MALICIOUS

Classifications: Injector Spyware

Threat Names: RedLine.E Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**AMD89270195629.exe**
ID	#10590951
MD5	3d8d0b6499504343f6953587c60d31a1
SHA1	1549a25522a89233948a3401ee73643e209ced1b
SHA256	f9547f1d7dea3927c4ddeaced997544c7bfc28b458fc188a717b10682f681040
File Size	531.50 KB
Report Created	2024-06-06 22:28 (UTC)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (27 rules, 136 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 #3) msbuild.exe.			
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
	• Sample enumerates processes, 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 #3) msbuild.exe takes screenshots and potentially exfiltrates data.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) amd89270195629.exe modifies memory of (process #3) msbuild.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #1) amd89270195629.exe alters context of (process #3) msbuild.exe.			
4/5	Reputation	Malicious file detected via reputation	1	-
	• Reputation analysis labels file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\d3d9.dll" as Mal/Generic-S.			
4/5	Reputation	Malicious host or URL detected via reputation	1	-
	• Resolved domain "spahere.top" is a known malicious domain and was reported as "Malware".			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #3) 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 #3) 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 #3) msbuild.exe tries to detect firewall via WMI query: "SELECT * FROM FirewallProduct".			
3/5	Data Collection	Takes screenshot	1	-
	• (Process #3) msbuild.exe takes a screenshot using BitBlt API.			
2/5	Discovery	Enumerates running processes	1	-
	• (Process #3) msbuild.exe enumerates running processes via WMI query SELECT * FROM Win32_Process Where SessionId='1'.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #3) msbuild.exe queries OS version via WMI query: SELECT * FROM Win32_OperatingSystem.			

Score	Category	Operation	Count	Classification
2/5	Discovery	Collects hardware properties	3	-
	• (Process #3) msbuild.exe queries hardware properties via WMI: SELECT * FROM Win32_DiskDrive. • (Process #3) msbuild.exe queries hardware properties via WMI: SELECT * FROM Win32_Processor. • (Process #3) msbuild.exe queries hardware properties via WMI: SELECT * FROM Win32_VideoController.			
2/5	Discovery	Searches for sensitive FTP data	1	-
	• (Process #3) msbuild.exe searches for sensitive data of FTP application "Total Commander" by file.			
2/5	Discovery	Searches for sensitive browser data	23	-
	• (Process #3) msbuild.exe searches for sensitive data of web browser "Chromium" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Google Chrome" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Opera" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Maple Studio" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "7Star" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "CentBrowser" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Chedot" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Vivaldi" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Kometa" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Elements Browser" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Epic Privacy Browser" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Uran" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Orbitum" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Comodo Dragon" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Torch" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Yandex Browser" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Sputnik" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "CocCoc" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Mozilla Firefox" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "k-Meleon" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Comodo IceDragon" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Cyberfox" by file. • (Process #3) msbuild.exe searches for sensitive data of web browser "Internet Explorer / Edge" by file.		
2/5	Discovery	Searches for sensitive mail data	1	-
	• (Process #3) msbuild.exe searches for sensitive data of mail application "Mozilla Thunderbird" by file.			
2/5	Discovery	Searches for cryptocurrency wallet locations	2	-
	• (Process #3) msbuild.exe searches for the cryptocurrency wallet "Electrum Bitcoin Wallet" for "BTC". • (Process #3) msbuild.exe searches for the cryptocurrency wallet "Exodus Cryptocurrency Wallet".			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) amd89270195629.exe starts (process #3) msbuild.exe with a hidden window.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) amd89270195629.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Privilege Escalation	Enables process privileges	2	-

Score	Category	Operation	Count	Classification
		• (Process #3) msbuild.exe enables process privilege "SeDebugPrivilege". • (Process #5) wmiprvse.exe enables process privilege "SeDebugPrivilege".		
1/5	Obfuscation	Reads from memory of another process	81	-

