MALICIOUS

Classifications: Spyware | Backdoor | Injector

Threat Names: RedLine.E | Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-64)**
File Name	**project.exe**
ID	#10723777
MD5	e9c6afa3e88ae62a18ef5ac3a6ac6108
SHA1	f7a14d8a3906808de1b7181e9c369439c95ae80b
SHA256	be735fb6d9811ebc95011003c79b1df34a438e765f9a2065c1ef98930e72c698
File Size	82981.92 KB
Report Created	2024-06-27 06:00 (UTC+2)
Target Environment	windows 10 (64bit 20H1 -EN-) | exe

OVERVIEW

VMRay Threat Identifiers (39 rules, 184 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	RedLine configuration was extracted	1	Spyware
	• A configuration for RedLine was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
	• YARA detected "RedLine_E" from ruleset "Malware" in memory dump data from (process #18) msbuild.exe.			
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
	• Sample enumerates processes, queries network configuration, collects hardware information and collects operating system information which indicates system fingerprinting.			
5/5	Data Collection	Combination of other detections shows multiple input capture behaviors	1	Spyware
	• (Process #18) msbuild.exe takes screenshots and potentially exfiltrates data.			
4/5	Defense Evasion	Modifies Windows Defender configuration	1	-
	• (Process #9) powershell.exe uses (Process #11) powershell.exe to add C:\Users\OqXZRaykm\Desktop\project.exe to Windows Defender exclusions.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #14) driver1.exe modifies memory of (process #18) msbuild.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #14) driver1.exe alters context of (process #18) msbuild.exe.			
4/5	Reputation	Malicious file detected via reputation	1	-
	• Reputation analysis labels file "C:\ProgramData\driver1.exe" as Mal/Generic-S.			
3/5	Data Collection	Takes screenshot	1	-
	• (Process #18) msbuild.exe takes a screenshot using BitBlt API.			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #18) msbuild.exe tries to detect antivirus software via WMI query: "SELECT * FROM AntivirusProduct".			
3/5	Defense Evasion	Tries to detect the presence of anti-spyware software	1	-
	• (Process #18) msbuild.exe tries to detect anti-spyware software via WMI query: "SELECT * FROM AntiSpyWareProduct".			
3/5	Defense Evasion	Tries to detect the presence of firewall software	1	-
	• (Process #18) msbuild.exe tries to detect firewall via WMI query: "SELECT * FROM FirewallProduct".			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #1) project.exe tries to detect "wine" by calling GetProcAddress() on "wine_get_version".			
2/5	Discovery	Collects hardware properties	5	-

Score	Category	Operation	Count	Classification
	• (Process #1) project.exe queries hardware properties via WMI: SELECT PNPDeviceID, Size FROM Win32_DiskDrive . • (Process #6) wmic.exe queries hardware properties via WMI: SELECT Name FROM win32_VideoController. • (Process #18) msbuild.exe queries hardware properties via WMI: SELECT * FROM Win32_DiskDrive. • (Process #18) msbuild.exe queries hardware properties via WMI: SELECT * FROM Win32_Processor. • (Process #18) msbuild.exe queries hardware properties via WMI: SELECT * FROM Win32_VideoController.			
2/5	Defense Evasion	Accesses physical drive	1	-
	• (Process #1) project.exe accesses physical drive "\\.\PHYSICALDRIVE0".			
2/5	Discovery	Enumerates running processes	1	-
	• (Process #18) msbuild.exe enumerates running processes via WMI query SELECT * FROM Win32_Process Where SessionId='1'.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #18) msbuild.exe reads the network adapters' addresses by API.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #18) msbuild.exe queries OS version via WMI query: SELECT * FROM Win32_OperatingSystem.			
2/5	Discovery	Searches for sensitive FTP data	1	-
	• (Process #18) msbuild.exe searches for sensitive data of FTP application "Total Commander" by file.			
2/5	Discovery	Searches for sensitive browser data	23	-
	• (Process #18) msbuild.exe searches for sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Chromium" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Google Chrome" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Opera" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Maple Studio" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "7Star" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "CentBrowser" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Chedot" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Vivaldi" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Kometa" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Elements Browser" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Epic Privacy Browser" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Uran" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Orbitum" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Comodo Dragon" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Torch" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Yandex Browser" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Sputnik" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "CocCoc" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Mozilla Firefox" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "k-Meleon" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Comodo IceDragon" by file. • (Process #18) msbuild.exe searches for sensitive data of web browser "Cyberfox" by file.		
2/5	Discovery	Searches for cryptocurrency wallet locations	2	-
	• (Process #18) msbuild.exe searches for the cryptocurrency wallet "Electrum Bitcoin Wallet" for "BTC". • (Process #18) msbuild.exe searches for the cryptocurrency wallet "Exodus Cryptocurrency Wallet".			

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #18) msbuild.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Discovery	Searches for sensitive mail data	1	-
	• (Process #18) msbuild.exe searches for sensitive data of mail application "Mozilla Thunderbird" by file.			
2/5	Network Connection	Sets up server that accepts incoming connections	3	Backdoor
	• (Process #1) project.exe starts a TCP server listening on port 49803. • (Process #1) project.exe starts a TCP server listening on port 49797. • (Process #1) project.exe starts a TCP server listening on port 49804.			
2/5	Heuristics	Signed executable failed signature validation	1	-
	• C:\Users\OqXZRaykm\Desktop\project.exe is signed, but signature validation failed.			
1/5	Privilege Escalation	Enables process privileges	3	-
	• (Process #1) project.exe enables process privilege "SeDebugPrivilege". • (Process #5) wmiprvse.exe enables process privilege "SeDebugPrivilege". • (Process #18) msbuild.exe enables process privilege "SeDebugPrivilege".			
1/5	Hide Tracks	Creates process with hidden window	7	-
	• (Process #1) project.exe starts (process #6) wmic.exe with a hidden window. • (Process #1) project.exe starts (process #7) tasklist.exe with a hidden window. • (Process #1) project.exe starts (process #9) powershell.exe with a hidden window. • (Process #9) powershell.exe starts (process #11) powershell.exe with a hidden window. • (Process #1) project.exe starts (process #13) wmic.exe with a hidden window. • (Process #1) project.exe starts (process #14) driver1.exe with a hidden window. • (Process #14) driver1.exe starts (process #18) msbuild.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	100	-

