MALICIOUS

Classifications: Backdoor

Threat Names: -

Verdict Reason: -

Sample Type	**MSI Setup**
File Name	**fb9f0bf2b71bf576053c56cb913ea4e93581fc9d3aa9d6d8a0ae572a1622f050.msi**
ID	#5069519
MD5	6cf5ad7a7d1b7bab0c62e246cf41a985
SHA1	b06a03adc550ead96534f5e723395c4e16bfdf44
SHA256	fb9f0bf2b71bf576053c56cb913ea4e93581fc9d3aa9d6d8a0ae572a1622f050
File Size	3968.00 KB
Report Created	2022-08-05 21:46 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | msi

OVERVIEW

VMRay Threat Identifiers (20 rules, 50 matches)

Score	Category	Operation	Count	Classification
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
	• Based on a combination of other detections, the sample queries the configuration of the host and the local network.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #15) anydesk.exe tries to delete zone identifier of file "C:\ProgramData\AnyDesk\AnyDesk.exe".			
3/5	System Modification	Modifies system configuration	1	-
	• (Process #12) install.exe sets "c:\windows\system32\cmd.exe" as debugger for the application "sethc.exe".			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #2) msiexec.exe has a thread which sleeps more than 5 minutes.			
2/5	Discovery	Reads network adapter information	2	-
	• (Process #30) anydesk.exe reads the network adapters' addresses by API. • (Process #36) anydesk.exe reads the network adapters' addresses by API.			
2/5	Network Connection	Sets up server that accepts incoming connections	2	Backdoor
	• (Process #36) anydesk.exe starts a TCP server listening on port 7070. • (Process #30) anydesk.exe starts a TCP server listening on port 7070.			
1/5	Privilege Escalation	Enables process privilege	3	-
	• (Process #2) msiexec.exe enables process privilege "SeSecurityPrivilege, SeUnsolicitedInputPrivilege, SeSystemtimePrivilege, SeUns... ...ackupPrivilege, SeUnsolicitedInputPrivilege, SeRemoteShutdownPrivilege, SeUnsolicitedInputPrivilege, SeUnsolicitedInputPrivilege". • (Process #2) msiexec.exe enables process privilege "SeRestorePrivilege, SeUnsolicitedInputPrivilege". • (Process #12) install.exe enables process privilege "SeRemoteShutdownPrivilege".			
1/5	System Modification	Modifies operating system directory	7	-
	• (Process #2) msiexec.exe creates file "C:\Windows\Installer\1876eff.msi" in the OS directory. • (Process #2) msiexec.exe creates file "C:\Windows\Installer\1876f00.ipi" in the OS directory. • (Process #2) msiexec.exe modifies file "C:\Windows\Installer\MSI8868.tmp" in the OS directory. • (Process #2) msiexec.exe creates file "C:\Windows\Installer\MSI8868.tmp" in the OS directory. • (Process #2) msiexec.exe modifies file "C:\Windows\Installer\MSI8ECF.tmp" in the OS directory. • (Process #2) msiexec.exe modifies file "C:\Windows\Installer\MSIA7FC.tmp" in the OS directory. • (Process #2) msiexec.exe modifies file "C:\Windows\Installer\MSI2306.tmp" in the OS directory.			
1/5	Hide Tracks	Creates process with hidden window	4	-
	• (Process #2) msiexec.exe starts (process #2) msiexec.exe with a hidden window. • (Process #9) msiexec.exe starts (process #10) icacls.exe with a hidden window. • (Process #9) msiexec.exe starts (process #11) expand.exe with a hidden window. • (Process #12) install.exe starts (process #12) install.exe with a hidden window.			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #12) install.exe adds "0" to Windows startup via registry.			

Score	Category	Operation	Count	Classification
1/5	Mutex	Creates mutex	7	-
	• (Process #15) anydesk.exe creates mutex with name "Local\ad_trace_mtx". • (Process #30) anydesk.exe creates mutex with name "Local\ad_trace_mtx". • (Process #30) anydesk.exe creates mutex with name "Global\ad_707_gsystem_mtx". • (Process #30) anydesk.exe creates mutex with name "Global\ad_connect_queue_2452_2298657072_mtx". • (Process #36) anydesk.exe creates mutex with name "Local\ad_trace_mtx". • (Process #36) anydesk.exe creates mutex with name "Global\ad_707_gsystem_mtx". • (Process #36) anydesk.exe creates mutex with name "Global\ad_connect_queue_1308_3747059072_mtx".		
1/5	Persistence	Installs system service	1	-
	• (Process #15) anydesk.exe installs service "AnyDesk" via CreateServiceW.			
1/5	Discovery	Tries to get network statistics	1	-
	• (Process #30) anydesk.exe gets network statistics via API.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #30) anydesk.exe enumerates running processes.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #30) anydesk.exe resolves host name "boot.net.anydesk.com" to IP "49.12.130.237".			
1/5	Network Connection	Connects to remote host	6	-
	• (Process #30) anydesk.exe opens an outgoing TCP connection to host "49.12.130.237:6568". • (Process #30) anydesk.exe opens an outgoing TCP connection to host "49.12.130.237:443". • (Process #36) anydesk.exe opens an outgoing TCP connection to host "49.12.130.237:80". • (Process #30) anydesk.exe opens an outgoing TCP connection to host "49.12.130.237:80". • (Process #36) anydesk.exe opens an outgoing TCP connection to host "49.12.130.237:443". • (Process #36) anydesk.exe opens an outgoing TCP connection to host "49.12.130.237:6568".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #30) anydesk.exe tries to connect to TCP port 6568 at 49.12.130.237.			
1/5	Obfuscation	Resolves API functions dynamically	4	-
	• (Process #2) msiexec.exe resolves 63 API functions by name. • (Process #15) anydesk.exe resolves 295 API functions by name. • (Process #30) anydesk.exe resolves 307 API functions by name. • (Process #36) anydesk.exe resolves 300 API functions by name.			
1/5	Execution	Drops PE file	4	-
	• (Process #2) msiexec.exe drops file "C:\Windows\Installer\MSI2306.tmp". • (Process #2) msiexec.exe drops file "C:\Windows\Installer\MSI8ECF.tmp". • (Process #30) anydesk.exe drops file "C:\ProgramData\AnyDesk\AnyDesk.exe". • (Process #15) anydesk.exe drops file "c:\programdata\anydesk.exe".			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\ProgramData\AnyDesk\AnyDesk.exe".			
-	Trusted	Known clean file	3	-

Score	Category	Operation	Count	Classification
		• File "C:\Windows\Installer\MSI2306.tmp" is a known clean file. • File "" is a known clean file. • Embedded file "C:\ProgramData\AnyDesk\AnyDesk.exe" is a known clean file.		