- (Process #5) wmiprvse.exe reads from winlogon.exe.
- (Process #5) wmiprvse.exe reads from lsass.exe.
- (Process #5) wmiprvse.exe reads from svchost.exe.
- (Process #5) wmiprvse.exe reads from dwm.exe.
- (Process #5) wmiprvse.exe reads from (process #4) svchost.exe.
- (Process #5) wmiprvse.exe reads from spoolsv.exe.
- (Process #5) wmiprvse.exe reads from sihost.exe.
- (Process #5) wmiprvse.exe reads from runtimebroker.exe.
- (Process #5) wmiprvse.exe reads from taskhostw.exe.
- (Process #5) wmiprvse.exe reads from explorer.exe.
- (Process #5) wmiprvse.exe reads from shellexperiencehost.exe.
- (Process #5) wmiprvse.exe reads from searchui.exe.
- (Process #5) wmiprvse.exe reads from wmiadap.exe.
- (Process #5) wmiprvse.exe reads from backgroundtaskhost.exe.
- (Process #5) wmiprvse.exe reads from iexplore.exe.
- (Process #5) wmiprvse.exe reads from (process #6) wmiprvse.exe.
- (Process #5) wmiprvse.exe reads from fineperform.exe.
- (Process #5) wmiprvse.exe reads from cause_begin_until.exe.
- (Process #5) wmiprvse.exe reads from speak.exe.
- (Process #5) wmiprvse.exe reads from recently-include-conference.exe.
- (Process #5) wmiprvse.exe reads from bill_difficult_his.exe.
- (Process #5) wmiprvse.exe reads from marriage.exe.
- (Process #5) wmiprvse.exe reads from produceparent.exe.
- (Process #5) wmiprvse.exe reads from withprofessionalhe.exe.
- (Process #5) wmiprvse.exe reads from explain room little.exe.
- (Process #5) wmiprvse.exe reads from better-then-professional.exe.
- (Process #5) wmiprvse.exe reads from yes.exe.
- (Process #5) wmiprvse.exe reads from service outside friend.exe.
- (Process #5) wmiprvse.exe reads from into-large.exe.
- (Process #5) wmiprvse.exe reads from subject_whether.exe.
- (Process #5) wmiprvse.exe reads from strategy.exe.
- (Process #5) wmiprvse.exe reads from spend.exe.
- (Process #5) wmiprvse.exe reads from fall.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 ncftp.exe.
- (Process #5) wmiprvse.exe reads from notepad.exe.
- (Process #5) wmiprvse.exe reads from operamail.exe.
- (Process #5) wmiprvse.exe reads from outlook.exe.
- (Process #5) wmiprvse.exe reads from pidgin.exe.
- (Process #5) wmiprvse.exe reads from scriptftp.exe.
- (Process #5) wmiprvse.exe reads from skype.exe.
- (Process #5) wmiprvse.exe reads from smartftp.exe.
- (Process #5) wmiprvse.exe reads from thunderbird.exe.
- (Process #5) wmiprvse.exe reads from trillian.exe.
- (Process #5) wmiprvse.exe reads from webdrive.exe.
- (Process #5) wmiprvse.exe reads from whatsapp.exe.
- (Process #5) wmiprvse.exe reads from winscp.exe.

Score	Category	Operation	Count	Classification
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #3) msbuild.exe tries to gather information about application "Steam" by registry. • (Process #3) msbuild.exe tries to gather information about application "FileZilla" by file.			
1/5	Network Connection	Performs DNS request	2	-
	• (Process #3) msbuild.exe resolves hostname "t.me" to IP "149.154.167.99". • (Process #3) msbuild.exe resolves hostname "spahere.top" to IP "65.21.63.6".			
1/5	Network Connection	Connects to remote host	2	-
	• (Process #3) msbuild.exe opens an outgoing TCP connection to host "149.154.167.99:443". • (Process #3) msbuild.exe opens an outgoing TCP connection to host "65.21.63.6:443".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #3) msbuild.exe resolves 51 API functions by name.			

