

# PROJECT ON MALWARE ANALYSIS

BY: Gagan Malhotra  
(Team Hackerslounge)

# key Findings :

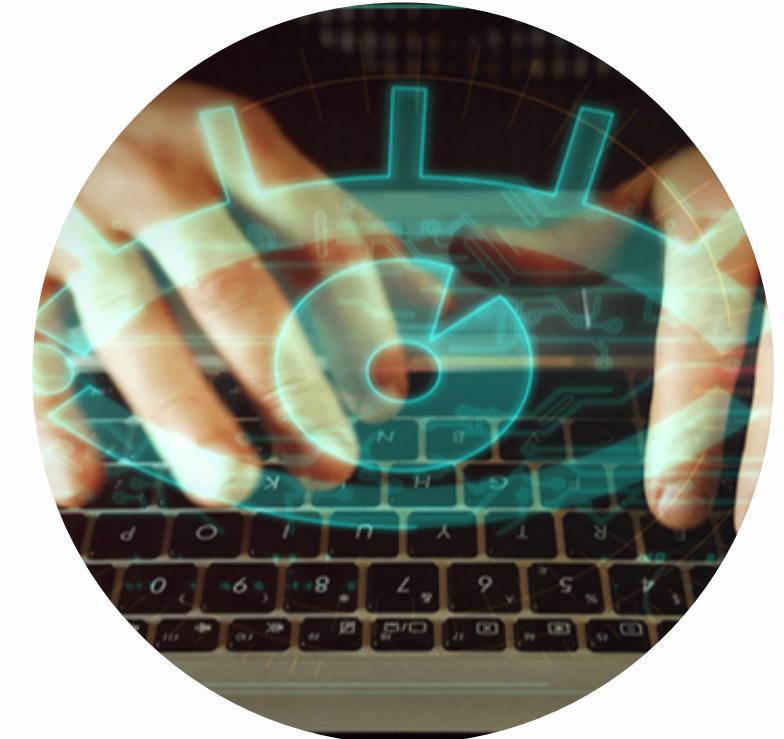
**Malicious files Name:** 1.Malz3

2.AliceInWonderland.pd

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



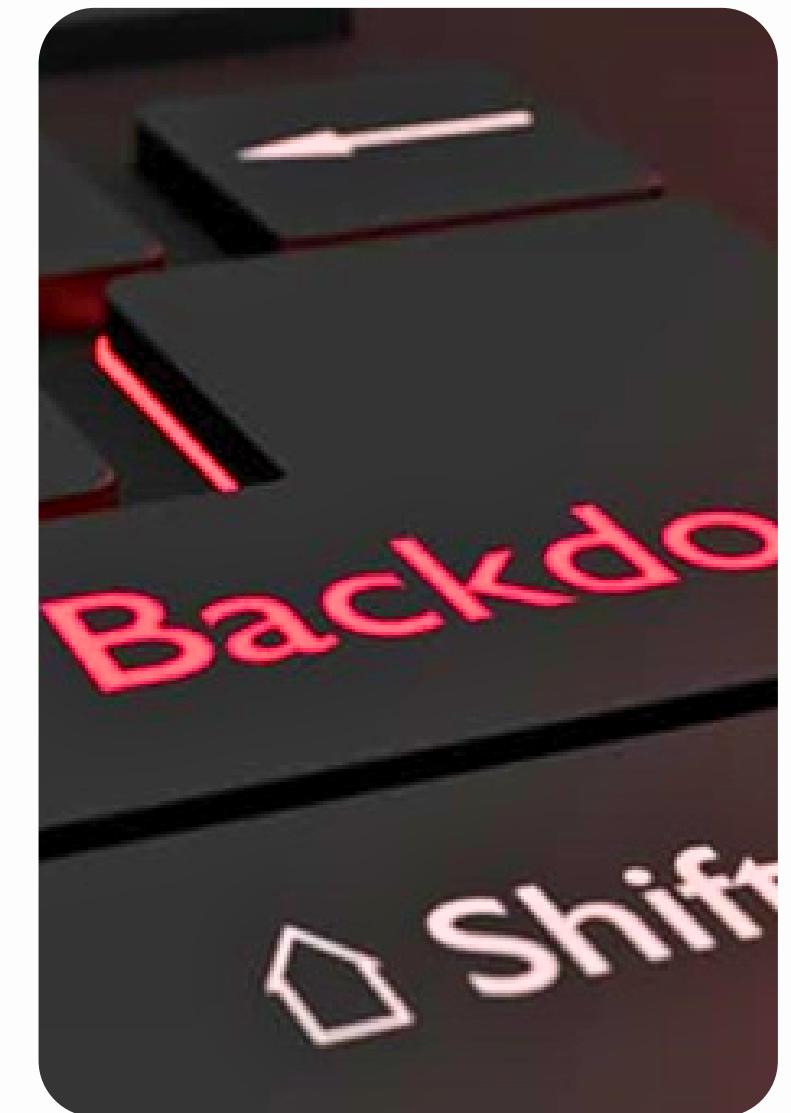
.**Key Logger** a form of malware or hardware that keeps track of and records your keystrokes as you type



