PROJECT ON MALWARE ANALYSIS

BY: Gagan Malhotra
(Team Hackerslounge)

key Findings :

Malicious files Name: 1.Malz3
2.AliceInWonderland.pd

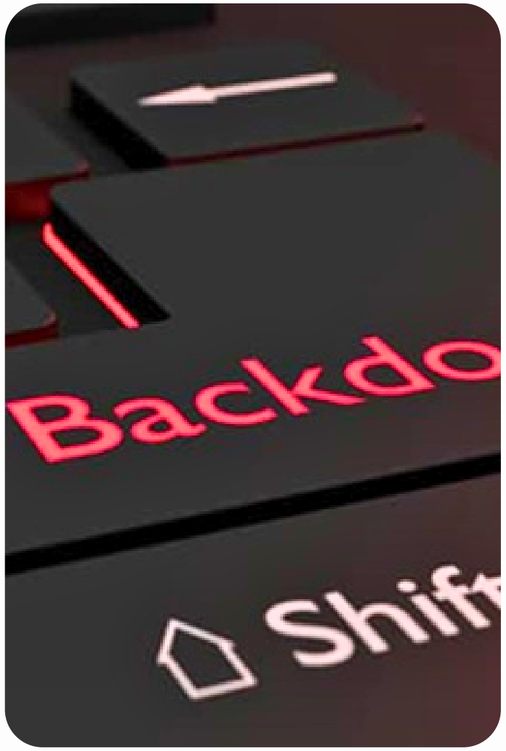
. **Trojan horse** is a type of virus that disguise computer as a legitimate program

.**Key Logger** a form of malware or hardware that keeps track of and records your keystrokes as you type

About Incident

The file Unconfirmed infected from trojan and Keylogger is downloaded into the system from unknown source

. Trojan Horse is a malware that looks like a genuine file but it is a infected file
. This malware can also give the remote access to the attacker
. Infect system performance
. Can effect the system in many other ways
.