Malware Configuration: RedLine

Metadata	Key	Extracted Value
Version	Value	1
Mission ID	Value	6132932315_99
Encryption Key	Key Algorithm	VGhpZ2dpbmc= xor
URL	Url	https://t.me/+7Lir0e4Gw381MDhi*https://steamcommunity.com/id/993846634744/

Mitre ATT&CK Matrix

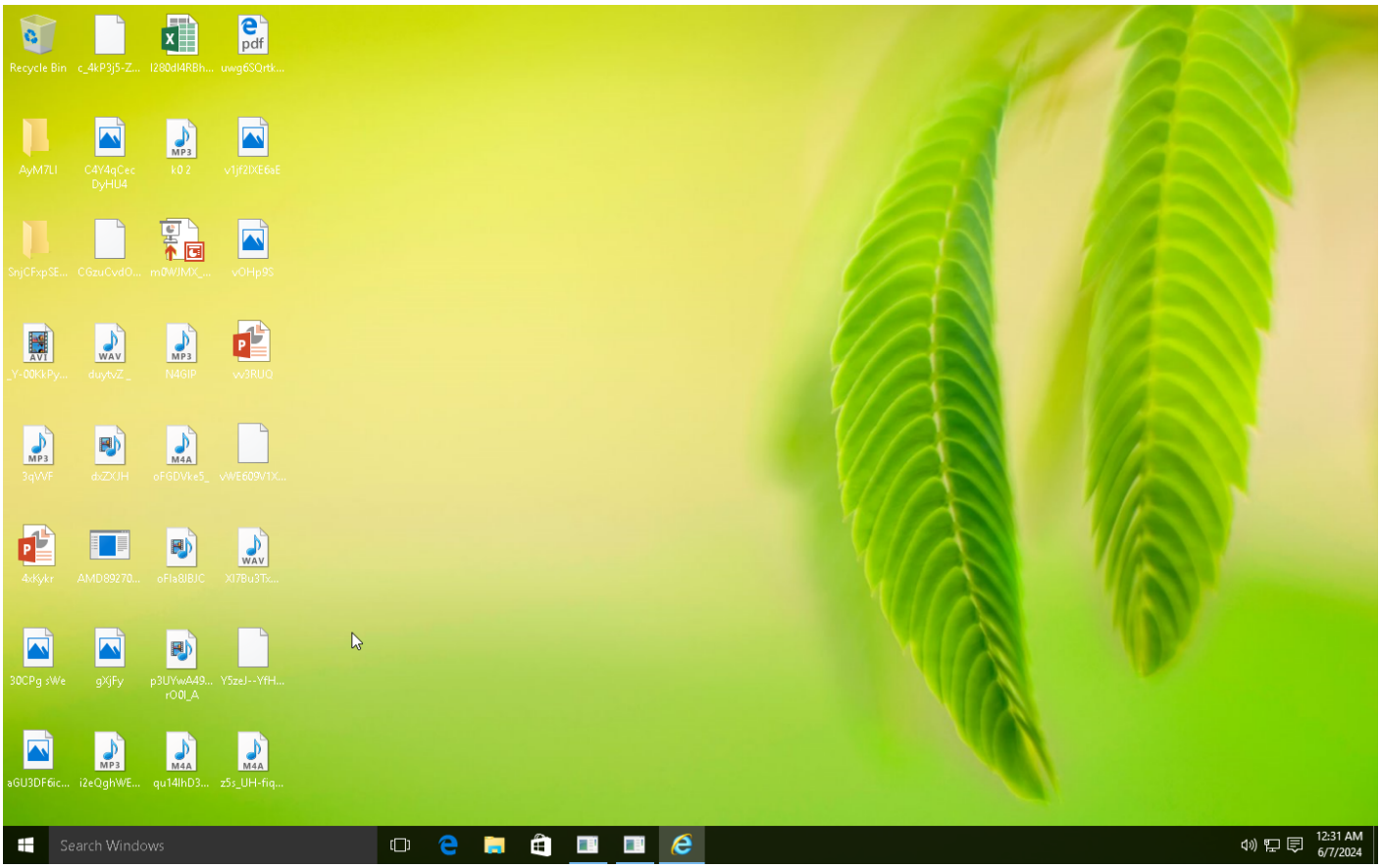
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1143 Hidden Window	#T1081 Credentials in Files	#T1082 System Information Discovery		#T1119 Automated Collection			
				#T1045 Software Packing	#T1056 Input Capture	#T1012 Query Registry		#T1005 Data from Local System			
						#T1063 Security Software Discovery		#T1113 Screen Capture			
						#T1083 File and Directory Discovery		#T1056 Input Capture			