- (Process #5) wmiprvse.exe reads from winlogon.exe.
- (Process #5) wmiprvse.exe reads from lsass.exe.
- (Process #5) wmiprvse.exe reads from fontdrvhost.exe.
- (Process #5) wmiprvse.exe reads from svchost.exe.
- (Process #5) wmiprvse.exe reads from dwm.exe.
- (Process #5) wmiprvse.exe reads from (process #3) svchost.exe.
- (Process #5) wmiprvse.exe reads from (process #16) svchost.exe.
- (Process #5) wmiprvse.exe reads from (process #21) svchost.exe.
- (Process #5) wmiprvse.exe reads from spoolsv.exe.
- (Process #5) wmiprvse.exe reads from sihost.exe.
- (Process #5) wmiprvse.exe reads from (process #23) svchost.exe.
- (Process #5) wmiprvse.exe reads from taskhostw.exe.
- (Process #5) wmiprvse.exe reads from (process #22) explorer.exe.
- (Process #5) wmiprvse.exe reads from startmenuexperiencehost.exe.
- (Process #5) wmiprvse.exe reads from runtimebroker.exe.
- (Process #5) wmiprvse.exe reads from searchapp.exe.
- (Process #5) wmiprvse.exe reads from trustedinstaller.exe.
- (Process #5) wmiprvse.exe reads from tiworker.exe.
- (Process #5) wmiprvse.exe reads from (process #4) wmiprvse.exe.
- (Process #5) wmiprvse.exe reads from wmiadap.exe.
- (Process #5) wmiprvse.exe reads from musnotification.exe.
- (Process #5) wmiprvse.exe reads from devicecensus.exe.
- (Process #5) wmiprvse.exe reads from useroobebroker.exe.
- (Process #5) wmiprvse.exe reads from iexplore.exe.
- (Process #5) wmiprvse.exe reads from mousocoreworker.exe.
- (Process #5) wmiprvse.exe reads from population-successful.exe.
- (Process #5) wmiprvse.exe reads from key_boy_method.exe.
- (Process #5) wmiprvse.exe reads from conference_animal.exe.
- (Process #5) wmiprvse.exe reads from evidence-write.exe.
- (Process #5) wmiprvse.exe reads from building_on.exe.
- (Process #5) wmiprvse.exe reads from professor.exe.
- (Process #5) wmiprvse.exe reads from total patient memory.exe.
- (Process #5) wmiprvse.exe reads from accept_yet_pick.exe.
- (Process #5) wmiprvse.exe reads from much.exe.
- (Process #5) wmiprvse.exe reads from low_style.exe.
- (Process #5) wmiprvse.exe reads from argue.exe.
- (Process #5) wmiprvse.exe reads from ground_stop_part.exe.
- (Process #5) wmiprvse.exe reads from question_interest.exe.
- (Process #5) wmiprvse.exe reads from home government.exe.
- (Process #5) wmiprvse.exe reads from item-analysis-heavy.exe.
- (Process #5) wmiprvse.exe reads from goal.exe.
- (Process #5) wmiprvse.exe reads from walkintoland.exe.
- (Process #5) wmiprvse.exe reads from 3dftp.exe.
- (Process #5) wmiprvse.exe reads from absolutetelnet.exe.
- (Process #5) wmiprvse.exe reads from alftp.exe.
- (Process #5) wmiprvse.exe reads from barca.exe.
- (Process #5) wmiprvse.exe reads from bitkinex.exe.
- (Process #5) wmiprvse.exe reads from coreftp.exe.
- (Process #5) wmiprvse.exe reads from far.exe.
- (Process #5) wmiprvse.exe reads from filezilla.exe.
- (Process #5) wmiprvse.exe reads from flashfxp.exe.
- (Process #5) wmiprvse.exe reads from fling.exe.
- (Process #5) wmiprvse.exe reads from foxmailincmail.exe.
- (Process #5) wmiprvse.exe reads from gmailnotifierpro.exe.
- (Process #5) wmiprvse.exe reads from icq.exe.
- (Process #5) wmiprvse.exe reads from leechftp.exe.
- (Process #5) wmiprvse.exe reads from sppextcomobj.exe.
- (Process #5) wmiprvse.exe reads from smartftp.exe.
- (Process #5) wmiprvse.exe reads from shellexperiencehost.exe.
- (Process #5) wmiprvse.exe reads from operamailexe.

Score	Category	Operation	Count	Classification
1/5	Discovery	Executes WMI query	1	-
	• (Process #13) wmic.exe executes WMI query: SELECT UUID FROM Win32_ComputerSystemProduct.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #14) driver1.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Discovery	Possibly does reconnaissance	3	-
	• (Process #18) msbuild.exe tries to gather information about application "Steam" by registry. • (Process #18) msbuild.exe tries to gather information about application "FileZilla" by file. • (Process #18) msbuild.exe tries to gather information about application "Mozilla Firefox" by file.			
1/5	Network Connection	Performs DNS request	2	-
	• (Process #18) msbuild.exe resolves hostname "aw.knocin.xyz" to IP "78.47.64.127". • (Process #18) msbuild.exe resolves hostname "t.me" to IP "149.154.167.99".			
1/5	Network Connection	Connects to remote host	4	-
	• (Process #1) project.exe opens an outgoing TCP connection to host "147.45.47.37:1445". • (Process #1) project.exe opens an outgoing TCP connection to host "147.45.47.37:1488". • (Process #18) msbuild.exe opens an outgoing TCP connection to host "78.47.64.127:3306". • (Process #18) msbuild.exe opens an outgoing TCP connection to host "149.154.167.99:443".			
1/5	Network Connection	Downloads file	1	-
	• (Process #1) project.exe downloads file via http from hxxp://147[.]45[.]47[.]37:1488/thot/thot.rar.			
1/5	Network Connection	Tries to connect using an uncommon port	3	-
	• (Process #1) project.exe tries to connect to TCP port 1445 at 147.45.47.37. • (Process #1) project.exe tries to connect to TCP port 1488 at 147.45.47.37. • (Process #18) msbuild.exe tries to connect to TCP port 3306 at 78.47.64.127.			
1/5	Obfuscation	Resolves API functions dynamically	2	-
	• (Process #1) project.exe resolves 108 API functions by name. • (Process #18) msbuild.exe resolves 52 API functions by name.			
1/5	Execution	Drops PE file	1	-
	• (Process #1) project.exe drops file "C:\ProgramData\driver1.exe".			
1/5	Defense Evasion	Loads a dropped DLL	1	-
	• (Process #14) driver1.exe loads dropped DLL d3d9.dll.			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\ProgramData\driver1.exe".			