# 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

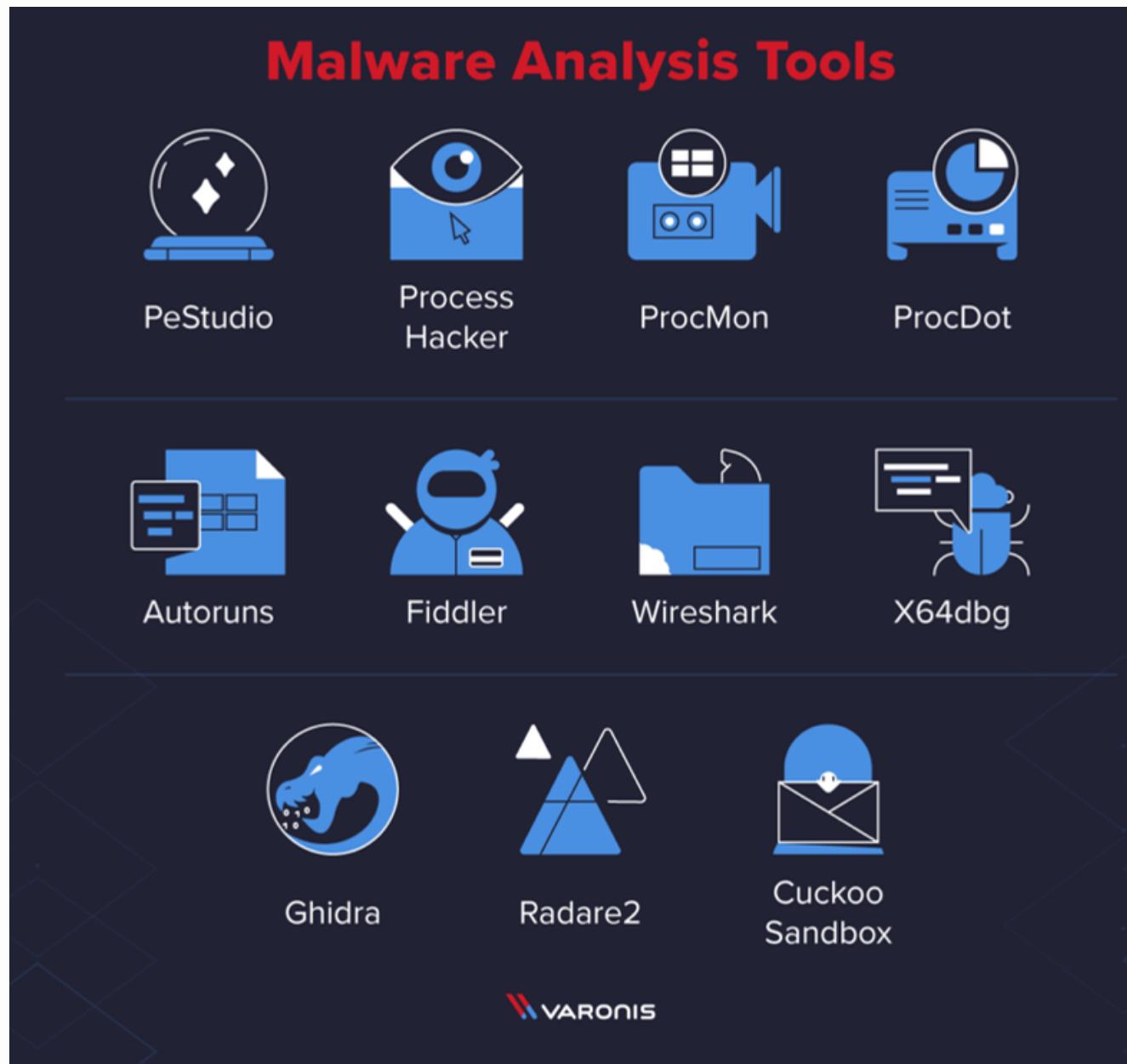
.Is a form of virus that keeps record on your keystrokes

