DYNAMIC ANALYSIS REPORT

#15494396

MALICIOUS

Classifications: Injector Spyware

Threat Names: RedLine.Ev1 RedLine.E

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe**
ID	#8680769
MD5	7278b6ce3ddda7dba2473e0392e54ea6
SHA1	3b406f221237fe9bfce48daa9033eda93ecc9b94
SHA256	6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49
File Size	7516.50 KB
Report Created	2023-08-25 08:41 (UTC)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (27 rules, 144 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 #2) vbc.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 #2) vbc.exe takes screenshots and potentially exfiltrates data.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) 6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe modifies memory of (process #2) vbc.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #1) 6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe alters context of (process #2) vbc.exe.			
4/5	Reputation	Malicious file detected via reputation	1	-
	• The sample itself is a known malicious file.			
3/5	Data Collection	Takes screenshot	1	-
	• (Process #2) vbc.exe takes a screenshot using BitBlt API.			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #2) vbc.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 #2) vbc.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 #2) vbc.exe tries to detect firewall via WMI query: "SELECT * FROM FirewallProduct".			
2/5	Discovery	Executes WMI query	8	-
	• (Process #2) vbc.exe executes WMI query: SELECT * FROM Win32_DiskDrive. • (Process #2) vbc.exe executes WMI query: SELECT * FROM Win32_Process Where SessionId='1'. • (Process #2) vbc.exe executes WMI query: SELECT * FROM Win32_Processor. • (Process #2) vbc.exe executes WMI query: SELECT * FROM Win32_VideoController. • (Process #2) vbc.exe executes WMI query: SELECT * FROM Win32_OperatingSystem. • (Process #2) vbc.exe executes WMI query: SELECT * FROM AntivirusProduct. • (Process #2) vbc.exe executes WMI query: SELECT * FROM AntiSpyWareProduct. • (Process #2) vbc.exe executes WMI query: SELECT * FROM FirewallProduct.			

Score	Category	Operation	Count	Classification
2/5	Discovery	Collects hardware properties	1	-
	• (Process #2) vbc.exe queries hardware properties via WMI.			
2/5	Discovery	Enumerates running processes	1	-
	• (Process #2) vbc.exe enumerates running processes via WMI.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #2) vbc.exe queries OS version via WMI.			
2/5	Discovery	Searches for sensitive browser data	23	-
	• (Process #2) vbc.exe searches for sensitive data of web browser "Chromium" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Google Chrome" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Opera" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Maple Studio" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "7Star" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "CentBrowser" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Chedot" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Vivaldi" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Kometa" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Elements Browser" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Epic Privacy Browser" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Uran" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Orbitum" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Comodo Dragon" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Torch" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Yandex Browser" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Sputnik" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "CocCoc" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Mozilla Firefox" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "k-Meleon" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Comodo IceDragon" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Cyberfox" by file. • (Process #2) vbc.exe searches for sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Discovery	Searches for sensitive mail data	1	-
	• (Process #2) vbc.exe searches for sensitive data of mail application "Mozilla Thunderbird" by file.			
2/5	Discovery	Searches for sensitive FTP data	1	-
	• (Process #2) vbc.exe searches for sensitive data of ftp application "Total Commander" by file.			
2/5	Discovery	Searches for cryptocurrency wallet locations	2	-
	• (Process #2) vbc.exe searches for the cryptocurrency wallet "Electrum Bitcoin Wallet" for "BTC". • (Process #2) vbc.exe searches for the cryptocurrency wallet "Exodus Cryptocurrency Wallet".			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) 6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe starts (process #2) vbc.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	86	-