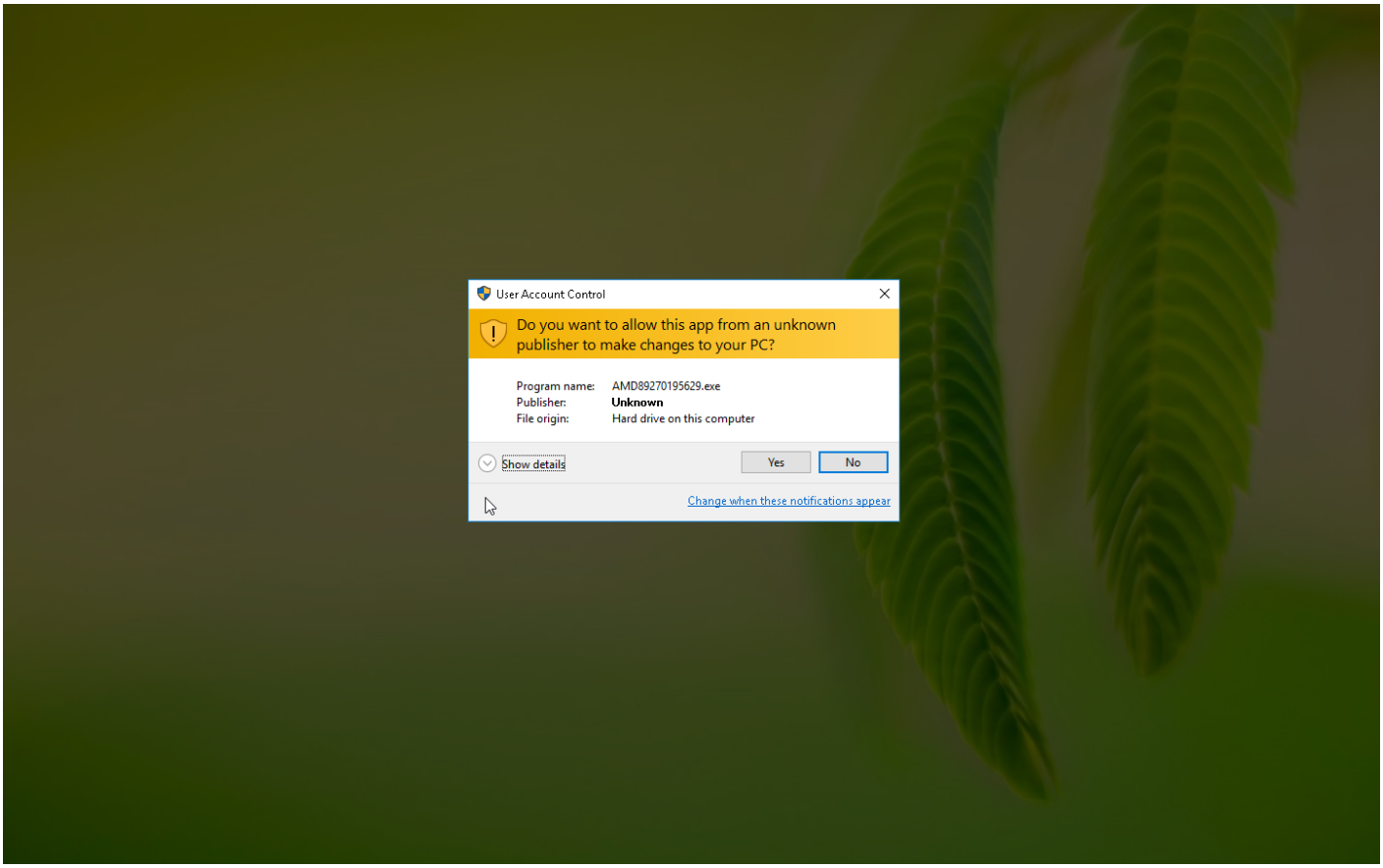
Sample Information

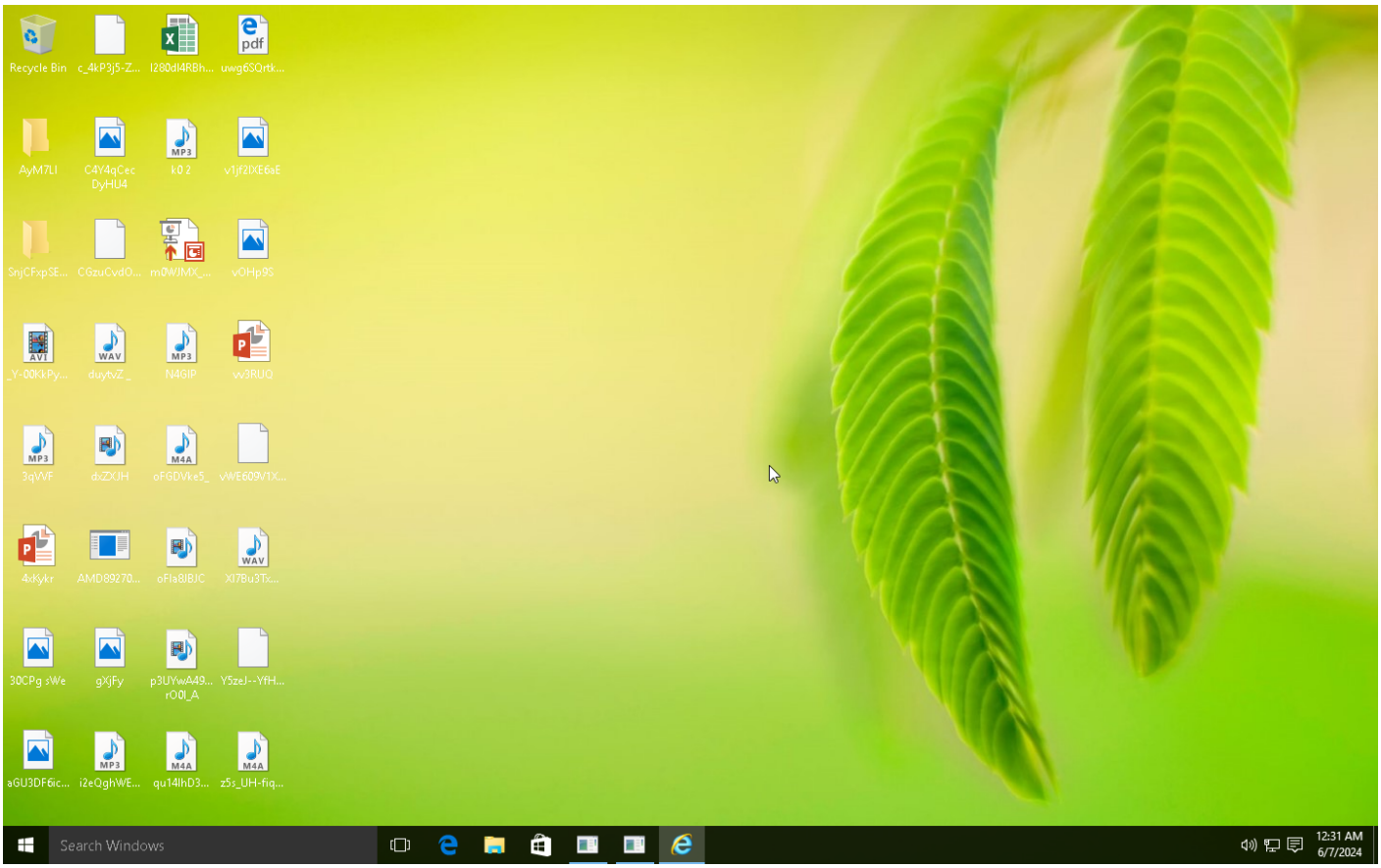
ID	#10590951
MD5	3d8d0b6499504343f6953587c60d31a1
SHA1	1549a25522a89233948a3401ee73643e209ced1b
SHA256	f9547f1d7dea3927c4ddeaced997544c7bfc28b458fc188a717b10682f681040
SSDeep	12288:UgplY5LqlDuuH719kcHZJh18HL3q7brnceBtfGZbBykQFNgrW2q8kbAmz/d6Hb3g:UgplY5LqldHnx
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	AMD89270195629.exe
File Size	531.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