. 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



**incident Severity level**



## Tool Used



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

.

# VIRUS TOTAL DETECTION REPORT

The screenshot shows a detailed analysis report for a file. At the top left is a circular icon with a red '6' and a '1/64' rating. To its right is a large file hash: 399baec032addc732429777a0ba2dd48a4e9c9dc93b7580fd8765447605ed4587. Below the hash is the file name 'MalzUp'. On the right side, there are fields for 'Size' (1.19 MB) and 'Last Analysis Date' (2 days ago). A 'ZIP' download button is also present. Below the file details is a horizontal bar with various detection tags: zip, self-process-name, self-delete, encrypted, contains-elf, checks-network-adapters, long-sleeps, checks-user-input, contains-pe, detect-debug-environment, and persistence. At the bottom left is a 'Community Score' section with a progress bar.

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY (6)

[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 (6)

[Do you want to automate checks?](#)

Avast	<span>●</span> Other/Malware-gen [Tr]	AVG	<span>●</span> Other/Malware-gen [Tr]
Daric	<span>●</span> Malicious (moderate Confidence)	Fortinet	<span>●</span> Data/PasswordProtected
NANO-Antivirus	<span>●</span> Trojan/Win32.Agent.lnwsg	Skyhigh (SWG)	<span>●</span> Artemis
Acronis (static ML)	<span>✓</span> Undetected	AhnLab-V3	<span>✓</span> Undetected
Allsafe	<span>✓</span> Undetected	AIYies	<span>✓</span> Undetected

# Threat capabilities & Behaviour



**.TROJAN HORSE :**

SOURCE : .EXE FILE DOWNLOADED  
FROM ZOOM CALL

.DESTINATION IP : 192.168.0.0

. SYSTEM INFECTED : LAPTOP-QCTPI43G

# Threat capabilities & 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

pestudio 9.15 • Malware Initial Assessment • www.wnit.or.com [c:/users/administrator/downloads/aliceinwonderland.pdf.exe]