Malware Configuration: RedLine

Metadata	Key	Extracted Value
Version	Value	1
Mission ID	Value	5213892547_99
Encryption Key	Key Algorithm	VGhpZ2dpbmc= xor
URL	Url	https://t.me/+J_Z1QGHfHko0MGZi*https://steamcommunity.com/id/elcadillac

Mitre ATT&CK Matrix

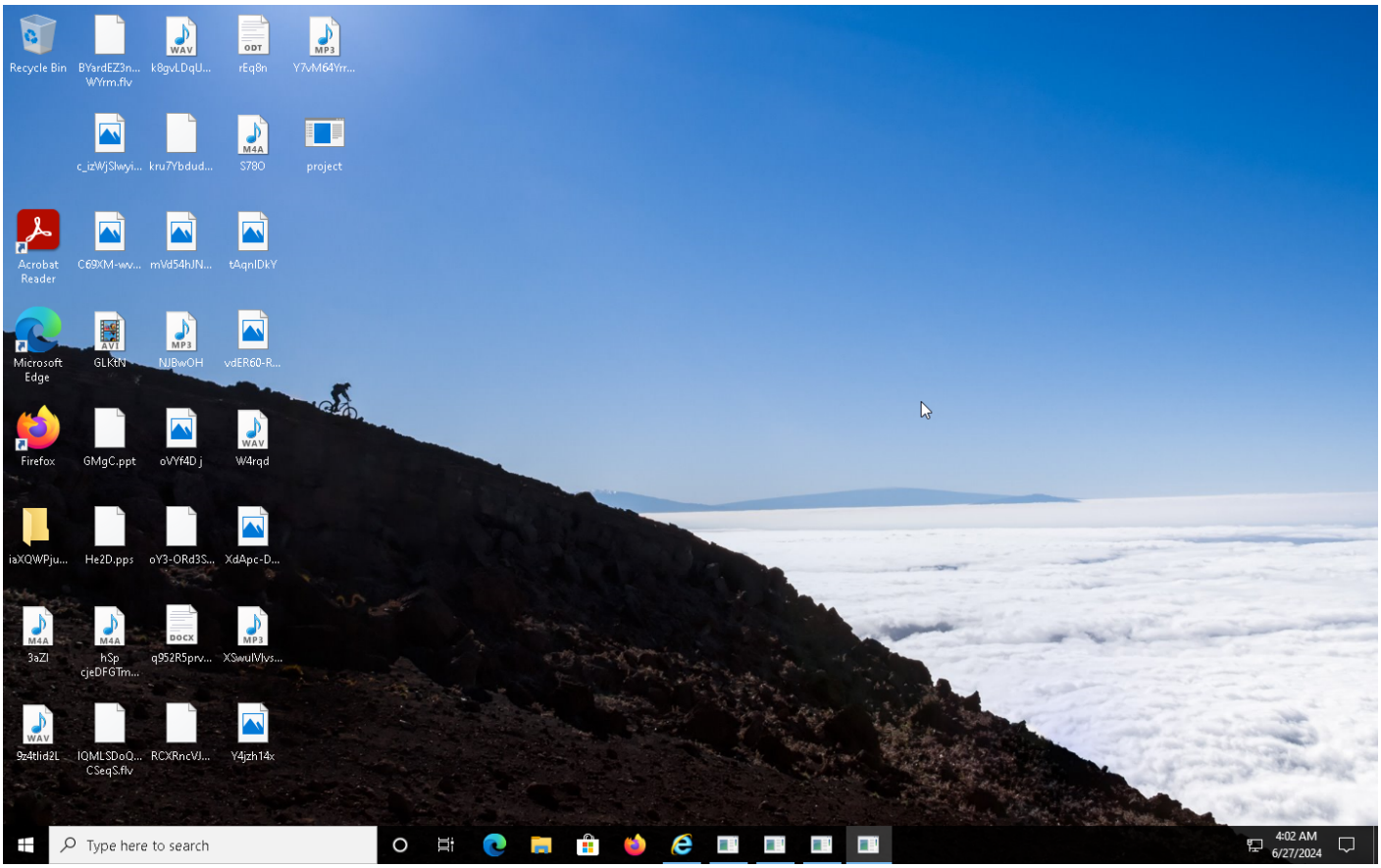
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1497 Virtualization/ Sandbox Evasion	#T1081 Credentials in Files	#T1497 Virtualization/ Sandbox Evasion	#T1105 Remote File Copy	#T1113 Screen Capture	#T1071 Standard Application Layer Protocol		
	#T1047 Windows Management Instrumentation			#T1143 Hidden Window	#T1056 Input Capture	#T1082 System Information Discovery		#T1119 Automated Collection	#T1105 Remote File Copy		
				#T1006 File System Logical Offsets	#T1552.001 Credentials In Files	#T1016 System Network Configuration Discovery		#T1005 Data from Local System	#T1065 Uncommonly Used Port		
				#T1045 Software Packing	#T1056 Input Capture	#T1083 File and Directory Discovery		#T1056 Input Capture	#T1071.001 Web Protocols		
				#T1497.001 System Checks		#T1012 Query Registry		#T1113 Screen Capture	#T1105 Ingress Tool Transfer		
				#T1564.003 Hidden Window		#T1063 Security Software Discovery		#T1119 Automated Collection	#T1571 Non-Standard Port		
				#T1006 Direct Volume Access		#T1497.001 System Checks		#T1005 Data from Local System			
				#T1027.002 Software Packing		#T1082 System Information Discovery		#T1056 Input Capture			
						#T1016 System Network Configuration Discovery					
						#T1083 File and Directory Discovery					
						#T1012 Query Registry					
						#T1518.001 Security Software Discovery					