- (Process #1) 6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe reads from (process #2) vbc.exe.
- (Process #4) wmiprvse.exe reads from winlogon.exe.
- (Process #4) wmiprvse.exe reads from lsass.exe.
- (Process #4) wmiprvse.exe reads from svchost.exe.
- (Process #4) wmiprvse.exe reads from dwm.exe.
- (Process #4) wmiprvse.exe reads from (process #3) svchost.exe.
- (Process #4) wmiprvse.exe reads from (process #8) svchost.exe.
- (Process #4) wmiprvse.exe reads from spoolsv.exe.
- (Process #4) wmiprvse.exe reads from sihost.exe.
- (Process #4) wmiprvse.exe reads from runtimebroker.exe.
- (Process #4) wmiprvse.exe reads from explorer.exe.
- (Process #4) wmiprvse.exe reads from taskhostw.exe.
- (Process #4) wmiprvse.exe reads from shellexperiencehost.exe.
- (Process #4) wmiprvse.exe reads from searchui.exe.
- (Process #4) wmiprvse.exe reads from (process #5) wmiprvse.exe.
- (Process #4) wmiprvse.exe reads from applicationframehost.exe.
- (Process #4) wmiprvse.exe reads from systemsettings.exe.
- (Process #4) wmiprvse.exe reads from iexplore.exe.
- (Process #4) wmiprvse.exe reads from face.exe.
- (Process #4) wmiprvse.exe reads from relationship short town.exe.
- (Process #4) wmiprvse.exe reads from appear.exe.
- (Process #4) wmiprvse.exe reads from controlmachine.exe.
- (Process #4) wmiprvse.exe reads from central.exe.
- (Process #4) wmiprvse.exe reads from oh-article.exe.
- (Process #4) wmiprvse.exe reads from returnrecent.exe.
- (Process #4) wmiprvse.exe reads from forget dinner local.exe.
- (Process #4) wmiprvse.exe reads from sure.exe.
- (Process #4) wmiprvse.exe reads from indeed.exe.
- (Process #4) wmiprvse.exe reads from lie.exe.
- (Process #4) wmiprvse.exe reads from decide.exe.
- (Process #4) wmiprvse.exe reads from research.exe.
- (Process #4) wmiprvse.exe reads from read_task_at.exe.
- (Process #4) wmiprvse.exe reads from remain_reality_probably.exe.
- (Process #4) wmiprvse.exe reads from they_option_approach.exe.
- (Process #4) wmiprvse.exe reads from practice.exe.
- (Process #4) wmiprvse.exe reads from 3dftp.exe.
- (Process #4) wmiprvse.exe reads from absolutetelnet.exe.
- (Process #4) wmiprvse.exe reads from alftp.exe.
- (Process #4) wmiprvse.exe reads from barca.exe.
- (Process #4) wmiprvse.exe reads from bitkinex.exe.
- (Process #4) wmiprvse.exe reads from coreftp.exe.
- (Process #4) wmiprvse.exe reads from far.exe.
- (Process #4) wmiprvse.exe reads from filezilla.exe.
- (Process #4) wmiprvse.exe reads from flashfxp.exe.
- (Process #4) wmiprvse.exe reads from fling.exe.
- (Process #4) wmiprvse.exe reads from foxmailincmail.exe.
- (Process #4) wmiprvse.exe reads from gmailnotifierpro.exe.
- (Process #4) wmiprvse.exe reads from icq.exe.
- (Process #4) wmiprvse.exe reads from leechftp.exe.
- (Process #4) wmiprvse.exe reads from ncftp.exe.
- (Process #4) wmiprvse.exe reads from notepad.exe.
- (Process #4) wmiprvse.exe reads from operamail.exe.
- (Process #4) wmiprvse.exe reads from outlook.exe.
- (Process #4) wmiprvse.exe reads from pidgin.exe.
- (Process #4) wmiprvse.exe reads from scriptftp.exe.
- (Process #4) wmiprvse.exe reads from skype.exe.
- (Process #4) wmiprvse.exe reads from smartftp.exe.
- (Process #4) wmiprvse.exe reads from thunderbird.exe.
- (Process #4) wmiprvse.exe reads from trillian.exe.
- (Process #4) wmiprvse.exe reads from webdrive.exe.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.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 privilege	2	-
	• (Process #2) vbc.exe enables process privilege "SeDebugPrivilege". • (Process #4) wmiprvse.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #2) vbc.exe tries to gather information about application "FileZilla" by file. • (Process #2) vbc.exe tries to gather information about application "Steam" by registry.			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #2) vbc.exe opens an outgoing TCP connection to host "91.103.252.39:7899".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #2) vbc.exe tries to connect to TCP port 7899 at 91.103.252.39.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #2) vbc.exe resolves 53 API functions by name.			