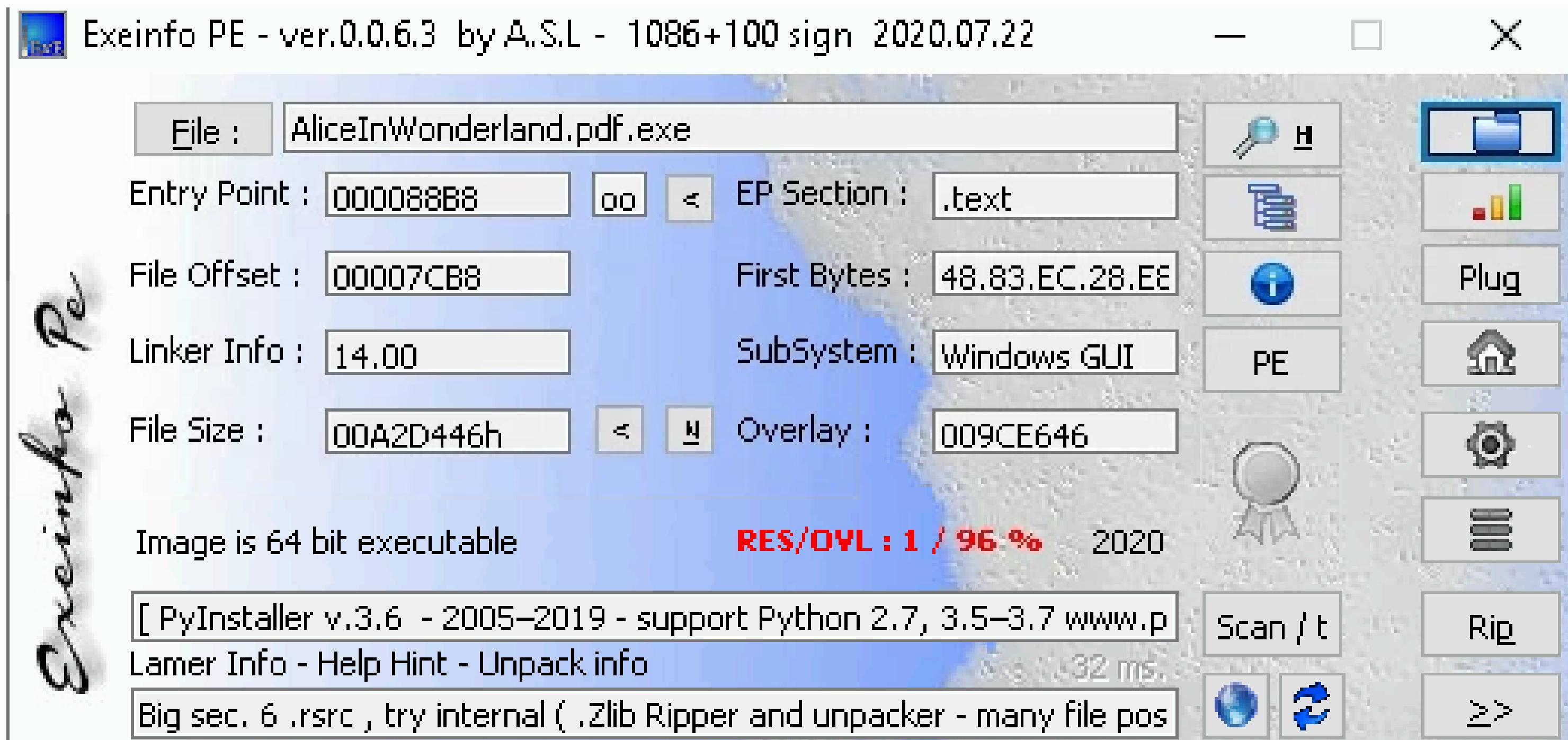
file settings about

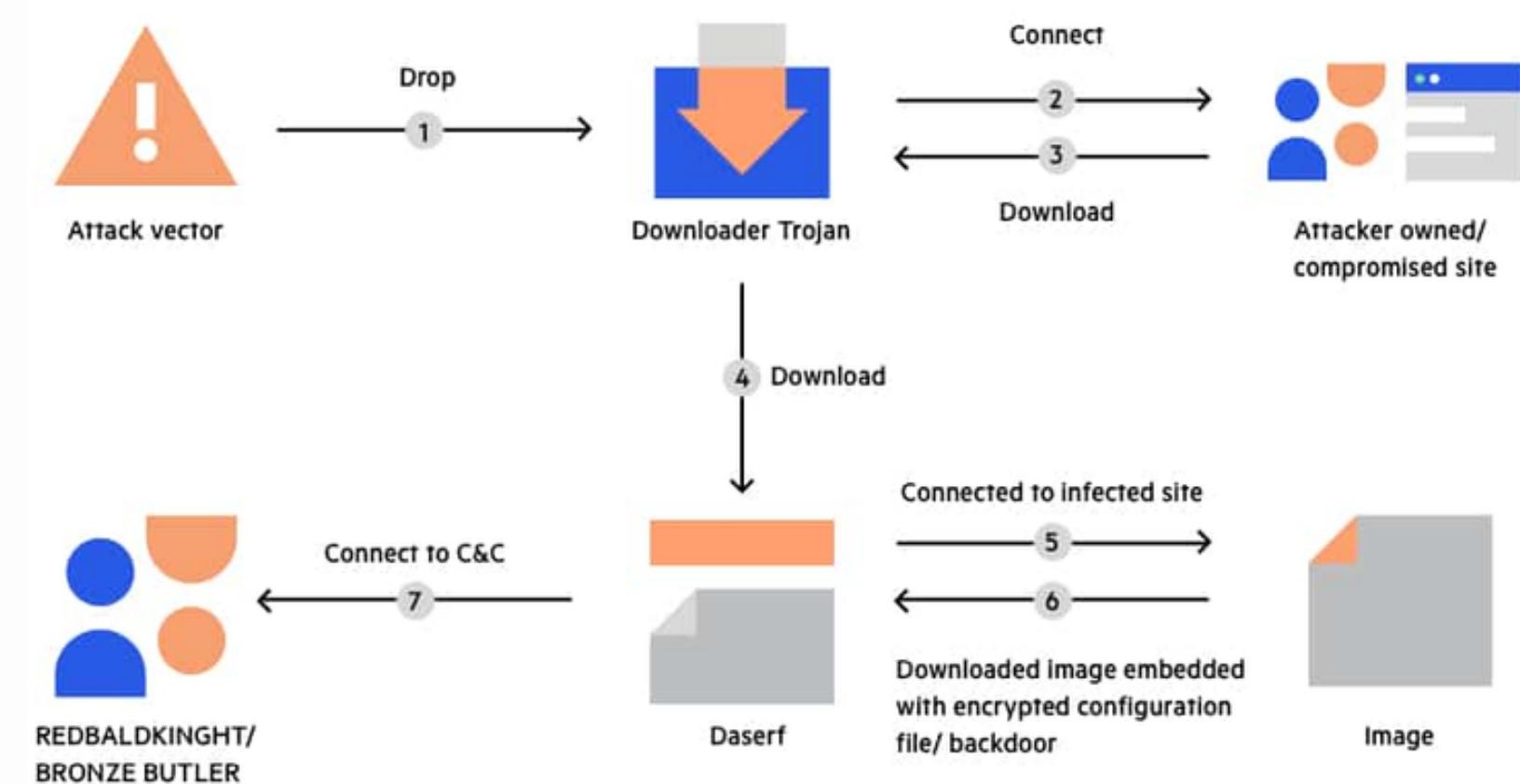
File View Insert Tools Options Help

property	value
md5	<a href="#">918262B6CB56033DBEDA6BBCDCD743A1</a>
sha1	<a href="#">773F58638DC8E7CEE680005AF2018AF11EDC1E9E</a>
sha256	<a href="#">32FBE68CB470344FEF85E0FD087C98C787731E20E39176A054A37CAF736600AED</a>
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 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z ... - . - - - - - - - - - - - - - - - - - - - - - -
file-size	10671174 (bytes)
size-without-overlay	wait...
entropy	7.990
imphash	<a href="#">8038FF70F188E7D568B5CCC73687C4E</a>
signature	n/a
entry-point	40 80 EC 28 E8 4F 05 00 00 48 83 C4 28 E9 82 FE FF FF OC CC 40 53 48 83 EC 20 48 89 D9 33 C9 FF 15
file-version	n/a
description	n/a
file-type	executable
cpu	64-bit
subsystem	GUI
compiler-stamp	0x6FB4E109 (Wed Nov 18 08:53:29 2020)
debugger-stamp	0x5FB4E109 (Wed Nov 18 08:53:29 2020)

# 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 Registry  
. Create File

The screenshot shows two windows from the Process Monitor application. The left window is a timeline of events, and the right window is a process tree.

