Analysis of Zeus Banking Trojan Report

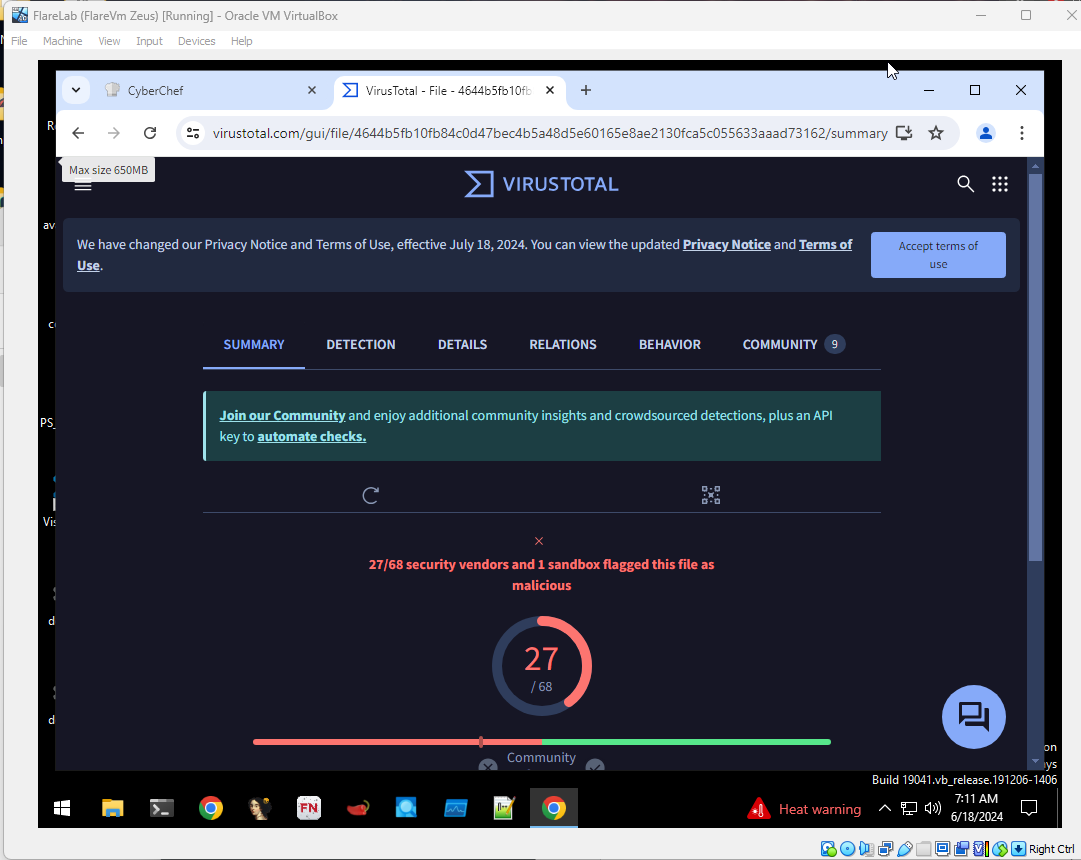
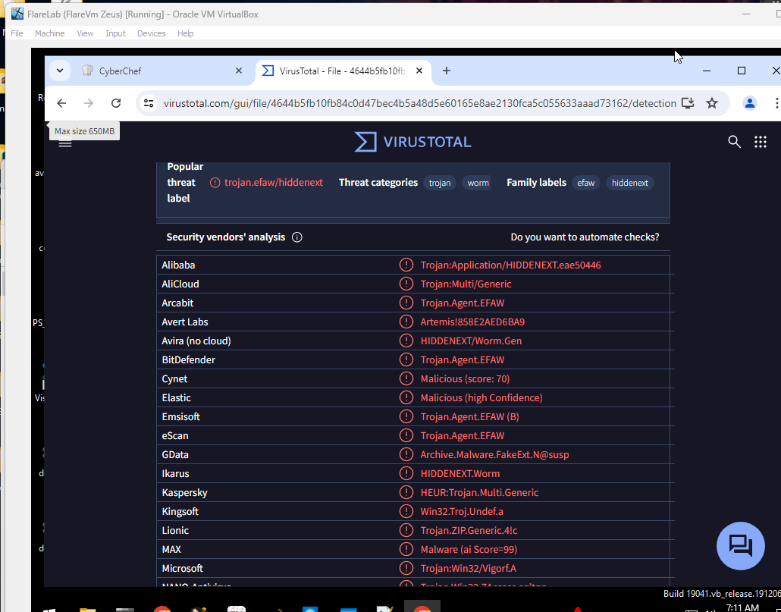
Lab/Project

Ali Charty

2024

**Fingerprint**

Screenshot showing the VirusTotal analysis results for the Zeus Trojan sample, identifying it as malicious based on multiple antivirus engines.



Hashes:

Screenshot of PE Studio displaying the calculated hashes (MD5, SHA-1, SHA-256) for the Zeus Trojan sample.

A screenshot of a computer

Description automatically generated

Invoice\_2318362983713\_823931342io.pdf.exe

**Basic Static Analysis**

Pestudio

A screenshot of a computer

Description automatically generated

corect.com yielded no interesting findings. (Romanian)

A screenshot of a computer

Description automatically generated

API calls

List of API calls extracted from the Zues Trojan, including descriptions of their functionality.

A screenshot of a computer

Description automatically generated

GetAsyncKeyState: Determines whether a key is up or down at the time the function is called, and whether the key was pressed after a previous call to **GetAsyncKeyState**.

A screenshot of a computer

Description automatically generated

SHLWAPI.dll

KERNEL32.dll

USER32.dll

Capa Output

Screenshot of the Capa tool output, showing the capabilities of the Zeus Trojan and mapping them to the MITRE ATT&CK framework.A computer screen shot of a blue screen

Description automatically generated

**Advanced Static Analysis**

A screenshot of a computer program

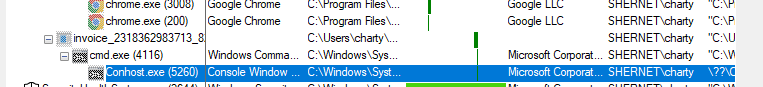
Description automatically generated

Screenshot of Cutter tool, pinpointing the location of Kernel32.dll within the disassembled code of the Zeus Trojan.



**Basic Dynamic Analysis**

Screenshot from Process Monitor, displaying the process tree and highlighting the parent-child relationship between malicious processes spawned by the Zeus Trojan.



A screenshot of a computer

Description automatically generated

Screenshot from Process Monitor, showing a hidden command line session created by the Zeus Trojan for executing commands.

A screen shot of a computer

Description automatically generated

Network based indicator

Screenshot from Wireshark, capturing the network traffic generated by the Zeus Trojan and highlighting any suspicious connections.

A screenshot of a computer

Description automatically generated

**YARA (IOC)**

Yara rule created for detecting the Zues Trojan, based on unique strings and characteristics identified during the analysis.

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**