ID: 562521
Sample Name:
SecuriteInfo.com.MSIL.Kryptik.AECS.24576.13236
Cookbook: default.jbs
Time: 00:10:18
Date: 29/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

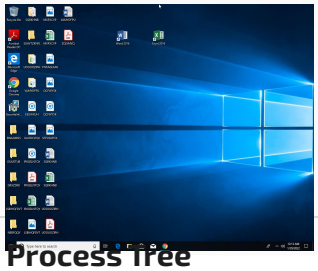
Windows Analysis Report

SecuriteInfo.com.MSIL.Kryptik.AECS.24576.13236

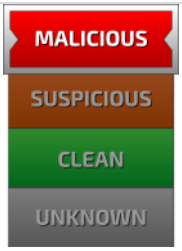
Overview

General Information

Sample Name:	SecuriteInfo.com.MSIL.Kryptik.AECS.24576.13236 (renamed file extension from 13236 to msi)
Analysis ID:	562521
MD5:	1d59589778c525..
SHA1:	ad4584c1b77348..
SHA256:	1f95063441e9d2..
Tags:	msi njrat
Infos:	



Detection



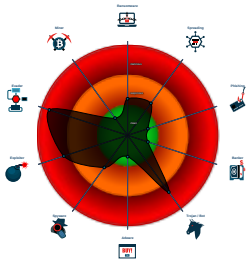
Njrat

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AntiVM3
- Yara detected Njrat
- Multi AV Scanner detection for drop…
- Creates an autostart registry key po…
- Sigma detected: Bad Opsec Default…
- Uses netsh to modify the Windows …
- Writes to foreign memory regions
- .NET source code references suspic…
- Contains functionality to hide user a…

Classification



Process Tree

- **System is w10x64**
- msiexec.exe (PID: 6712 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\SecuriteInfo.com.MSIL.Kryptik.AECS.24576.msi" MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 6128 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - msiexec.exe (PID: 6992 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 8427D5518DE818285DF2E5650B3C2701 MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
    - icacls.exe (PID: 5596 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\." /SETINTEGRITYLEVEL (CI)(OI)HIGH MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 5520 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - expand.exe (PID: 4552 cmdline: "C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files MD5: 8F8C20238C1194A428021AC62257436D)
      - conhost.exe (PID: 6740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - server.exe (PID: 7028 cmdline: "C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files\server.exe" MD5: CD4D919B4FC88C9D6F03C864A181E40F)
      - AddInProcess.exe (PID: 6312 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess.exe MD5: 11D8A500C4C0FBAF20EBDB8CDF6EA452)
      - InstallUtil.exe (PID: 6304 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
      - AddInProcess.exe (PID: 7104 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess.exe MD5: 11D8A500C4C0FBAF20EBDB8CDF6EA452)
      - RegSvcs.exe (PID: 7148 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
        - netsh.exe (PID: 6520 cmdline: netsh firewall add allowedprogram "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" "RegSvcs.exe" ENABLE MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
          - conhost.exe (PID: 2092 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - icacls.exe (PID: 5164 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\." /SETINTEGRITYLEVEL (CI)(OI)LOW MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 5576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 5568 cmdline: C:\Windows\system32\cmd.exe /c rd /s /q "C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files" MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 3848 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" .. MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- msdtc.exe (PID: 6320 cmdline: C:\Windows\System32\msdtc.exe MD5: 9A94F32C1DC90A7E5A35D0F820A8FB1D)
- RegSvcs.exe (PID: 6972 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" .. MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 7020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 984 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" .. MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.721799355.0000000005A51000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
0000000B.00000002.721299654.00000000045A6000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
0000000F.00000000.709022701.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
0000000F.00000000.709022701.0000000000402000.00000040.00000400.00020000.00000000.sdmp	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x6dbd:$a1: netsh firewall add allowedprogram • 0x6d8d:$a2: SEE_MASK_NOZONECHECKS • 0x6fad:$b1: [TAP] • 0x6ea9:$c3: cmd.exe /c ping
0000000F.00000000.709022701.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x6d8d:$reg: SEE_MASK_NOZONECHECKS • 0x6a7c:$msg: Execute ERROR • 0x6ad4:$msg: Execute ERROR • 0x6ea9:$ping: cmd.exe /c ping 0 -n 2 & del