Mitre ATT&CK Matrix

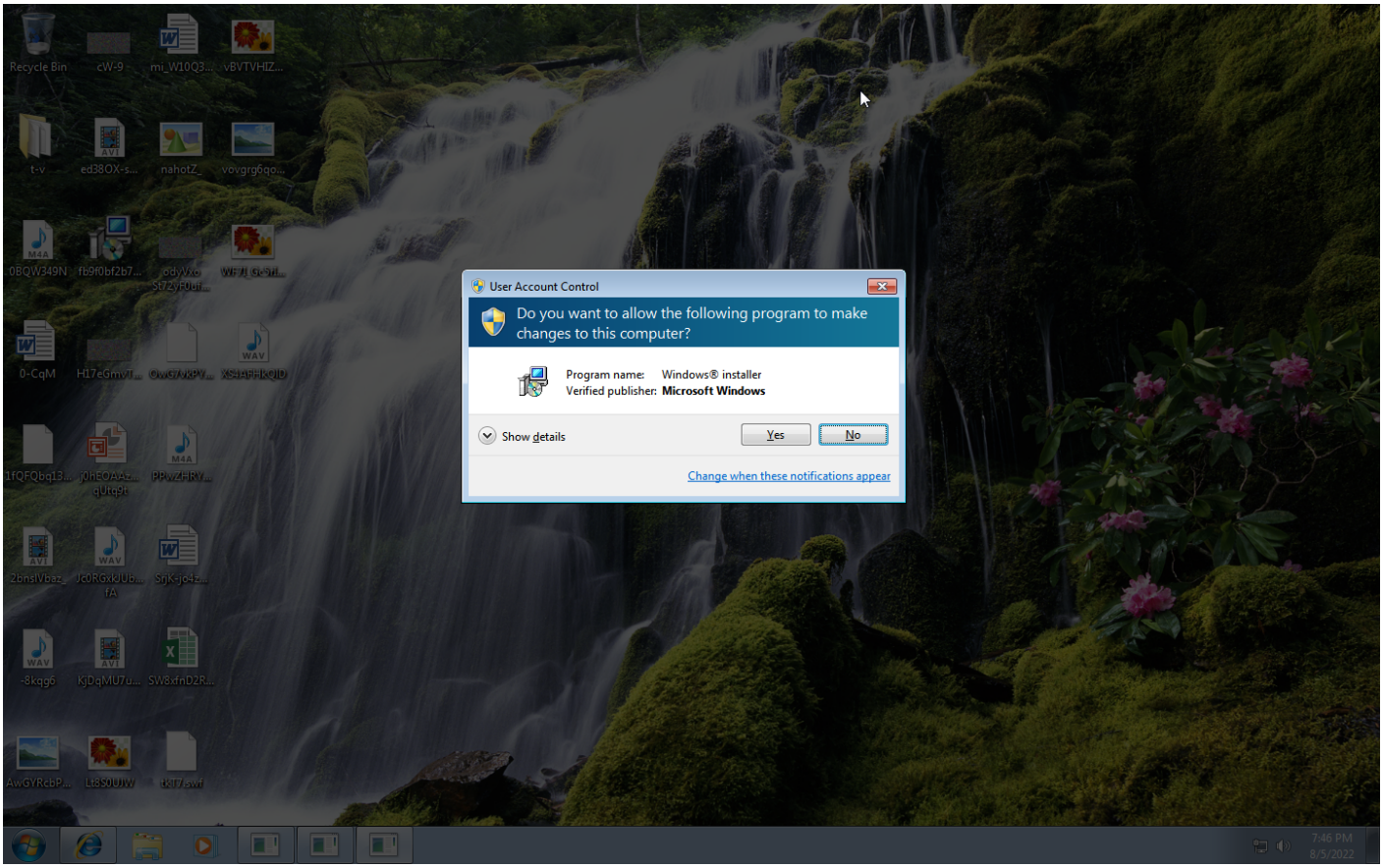
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1183 Image File Execution Options Injection	#T1183 Image File Execution Options Injection	#T1143 Hidden Window		#T1016 System Network Configuration Discovery			#T1065 Uncommonly Used Port		
		#T1060 Registry Run Keys / Startup Folder	#T1050 New Service	#T1112 Modify Registry		#T1049 System Network Connections Discovery					
		#T1050 New Service		#T1183 Image File Execution Options Injection		#T1057 Process Discovery					
				#T1096 NTFS File Attributes		#T1082 System Information Discovery					
				#T1045 Software Packing							

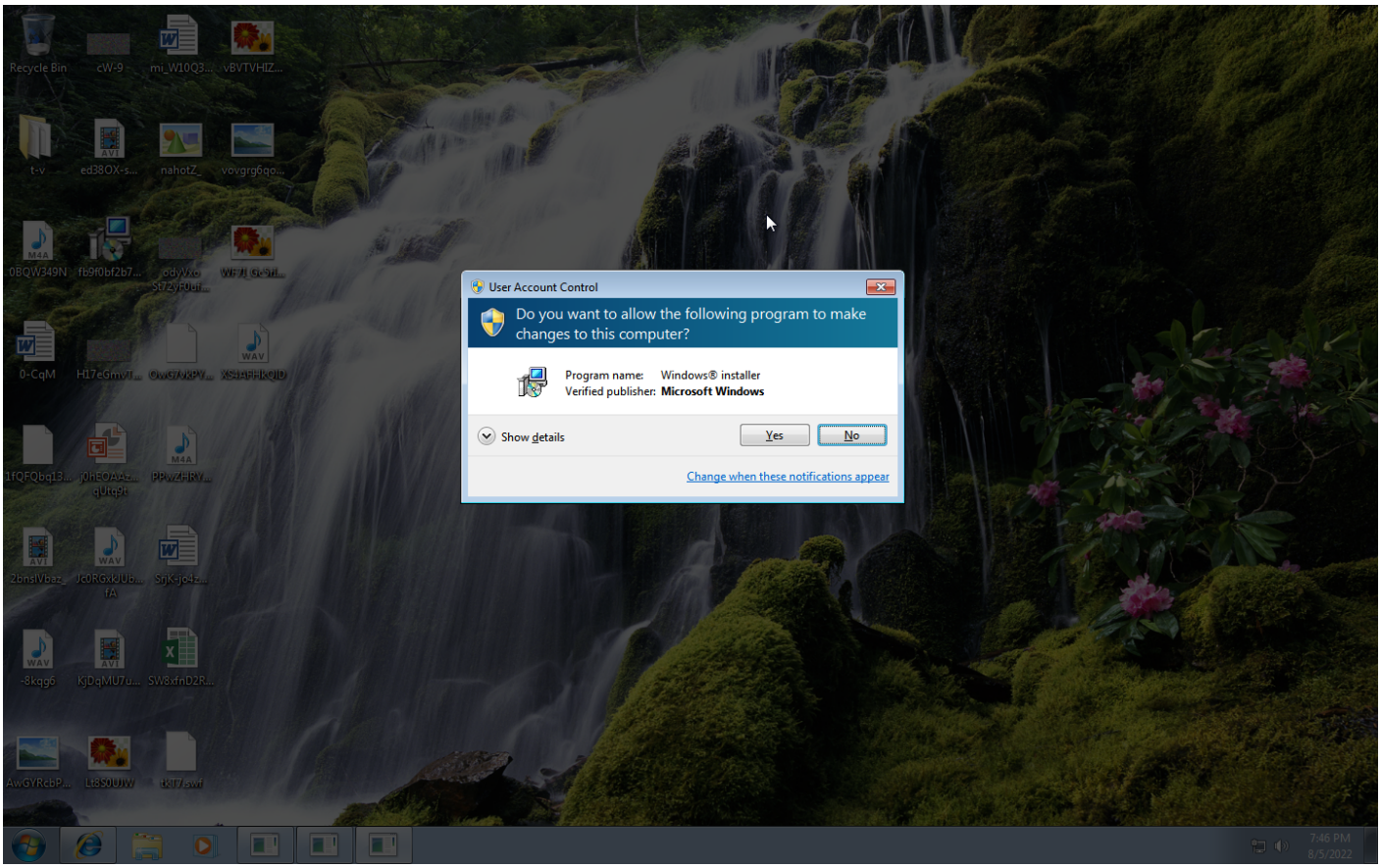
Sample Information

ID	#5069519
MD5	6cf5ad7a7d1b7bab0c62e246cf41a985
SHA1	b06a03adc550ead96534f5e723395c4e16bfdf44
SHA256	fb9f0bf2b71bf576053c56cb913ea4e93581fc9d3aa9d6d8a0ae572a1622f050
SSDeep	98304:pp+vXhd7YjjTcLO6KnQh5YUNa/ckQGQCWijuYAHw:+zkTcilYUNuNCAuPH
File Name	fb9f0bf2b71bf576053c56cb913ea4e93581fc9d3aa9d6d8a0ae572a1622f050.msi
File Size	3968.00 KB
Sample Type	MSI Setup
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 21:46 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	27
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