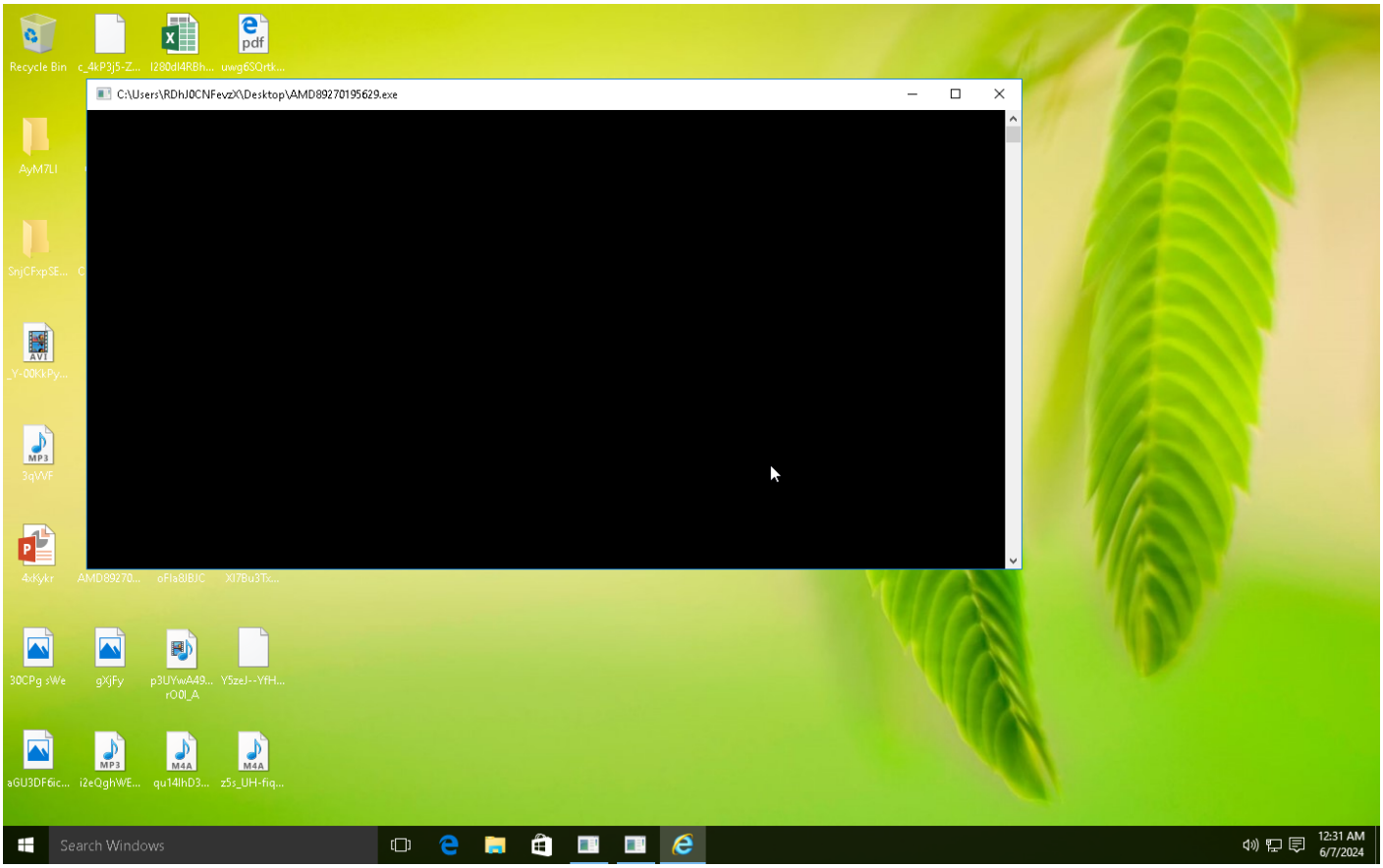
Analysis Information

Creation Time	2024-06-06 22:28 (UTC)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	4
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
Search Windows
12:31 AM
6/7/2024


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: AMD89270195629.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

1343.87 KB total sent

28.30 KB total received

2 ports 443, 53

3 contacted IP addresses

13 URLs extracted

1 files downloaded

2 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

1 sessions, 898 bytes sent, 19.30 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://telegram[.]org/img/apple-touch-icon.png	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/css/font-roboto.css?1	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/js/tgwallpaper.min.js?3	-	-	-	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/img/website_icon.svg?4	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/img/favicon-16x16.png	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/css/telegram.css?237	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/dl?tme=04e47454cc45897090_81568605585544417 9	-	-	-	0 bytes	CLEAN
GET	hxxp://telegram[.]org/css/bootstrap.min.css?3	-	-	-	0 bytes	CLEAN
GET	hxxps://web[.]telegram[.]org	-	-	-	0 bytes	CLEAN
GET	hxxps://t[.]me/+7Lir0e4Gw381MDhi	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	t[.]me	NO_ERROR	149.154.167.99	-	CLEAN
A	spahere[.]top	NO_ERROR	65.21.63.6	-	MALICIOUS

BEHAVIOR

Process Graph

Process #1: amd89270195629.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\amd89270195629.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\AMD89270195629.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 177064, Reason: Analysis Target
