[XXXXXXXXXX] | Malware Analysis

Jerry Haymaker

Indiana University–Purdue University Indianapolis

Advanced Network Security – [XXXXXXXXXXXXXXXX]

[XXXXXXXXXXXXXXX]

Author Note

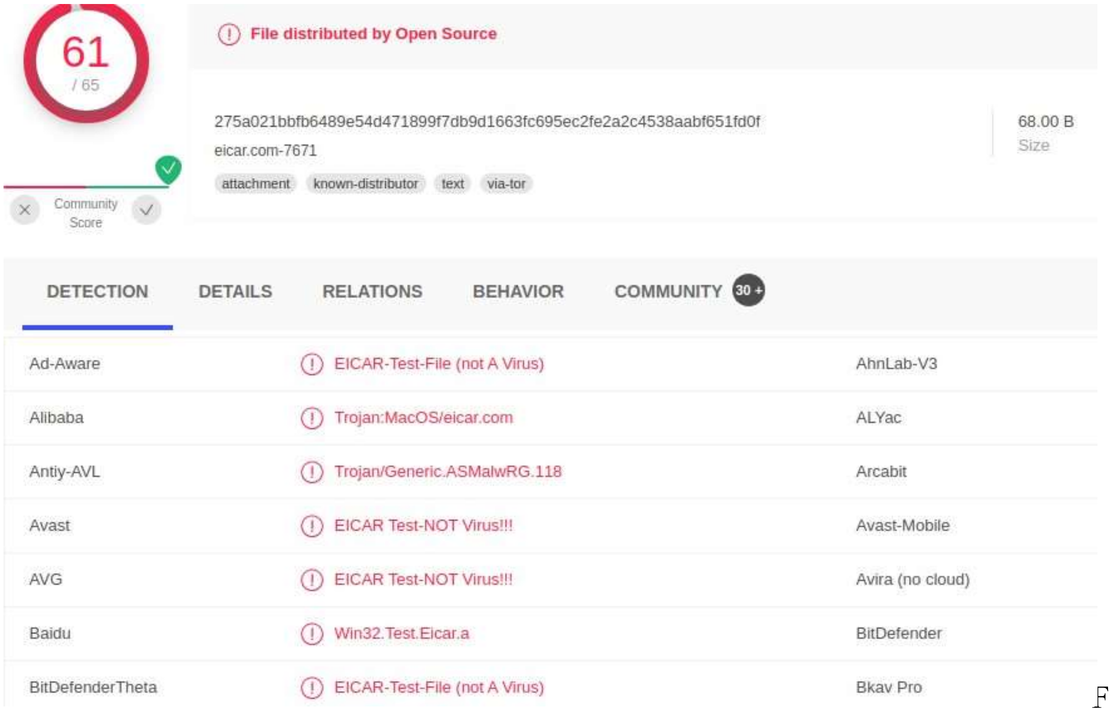
An assignment submitted to the Cyber Security Information Assurance Program at Indiana University–Purdue University Indianapolis in partial fulfillment of the requirements belonging to the Bachelor of Science Degree in Cyber Security.

Abstract

In this lab I have been tasked with analyzing files that are considered malicious. The tools I will be using are eicar, Microsoft word/macros, CyberChef, Any.Run, and VirusTotal. First, we will use VirusToal, an online antivirus that can scan files and websites for malicious activity. We will be examining the eicar antivirus test file. Secondly, we will look at a publicly submitted malware sample on AnyRun. Lastly, we will examine the MalDoc and discover what the macros are trying to do.

Discussion

My first task in the lab was to examine the eicar file on VirusTotal. Upon uploading the file to eicar it found 61 out of 65 detections please see fig.1. One of the tags of the file was known-distributor and disturbed by open source. Looking at the details of section on VirusTotal shows us all of the hashes and history of the file. Such as it was first seen in 2005, please see fig.2.



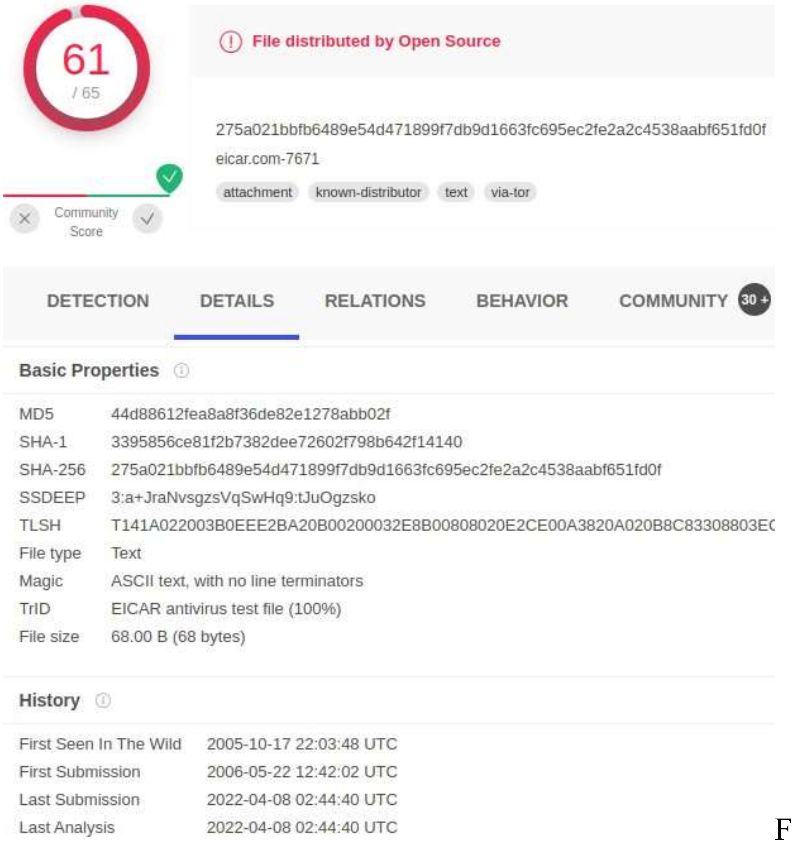
File distributed by Open Source

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
eicar.com-7671
attachment known-distributor text via-tor