User Account Control
Do you want to allow the following program to make changes to this computer?
Program name: Windows® installer
Verified publisher: Microsoft Windows
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

3.21 KB total sent

2.66 KB total received

5 ports 6568, 80, 53, 443, 445

2 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

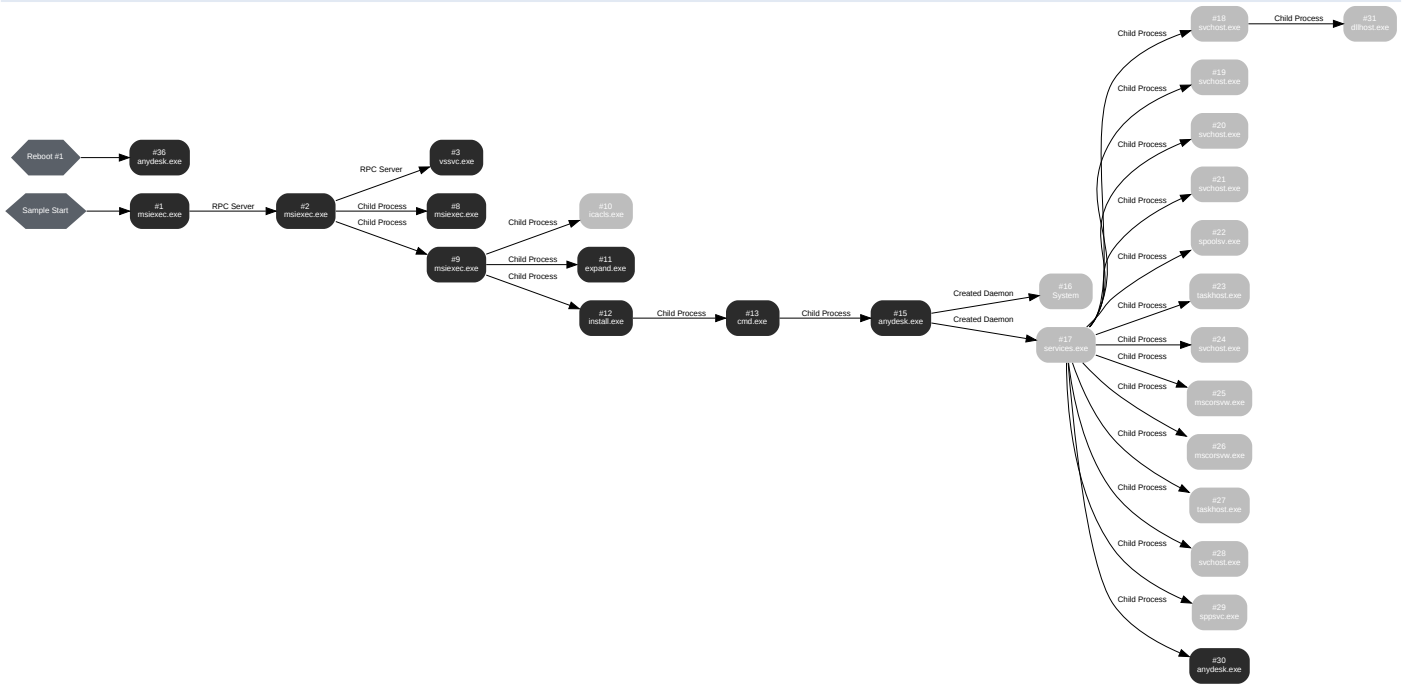
0 sessions, 0 bytes sent, 0 bytes received

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	boot.net.anydesk.com	NO_ERROR	49.12.130.237		NA

BEHAVIOR

Process Graph



Process #1: msiexec.exe

ID	1
File Name	c:\windows\system32\msiexec.exe
Command Line	"C:\Windows\System32\msiexec.exe" /i "C:\Users\KEECFM~1\Desktop\fb9f0bf2b71bf576053c56cb913ea4e93581fc9d3aa9d6d8a0ae572a1622f050.msi"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 49893, Reason: Analysis Target
Unmonitor End Time	End Time: 210592, Reason: Terminated
Monitor duration	160.70s
Return Code	1073807364
PID	3848
Parent PID	-
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	6
Module	5
File	2

Process #2: msiexec.exe

ID	2
File Name	c:\windows\system32\msiexec.exe
Command Line	C:\Windows\system32\msiexec.exe /V
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63638, Reason: RPC Server
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	233.38s
Return Code	Unknown
PID	3888
Parent PID	3848
Bitness	64 Bit

Dropped Files (15)

File Name	File Size	SHA256	YARA Match
C:\Windows\Installer\1876f00.ipi	20.00 KB	369d4970317d511ad452ad224b5d89a43c5cb4be88f9098f43b2b47e1cf7063a	✖
-	8787.71 KB	f6b730b7200cb7886a2edc1a4e8238774a8cf68aa96788b84567ea4d2d23cbb6	✖
C:\Windows\Installer\MSI2306.tmp	208.00 KB	d01af2b8c692dffb04a5a04e3ccd0d0a3b2c67c8fc45a4b68c0a065b4e64cc3d	✖
C:\Users\KEECFM~1\Desktop\fb9f0bf2b71bf576053c56cb913ea4e93581fc9d3aa9d6d8a0ae572a1622f050.msi	3968.00 KB	fb9f0bf2b71bf576053c56cb913ea4e93581fc9d3aa9d6d8a0ae572a1622f050	✖
-	3.03 KB	b578195e3269fa0f78384606a7ae76fa79c73c95ea05ff7df4d8ca8d31f85a33	✖
C:\Windows\Installer\MSI8868.tmp	418.07 KB	a8c2ca783c081ca354cca0258404babdc3449687b2e01ee6f139e953a0e86982	✖
C:\Windows\Installer\1876f00.ipi	20.00 KB	68a761b0e8bf4a1285e3dedce6c1cc732176118542cf730c28b3bfda5ab8f71c	✖
C:\Config.Msi\1876f01.rbs	740 bytes	e72faf012b929b1fc3b6ab0d7c0e9c01580e9cadb7263c3edf1c4bfa6aceda7f	✖
-	68.00 KB	227150f6222719008f63bd91ffbd08fcdbfbf91f129d178ba378cecfb06c3342	✖
-	512 bytes	076a27c79e5ace2a3d47f9dd2e83e4ff6ea8872b3c2218f66c92b89b55f36560	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Config.Msi\MSIA7BD.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Config.Msi\MSI36A6.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Windows\Installer\MSIA7FC.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	1510
Module	129

