MALICIOUS

Classifications: Trojan, Banker

Threat Names: Ursnif, Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe**
ID	#7197931
MD5	aa37b36ea7ba39b6c00ae1b01bada3f7
SHA1	90545746e5b23fcdf7db1fa5c30588df2f4c31bf
SHA256	a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7
File Size	177.50 KB
Report Created	2023-03-20 14:03 (UTC+1)
Target Environment	win10_64_20h1_en_base | exe

OVERVIEW

VMRay Threat Identifiers (7 rules, 8 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	2	Banker, Trojan
	• Rule "Ursnif_Gen_C2_Format" from ruleset "Malware" has matched on a memory dump for (process #1) a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe. • Rule "Ursnif_Gen_C2_Format" from ruleset "Malware" has matched on the function strings for (process #1) a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
3/5	Network Connection	All network connection attempts failed	1	-
	• Host "checklist.skype.com" is unavailable.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #1) a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe has a thread which sleeps more than 5.0 minutes.			
1/5	User Data Modification	Uses encryption API	1	-
	• (Process #1) a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe uses above average number of encryption APIs.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe resolves 134 API functions by name.			
1/5	Obfuscation	Overwrites code	1	-
	• (Process #5) wmiprvse.exe overwrites code to possibly hide behavior.			

Mitre ATT&CK Matrix

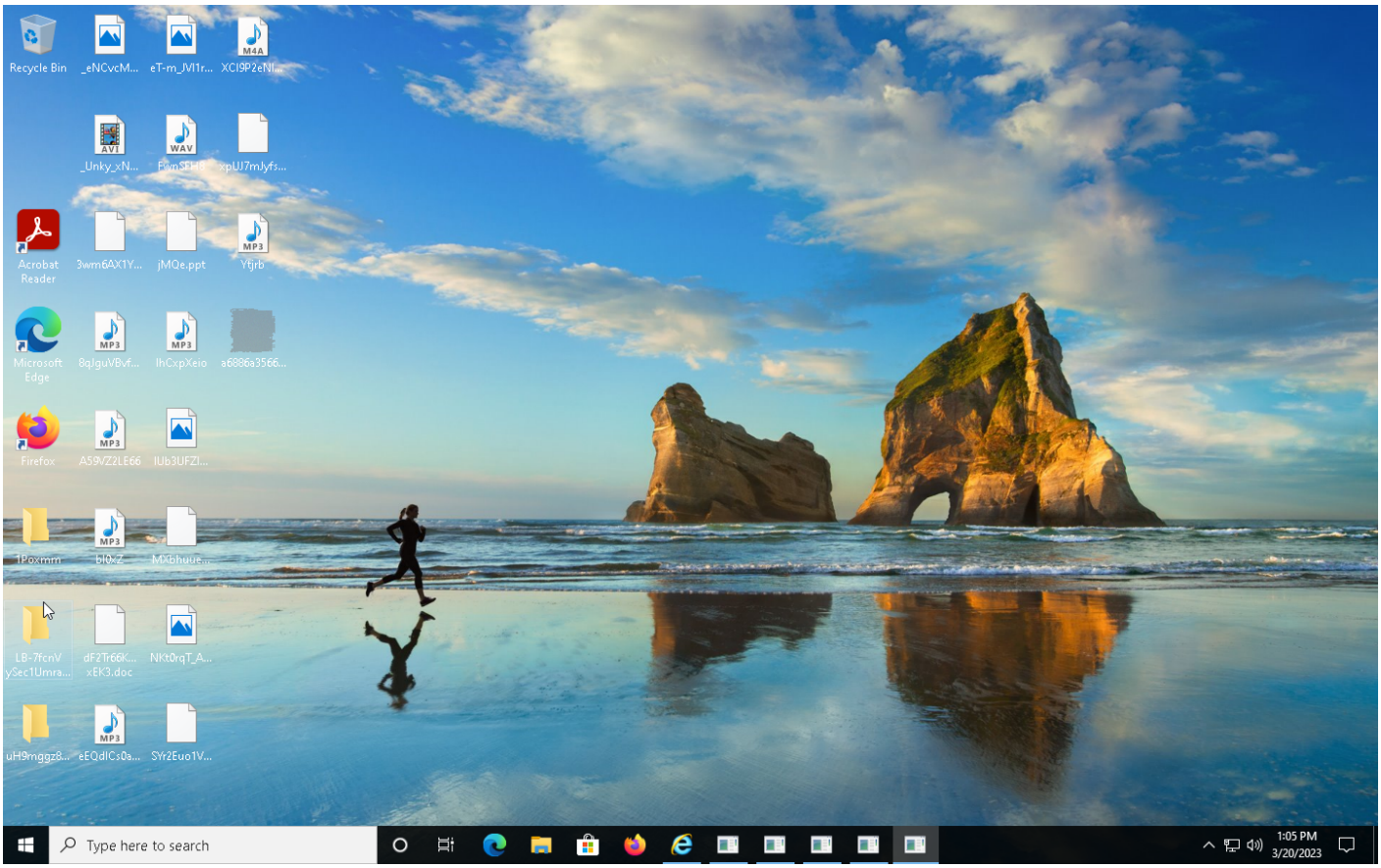
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1045 Software Packing							