Malware Configuration: RedLine

Metadata	Key	Extracted Value
Version	Value	1
Mission ID	Value	metafile
Socket	Address Port Network Protocol C2 Listen	91.103.252.39 7899 tcp ✔ ✖

Mitre ATT&CK Matrix

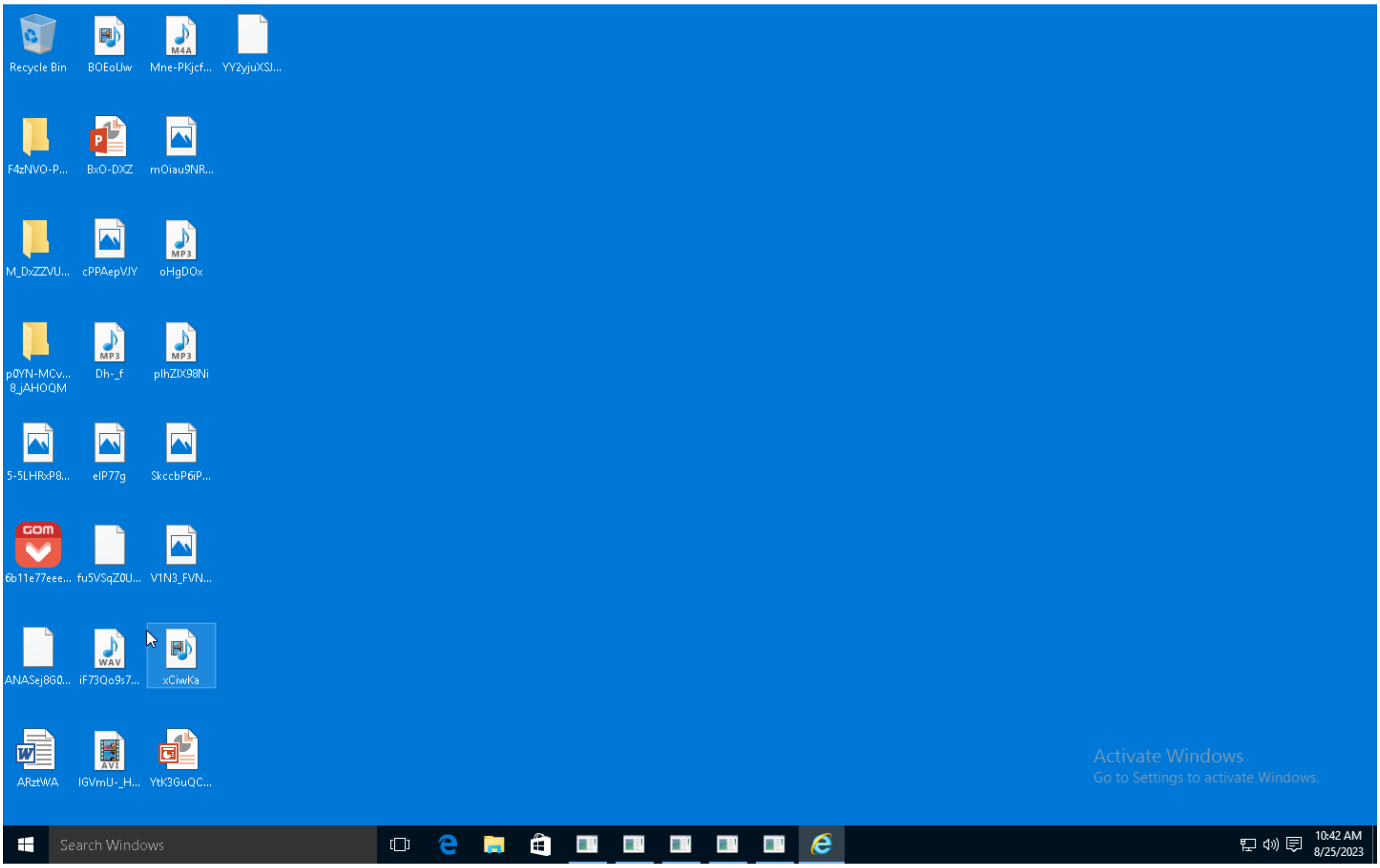
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1143 Hidden Window	#T1081 Credentials in Files	#T1082 System Information Discovery		#T1119 Automated Collection	#T1065 Uncommonly Used Port		
				#T1045 Software Packing	#T1056 Input Capture	#T1083 File and Directory Discovery		#T1005 Data from Local System			
						#T1063 Security Software Discovery		#T1113 Screen Capture			
						#T1012 Query Registry		#T1056 Input Capture			