Unmonitor End Time	End Time: 208422, Reason: Terminated
Monitor duration	31.36s
Return Code	0
PID	4628
Parent PID	-
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\d3d9.dll	235.00 KB	a4d74fff85db049e69c37bd84963294c72bbb56a22237f4361d3300b2f6c8659	✖

Host Behavior

Type	Count
Registry	1
Module	31
Environment	2
File	15
Process	2
-	3
-	7

Process #3: msbuild.exe

ID	3
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\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 201066, Reason: Child Process
Unmonitor End Time	End Time: 351902, Reason: Terminated
Monitor duration	150.84s
Return Code	0
PID	2768
Parent PID	4628
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\amd89270195629.exe	0x1230	0x3d0000(3997696)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\amd89270195629.exe	0x1230	0x3d2000(4005888)	0x1ac00	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\amd89270195629.exe	0x1230	0x3ee000(4120576)	0x600	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\amd89270195629.exe	0x1230	0x3f0000(4128768)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\amd89270195629.exe	0x1230	0x5ed008(6213640)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\amd89270195629.exe	0x1230 / 0x1350	0x778b8fe0(2005635040)	-	✔	1

Host Behavior

Type	Count
Registry	645
User	3
System	15
-	11
Module	69
COM	272
-	13
File	341
Environment	8
-	2
Keyboard	3

Network Behavior

Type	Count
HTTPS	1
DNS	2
TCP	2

Process #4: svchost.exe

ID	4
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 218502, Reason: RPC Server
Unmonitor End Time	End Time: 417092, Reason: Terminated by timeout
Monitor duration	198.59s
Return Code	Unknown
PID	1012
Parent PID	2768
Bitness	64 Bit