**Timeline (Left Window):**

Time	Process Name	PID	Operation	Path	Result	Detail
7:01:3...	Aladdinwonder...	2488	CreateFile	C:\Temp\Secret\2023-11-30-190109_2...	SUCCESS	Desired Access: G...
7:01:3...	Aladdinwonder...	2488	QueryInformation...	C:\Temp\Secret\2023-11-30-190109_2...	SUCCESS	VolumeCreationTim...
7:01:3...	Aladdinwonder...	2488	QueryAllInfor...	C:\Temp\Secret\2023-11-30-190109_2...	BUFFER OVERFL...	CreationTime: 11/3...
7:01:3...	Aladdinwonder...	2488	WriteFile	C:\Temp\Secret\2023-11-30-190109_2...	SUCCESS	Offset: 0, Length: 2...
7:01:3...	Aladdinwonder...	2488	CloseFile	C:\Temp\Secret\2023-11-30-190109_2...	SUCCESS	
7:01:3...	Aladdinwonder...	2488	Thread Create		SUCCESS	Thread ID: 5336
7:01:3...	Aladdinwonder...	2488	Thread Exit		SUCCESS	Thread ID: 3808...
7:01:3...	cmd.exe	3168	RegCloseKey	HKCU\Software\Classes	SUCCESS	
7:01:3...	cmd.exe	3168	Thread Exit		SUCCESS	Thread ID: 4460...
7:01:3...	invhost.exe	236	TOP Send	10.0.20.137.3389 -> 10.0.21.101.54842	SUCCESS	Length: 256, stati...
7:01:3...	invhost.exe	236	TOP Receive	10.0.20.137.3389 -> 10.0.21.101.54842	SUCCESS	Length: 39, sequen...
7:01:3...	invhost.exe	236	TOP Send	10.0.20.137.3389 -> 10.0.21.101.54842	SUCCESS	Length: 536, stati...
7:01:4...	Aladdinwonder...	5332	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
7:01:4...	Aladdinwonder...	2488	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
7:01:4...	Aladdinwonder...	5332	RegOpenKey	HKLM\SOFTWARE\Microsoft\KMSwitch	SUCCESS	Desired Access: AL...
7:01:4...	Aladdinwonder...	2488	RegOpenKey	HKLM\SOFTWARE\Microsoft\KMSwitch	SUCCESS	Desired Access: AL...
7:01:4...	Aladdinwonder...	5332	RegCloseKey	HKLM\SOFTWARE\Microsoft\KMSwitch	SUCCESS	
7:01:4...	Aladdinwonder...	2488	RegCloseKey	HKLM\SOFTWARE\Microsoft\KMSwitch	SUCCESS	
7:01:4...	chrome.exe	2080	Thread Exit		SUCCESS	Thread ID: 3620...
7:01:4...	chrome.exe	2080	Thread Exit		SUCCESS	Thread ID: 872, UI...
7:01:4...	invhost.exe	236	TOP Receive	10.0.20.137.3389 -> 10.0.21.101.54842	SUCCESS	Length: 39, sequen...
7:01:4...	invhost.exe	236	TOP Send	10.0.20.137.3389 -> 10.0.21.101.54842	SUCCESS	Length: 366, stati...
7:01:4...	invhost.exe	236	TOP Send	10.0.20.137.3389 -> 10.0.21.101.54842	SUCCESS	Length: 37, stati...
7:01:4...	MoMyRing.exe	2904	CreateFile	C:\Windows\System32\prephys.dll	SUCCESS	Desired Access: R...
7:01:4...	MoMyRing.exe	2904	CreateFile	C:\Windows\System32\prephys.dll	OPLOCK HANDLE...	Control: FSCTL_R...
7:01:4...	MoMyRing.exe	2904	CreateFile	C:\Windows\System32\prephys.dll	SUCCESS	Control: P_FLUSH_L...