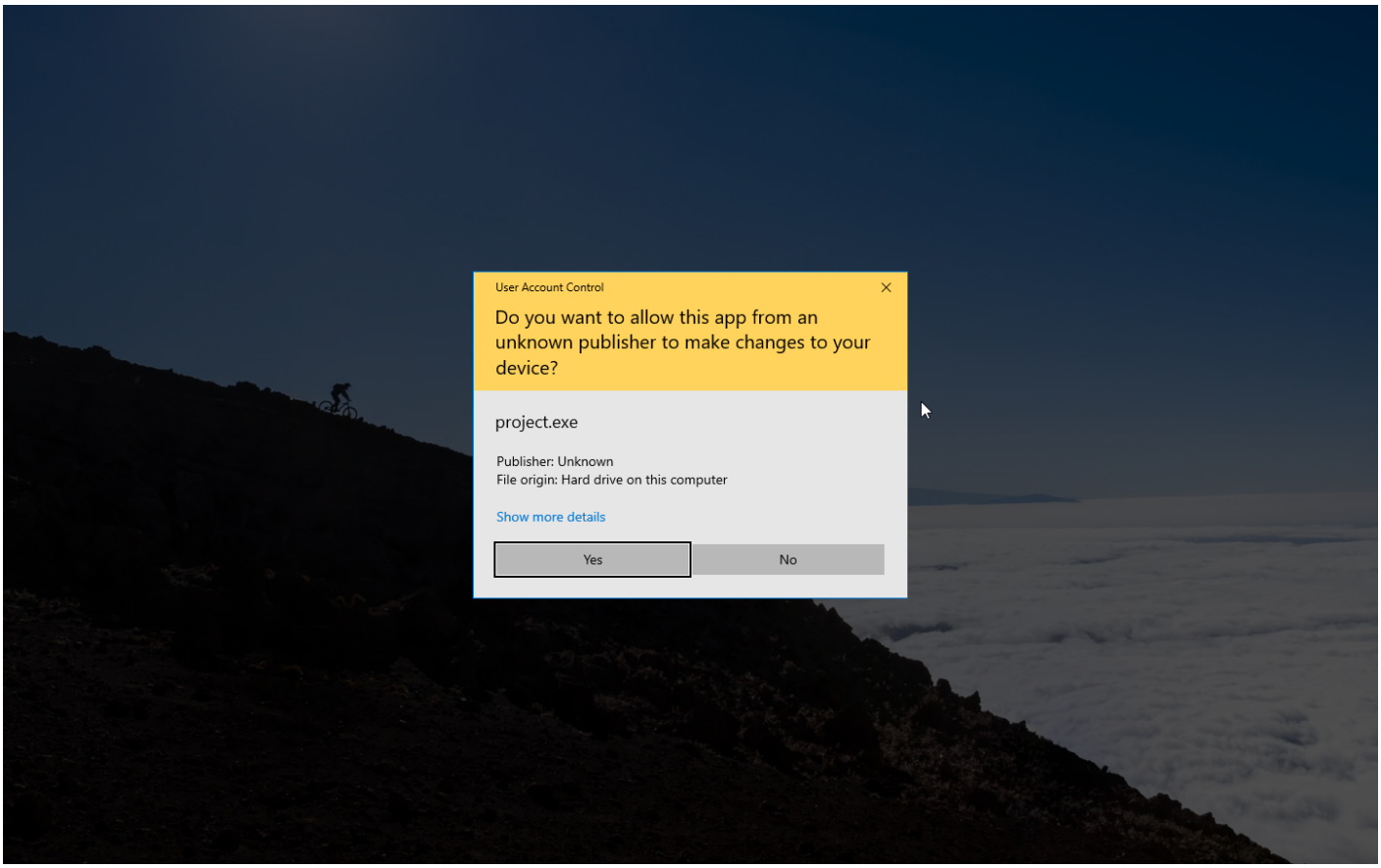
Sample Information

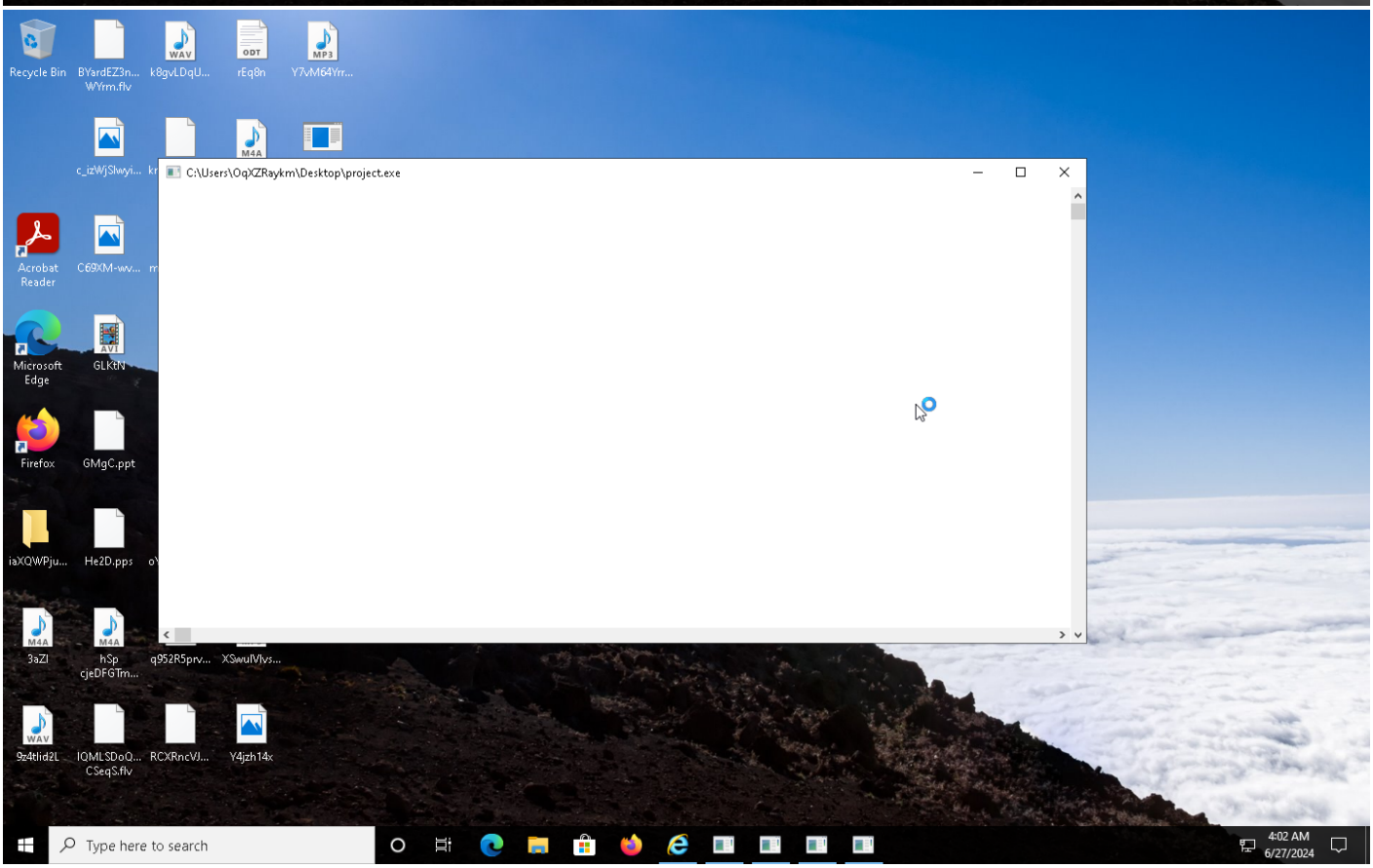
ID	#10723777
MD5	e9c6afa3e88ae62a18ef5ac3a6ac6108
SHA1	f7a14d8a3906808de1b7181e9c369439c95ae80b
SHA256	be735fb6d9811ebc95011003c79b1df34a438e765f9a2065c1ef98930e72c698
SSDeep	786432:Z/i5jul6pr3WPPzFCmoFuTF0XUZpMgniP3l3gennj2:ZbASPrVpMgZUi
ImpHash	ea509d361799935a94335b88f534a970
File Name	project.exe
File Size	82981.92 KB
Sample Type	Windows Exe (x86-64)
Has Macros	✔

Analysis Information

Creation Time	2024-06-27 06:00 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	11
Execution Successful	True
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	1


Recycle Bin
Acrobat Reader
Microsoft Edge
Firefox
Type here to search
4:02 AM
6/27/2024