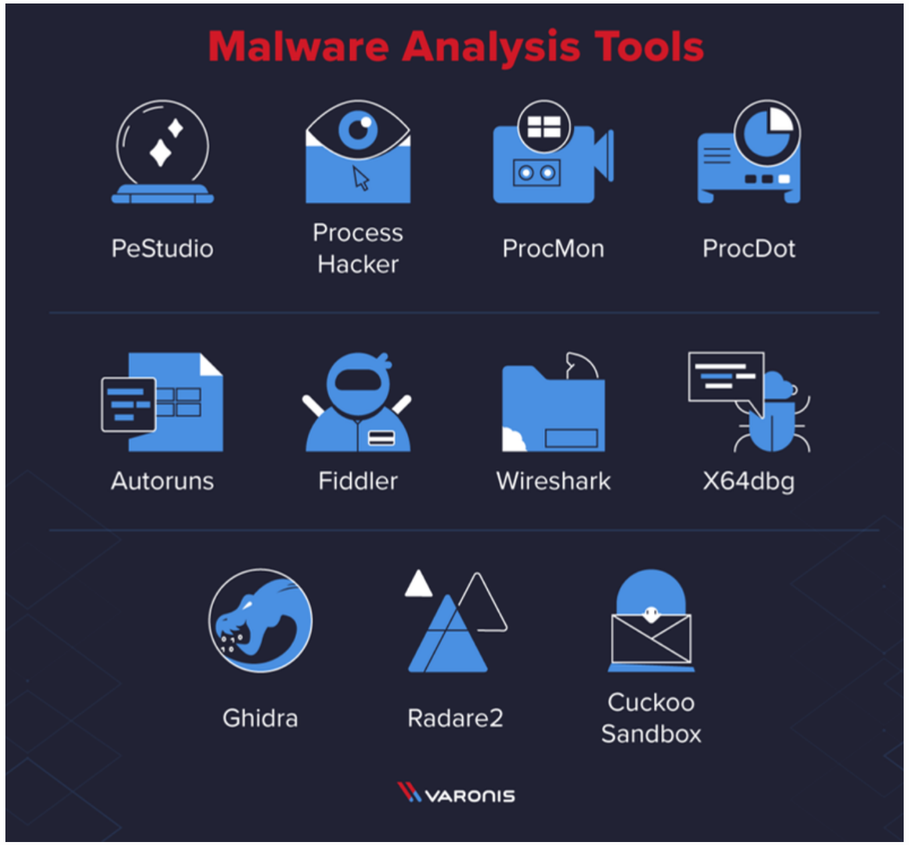
KEY LOGGER

.Is a form of virus that keeps record on your keystrokes

. It Send all thre information to the hacker using C&C Server

. The Hacker keeps record on the key strokes and locate username and password

Information



File Downloaded :
29/11/2023 on 5:30 pm

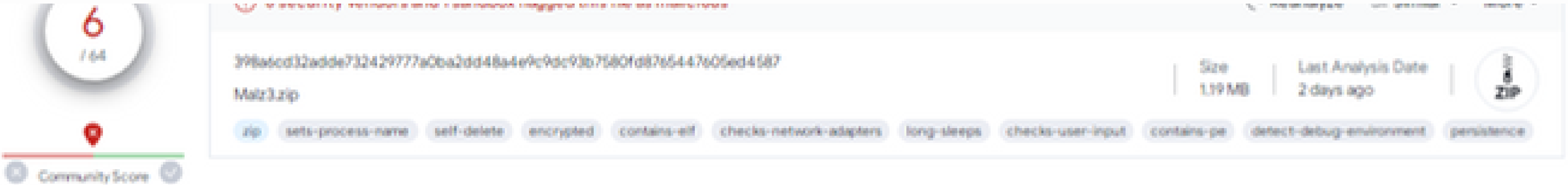
100%

incident Severity level

Tool Used

. Virus Total
. Procmon
. TCPview
.PeStudio
.Autoruns
. ExinfoPe
.

VIRUS TOTAL DETECTION REPORT



DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 5

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

This file is password-protected, security vendors may not have been able to look into it

Security vendors' analysis

Do you want to automate checks?

Avast	Other:Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]
Elastic	Malicious (moderate Confidence)	Fortinet	Data/PasswordProtected
NANO-Antivirus	Trojan.Win32.Agent.wwxg	Skyhigh (SWG)	Artemis
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected

Threat capabilites & Behaviour

.TROJAN HORSE :

SOURCE : .EXE FILE DOWNLOADED FROM ZOOM CALL

.DESTINATION IP : 192.168.0.0

. SYSTEM INFECTED : LAPTOP-QCTPI43G

Threat capabilites & Behaviour

.KEY LOGGER :