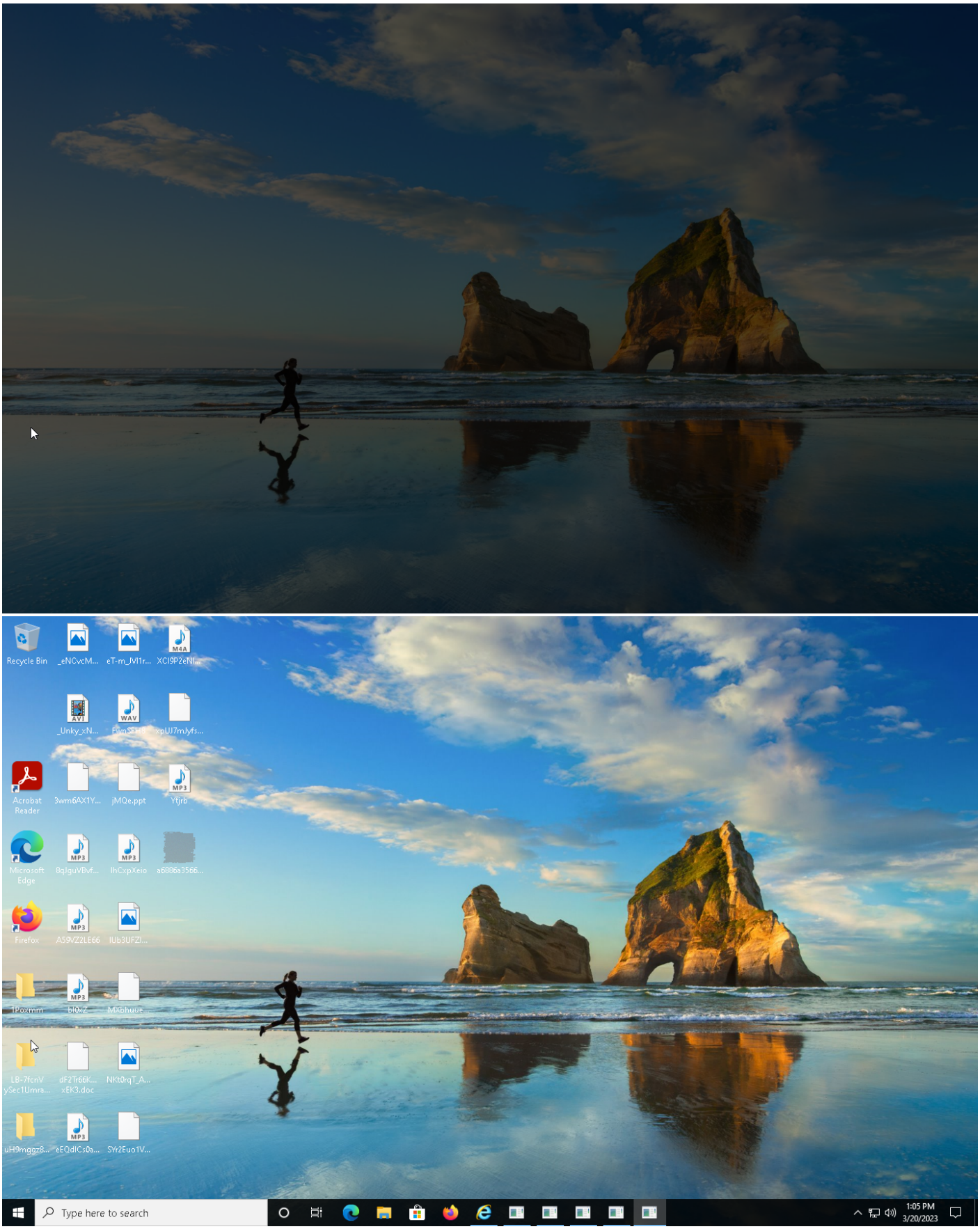
Sample Information

ID	#7197931
MD5	aa37b36ea7ba39b6c00ae1b01bada3f7
SHA1	90545746e5b23fcdf7db1fa5c30588df2f4c31bf
SHA256	a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7
SSDeep	3072:sKUXgTGIAmez+JQAxHun7YB5ahAWIS5UQjV:0gTfBfxAkBSAP5
ImpHash	0c16d61a145a6038e0c4acd3e1db8764
File Name	a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe
File Size	177.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2023-03-20 14:03 (UTC+1)
Analysis Duration	00:03:14
Termination Reason	Timeout
Number of Monitored Processes	3
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	2


Recycle Bin
Acrobat Reader
Microsoft Edge
Firefox
Type here to search
1:05 PM
3/20/2023



Screenshots truncated

NETWORK

General

65 bytes total sent

65 bytes total received

1 ports 53

1 contacted IP addresses

1 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

1 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

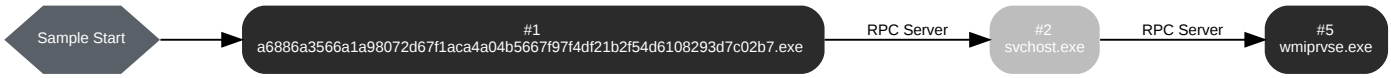
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://checklist[.]skype[.]com/drew/7N8FVl1l9AJ8t_/2FXBBGv5f0p0hYnEyD7Lt/DMqfQBAkw71EWHGO/g1f_2FZGE4xmjwn/l4lIEGW028NXmwEgg6/Afg8c... ...MQAnof9zlC1S3pa5mcWIcV/RkplMIeDPs/Pl_2FmjyX_2FZpC90/fqrcYZetlSsw/NAQybG2gf5f/F_2BAss7PTFanx/0Eota8Pwqb9uV2dw85xrt/Zds5GUbaT/Ib.jlk	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	checklist[.]skype[.]com	NX_DOMAIN	-	-	SUSPICIOUS

BEHAVIOR

Process Graph



Process #1: a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe

ID	1
File Name	c:\users\oqxzraykm\desktop\a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe
Command Line	"C:\Users\OqXZRaykm\Desktop\a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe"
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 128363, Reason: Analysis Target
Unmonitor End Time	End Time: 317630, Reason: Terminated by timeout
Monitor duration	189.27s
Return Code	Unknown
PID	5636
Parent PID	2632
Bitness	32 Bit

Host Behavior

Type	Count
System	20838
Module	219
File	3
Environment	1
-	4
User	4
COM	1
-	1

Network Behavior

Type	Count
HTTP	1
TCP	1

Process #2: svchost.exe

ID	2
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 312530, Reason: RPC Server
Unmonitor End Time	End Time: 317630, Reason: Terminated by timeout
Monitor duration	5.10s
Return Code	Unknown
PID	324
Parent PID	5636
Bitness	64 Bit