Screenshots truncated

NETWORK

General

1523.88 KB total sent

300.15 KB total received

5 ports 1445, 3306, 1488, 53, 443

4 contacted IP addresses

13 URLs extracted

4 files downloaded

1 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

4 URLs contacted, 2 servers

4 sessions, 2.13 KB sent, 288.93 KB received

HTTP Requests

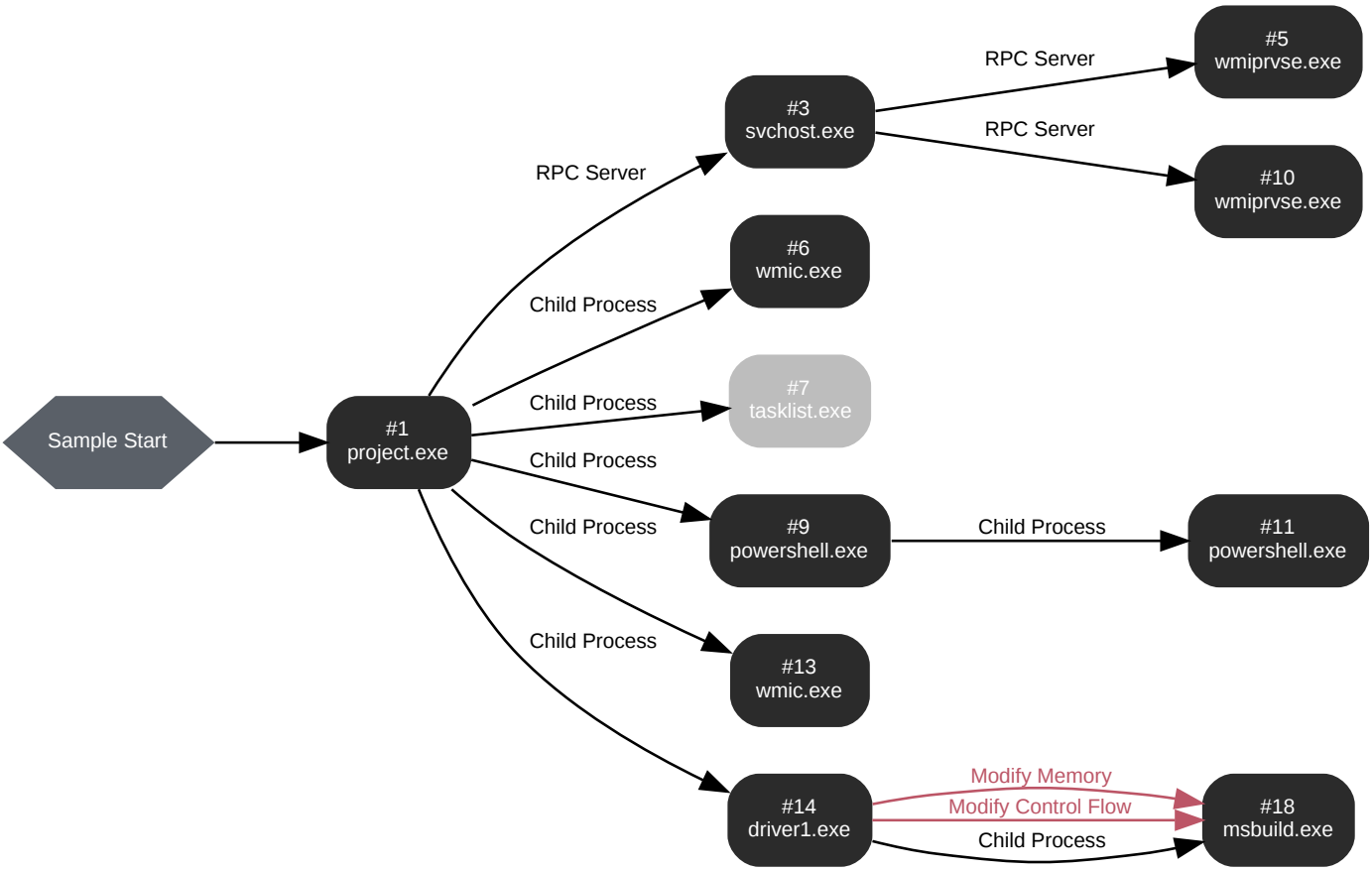
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://telegram[.]org/dl?tme=a1fa6b9791b4d00d4e_10461190331160479626	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/img/website_icon.svg?4	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/css/font-roboto.css?1	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/img/apple-touch-icon.png	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/img/favicon-32x32.png	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/img/favicon.ico	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/css/bootstrap.min.css?3	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/img/favicon-16x16.png	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/css/telegram.css?237	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/js/tgwallpaper.min.js?3	-	-	-	0 bytes	CLEAN
GET	hxxp://147[.]45[.]47[.]37:1445/user72145/json	-	-	-	0 bytes	CLEAN
GET	hxxp://147[.]45[.]47[.]37:1445/user72145?reason=MTgzN0ZBM0ltODQwRC1FOEJFLTQ2NTMtMjAzMDQwNTA2MDk5aWxvdmVpdA==	-	-	-	0 bytes	CLEAN
GET	hxxp://147[.]45[.]47[.]37:1488/thot/thot.rar	-	-	-	0 bytes	
GET	hxxps://web[.]telegram[.]org	-	-	-	0 bytes	CLEAN
GET	hxxps://t[.]me/+J_Z1QGHfHko0MGZi	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	aw[.]knocin[.]xyz	NO_ERROR	78.47.64.127	-	CLEAN
A	t[.]me	NO_ERROR	149.154.167.99	-	CLEAN

BEHAVIOR

Process Graph



Process #1: project.exe

ID	1
File Name	c:\users\oqxzraykm\desktop\project.exe
Command Line	"C:\Users\OqXZRaykm\Desktop\project.exe"
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 162840, Reason: Analysis Target
Unmonitor End Time	End Time: 313365, Reason: Terminated
Monitor duration	150.53s
Return Code	0
PID	5784
Parent PID	-
Bitness	64 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\ProgramData\driver1.exe	558.50 KB	29d3deeb4cd5a45eef40bae38033d9dd4a4898d2659ba16b93666e2bfe55ac35	✖
C:\ProgramData\driver1.rar	259.84 KB	8103f74aedf1f42289b823a56ef991c61d33e35e2b28e2388961a31b2a87491f	✖

Host Behavior

Type	Count
Module	150
System	52
File	594
-	16
Environment	595
User	2
Registry	1297
COM	12
-	2
-	292
Process	5
Window	1

Network Behavior

Type	Count
HTTP	3
TCP	3

Process #3: svchost.exe

ID	3
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: 186601, Reason: RPC Server
Unmonitor End Time	End Time: 404114, Reason: Terminated by timeout
Monitor duration	217.51s
Return Code	Unknown
PID	8
Parent PID	5784
Bitness	64 Bit