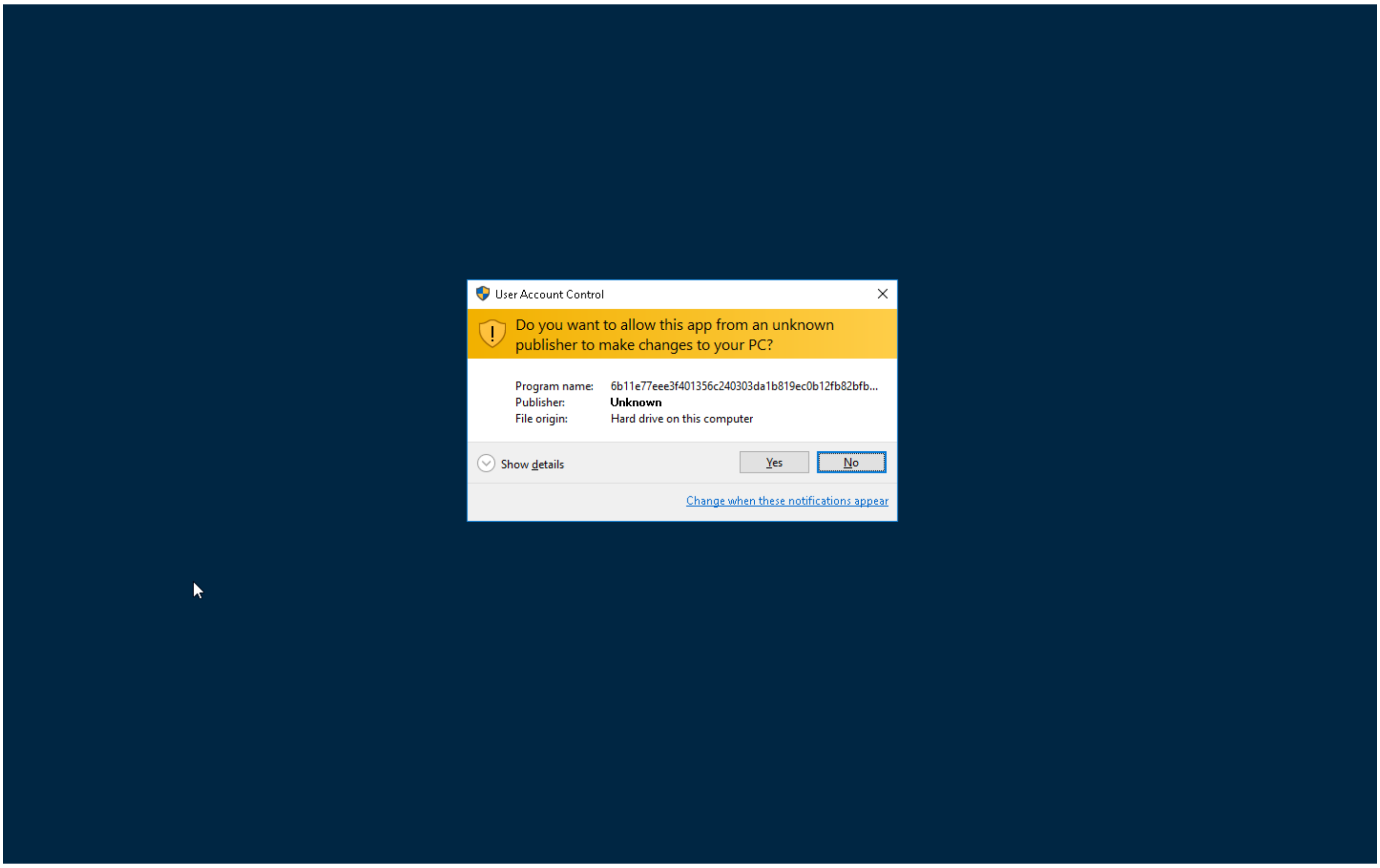
Sample Information

ID	#8680769
MD5	7278b6ce3ddda7dba2473e0392e54ea6
SHA1	3b406f221237fe9bfce48daa9033eda93ecc9b94
SHA256	6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49
SSDeep	196608:+dgX4LVznF3zQgkIRflnOzSc4pGRo9Jvy:3UzdzqIRtnYSi6zvy
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe
File Size	7516.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2023-08-25 08:41 (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

