malicious sample. Follow all instructions within the courses and listed resources.
- Disclaimers:
  1. I take no responsibility or accountability for infection of malicious software, programs, files onto any computer or workstation.
  2. This project and videos are for educational purposes only. I do not condone the development, use of, or spreading of programs to intentionally harm assets, networks, or individuals.