Host Behavior

Type	Count
Registry	8
System	2

Process #5: wmiprvse.exe

ID	5
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 186601, Reason: RPC Server
Unmonitor End Time	End Time: 404114, Reason: Terminated by timeout
Monitor duration	217.51s
Return Code	Unknown
PID	2340
Parent PID	8
Bitness	64 Bit

Host Behavior

Type	Count
Module	48
User	9
System	1230
Process	4182
-	7077
Registry	2
COM	2

Process #6: wmic.exe

ID	6
File Name	c:\windows\system32\wbem\wmic.exe
Command Line	wmic path win32_VideoController get name
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 190211, Reason: Child Process
Unmonitor End Time	End Time: 194113, Reason: Terminated
Monitor duration	3.90s
Return Code	0
PID	4644
Parent PID	5784
Bitness	64 Bit

Host Behavior

Type	Count
Module	9
COM	9
System	7
Registry	6
File	8
-	1

Process #7: tasklist.exe

ID	7
File Name	c:\windows\system32\tasklist.exe
Command Line	tasklist
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 191890, Reason: Child Process
Unmonitor End Time	End Time: 197235, Reason: Terminated
Monitor duration	5.34s
Return Code	0
PID	4688
Parent PID	5784
Bitness	64 Bit

Process #9: powershell.exe

ID	9
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	powershell -WindowStyle hidden -Command "Add-MpPreference -ExclusionPath \"C:\ProgramData\";" powershell -WindowStyle hidden -Command "Add-MpPreference -ExclusionPath \"C:\Users\OqXZRaykm\Desktop\project.exe\""
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 202506, Reason: Child Process
Unmonitor End Time	End Time: 280981, Reason: Terminated
Monitor duration	78.47s
Return Code	1
PID	4968
Parent PID	5784
Bitness	64 Bit

Host Behavior

Type	Count
Environment	60
Registry	70
File	526
System	44
-	26
Module	11
COM	4
Process	1

Process #10: wmiprvse.exe

ID	10
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 240186, Reason: RPC Server
Unmonitor End Time	End Time: 372296, Reason: Terminated
Monitor duration	132.11s
Return Code	0
PID	3816
Parent PID	8
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Mutex	1
Module	23
Registry	6
File	1

Process #11: powershell.exe

ID	11
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle hidden -Command Add-MpPreference -ExclusionPath C:\Users\OqXZRaykm\Desktop\project.exe
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 247560, Reason: Child Process
Unmonitor End Time	End Time: 280481, Reason: Terminated
Monitor duration	32.92s
Return Code	1
PID	4508
Parent PID	4968
Bitness	64 Bit

Host Behavior

Type	Count
Environment	52
Registry	70
File	514
System	44
-	26
Module	11
COM	4

Process #13: wmic.exe

ID	13
File Name	c:\windows\system32\wbem\wmic.exe
Command Line	wmic csproduct get uuid
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 283022, Reason: Child Process
Unmonitor End Time	End Time: 286945, Reason: Terminated
Monitor duration	3.92s
Return Code	0
PID	232
Parent PID	5784
Bitness	64 Bit

Host Behavior

Type	Count
Module	9
COM	9
System	7
Registry	6
File	8
-	1

Process #14: driver1.exe

ID	14
File Name	c:\programdata\driver1.exe
Command Line	C:\ProgramData\driver1.exe
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 284840, Reason: Child Process
Unmonitor End Time	End Time: 312525, Reason: Terminated
Monitor duration	27.68s
Return Code	0
PID	4304
Parent PID	5784
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\OqXZRaykm\AppData\Roaming\d3d9.dll	237.00 KB	9404863d23f85e6a1480bc2490a391042fa33287db5bbafd21cefccceed2d10c	✖

Host Behavior

Type	Count
Registry	1
File	15
Module	30
Environment	1
Process	2
-	3
-	7

Process #18: msbuild.exe

ID	18
File Name	c:\windows\microsoft.net\framework\v4.0.30319\msbuild.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe"
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 302431, Reason: Child Process
Unmonitor End Time	End Time: 376542, Reason: Terminated
Monitor duration	74.11s
Return Code	0
PID	4280
Parent PID	4304
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#14: c:\programdata\driver1.exe	0x1634	0x410000(4259840)	0x200	✔	1
Modify Memory	#14: c:\programdata\driver1.exe	0x1634	0x412000(4268032)	0x1ac00	✔	1
Modify Memory	#14: c:\programdata\driver1.exe	0x1634	0x42e000(4382720)	0x600	✔	1
Modify Memory	#14: c:\programdata\driver1.exe	0x1634	0x430000(4390912)	0x200	✔	1
Modify Memory	#14: c:\programdata\driver1.exe	0x1634	0x2d5008(2969608)	0x4	✔	1
Modify Control Flow	#14: c:\programdata\driver1.exe	0x1634 / 0x10bc	0x77db3670(2010855024)	-	✔	1

Host Behavior

Type	Count
Registry	522
User	3
System	17
-	11
Module	72
COM	728
-	18
File	1082
Environment	8
-	2
Keyboard	3