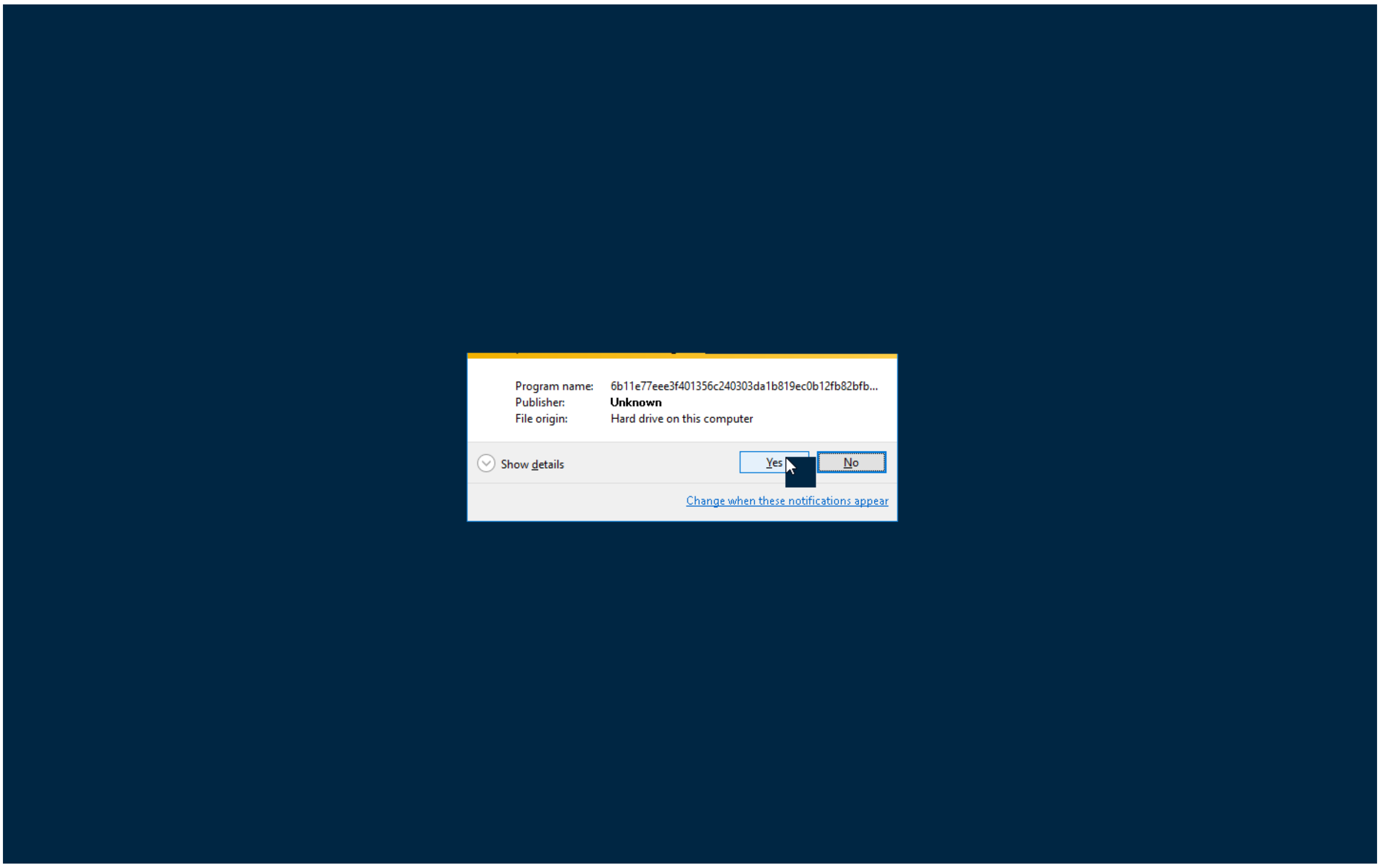




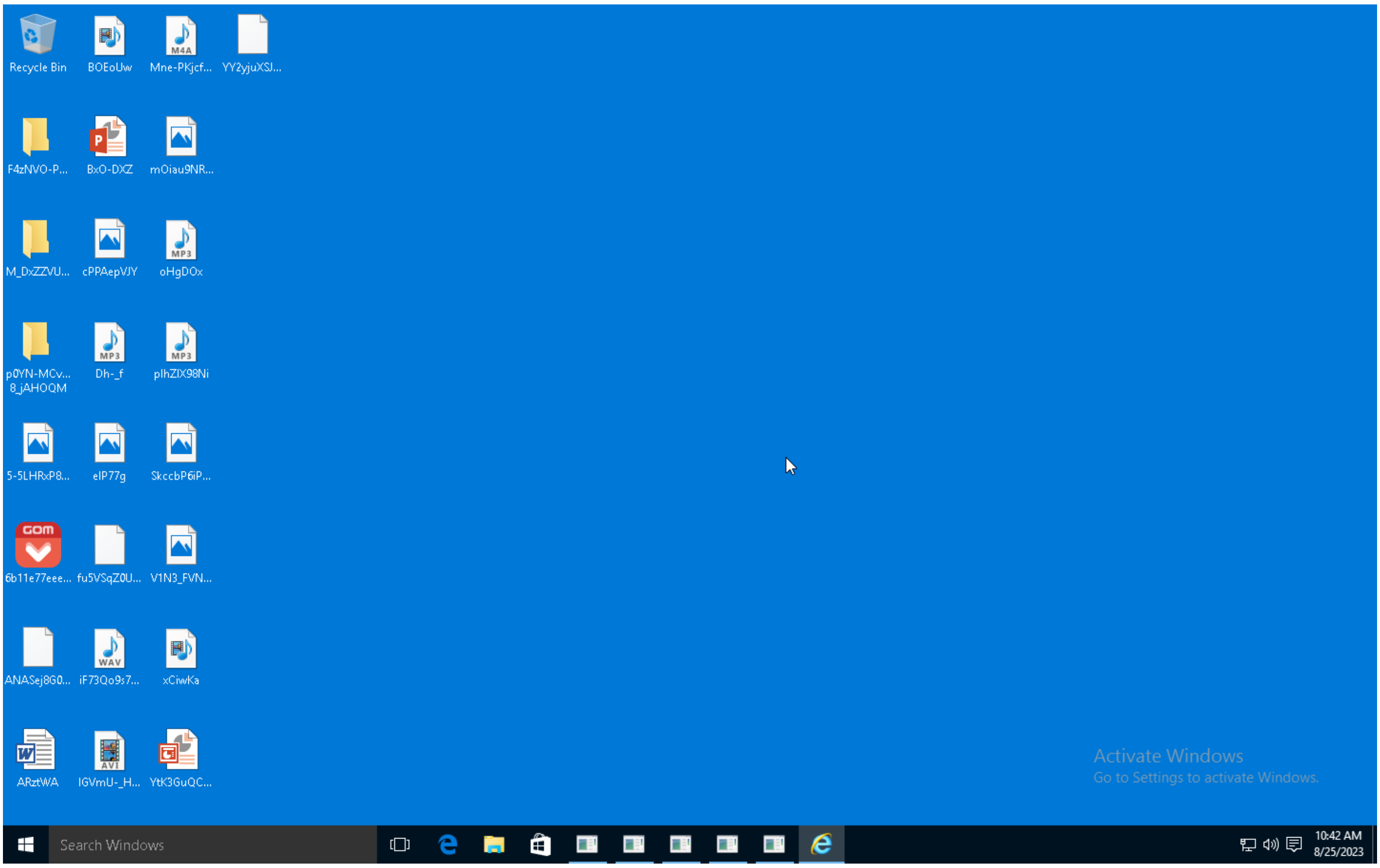
User Account Control

Do you want to allow this app from an unknown publisher to make changes to your PC?

Program name: 6b11e77eee3f401356c240303da1b819ec0b12fb82bfb...
Publisher: **Unknown**
File origin: Hard drive on this computer



Program name: 6b11e77eee3f401356c240303da1b819ec0b12fb82bfb...
Publisher: Unknown
File origin: Hard drive on this computer



NETWORK

General

443.61 KB total sent

7.75 KB total received

1 ports 7899

1 contacted IP addresses

0 URLs extracted

0 files downloaded

1 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

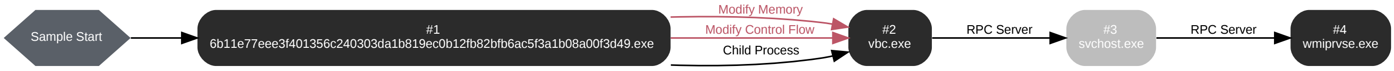
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 64793, Reason: Analysis Target