**Process Tree (Right Window):**

Process	Description	Image Path	Life Time	Company
cmd.exe (1260)		C:\Windows\system...		
explorer.exe (2740)	Windows Explorer	C:\Windows\Explor...		
Aladdinwonderland.pdf.exe (4432)		C:\Users\Administr...		
Aladdinwonderland.pdf.exe (2488)		C:\Users\Administr...		
cmd.exe (3168)		C:\Windows\system...		
conhost.exe (4712)		C:\Windows\system...		
chrome.exe (2080)		C:\Program Files\...		
chrome.exe (132)		C:\Program Files\...		
chrome.exe (4972)		C:\Program Files\...		
chrome.exe (32300)		C:\Program Files\...		
chrome.exe (4756)		C:\Program Files\...		
chrome.exe (40660)		C:\Program Files\...		
chrome.exe (5360)		C:\Program Files\...		
chrome.exe (5076)		C:\Program Files\...		
chrome.exe (4324)		C:\Program Files\...		
Procmon64.exe (6120)	Process Monitor	C:\Users\Administr...		Syndicale - www...
Aladdinwonderland.pdf.exe (5040)		C:\Users\Administr...		
Aladdinwonderland.pdf.exe (5332)		C:\Users\Administr...		

# 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

Autoruns [EC2AMAZ-L3L528P\Administrator] - Sysinternals: www.sysinternals.com

File Entry Options User Help

Filter:

AppInit KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Office

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURIT...	(Verified) Microsoft Corporation	c:\windows\system32\mscor...	8/8/2018 3:18 AM	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				8/31/2021 12:38 PM	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURIT...	(Verified) Microsoft Corporation	c:\windows\syswow64\msc...	8/8/2018 3:28 AM	
<input checked="" type="checkbox"/> Task Scheduler					
<input type="checkbox"/> Amazon Ec2 L...	Windows PowerShell	(Verified) Microsoft Windows	c:\windows\system32\windo...	1/23/1938 11:20 AM	
<input checked="" type="checkbox"/> General Syste...			c:\users\administor\downl...	11/18/2020 8:53 AM	
<input checked="" type="checkbox"/> GoogleUpdate...	Google Installer	(Verified) Google LLC	c:\program files (x86)\google...	7/27/2021 12:25 AM	
<input checked="" type="checkbox"/> GoogleUpdate...	Google Installer	(Verified) Google LLC	c:\program files (x86)\google...	7/27/2021 12:25 AM	
<input checked="" type="checkbox"/> HKLM\System\CurrentControlSet\Services				11/30/2023 6:43 PM	
<input checked="" type="checkbox"/> AmazonSSMAg...	Amazon SSM Agent: Amazo...	(Verified) Amazon.com Servi...	c:\program files\amazon\ss...	1/1/1970 12:00 AM	
<input checked="" type="checkbox"/> AWSLiteAgent	AW/S Lite Guest Agent: Aw...	(Verified) Amazon Web Servi...	c:\program files\amazon\xen...	12/16/2019 7:58 PM	
<input checked="" type="checkbox"/> cfn-hup	CloudFormation cfn-hup: CloudFormation cfn-hup for Windows		c:\program files\amazon\cfn...	2/21/2021 7:31 PM	