68.00 B
Size

Ad-Aware	EICAR-Test-File (not A Virus)	AhnLab-V3
Alibaba	Trojan:MacOS/eicar.com	ALYac
Antiy-AVL	Trojan/Generic.ASMalwRG.118	Arcabit
Avast	EICAR Test-NOT Virus!!!	Avast-Mobile
AVG	EICAR Test-NOT Virus!!!	Avira (no cloud)
Baidu	Win32.Test.Eicar.a	BitDefender
BitDefenderTheta	EICAR-Test-File (not A Virus)	Bkav Pro

Fig.1



File distributed by Open Source

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
eicar.com-7671
attachment known-distributor text via-tor

Basic Properties

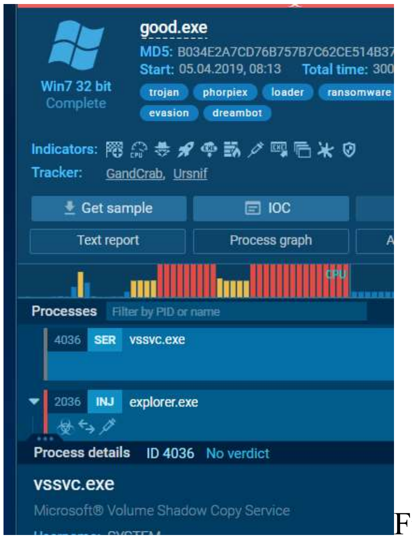
MD5	44d88612fea8a8f36de82e1278abb02f
SHA-1	3395856ce81f2b7382dee72602f798b642f14140
SHA-256	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
SSDEEP	3:a+JraNvsgzsVqSwHq9:tJuOgzsko
TLSH	T141A022003B0EEE2BA20B00200032E8B00808020E2CE00A3820A020B8C83308803E
File type	Text
Magic	ASCII text, with no line terminators
TrID	EICAR antivirus test file (100%)
File size	68.00 B (68 bytes)

History

First Seen In The Wild	2005-10-17 22:03:48 UTC
First Submission	2006-05-22 12:42:02 UTC
Last Submission	2022-04-08 02:44:40 UTC
Last Analysis	2022-04-08 02:44:40 UTC

Fig.2

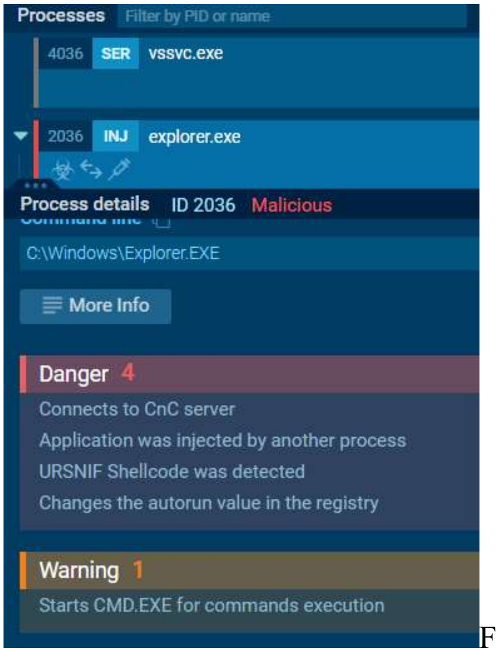
Secondly, we will look at publicly submitted samples of malware on any.run. The file I chose was good.exe. The MD5 hash is b034e2a7cd76b757b7c62ce514b378b4. It is categorized as trojan, phorpiex, loader, ransomware. Gandcrab, miner, gozi, ursnif, evasion, dreambot. Good.exe first gets on to the machine be volume shadow copy service, please see fig.3. Next the malware connects to the CnC server and changes the autorun value in the registry, please see fig.4. After this the malware downloads executable files from the internet and deletes the shadow copies. Lastly, it renames files like ransomware, installs miner malware, and checks for external IPs.



good.exe
MD5: B034E2A7CD76B757B7C62CE514B37
Start: 05.04.2019, 08:13 Total time: 300
Win7 32 bit
Complete
Indicators:
Tracker: GandCrab, Ursnif

Processes
4036 SER vssvc.exe
2036 INJ explorer.exe
Process details ID 4036 No verdict
vssvc.exe
Microsoft® Volume Shadow Copy Service

Fig.3



Processes
4036 SER vssvc.exe
2036 INJ explorer.exe
Process details ID 2036 Malicious
C:\Windows\Explorer.EXE

Danger 4
Connects to CnC server
Application was injected by another process
URSNIF Shellcode was detected
Changes the autorun value in the registry

Warning 1
Starts CMD.EXE for commands execution

Fig.4

Next, we will look at a macro file. The macro word file is named WellLookatyou.docm. Looking at the macro setting txt, we find that there is a string encoded in base64.

Summary

In this we used tools such as eicar, Microsoft word/macros, CyberChef, Any.Run, and VirusTotal to examine malicious files. Eicar can be used to test antivirus software while you can check publicly submitted malware on AnyRun to run analysis on. Lastly, we looked at malicious macros in word docs. These can be very well hidden depending on the obfuscation.