Process #5: wmiprvse.exe

ID	5
File Name	c:\windows\syswow64\wbem\wmiprvse.exe
Command Line	C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 315511, Reason: RPC Server
Unmonitor End Time	End Time: 317630, Reason: Terminated by timeout
Monitor duration	2.12s
Return Code	Unknown
PID	2380
Parent PID	324
Bitness	32 Bit

Host Behavior

Type	Count
System	6
Mutex	1
Module	23
Registry	15
File	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7	C:\Users\OqXZRaykm\Desktop\a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe	Sample File	177.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\OqXZRaykm\Desktop\a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe	Accessed File, Sample File	Access	MALICIOUS
C:\Windows\system32\WBEM\Logs\	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://checklist[.]skype[.]com/drew/7N8FVI1I9AJ8t_/2FXBBGv5f0p0hYnEyD7Lt/DMqfQBAkw71EWHGO/g1f_2FZGE4xmjwn/l4lIEGW028NXmwEgg6/Afg8c...MQAnof9zlC1S3pa5mcWIcV/RkpIMIeDPs/PI_2FmjyX_2FZpC90/fqrcYZetISsw/NAQybG2gf5f/F_2BAss7PTFanx/0Eota8Pwqb9uV2dw85xrt/Zds5GUbaT/Ib.jlk	Extracted	-	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
checklist[.]skype[.]com	-	-	-	SUSPICIOUS

Mutex

Name	Operations	Parent Process Name	Verdict
-	access	wmiprvse.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\IE10RunOnceLastShown	write, access	wmiprvse.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\IE10RunOnceLastShown_TIMESTAMP	write, access	wmiprvse.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\Check_Associations	write, access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM\EnableObjectValidation	read, access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM	access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM	access, create	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer	access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\AmsiEnable	read, access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version	read, access	wmiprvse.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main	access	wmiprvse.exe	CLEAN

Process

Process Name	Commandline	Verdict
a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe	"C:\Users\OqXZRaykm\Desktop\a6886a3566a1a98072d67f1aca4a04b5667f97f4df21b2f54d6108293d7c02b7.exe"	MALICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs -p	CLEAN
wmiprvse.exe	C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	Ursnif_Gen_C2_Format	C2 format string of multiple Ursnif variants	Memory Dump	-	Banker, Trojan	5/5
Malware	Ursnif_Gen_C2_Format	C2 format string of multiple Ursnif variants	Function Strings	-	Banker, Trojan	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_20h1_en_base
Description	-
Architecture	x86 64-bit
Operating System	Windows 10 20H1
Kernel Version	10.0.19041.208 (dc9233f8-5819-e3d0-929a-7bde0b87f0b9)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2023.1.0
Dynamic Engine Version	2023.1.0 / 01/31/2023 04:27
Static Engine Version	2023.1.0.0 / 2023-01-31 03:00:19
AV Exceptions Version	2023.1.1.6 / 2023-02-03 15:34:21
Link Detonation Heuristics Version	2023.1.1.12 / 2023-02-20 08:47:29
Smart Memory Dumping Rules Version	2023.1.1.6 / 2023-02-03 15:34:21
Config Extractors Version	2023.1.1.16 / 2023-03-09 20:16:03
Signature Trust Store Version	2023.1.1.7 / 2023-02-06 18:37:42
VMRay Threat Identifiers Version	2023.1.1.16 / 2023-03-09 20:16:03
YARA Built-in Ruleset Version	2023.1.1.16

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	Not installed
Microsoft Office Version	Not installed
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.207.19041.0
Chrome Version	Not installed
Firefox Version	108.0
Flash Version	Not installed
Java Version	8.0.3610.9

System Information

Sample Directory	C:\Users\OqXZRaykm\Desktop
Computer Name	PXTHFFRYO7
User Domain	PXTHFFRYO7
User Name	OqXZRaykm
User Profile	C:\Users\OqXZRaykm
Temp Directory	C:\Users\OQXZRA~1\AppData\Local\Temp

System Root	C:\Windows