Unmonitor End Time	End Time: 95402, Reason: Terminated
Monitor duration	30.61s
Return Code	0
PID	3236
Parent PID	2024
Bitness	32 Bit

Host Behavior

Type	Count
Registry	1
File	1
Process	1
-	3
-	7

Process #2: vbc.exe

ID	2
File Name	c:\windows\microsoft.net\framework\v4.0.30319\vbc.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 81218, Reason: Child Process
Unmonitor End Time	End Time: 190679, Reason: Terminated
Monitor duration	109.46s
Return Code	0
PID	564
Parent PID	3236
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\6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe	0xc9c	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe	0xc9c	0x402000(4202496)	0x21800	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe	0xc9c	0x424000(4341760)	0x9c00	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe	0xc9c	0x42e000(4382720)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe	0xc9c	0x2db008(2994184)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe	0xc9c / 0x4ec	0x4236ae(4339374)	-	✔	1

Host Behavior

Type	Count
Module	69
Environment	2
Registry	339
File	337
User	3
-	3
COM	202
-	12

Type	Count
Keyboard	3
System	2

Network Behavior

Type	Count
TCP	1

Process #3: svchost.exe

ID	3
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: 157906, Reason: RPC Server
Unmonitor End Time	End Time: 304873, Reason: Terminated by timeout
Monitor duration	146.97s
Return Code	Unknown
PID	856
Parent PID	564
Bitness	64 Bit