SOURCE : PDF FILE DOWNLOADED FROM Social Website

.DESTINATION IP : 192.168.0.0

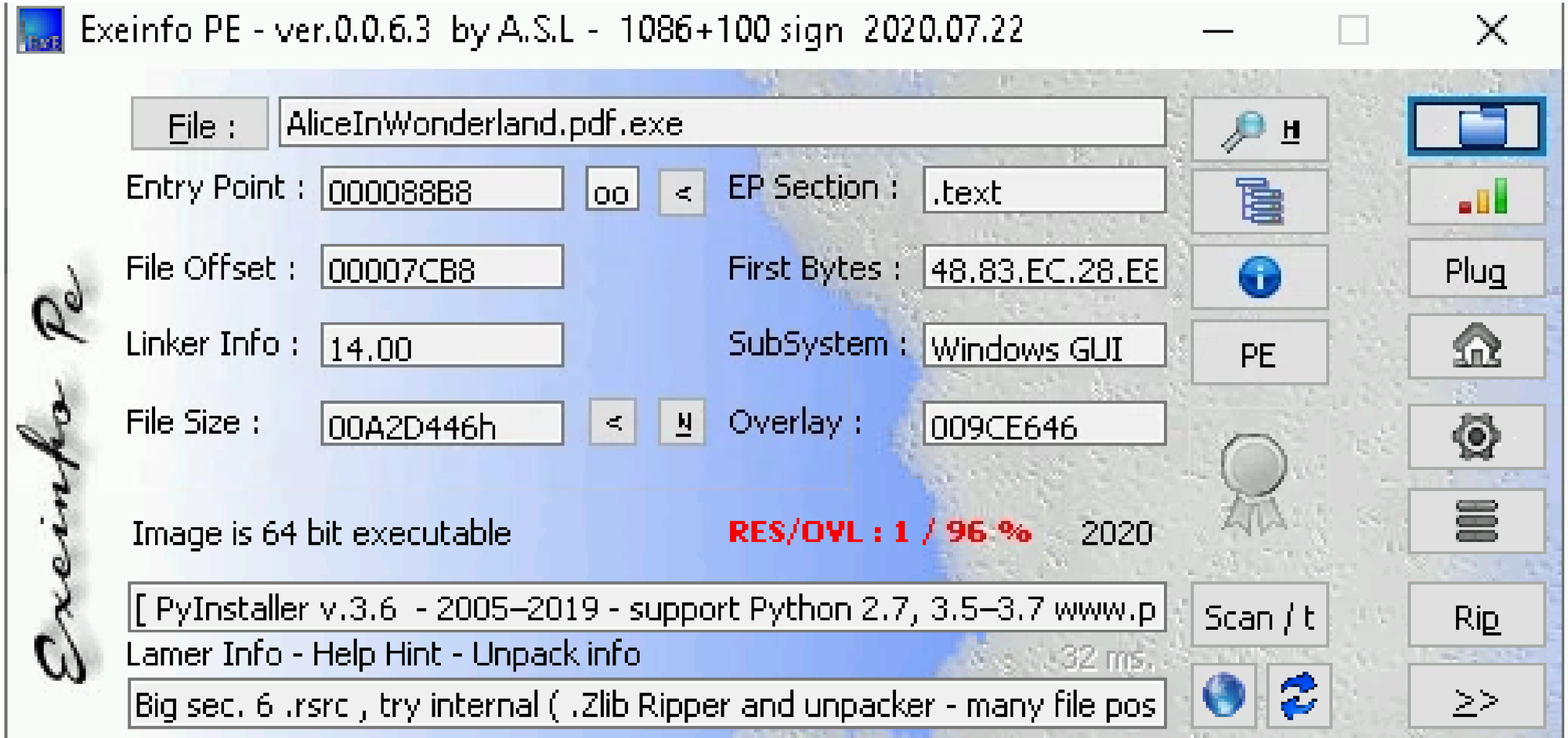
. SYSTEM INFECTED : LAPTOP-QCTPI43G

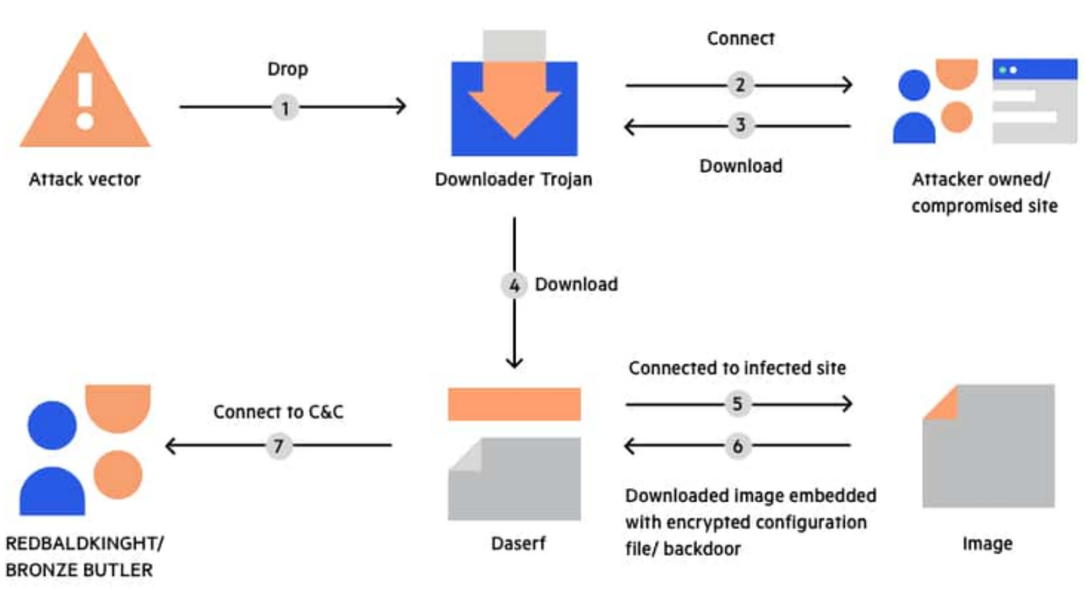
PEstudio report

41 Vendors caught this file as malicious

Report of Exinfope

Digital Certificate IS Missing.