Type	Count
Mutex	2
Registry	727
-	14
User	45
Environment	172
Window	2
File	503
COM	4
Process	3

Process #3: vssvc.exe

ID	3
File Name	c:\windows\system32\vssvc.exe
Command Line	C:\Windows\system32\vssvc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 70742, Reason: RPC Server
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	226.28s
Return Code	Unknown
PID	3928
Parent PID	3888
Bitness	64 Bit

Host Behavior

Type	Count
System	3

Process #8: msiexec.exe

ID	8
File Name	c:\windows\syswow64\msiexec.exe
Command Line	C:\Windows\syswow64\MsiExec.exe -Embedding 15C2A74905FE813C1C1C8CDCF151DE4D
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 130678, Reason: Child Process
Unmonitor End Time	End Time: 206020, Reason: Terminated
Monitor duration	75.34s
Return Code	1073807364
PID	320
Parent PID	3888
Bitness	32 Bit

Dropped Files (19)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	556 bytes	1dc41c1f212125f44c42baaeb00a3402e8e19257fbb20123dd24fd7c5412b48d	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	376 bytes	0ee9cd006768810ec0fd7f40dac9570b1b718849d74a58a091f5a74964ec8fed	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	250 bytes	133f38f53e831d9c1f3e0ef29cf5542c8ab2b9d6dd1c1a5ae0fe134f7c10bf39	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	522 bytes	7c75643b0869803ca12db1913f0a2ebfccdb69f7f812448358f28c5aed222819	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	646 bytes	9fe6a6bf86ebab1c3a9f6dc4df4bd2a265c501276ac227e57dbd62c10d19c51b	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	334 bytes	b6f20d2b6f7fc11474f3f37becbc1d42f417f474254c11a6a788ec6183482815	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	580 bytes	1855c366f25876b91db995f6c5b8fd59b65da1536013b1ba5b14c7323634a4c4	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	1.14 KB	58810cd2764e951e7170488bd6351db35bc10d69a9557c68449646892b754942	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\files.cab	3721.70 KB	a929c064c064a1b5013b8fbce01feb7ae08e6bd9b05106dcda8320f9db0fb13d	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	1.41 KB	f5d6af499ec4e83960097c994a8838d993a36844e63c03d2cd94cf3612910a38	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	1.10 KB	20cfab35403d0daa886a287e65e964f0d36ff2b01963ba3d725f8231254ef338	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	294 bytes	effb26504044d25e882310d5b1e800be1a2450f85d9250679b2236b48903d3b6	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	666 bytes	06498734b1e071e4fddc03effab417a58e86091c03fab1e45e8f58d65fc0a2eb	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	1.05 KB	8f3cd45fb1e3d8d472fc7b27739e78a72c69688cad974ba206dedbeed9c11f85	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	844 bytes	78289a3decdf0d00d469739189129687487d16bb44d60218c6e511c2512a292e	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	196 bytes	4200a80a055888e50bdaeb58293dcc0d47f9c50deae1c7daa894332af4470f6a	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	1.01 KB	6fbbbcd35e9723b71e005f37608d59b4cc7b8756b419ea30277b1ed54692dfb4	✖
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	1.20 KB	94d78d9395d2775d7d86b4ef45fc5d3d82508aff79c2026ffe7d882cfc7d552a	✖

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	626 bytes	a1c73dfd3110ddaeeb177e61e0358c8810dd4b29acb28820be8079b2cc9a5aff	✖

Host Behavior

Type	Count
System	7
Module	41
Process	2
File	341
Registry	1
-	2
COM	1
Environment	1
User	1

Process #9: msiexec.exe

ID	9
File Name	c:\windows\syswow64\msiexec.exe
Command Line	C:\Windows\syswow64\MsiExec.exe -Embedding ADDCD9128E57B274A403CFC05E47C1FC M Global\MSI0000
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 149958, Reason: Child Process
Unmonitor End Time	End Time: 206020, Reason: Terminated
Monitor duration	56.06s
Return Code	1073807364
PID	908
Parent PID	3888
Bitness	32 Bit

Host Behavior

Type	Count
System	8
Module	56
Process	5
File	308
Registry	1
-	2
COM	1
Environment	1
User	1
Window	1

Process #10: icacls.exe

ID	10
File Name	c:\windows\syswow64\icacls.exe
Command Line	"C:\Windows\system32\ICACLS.EXE" "C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\." /SETINTEGRITYLEVEL (CI)(OI)HIGH
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 156420, Reason: Child Process
Unmonitor End Time	End Time: 157549, Reason: Terminated
Monitor duration	1.13s
Return Code	0
PID	3360
Parent PID	908
Bitness	32 Bit

Process #11: expand.exe

ID	11
File Name	c:\windows\syswow64\expand.exe
Command Line	"C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files
Initial Working Directory	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\
Monitor Start Time	Start Time: 157294, Reason: Child Process
Unmonitor End Time	End Time: 160136, Reason: Terminated
Monitor duration	2.84s
Return Code	0
PID	3416
Parent PID	908
Bitness	32 Bit

Host Behavior

Type	Count
System	4
Module	4
File	12

Process #12: install.exe

ID	12
File Name	c:\users\keecfmwgj\appdata\local\temp\mw-ed03fe6a-6d69-41db-94de-aca9dc9763e3\files\install.exe
Command Line	"C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\files\install.exe"
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 159664, Reason: Child Process
Unmonitor End Time	End Time: 204720, Reason: Terminated
Monitor duration	45.06s
Return Code	3221225786
PID	3564
Parent PID	908
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
c:\programdata\anydesk.exe	3740.12 KB	af61905129f377f5934b3bbf787e8d2417901858bb028f40f02200e985ee62f6	✖
log1.txt	13 bytes	a8c0656b85d708b1c93db91ddab77ceaa332fe6a572313e539749f41e3ff4304	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
File	5
User	1
Module	6
Registry	12
-	2
Process	1
-	1
System	322

Process #13: cmd.exe

ID	13
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd /c c:\programdata\anydesk.exe --install C:\ProgramData\AnyDesk --silent
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 162294, Reason: Child Process
Unmonitor End Time	End Time: 205324, Reason: Terminated
Monitor duration	43.03s
Return Code	1073807364
PID	3544
Parent PID	3564
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	3
File	1
Process	1

Process #15: anydesk.exe

ID	15
File Name	c:\programdata\anydesk.exe
Command Line	c:\programdata\anydesk.exe --install C:\ProgramData\AnyDesk --silent
Initial Working Directory	C:\Windows\SysWOW64\
Monitor Start Time	Start Time: 163685, Reason: Child Process
Unmonitor End Time	End Time: 205268, Reason: Terminated
Monitor duration	41.58s
Return Code	1073807364
PID	3604
Parent PID	3544
Bitness	32 Bit

Dropped Files (6)