Click to see the 33 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
15.0.RegSvcs.exe.400000.0.unpack	CN_disclosed_20180208_c	Detects malware from disclosed CN malware set	Florian Roth	• 0x70a9:$x1: cmd.exe /c ping 0 -n 2 & del " • 0x6cba:$s3: Executed As • 0x6c98:$s6: Download ERROR
15.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
15.0.RegSvcs.exe.400000.0.unpack	MALWARE_Win_NjRAT	Detects NjRAT / Bladabindi	ditekSHen	• 0x7049:$s1: netsh firewall delete allowedprogram • 0x6fbd:$s2: netsh firewall add allowedprogram • 0x70a9:$s3: 63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 20 00 2F 00 63 00 20 00 70 00 69 00 6E 00 67 • 0x6c7c:$s4: Execute ERROR • 0x6cd4:$s4: Execute ERROR • 0x6c98:$s5: Download ERROR
15.0.RegSvcs.exe.400000.0.unpack	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x6fbd:$a1: netsh firewall add allowedprogram • 0x6f8d:$a2: SEE_MASK_NOZONECHECKS • 0x71ad:$b1: [TAP] • 0x70a9:$c3: cmd.exe /c ping
15.0.RegSvcs.exe.400000.0.unpack	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x6f8d:$reg: SEE_MASK_NOZONECHECKS • 0x6c7c:$msg: Execute ERROR • 0x6cd4:$msg: Execute ERROR • 0x70a9:$ping: cmd.exe /c ping 0 -n 2 & del

Click to see the 103 entries

Sigma Overview

System Summary

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Jbx Signature Overview

AV Detection

Multi AV Scanner detection for submitted file

Yara detected Njrat

Multi AV Scanner detection for dropped file

Exploits

Yara detected UAC Bypass using CMSTP

Networking

Uses dynamic DNS services

E-Banking Fraud

Yara detected Njrat

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Boot Survival

Creates an autostart registry key pointing to binary in C:\Windows

Creates autostart registry keys with suspicious names

Hooking and other Techniques for Hiding and Protection

Contains functionality to hide user accounts

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings

Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Stealing of Sensitive Information