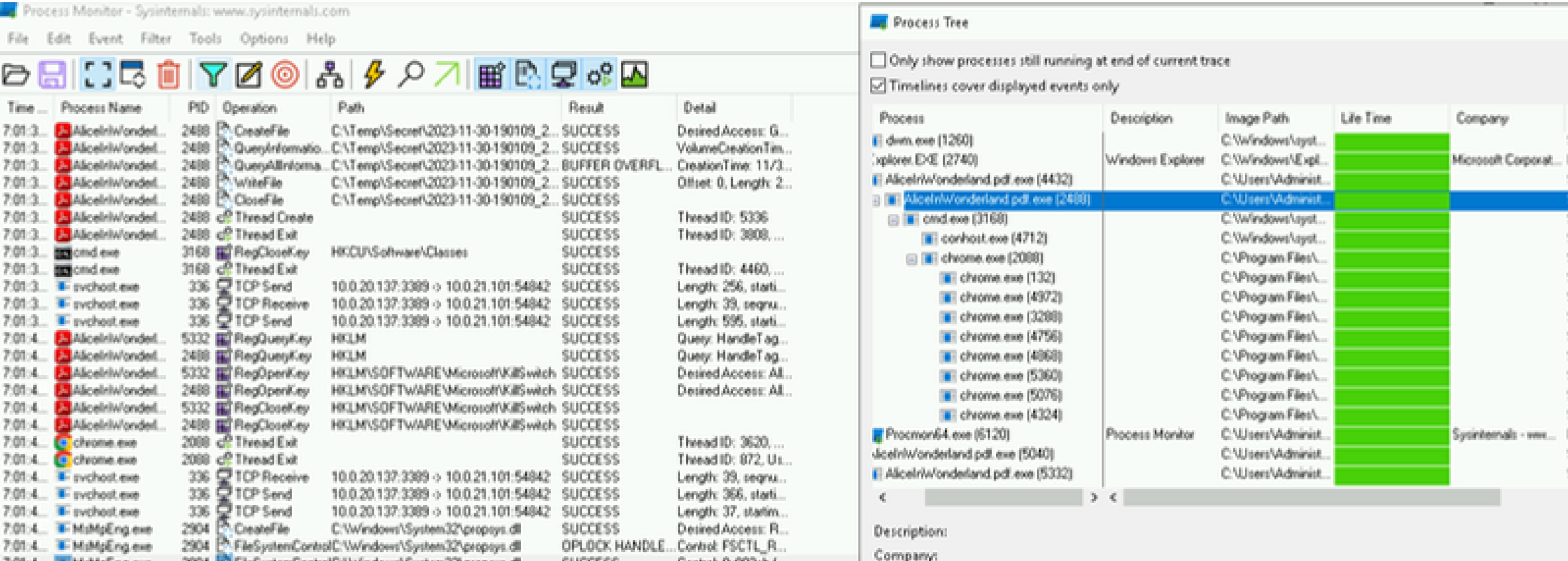
ATTACK CYCLE

1. Sucessfully Dropped
2. Infected file got downloaded
3. Detected Before Execution

Process Monitor report after attack

process done by malware: . Create Registary

. Create File



Recommendation & Prevention

Recommendation 1

- Never download or install software from a source you don’t trust completely

Recommendation 2

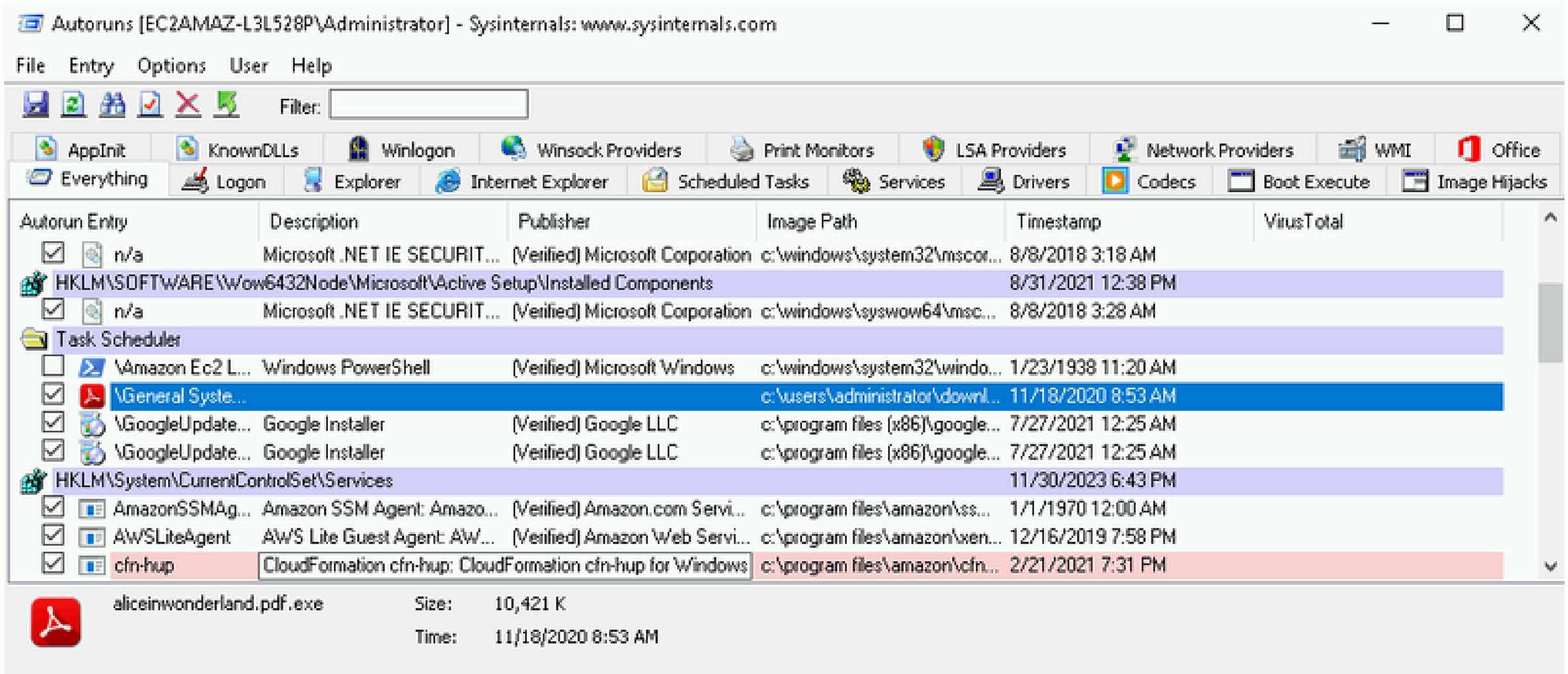
- Never open an attachment or run a program sent to you in an email from someone you don’t know.

Recommendation 3

- Keep all software on your computer up to date with the latest patches
- Make sure a Trojan antivirus is installed and running on your computer

Anyrun Report

Auto Execution of file must get stopped



Conclusion

Hence the file got downloaded but it get detected before execution but trojan horse is a very dangerous virus and can effect the whole system properly and also lead to the losses for the organisation as it allows to give the backdoor access to the attacker

Here's the Statistical data of top 10 consumer malware till 2020

Top 10 consumer malware categories 2020 compared to 2019

	Threats	2019	2020	% Change
1	Adware	41,151,954	31,502,039	-23%
2	Trojan	27,391,382	23,729,868	-13%
3	HackTool	6,437,673	15,882,958	147%
4	RiskwareTool	14,180,159	12,346,354	-13%
5	Spyware	1,960,652	2,434,723	24%
6	Worm	2,284,877	2,075,855	-9%
7	Backdoor	3,614,672	1,819,980	-50%
8	Rogue	501,146	1,050,713	110%
9	CrackTool	1,247,364	843,811	-32%
10	Virus	766,925	581,829	-24%

THANK YOU

For Your Attention