File Name	File Size	SHA256	YARA Match
C:\ProgramData\AnyDesk\system.conf	455 bytes	93e9b6f83e46b026979cafc9d6cb022eea8025bf6311e36470312afb76f0a7bf	✖
C:\ProgramData\AnyDesk\AnyDesk.exe	3740.12 KB	af61905129f377f5934b3bbf787e8d2417901858bb028f40f02200e985ee62f6	✖
C:\ProgramData\AnyDesk\system.conf	398 bytes	99860d4dfbf1a10a93a81c4b9e7ba050baab11a1df3530168b91c3b8f0061ddf	✖
C:\ProgramData\AnyDesk\system.conf	422 bytes	be72d2a496f9407ec2a4fb2da2bd16d8cb986f1d52cfe7b24202c08ff59a1267	✖
C:\Users\kEecfMwgj\AppData\Roaming\AnyDesk\ad.trace	3.41 KB	048f7a1ddae30fe824f1fdaf4550529b98a9fa4fb66ce30ed31f56d377a71b11	✖
C:\ProgramData\AnyDesk\system.conf	455 bytes	eaeceece55f1c16b178b70fcb07f78e2a453ff63bce81e4b32df93843aa1e98e	✖

Host Behavior

Type	Count
Module	381
System	34
Environment	1
File	24
Mutex	1
Registry	50
-	12
COM	1

Process #16: System

ID	16
File Name	System
Command Line	-
Initial Working Directory	-
Monitor Start Time	Start Time: 180543, Reason: Created Daemon
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	116.47s
Return Code	Unknown
PID	4
Parent PID	-
Bitness	64 Bit

Process #17: services.exe

ID	17
File Name	c:\windows\system32\services.exe
Command Line	C:\Windows\system32\services.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180543, Reason: Created Daemon
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	116.47s
Return Code	Unknown
PID	460
Parent PID	3604
Bitness	64 Bit

Process #18: svchost.exe

ID	18
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k DcomLaunch
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180543, Reason: Child Process
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	116.47s
Return Code	Unknown
PID	592
Parent PID	460
Bitness	64 Bit

Process #19: svchost.exe

ID	19
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k RPCSS
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180543, Reason: Child Process
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	116.47s
Return Code	Unknown
PID	660
Parent PID	460
Bitness	64 Bit

Process #20: svchost.exe

ID	20
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180543, Reason: Child Process
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	116.47s
Return Code	Unknown
PID	708
Parent PID	460
Bitness	64 Bit

Process #21: svchost.exe

ID	21
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180543, Reason: Child Process
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	116.47s
Return Code	Unknown
PID	820
Parent PID	460
Bitness	64 Bit

Process #22: spoolsv.exe

ID	22
File Name	c:\windows\system32\spoolsv.exe
Command Line	C:\Windows\System32\spoolsv.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180543, Reason: Child Process
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	116.47s
Return Code	Unknown
PID	1108
Parent PID	460
Bitness	64 Bit

Process #23: taskhost.exe

ID	23
File Name	c:\windows\system32\taskhost.exe
Command Line	"taskhost.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180543, Reason: Child Process
Unmonitor End Time	End Time: 212432, Reason: Terminated
Monitor duration	31.89s
Return Code	1073807364
PID	1140
Parent PID	460
Bitness	64 Bit

Process #24: svchost.exe

ID	24
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180543, Reason: Child Process
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	116.47s
Return Code	Unknown
PID	1172
Parent PID	460
Bitness	64 Bit

Process #25: mscorsvw.exe

ID	25
File Name	c:\windows\microsoft.net\framework\v4.0.30319\mscorsvw.exe
Command Line	C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180543, Reason: Child Process
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	116.47s
Return Code	Unknown
PID	1312
Parent PID	460
Bitness	32 Bit

Process #26: mscorsvw.exe

ID	26
File Name	c:\windows\microsoft.net\framework64\v4.0.30319\mscorsvw.exe
Command Line	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180543, Reason: Child Process
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	116.47s
Return Code	Unknown
PID	1368
Parent PID	460
Bitness	64 Bit

Process #27: taskhost.exe

ID	27
File Name	c:\windows\system32\taskhost.exe
Command Line	taskhost.exe $(Arg0)
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180543, Reason: Child Process
Unmonitor End Time	End Time: 212729, Reason: Terminated
Monitor duration	32.19s
Return Code	0
PID	1084
Parent PID	460
Bitness	64 Bit

Process #28: svchost.exe

ID	28
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180543, Reason: Child Process
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	116.47s
Return Code	Unknown
PID	276
Parent PID	460
Bitness	64 Bit

Process #29: sppsvc.exe

ID	29
File Name	c:\windows\system32\sppsvc.exe
Command Line	C:\Windows\system32\sppsvc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180543, Reason: Child Process
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	116.47s
Return Code	Unknown
PID	2272
Parent PID	460
Bitness	64 Bit

Process #30: anydesk.exe

ID	30
File Name	c:\programdata\anydesk\anydesk.exe
Command Line	"C:\ProgramData\AnyDesk\AnyDesk.exe" --service
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180747, Reason: Child Process
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	116.27s
Return Code	Unknown
PID	2452
Parent PID	460
Bitness	32 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
C:\ProgramData\AnyDesk\service.conf	2.70 KB	9c0b9c9492d4a1b4c57e6d51ba8a7c74c7d2a82cffedae57ab8b3f7458367955	✖
C:\ProgramData\AnyDesk\service.conf	1.71 KB	c715e97bad4c1ee928c1cc47b9c700525af9654d7eb080bfe7ba5f1adc207364	✖
C:\ProgramData\AnyDesk\ad_svc.trace	10.15 KB	01546d505366a19f0097314f3f300db3efd08b404d2231b19a713c4f7cdf94b0	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	428
System	803
Environment	1
File	61
Mutex	11
Registry	468
-	14
COM	8
-	1
Process	112
-	6

Network Behavior

Type	Count
DNS	2
TCP	4

Process #31: dllhost.exe

ID	31
File Name	c:\windows\system32\dllhost.exe
Command Line	C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 182247, Reason: Child Process
Unmonitor End Time	End Time: 205115, Reason: Terminated
Monitor duration	22.87s
Return Code	1073807364
PID	2464
Parent PID	592
Bitness	64 Bit

Process #36: anydesk.exe

ID	36
File Name	c:\programdata\anydesk\anydesk.exe
Command Line	"C:\ProgramData\AnyDesk\AnyDesk.exe" --service
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 276265, Reason: Autostart
Unmonitor End Time	End Time: 297017, Reason: Terminated by timeout
Monitor duration	20.75s
Return Code	Unknown
PID	1308
Parent PID	3604
Bitness	32 Bit

Host Behavior

Type	Count
Module	417
System	139
Environment	1
File	35
Mutex	10
Registry	170
-	12
COM	7
-	1
-	4