Process #4: wmiprvse.exe

ID	4
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: 157906, Reason: RPC Server
Unmonitor End Time	End Time: 304873, Reason: Terminated by timeout
Monitor duration	146.97s
Return Code	Unknown
PID	4484
Parent PID	856
Bitness	64 Bit

Host Behavior

Type	Count
System	232
User	2
Process	774
-	1316
Registry	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49	C:\Users\RDhJ0CNFevzX\Desktop\6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe	Sample File	7516.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
6e2122081e550417fa35e4dc20e7a15fb86686aa5f19021b69dae4c6e444b4ba	-	Memory Dump	192.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe	Sample File	-	MALICIOUS
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe.config	Accessed File	Access	CLEAN
C:\Program Files\Internet Explorer\iexplore.exe	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\sitemanager.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\SystemCache	Accessed File	Access, Create	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.Config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\NordVPN	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe	Accessed File	Access	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
91.103.252.39	-	United Kingdom	TCP	MALICIOUS

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0018-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	vbc.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-0019-0409-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-0117-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-0117-0409-0000-0000000FF1CE}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\MPlayer2\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-001F-0409-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\MobileOptionPack	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-001B-0409-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-002C-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\Fontcore\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-002C-0409-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CSDVersion	read, access	vbc.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Clients\StartMenuInternet\IEXPLORE.EXE	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-012B-0409-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E2-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0044-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName	read, access	vbc.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0011-0000-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E1-0409-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001B-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\DisplayName	read, access	vbc.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\MobileOptionPack\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_CURRENT_USER\Software\Valve\Steam	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-0090-0409-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-00E1-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\DirectDrawEx	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\IE5BAKEX\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\IE5BAKEX\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\SchedulingAgent\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-0044-0409-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-001A-0409-0000-0000000FF1CE}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Net Framework Setup\NDP\v4\Client	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-00BA-0409-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{90160000-001F-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall\IE5BAKEX	access	vbc.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00A1-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0019-0409-0000-0000000FF1CE}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00BA-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Clients\StartMenuInternet\IEXPLORE.EXE\shell\open\command	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002C-0409-0000-0000000FF1CE}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E2-0409-0000-0000000FF1CE}	access	vbc.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0090-0409-0000-0000000FF1CE}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Clients\StartMenuInternet	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001A-0409-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{4A03706F-666A-4037-7777-5F2748764D10}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0115-0409-0000-0000000FF1CE}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe, vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-012B-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0019-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0117-0409-0000-0000000FF1CE}\DisplayVersion	read, access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001A-0409-0000-0000000FF1CE}\DisplayName	read, access	vbc.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	vbc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayVersion	read, access	vbc.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe	"C:\Users\RDhJ0CNFevzX\Desktop\6b11e77eee3f401356c240303da1b819ec0b12fb82bfb6ac5f3a1b08a00f3d49.exe"	MALICIOUS
vbc.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.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	win10_64_th2_en_mso2016
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	2023.3.1
Dynamic Engine Version	2023.3.1 / 07/17/2023 04:23
Static Engine Version	2023.3.1.0 / 2023-07-17 03:00:15
AV Exceptions Version	2023.3.1.2 / 2023-07-01 17:20:29
Link Detonation Heuristics Version	2023.3.1.18 / 2023-08-10 15:33:22
Smart Memory Dumping Rules Version	2023.3.1.2 / 2023-07-01 17:20:29
Config Extractors Version	2023.3.1.21 / 2023-08-17 15:24:36
Signature Trust Store Version	2023.3.1.2 / 2023-07-01 17:20:29
VMRay Threat Identifiers Version	2023.3.1.22 / 2023-08-20 08:30:38
YARA Built-in Ruleset Version	2023.3.1.21

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