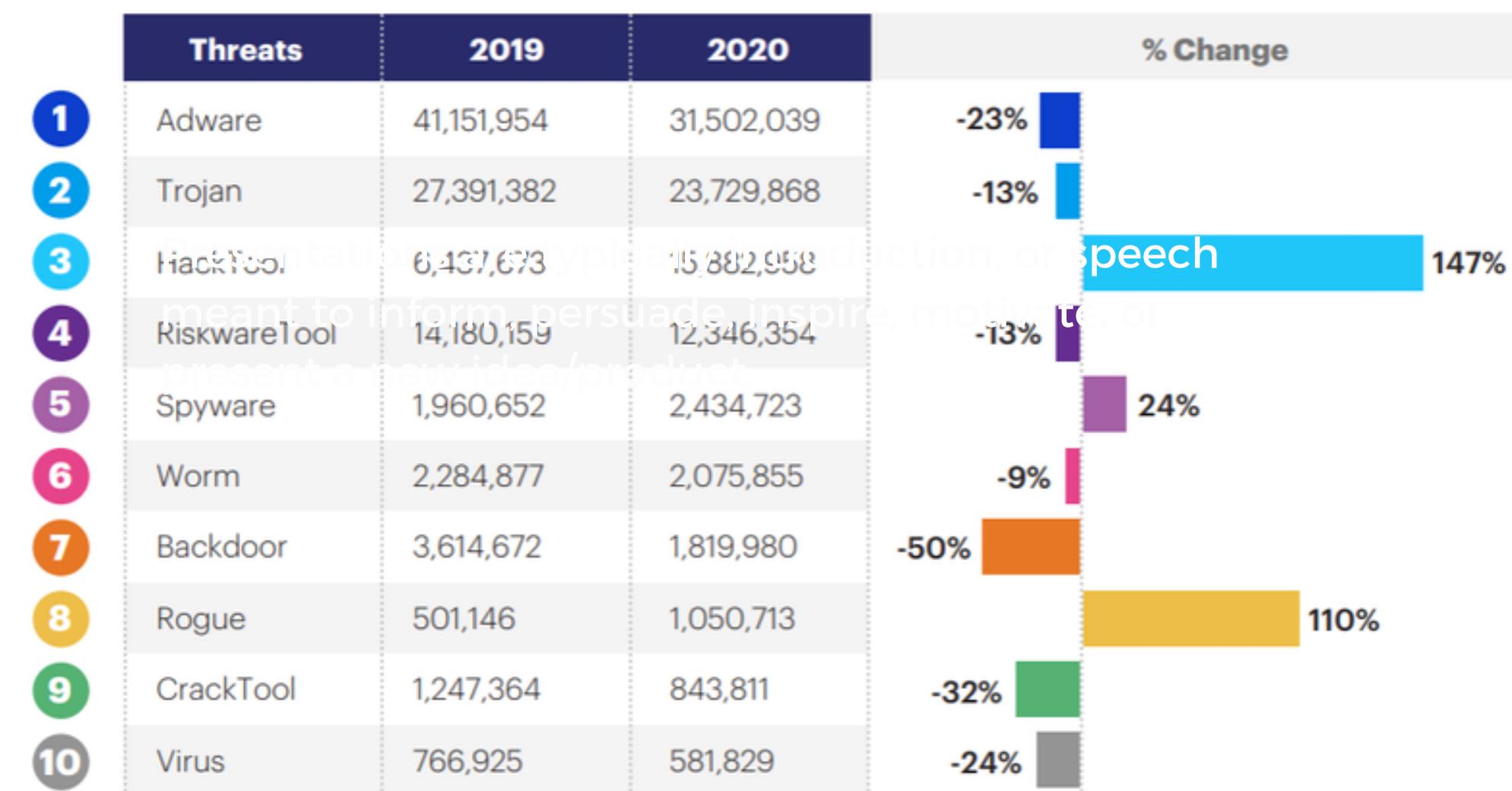
aliceinwonderland.pdf.exe Size: 10,421 K  
Time: 11/18/2020 8:53 AM

# 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





# **THANK YOU**

**For Your Attention**