Network Behavior

Type	Count
TCP	3

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
fb9f0bf2b71bf576053c56cb913ea4e93581fc9d3aa9d6d8a0ae572a1622f050	C:\Users\KEECFM~1\Desktop\fb9f0bf2b71bf576053c56cb913ea4e93581fc9d3aa9d6d8a0ae572a1622f050.msi, C:\Users\kEecfMwgj\Desktop\fb9f0bf2b71bf576053c56cb913ea4e93581fc9d3aa9d6d8a0ae572a1622f050.msi, C:\Windows\Installer\1876eff.msi	Sample File	3968.00 KB	application/x-msi	Access, Create, Delete, Read, Write	MALICIOUS
af61905129f377f5934b3bbf787e8d2417901858bb028f40f02200e985ee62f6	C:\ProgramData\AnyDesk\AnyDesk.exe, c:\programdata\anydesk.exe	Dropped File	3740.12 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	SUSPICIOUS
1dc41c1f212125f44c42baaeb00a3402e8e19257fbb20123dd24fd7c5412b48d	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	556 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
0ee9cd006768810ec0fd7f40dac9570b1b718849d74a58a091f5a74964ec8fed	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	376 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
133f38f53e831d9c1f3e0ef29cf5542c8ab2b9d6dd1c1a5ae0fe134f7c10bf39	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	250 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
7c75643b0869803ca12db1913f0a2ebfccdb69f7f812448358f28c5aed222819	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	522 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
9fe6a6bf86ebab1c3a9f6dc4df4bd2a265c501276ac227e57dbd62c10d19c51b	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	646 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
369d4970317d511ad452ad224b5d89a43c5cb4be88f9098f43b2b47e1cf7063a	C:\Windows\Installer\1876f00.ipi	Dropped File	20.00 KB	application/CDFV2	Access, Create, Delete	CLEAN
f6b730b7200cb7886a2edc1a4e8238774a8cf68aa96788b84567ea4d2d23cbb6	-	Dropped File	8787.71 KB	application/octet-stream	-	CLEAN
9c0b9c9492d4a1b4c57e6d51ba8a7c74c7d2a82cffedae57ab8b3f7458367955	C:\ProgramData\AnyDesk\service.conf	Dropped File	2.70 KB	text/plain	Access, Create, Read, Write	CLEAN
93e9b6f83e46b026979cafc9d6cb022eea8025bf6311e36470312afb76f0a7bf	C:\ProgramData\AnyDesk\system.conf	Dropped File	455 bytes	text/plain	Access, Create, Read, Write	CLEAN
d01af2b8c692dffb04a5a04e3ccd0d0a3b2c67c8fc45a4b68c0a065b4e64cc3d	C:\Windows\Installer\MSI2306.tmp, C:\Windows\Installer\MSI8ECF.tmp	Dropped File	208.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	CLEAN
ea057e896209478d8290a1b526cae84f2509678d866d08382614707f3b710d47	-	Extracted File	6.89 KB	image/png	-	CLEAN
beb6182ceab6ea0b0fdc0f41f8069632317e0f941419b75ede4145593cd6a21c	install.exe	Extracted File	3747.50 KB	application/vnd.microsoft.portable-executable	-	CLEAN
b578195e3269fa0f78384606a7ae76fa79c73c95ea05ff7df4d8ca8d31f85a33	-	Dropped File	3.03 KB	application/octet-stream	-	CLEAN
b6f20d2b6f7fc11474f3f37becbc1d42f417f474254c11a6a788ec6183482815	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	334 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
99860d4dfbf1a10a93a81c4b9e7ba050baab11a1df3530168b91c3b8f0061ddf	C:\ProgramData\AnyDesk\system.conf	Dropped File	398 bytes	text/plain	Access, Create, Read, Write	CLEAN
be72d2a496f9407ec2a4fb2da2bd16d8cb986f1d52cfe7b24202c08ff59a1267	C:\ProgramData\AnyDesk\system.conf	Dropped File	422 bytes	text/plain	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
1855c366f25876b91db995f6c5b8fd59b65da1536013b1ba5b14c7323634a4c4	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	580 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
58810cd2764e951e7170488bd6351db35bc10d69a9557c68449646892b754942	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	1.14 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
a929c064c064a1b5013b8fbce01feb7ae08e6bd9b05106dcda8320f9db0fb13d	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\files.cab, files.cab	Dropped File	3721.70 KB	application/vnd.ms-cab-compressed	Access, Create, Read, Write	CLEAN
f5d6af499ec4e83960097c994a8838d993a36844e63c03d2cd94cf3612910a38	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	1.41 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
a8c2ca783c081ca354cca0258404babdc3449687b2e01ee6f139e953a0e86982	C:\Windows\Installer\MSI8868.tmp	Dropped File	418.07 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
68a761b0e8bf4a1285e3dedce6c1cc732176118542cf730c28b3bfda5ab8f71c	C:\Windows\Installer\1876f00.ipi	Dropped File	20.00 KB	application/CDFV2	Access, Create, Delete	CLEAN
20cfab35403d0daa886a287e65e964f0d36ff2b01963ba3d725f8231254ef338	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	1.10 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
effb26504044d25e882310d5b1e800be1a2450f85d9250679b2236b48903d3b6	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	294 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
e72faf012b929b1fc3b6ab0d7c0e9c01580e9cadb7263c3edf1c4bfa6aceda7f	C:\Config.Msi\1876f01.rbs	Dropped File	740 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
06498734b1e071e4fddc03effab417a58e86091c03fab1e45e8f58d65fc0a2eb	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	666 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
048f7a1ddae30fe824f1fdaf4550529b98a9fa4fb66ce30ed31f56d377a71b11	C:\Users\kEecfMwgj\AppData\Roaming\AnyDesk\ad.trace	Dropped File	3.41 KB	text/plain	Access, Create, Write	CLEAN
c715e97bad4c1ee928c1cc47b9c700525af9654d7eb080bfe7ba5f1adc207364	C:\ProgramData\AnyDesk\service.conf	Dropped File	1.71 KB	text/plain	Access, Create, Read, Write	CLEAN
8f3cd45fb1e3d8d472fc7b27739e78a72c69688cad974ba206dedbeed9c11f85	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	1.05 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
01546d505366a19f0097314f3f300db3efd08b404d2231b19a713c4f7cdf94b0	C:\ProgramData\AnyDesk\ad_svc.trace	Dropped File	10.15 KB	text/plain	Access, Create, Write	CLEAN
78289a3decdf0d00d469739189129687487d16bb44d60218c6e511c2512a292e	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	844 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
4200a80a055888e50bdaeb58293dcc0d47f9c50deae1c7daa894332af4470f6a	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	196 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
6fbbbcd35e9723b71e005f37608d59b4cc7b8756b419ea30277b1ed54692dfb4	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	1.01 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
94d78d9395d2775d7d86b4ef45fc5d3d82508aff79c2026ffe7d882cfc7d552a	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	1.20 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
227150f62227190008f63bd91ffbd08fcdbfbf91f129d178ba378cecfb06c3342	-	Dropped File	68.00 KB	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
eaeceece55f1c16b178b70fcb07f78e2a453ff63bce81e4b32df93843aa1e98e	C:\ProgramData\AnyDesk\system.conf	Dropped File	455 bytes	text/plain	Access, Create, Read, Write	CLEAN
076a27c79e5ace2a3d47f9dd2e83e4ff6ea8872b3c2218f66c92b89b55f36560	-	Dropped File	512 bytes	application/octet-stream	-	CLEAN
a8c0656b85d708b1c93db91ddab77ceaa332fe6a572313e539749f41e3ff4304	log1.txt	Dropped File	13 bytes	text/plain	Access, Create, Write	CLEAN
a1c73dfd3110ddaeeb177e61e0358c8810dd4b29acb28820be8079b2cc9a5aff	C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File	626 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\KEECFM~1\Desktop\fb9f0bf2b71bf576053c56cb913ea4e93581fc9d3aa9d6d8a0ae572a1622f050.msi	Sample File, Accessed File, VM File	Access, Read	MALICIOUS
C:\Windows\Installer\1876eff.msi	Dropped File, Accessed File, VM File	Access, Create, Delete, Write	MALICIOUS
C:\	Accessed File	Access	CLEAN
C:\Windows\Installer\$PatchCache$\UnManaged	Accessed File	Access	CLEAN
0	-	-	CLEAN
C:\Windows\system32\sxs.DLL	Accessed File	Access	CLEAN
C:\Config.Msi	Accessed File	Access, Create, Delete	CLEAN
C:\ProgramData\AnyDesk\system.conf	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\ProgramData\AnyDesk	Accessed File	Access, Create	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\files.cab	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Windows\	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\msiwrapper.ini	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
c:\users\keecfmwgj\appdata\local\temp\~df397bf18cbdc5158c.tmp	Dropped File	-	CLEAN
C:\Windows\Installer\$PatchCache$\Managed\1926E8D15D0BCE53481466615F760A7F\CacheSize.txt	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\	Accessed File	Access, Create	CLEAN
System Paging File	Accessed File	Access, Read	CLEAN
c:\system volume information\spp\snapshot-2	Dropped File	-	CLEAN
C:\Windows\Installer\$PatchCache$\Managed\00006109A20000000100000000F01FEC\CacheSize.txt	Accessed File	Access	CLEAN
install.exe	Archive File	-	CLEAN
c:\lsarpc	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Config.Msi\	Accessed File	Access	CLEAN
C:\Config.Msi\1876f01.rbs	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\AnyDesk	Accessed File	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\AnyDesk\ad.trace	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
c:\wkssvc	Dropped File, Modified File, Not Extracted	-	CLEAN