Network Behavior

Type	Count
HTTPS	1
DNS	2

Type	Count
TCP	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
be735fb6d9811ebc95011003c79b1df34a438e765f9a2065c1ef98930e72c698	C:\Users\OqXZRaykm\Desktop\project.exe	Sample File	82981.92 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
29d3deeb4cd5a45eef40bae38033d9dd4a4898d2659ba16b93666e2bfe55ac35	C:\ProgramData\driver1.exe	Dropped File	558.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
d8d6bc1a3870df3b12f8a0d3fc2e4bbffde927b15a0f114dbeacdcf042f0d8ac	-	Memory Dump	136.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
8103f74aedf1f42289b823a56ef991c61d33e35e2b28e2388961a31b2a87491f	C:\ProgramData\driver1.rar	Downloaded File	259.84 KB	application/x-rar-compressed	Access, Create, Delete, Read, Write	
01b714a8ebda459f61a15f57b52c380626762af13b1c552954bdee3e441fcec0	-	Downloaded File	19 bytes	application/json	-	CLEAN
bfbd892f4552464fa7cbaeae034196312571874fcbd50cdcefc174db260d22ba	-	Downloaded File	1.19 KB	text/html	-	CLEAN
5d8dc7f92612ccf5258259d82b8d4cf24d1a995094b370bfbcafefac6974aed6	-	Downloaded File	11.99 KB	text/html	-	CLEAN
9404863d23f85e6a1480bc2490a391042fa33287db5bbafd21cefccceed2d10c	C:\Users\OqXZRaykm\AppData\Roaming\d3d9.dll	Dropped File	237.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\OqXZRaykm\Desktop\project.exe	Accessed File, Sample File	Access, Read	MALICIOUS
C:\ProgramData\driver1.rar	Accessed File, Downloaded File, Extracted File	Access, Create, Delete, Read, Write	CLEAN
C:\ProgramData\driver1.exe	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\OqXZRaykm\AppData\Roaming\d3d9.dll	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\system32\5a8dd6a129bf0d88c880de4bb5ded3c6520eaf3d6f667ed663e58f1bd400c535AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA... ...AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	Accessed File	Access	CLEAN
C:\Users\OqXZRaykm\Desktop\rclone.conf	Accessed File	Access	CLEAN
C:\Users\OqXZRaykm\AppData\Roaming\rclone\rclone.conf	Accessed File	Access	CLEAN
C:\Users\OqXZRaykm\.config\rclone\rclone.conf	Accessed File	Access	CLEAN
C:\Users\OqXZRaykm\.rclone.conf	Accessed File	Access	CLEAN
C:\Users\OqXZRaykm\AppData\Roaming\rclone	Accessed File	Access, Create	CLEAN
C:\Users\OqXZRaykm\AppData\Roaming	Accessed File	Access	CLEAN
wmic.com	Accessed File	Access	CLEAN
wmic.exe	Accessed File	Access	CLEAN
wmic.bat	Accessed File	Access	CLEAN
wmic.cmd	Accessed File	Access	CLEAN
wmic.vbs	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
wmic.vbe	Accessed File	Access	CLEAN
wmic.js	Accessed File	Access	CLEAN
wmic.jse	Accessed File	Access	CLEAN
wmic.wsf	Accessed File	Access	CLEAN
wmic.wsh	Accessed File	Access	CLEAN
wmic.msc	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.com	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.bat	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.cmd	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.vbs	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.vbe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.js	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.jse	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.wsf	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.wsh	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.msc	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.com	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.exe	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.bat	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.cmd	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.vbs	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.vbe	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.js	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.jse	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.wsf	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.wsh	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.msc	Accessed File	Access	CLEAN
C:\Windows\wmic.com	Accessed File	Access	CLEAN
C:\Windows\wmic.exe	Accessed File	Access	CLEAN
C:\Windows\wmic.bat	Accessed File	Access	CLEAN
C:\Windows\wmic.cmd	Accessed File	Access	CLEAN
C:\Windows\wmic.vbs	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\wmic.vbe	Accessed File	Access	CLEAN
C:\Windows\wmic.js	Accessed File	Access	CLEAN
C:\Windows\wmic.jse	Accessed File	Access	CLEAN
C:\Windows\wmic.wsf	Accessed File	Access	CLEAN
C:\Windows\wmic.wsh	Accessed File	Access	CLEAN
C:\Windows\wmic.msc	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\wmic.com	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\wmic.exe	Accessed File	Access	CLEAN
NUL	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\XSL-Mappings.xml	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\\texttable.xsl	Accessed File	Access	CLEAN
tasklist.com	Accessed File	Access	CLEAN
tasklist.exe	Accessed File	Access	CLEAN
tasklist.bat	Accessed File	Access	CLEAN
tasklist.cmd	Accessed File	Access	CLEAN
tasklist.vbs	Accessed File	Access	CLEAN
tasklist.vbe	Accessed File	Access	CLEAN
tasklist.js	Accessed File	Access	CLEAN
tasklist.jse	Accessed File	Access	CLEAN
tasklist.wsf	Accessed File	Access	CLEAN
tasklist.wsh	Accessed File	Access	CLEAN
tasklist.msc	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\tasklist.com	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\tasklist.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\tasklist.bat	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\tasklist.cmd	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\tasklist.vbs	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\tasklist.vbe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\tasklist.js	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\tasklist.jse	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\tasklist.wsf	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\tasklist.wsh	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\tasklist.msc	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\tasklist.com	Accessed File	Access	CLEAN
C:\Windows\system32\tasklist.exe	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE0	Accessed File	Access	CLEAN
powershell.com	Accessed File	Access	CLEAN
powershell.exe	Accessed File	Access	CLEAN
powershell.bat	Accessed File	Access	CLEAN
powershell.cmd	Accessed File	Access	CLEAN
powershell.vbs	Accessed File	Access	CLEAN
powershell.vbe	Accessed File	Access	CLEAN
powershell.js	Accessed File	Access	CLEAN
powershell.jse	Accessed File	Access	CLEAN
powershell.wsf	Accessed File	Access	CLEAN
powershell.wsh	Accessed File	Access	CLEAN
powershell.msc	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\powershell.com	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\powershell.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\powershell.bat	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\powershell.cmd	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\powershell.vbs	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\powershell.vbe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\powershell.js	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\powershell.jse	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\powershell.wsf	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\powershell.wsh	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\powershell.msc	Accessed File	Access	CLEAN
C:\Windows\system32\powershell.com	Accessed File	Access	CLEAN
C:\Windows\system32\powershell.exe	Accessed File	Access	CLEAN
C:\Windows\system32\powershell.bat	Accessed File	Access	CLEAN
C:\Windows\system32\powershell.cmd	Accessed File	Access	CLEAN
C:\Windows\system32\powershell.vbs	Accessed File	Access	CLEAN
C:\Windows\system32\powershell.vbe	Accessed File	Access	CLEAN
C:\Windows\system32\powershell.js	Accessed File	Access	CLEAN
C:\Windows\system32\powershell.jse	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\powershell.wsf	Accessed File	Access	CLEAN
C:\Windows\system32\powershell.wsh	Accessed File	Access	CLEAN
C:\Windows\system32\powershell.msc	Accessed File	Access	CLEAN
C:\Windows\powershell.com	Accessed File	Access	CLEAN
C:\Windows\powershell.exe	Accessed File	Access	CLEAN
C:\Windows\powershell.bat	Accessed File	Access	CLEAN
C:\Windows\powershell.cmd	Accessed File	Access	CLEAN
C:\Windows\powershell.vbs	Accessed File	Access	CLEAN
C:\Windows\powershell.vbe	Accessed File	Access	CLEAN
C:\Windows\powershell.js	Accessed File	Access	CLEAN
C:\Windows\powershell.jse	Accessed File	Access	CLEAN
C:\Windows\powershell.wsf	Accessed File	Access	CLEAN
C:\Windows\powershell.wsh	Accessed File	Access	CLEAN
C:\Windows\powershell.msc	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\powershell.com	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\powershell.exe	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\powershell.bat	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\powershell.cmd	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\powershell.vbs	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\powershell.vbe	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\powershell.js	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\powershell.jse	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\powershell.wsf	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\powershell.wsh	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\powershell.msc	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.com	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Windows	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Windows\System32\OpenSSH\	Accessed File	Access	CLEAN
C:\Users\OqXZRaykm\AppData\Local\Microsoft\WindowsApps	Accessed File	Access	CLEAN
C:\Users\OqXZRaykm\Documents\WindowsPowerShell\Modules	Accessed File	Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://t[.]me/+J_Z1QGHfHko0MGZi*https://steamcommunity.com/id/elcadillac	Extracted	149.154.167.99	United Kingdom	-	MALICIOUS
hxxp://147[.]45[.]47[.]37:1445/user72145/json	Extracted, Contacted	147.45.47.37	Russia	GET	CLEAN
hxxp://147[.]45[.]47[.]37:1488/thot/thot.rar	Extracted, Contacted	147.45.47.37	Russia	GET	CLEAN
hxxp://147[.]45[.]47[.]37:1445/user72145?reason=MTgzN0ZBM0ltODQwRC1FOEJFLTQ2NTMtMjAzMDQwNTA2MDk5aWxvdmVpdA==	Extracted, Contacted	147.45.47.37	Russia	GET	CLEAN
hxxps://t[.]me/+J_Z1QGHfHko0MGZi	Extracted, Contacted	149.154.167.99	United Kingdom	GET	CLEAN
hxxp://telegram[.]org/img/website_icon.svg?4	Extracted	-	-	-	CLEAN
hxxp://telegram[.]org/img/apple-touch-icon.png	Extracted	-	-	-	CLEAN
hxxp://telegram[.]org/img/favicon-32x32.png	Extracted	-	-	-	CLEAN
hxxp://telegram[.]org/img/favicon-16x16.png	Extracted	-	-	-	CLEAN
hxxp://telegram[.]org/img/favicon.ico	Extracted	-	-	-	CLEAN
hxxp://telegram[.]org/css/font-roboto.css?1	Extracted	-	-	-	CLEAN
hxxp://telegram[.]org/css/bootstrap.min.css?3	Extracted	-	-	-	CLEAN
hxxp://telegram[.]org/css/telegram.css?237	Extracted	-	-	-	CLEAN
hxxp://telegram[.]org	Extracted	-	-	-	CLEAN
hxxp://telegram[.]org/dl?tme=a1fa6b9791b4d00d4e_104611903311604796 26	Extracted	-	-	-	CLEAN
hxxp://telegram[.]org/js/tgwallpaper.min.js?3	Extracted	-	-	-	CLEAN
hxxps://web[.]telegram[.]org	Extracted	-	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
t[.]me	149.154.167.99	United Kingdom	DNS, HTTPS, TCP	CLEAN
telegram[.]org	-	-	-	CLEAN
web[.]telegram[.]org	-	-	-	CLEAN
aw[.]knocin[.]xyz	78.47.64.127	Germany	DNS, TCP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
147.45.47.37	-	Russia	TCP, HTTP	CLEAN
149.154.167.99	t[.]me	United Kingdom	DNS, HTTPS, TCP	CLEAN
78.47.64.127	aw[.]knocin[.]xyz	Germany	DNS, TCP	CLEAN