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: 218503, Reason: RPC Server
Unmonitor End Time	End Time: 417092, Reason: Terminated by timeout
Monitor duration	198.59s
Return Code	Unknown
PID	4388
Parent PID	1012
Bitness	64 Bit

Host Behavior

Type	Count
User	3
System	335
Process	1118
-	1895
Module	16
Registry	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f9547f1d7dea3927c4ddeaced997544c7bfc28b458fc188a717b10682f681040	C:\Users\RDhJ0CNFevzX\Desktop\AMD89270195629.exe	Sample File	531.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
a4d74fff85db049e69c37bd84963294c72bbb56a22237f4361d3300b2f6c8659	C:\Users\RDhJ0CNFevzX\AppData\Roaming\d3d9.dll	Dropped File	235.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
3d8873792e115de72e4f7b1aa1af1b123a8530ac8fe520251a7256fab448dc6b	-	Memory Dump	136.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
110976bbbb95a474a5562bff39dc00ef2fbdeb453cd44682b8e5e660ffaa47cd	-	Downloaded File	12.00 KB	text/html	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\AMD89270195629.exe	Accessed File, Sample File	Access	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\d3d9.dll	Accessed File, Dropped File	Access, Create, Write	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\KERNEL32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe.Config	Accessed File	Access, Read	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\NordVPEntity12N	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\sitemanager.xml	Accessed File	Access	CLEAN
C:\Program Files\Internet Explorer\iexplore.exe	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://t[.]me/+7Lir0e4Gw381MDhi*https://steamcommunity.com/id/993846634744/	Extracted	149.154.167.99	United Kingdom	-	MALICIOUS
hxxps://t[.]me/+7Lir0e4Gw381MDhi	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

URL	Category	IP Address	Country	HTTP Methods	Verdict
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=04e47454cc45897090_815686055855444179	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
spahere[.]top	65.21.63.6	Finland	TCP, DNS	MALICIOUS
t[.]me	149.154.167.99	United Kingdom	TCP, DNS, HTTPS	CLEAN
telegram[.]org	-	-	-	CLEAN
web[.]telegram[.]org	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
149.154.167.99	t[.]me	United Kingdom	TCP, DNS, HTTPS	CLEAN
65.21.63.6	spahere[.]top	Finland	TCP, DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	msbuild.exe, amd89270195629.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayName	read, access	msbuild.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}	access	msbuild.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName	read, access	msbuild.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	read, access	msbuild.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0011-0000-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0011-0000-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0011-0000-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0018-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0018-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0018-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0019-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0019-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0019-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001A-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001A-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001A-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001B-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001B-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001B-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002C-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002C-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002C-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0044-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0044-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0044-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-006E-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-006E-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-006E-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0090-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0090-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0090-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00A1-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00A1-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00A1-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00BA-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00BA-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00BA-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E1-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E1-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E1-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E2-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E2-0409-0000-0000000FF1CE}\DisplayName	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E2-0409-0000-0000000FF1CE}\DisplayVersion	read, access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0115-0409-0000-0000000FF1CE}	access	msbuild.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
amd89270195629.exe	"C:\Users\RDhJ0CNFevzX\Desktop\AMD89270195629.exe"	MALICIOUS
msbuild.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe"	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	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_th2_en_mso2016
Description	windows 10 (64bit TH2 -EN- MSO_2016)
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2024.2.1
Dynamic Engine Version	2024.2.1 / 03/23/2024 11:02
Static Engine Version	2024.2.1.0 / 2024-03-23 09:36:38
AV Exceptions Version	2024.2.1.5 / 2024-03-22 20:39:30
Link Detonation Heuristics Version	2024.2.1.29 / 2024-05-11 04:28:14
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.27 / 2024-05-02 14:06:04
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.31 / 2024-05-17 05:43:49
YARA Built-in Ruleset Version	2024.2.1.32

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp

System Root	C:\Windows