File Name	Category	Operations	Verdict
C:\ProgramData\AnyDesk\AnyDesk.exe	Dropped File, Accessed File, Extracted File	Access, Create, Write	CLEAN
files	Accessed File	Access, Create	CLEAN
C:\Windows\Installer\MSI8ECF.tmp	Dropped File, Accessed File	Access, Create, Delete, Write	CLEAN
c:\users\keecfmwgj\appdata\local\temp\~dfbb16f2a06510bc9b.tmp	Dropped File	-	CLEAN
C:\ProgramData\AnyDesk\AnyDesk.exe:Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Windows\Installer\1876f00.ipi	Dropped File, Accessed File	Access, Create, Delete	CLEAN
C:\Program Files (x86)\[BZ.COMPANYNAME]\	Accessed File	Access	CLEAN
C:\Windows\Installer\MSI2306.tmp	Dropped File, Accessed File	Access, Create, Delete, Write	CLEAN
C:\Config.Msi\MSIA7BD.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
C:\Windows\Installer\$PatchCache$\Managed\7FA53761D8D11863495A5C876AE18C23\CacheSize.txt	Accessed File	Access	CLEAN
C:\Windows\syswow64	Accessed File	Access	CLEAN
C:\Config.Msi\MSI36A6.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
log1.txt	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\KEECFM~1\Desktop\	Accessed File	Access	CLEAN
C:\Windows\Installer\MSI8868.tmp	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Windows\Installer\$PatchCache$\Managed\8F3854CA4966E374BB7723DCCFB99A04	Accessed File	Access	CLEAN
c:\programdata\anydesk.exe	Dropped File, Accessed File, Extracted File	Access, Create, Write	CLEAN
C:\Program Files (x86)\	Accessed File	Access	CLEAN
C:\Windows\Installer\$PatchCache$\Managed\00006109110000000000000000F01FEC\CacheSize.txt	Accessed File	Access	CLEAN
C:\Windows\Installer\$PatchCache$\Managed\1D5E3C0FEDA1E123187686FED06E995A\CacheSize.txt	Accessed File	Access	CLEAN
c:\users\keecfmwgj\appdata\local\temp\msi6b18b.log	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Windows\Installer	Accessed File	Access	CLEAN
c:\srvsvc	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Windows\Installer\	Accessed File	Access	CLEAN
c:\system volume information\spp\metadata-2	Dropped File	-	CLEAN
c:\samr	Dropped File, Modified File, Not Extracted	-	CLEAN
c:\system volume information\spp\onlinemetadatacache\{bc53f388-3229-4b5f-b588-f5cd90ddd73e}_ondisksnapshotprop	Dropped File	-	CLEAN
C:\Windows\Installer\MSIA7FC.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
C:\Windows\system32\	Accessed File	Access	CLEAN
C:\Windows\Installer\$PatchCache$\Managed\	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\fusion.dll	Accessed File	Access	CLEAN
C:\Windows\syswow64\MsiExec.exe	Accessed File	Access	CLEAN
C:\ProgramData\AnyDesk\service.conf	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
-	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\ProgramData\AnyDesk\ad_svc.trace	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
boot.net.anydesk.com	49.12.130.237	-	TCP, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
49.12.130.237	boot.net.anydesk.com	Germany	TCP, DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Global\ad_connect_queue_1308_3747059072_mtx	access	anydesk.exe	CLEAN
Global_MSIExecute	access	msiexec.exe	CLEAN
Local\ad_trace_mtx	delete, access	anydesk.exe	CLEAN
Global\ad_connect_queue_2452_2298657072_mtx	access	anydesk.exe	CLEAN
Global\ad_707_gsystem_mtx	delete, access	anydesk.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe\Debugger	write, access	install.exe	SUSPICIOUS
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Media\AnyDesk\Capabilities\ApplicationDescription	write, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\anynet.twofactorauthkey	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\1af2a8da7e60d0b429d7e6453b3d0182\InstanceType	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\2C47B0D78F3C1FA449F0DC97BAB4D2EC\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\anynet.listenport	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109611090400100000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\HelpPane.exe	create, access	install.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk\InstallLocation	write, read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109A20090400100000000F01FEC	access	msiexec.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\47586AF0B09600B498AA2B9864324194	access	msiexec.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\c1c4f01781cc94c4c8fb1542c0981a2a	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles.changeableinacceptwindow.filemanager	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides	access	anydesk.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles.changeableinacceptwindow.clipboard	read, access	anydesk.exe	CLEAN
HKEY_CLASSES_ROOT\.anydesk\DefaultIcon	write, create, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\7C9F8B73BF303523781852719CD9C700\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.permissions.privacyfeature	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.permissions.sysinfo	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\discovery.repeatinterval	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles._default.permissions.audio	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles.permissions.audio	read, access	anydesk.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\00006109440090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\000061091E0090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-4219442223-4223814209-3835049652-1000\Installer\Products\00006109610090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.permissions.whiteboard	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.frontendclipboardversion	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles._default.canswitchprofile	read, access	anydesk.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\00006109090090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles._default.changeableinacceptwindow.sysinfo	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles.canswitchprofile	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles.permissions.input	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\anynet.proxy.minsearchinterval	read, access	anydesk.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\76966AEE2E7916549A99C5223EDC4E82	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles.permissions.restart	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109440090400000000000F01FEC\InstanceType	read, access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles.permissions.clipboardfiles	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\discovery.multicastip	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles._default.changeableinacceptwindow.audio	read, access	anydesk.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-4219442223-4223814209-3835049652-1000\Installer\Products\62DBF9290209B993A9A757D1160F9B24	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles.permissions.userpointer	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\0000061091E0090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-4219442223-4223814209-3835049652-1000\Installer\Products\8F3854CA4966E374BB7723DCCFB99A04	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Rollback\Scripts\Wow6432KeyValue	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\D4DB3CB2ABAF4934397CA98CA262F32E\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\6E815EB96CCE9A53884E7857C57002F0	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109A20090400100000000F01FEC\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment\TMP	read, access	msiexec.exe	CLEAN
HKEY_USERS\S-1-5-18\Software\Policies\Microsoft\Windows\Installer	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-4219442223-4223814209-3835049652-1000\Installer\Products\00006109B210904000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-4219442223-4223814209-3835049652-1000\Installer\Products\000061091E0090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-4219442223-4223814209-3835049652-1000\Installer\Products\22BEFC8F7E2A1793E9ADB411DEFE1C58	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles.changeableinacceptwindow.whiteboard	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.changeableinacceptwindow.recordsession	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Rollback\Scripts\ScriptsDisabled	read, access	msiexec.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\00006109510090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk\VersionBuild	write, read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles._default.permissions.input	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles._default.permissions.userpointer	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\1af2a8da7e60d0b429d7e6453b3d0182	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.frontendclipboard	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-4219442223-4223814209-3835049652-1000\Installer\Products\000061091A00904000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles._default.pwd	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Media\AnyDesk	create, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\0000061091E0090400000000000F01FEC\InstanceType	read, access	msiexec.