Mutex

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

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CLASSES_ROOT\.386	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.386\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.3fr	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.3fr\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.3g2	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.3g2\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.3gp	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.3gp\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.3gp2	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.3gp2\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.3gpp	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.3gpp\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.3mf	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.3mf\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.a	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.a\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.aac	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.aac\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.ac3	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.ac3\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.accountpicture-ms	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.accountpicture-ms\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.acrobatsecuritysettings	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.acrobatsecuritysettings\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.adt	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.adt\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.adts	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.adts\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.ai	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.ai\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.aif	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.aif\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.aifc	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.aifc\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.aiff	access	project.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CLASSES_ROOT\.aiff\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.all	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.all\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.amr	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.amr\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.ani	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.ani\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.ans	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.ans\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.api	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.api\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.appcontent-ms	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.appcontent-ms\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.appinstaller	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.appinstaller\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.application	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.application\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.appref-ms	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.appref-ms\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.appx	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.appx\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.appxbundle	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.appxbundle\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.aps	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.aps\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.arc	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.arc\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.ari	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.ari\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.arj	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.arj\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.art	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.art\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.arw	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.arw\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.asa	access	project.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CLASSES_ROOT\.asa\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.asc	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.asc\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.ascx	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.ascx\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.asf	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.asf\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.asm	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.asm\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.asmx	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.asmx\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.asp	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.asp\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.aspx	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.aspx\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.asx	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.asx\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.au	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.au\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.avci	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.avci\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.avcs	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.avcs\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.avi	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.avi\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.avif	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.avif\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.avifs	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.avifs\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bas	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bas\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bat	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bat\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bay	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bay\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bcp	access	project.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CLASSES_ROOT\.bcp\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bin	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bin\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bkf	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bkf\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.blg	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.blg\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bmp	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bmp\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bsc	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.bsc\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.c	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.c\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.c5e2524a-ea46-4f67-841f-6a9465d9d515	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.c5e2524a-ea46-4f67-841f-6a9465d9d515\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cab	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cab\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.camp	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.camp\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cap	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cap\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cat	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cat\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cc	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cc\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cda	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cda\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cdmp	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cdmp\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cdx	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cdx\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cdxml	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cdxml\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cer	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cer\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cgm	access	project.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CLASSES_ROOT\.cgm\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.chk	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.chk\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.chm	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.chm\Content Type	access, read	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cls	access	project.exe	CLEAN
HKEY_CLASSES_ROOT\.cls\Content Type	access, read	project.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
driver1.exe	C:\ProgramData\driver1.exe	MALICIOUS
project.exe	"C:\Users\OqXZRaykm\Desktop\project.exe"	MALICIOUS
wmic.exe	wmic path win32_VideoController get name	SUSPICIOUS
powershell.exe	powershell -WindowStyle hidden -Command "Add-MpPreference -ExclusionPath \"C:\ProgramData\";" powershell -WindowStyle hidden -Command "Add-MpPreference -ExclusionPath \"C:\Users\OqXZRaykm\Desktop\project.exe\""	SUSPICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle hidden -Command Add-MpPreference -ExclusionPath C:\Users\OqXZRaykm\Desktop\project.exe	SUSPICIOUS
msbuild.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe"	SUSPICIOUS
tasklist.exe	tasklist	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN
wmic.exe	wmic csproduct get uuid	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs -p	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	RedLine_E	RedLine Stealer, RedLine.E variant	Memory Dump	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_20h1_en_base
Description	windows 10 (64bit 20H1 -EN-)
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	2024.3.1
Dynamic Engine Version	2024.3.1 / 06/10/2024 04:30
Static Engine Version	2024.3.1.0 / 2024-06-10 03:00:36
AV Exceptions Version	2024.3.1.2 / 2024-06-08 13:32:38
Link Detonation Heuristics Version	2024.3.1.3 / 2024-06-10 20:59:54
Smart Memory Dumping Rules Version	2024.3.1.2 / 2024-06-08 13:32:38
Config Extractors Version	2024.3.1.3 / 2024-06-10 20:59:54
Signature Trust Store Version	2024.3.1.2 / 2024-06-08 13:32:38
VMRay Threat Identifiers Version	2024.3.1.7 / 2024-06-20 14:30:49
YARA Built-in Ruleset Version	2024.3.1.7

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