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles.permissions.input	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles.changeableinacceptwindow.sysinfo	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109C2009040000000000F01FEC\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_CLASSES_ROOT\AnyDesk\DefaultIcon	write, create, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109A2009040010000000F01FEC\InstanceType	read, access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.frontendclipboardversion	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles._default.permissions.privacyfeature	read, access	anydesk.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\22BEFC8F7E2A1793E9ADB411DEFE1C58	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\anynet.listenport	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles.changeableinacceptwindow.blockinput	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies	access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment\USERNAME	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes	create, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109AB0090400000000000F01FEC\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles._default.changeableinacceptwindow.sas	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\C6F01EDE4F03AC245B7CDA9B504EB5CF\8F3854CA4966E374BB7723DCCFB99A04	delete, read, access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.updatetype	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-4219442223-4223814209-3835049652-1000\Installer\Products\21EE4A31AE32173319EEFE3BD6FDFFE3	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles.permissions.vpn	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment\PATHEXT	read, access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.permissions.lockdesk	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\anynet.proxy.type	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles.permissions.sysinfo	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles.salt	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109B2109040000000000F01FEC\InstanceType	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir (x86)	read, access	msiexec.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\00006109910090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._unattendedaccess.permissions.sas	read, access	anydesk.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.permissions.recordsession	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-4219442223-4223814209-3835049652-1000\Installer\Products\00006109A20090400100000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\6E8D947A316B3EB3F8F540C548BE2AB9\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.permissions.tcptunnel	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles.changeableinacceptwindow.audio	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\6E815EB96CCE9A53884E7857C57002F0\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\00006109B21090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\6E8D947A316B3EB3F8F540C548BE2AB9\InstanceType	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-4219442223-4223814209-3835049652-1000\Installer\Products\00006109A10090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.permissions.clipboardfiles	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\7FA53761D8D11863495A5C876AE18C23\InstanceType	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109610090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109E0090400000000000F01FEC\InstanceType	read, access	msiexec.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\00006109511090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles._default.changeableinacceptwindow.vpn	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109090090400000000000F01FEC\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\00006109110000000000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.salt	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles._default.permissions.clipboardfiles	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\wol.groupsync	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109C20090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109711090400000000000F01FEC\InstanceType	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\769666AEE2E7916549A99C5223EDC4E82\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109110000000000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\D4DB3CB2ABAF4934397CA98CA262F32E	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109AB0090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\62DBF9290209B993A9A757D1160F9B24\PackageCode	read, access	msiexec.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk\DisplayName	write, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.permissions.sas	read, access	anydesk.exe	CLEAN
HKEY_CLASSES_ROOT\AnyDesk\shell\open\command	write, create, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles.changeableinacceptwindow.sas	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.permissions.clipboard	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk\EstimatedSize	write, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109B10090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\76966AEE2E7916549A99C5223EDC4E82\InstanceType	read, access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.permissions.input	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles._default.permissions.clipboard	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\8F3854CA4966E374BB7723DCCFB99A04\InstallProperties	access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.pwd	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Defaults\security.permissionprofiles._default.changeableinacceptwindow.lockdesk	read, access	anydesk.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109910090400000000000F01FEC\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\c1c4f01781cc94c4c8fb1542c0981a2a\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109611090400100000000F01FEC\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\1926E8D15D0BCE53481466615F760A7F\PackageCode	read, access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00006109F100A0C00000000000F01FEC\InstanceType	read, access	msiexec.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\discovery.defaultbehavior	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\anynet.lastrelay	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles.changeableinacceptwindow.sas	read, access	anydesk.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\AnyDesk\Config\Overrides\security.permissionprofiles.changeableinacceptwindow.input	read, access	anydesk.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\Software\Microsoft\Installer\Products\62DBF9290209B993A9A757D1160F9B24	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\47586AF0B09600B498AA2B9864324194	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-4219442223-4223814209-3835049652-1000\Installer\Products\2C47B0D78F3C1FA449F0DC97BAB4D2EC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-4219442223-4223814209-3835049652-1000\Installer\Products\00006109440090400000000000F01FEC	access	msiexec.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\1926E8D15D0BCE53481466615F760A7F\InstanceType	read, access	msiexec.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
anydesk.exe	c:\programdata\anydesk.exe --install C:\ProgramData\AnyDesk --silent	MALICIOUS
msiexec.exe	C:\Windows\system32\msiexec.exe /V	SUSPICIOUS
install.exe	"C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\files\install.exe"	SUSPICIOUS
anydesk.exe	"C:\ProgramData\AnyDesk\AnyDesk.exe" --service	SUSPICIOUS
anydesk.exe	"C:\ProgramData\AnyDesk\AnyDesk.exe" --service	SUSPICIOUS
System	-	CLEAN
services.exe	C:\Windows\system32\services.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch	CLEAN
msiexec.exe	"C:\Windows\System32\msiexec.exe" /i "C:\Users\KEECFM~1\Desktop\fb9f0bf2b71bf576053c56cb913ea4e93581fc9d3aa9d6d8a0ae572a1622f050.msi"	CLEAN
vssvc.exe	C:\Windows\system32\vssvc.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k RPCSS	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted	CLEAN
msiexec.exe	C:\Windows\syswow64\MsiExec.exe -Embedding 15C2A74905FE813C1C1C8CDCF151DE4D	CLEAN
msiexec.exe	C:\Windows\syswow64\MsiExec.exe -Embedding ADDCD9128E57B274A403CFC05E47C1FC M Global\MSI0000	CLEAN
icacls.exe	"C:\Windows\system32\ICACLS.EXE" "C:\Users\KEECFM~1\AppData\Local\Temp\MW-ed03fe6a-6d69-41db-94de-aca9dc9763e3\." /SETINTEGRITYLEVEL (CI)(OI)HIGH	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted	CLEAN
expand.exe	"C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files	CLEAN
spoolsv.exe	C:\Windows\System32\spoolsv.exe	CLEAN
cmd.exe	cmd /c c:\programdata\anydesk.exe --install C:\ProgramData\AnyDesk --silent	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork	CLEAN
taskhost.exe	"taskhost.exe"	CLEAN
mscorsvw.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe	CLEAN
mscorsvw.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe	CLEAN
dllhost.exe	C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}	CLEAN
taskhost.exe	taskhost.exe $(Arg0)	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation	CLEAN
sppsvc.exe	C:\Windows\system32\sppsvc.exe	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.14 / 2022-08-03 12:19:21
YARA Built-in Ruleset Version	4.6.1.10

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	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH
User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp

System Root	C:\Windows