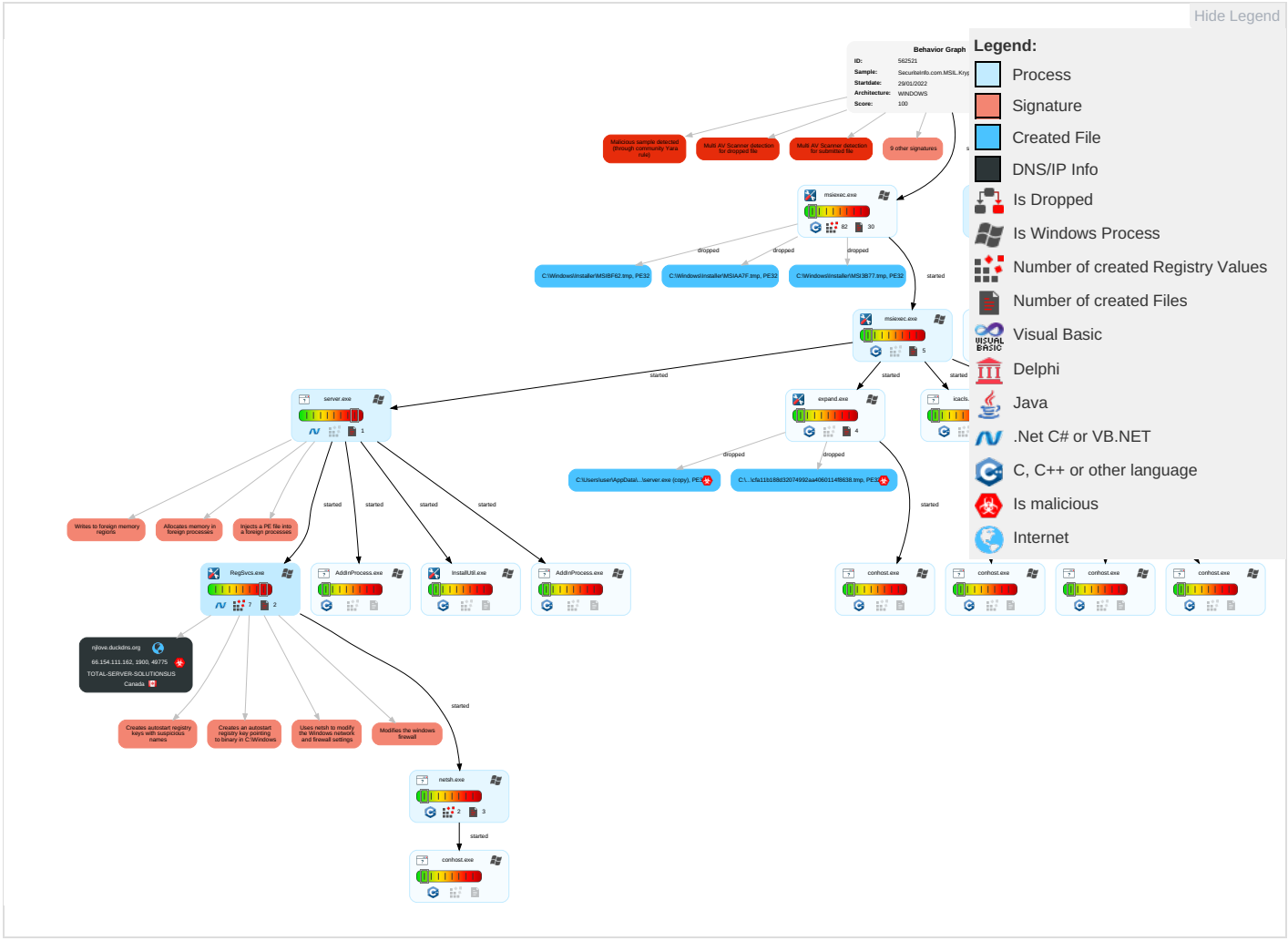
Yara detected Njrat

Remote Access Functionality

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
2 Replication Through Removable Media	1 Native API	1 DLL Side-Loading	1 DLL Side-Loading	2 1 Disable or Modify Tools	1 Input Capture	1 1 Peripheral Device Discovery	2 Replication Through Removable Media	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 Windows Service	1 Windows Service	2 Obfuscated Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	2 1 Registry Run Keys / Startup Folder	3 1 2 Process Injection	3 Software Packing	Security Account Manager	1 3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	1 Services File Permissions Weakness	2 1 Registry Run Keys / Startup Folder	1 Timestomp	NTDS	1 Query Registry	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 Services File Permissions Weakness	1 DLL Side-Loading	LSA Secrets	2 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 File Deletion	Cached Domain Credentials	2 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 Masquerading	DCSync	2 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	3 1 2 Process Injection	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Users	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Services File Permissions Weakness	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

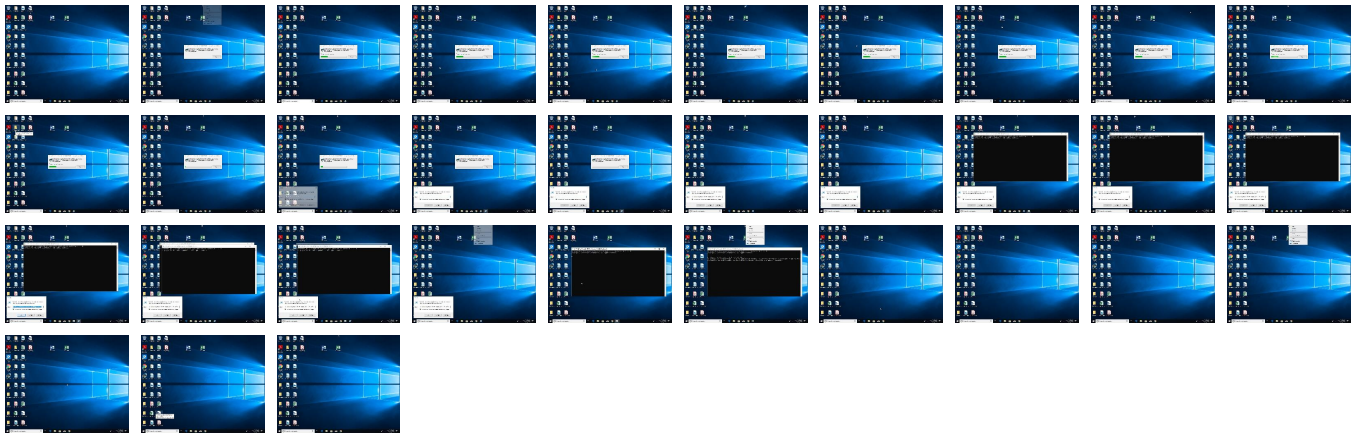
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.MSIL.Kryptik.AECS.24576.msi	9%	Virustotal		Browse
SecuriteInfo.com.MSIL.Kryptik.AECS.24576.msi	0%	Metadefender		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files\02f017f8dcfd4885887fe1ceb996bbc7dpx.tmp\cfa11b188d32074992aa4060114f8638.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files\02f017f8dcfd4885887fe1ceb996bbc7dpx.tmp\cfa11b188d32074992aa4060114f8638.tmp	16%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files\server.exe (copy)	16%	Virustotal		Browse
C:\Windows\Installer\MSI3B77.tmp	0%	Virustotal		Browse
C:\Windows\Installer\MSI3B77.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSI3B77.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSIAA7F.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSIAA7F.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSIBF62.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSIBF62.tmp	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
15.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
11.2.server.exe.3399760.1.unpack	100%	Avira	HEUR/AGEN.1131353		Download File
15.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
15.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
15.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
15.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
njlove.duckdns.org	2%	Virustotal		Browse

URLs

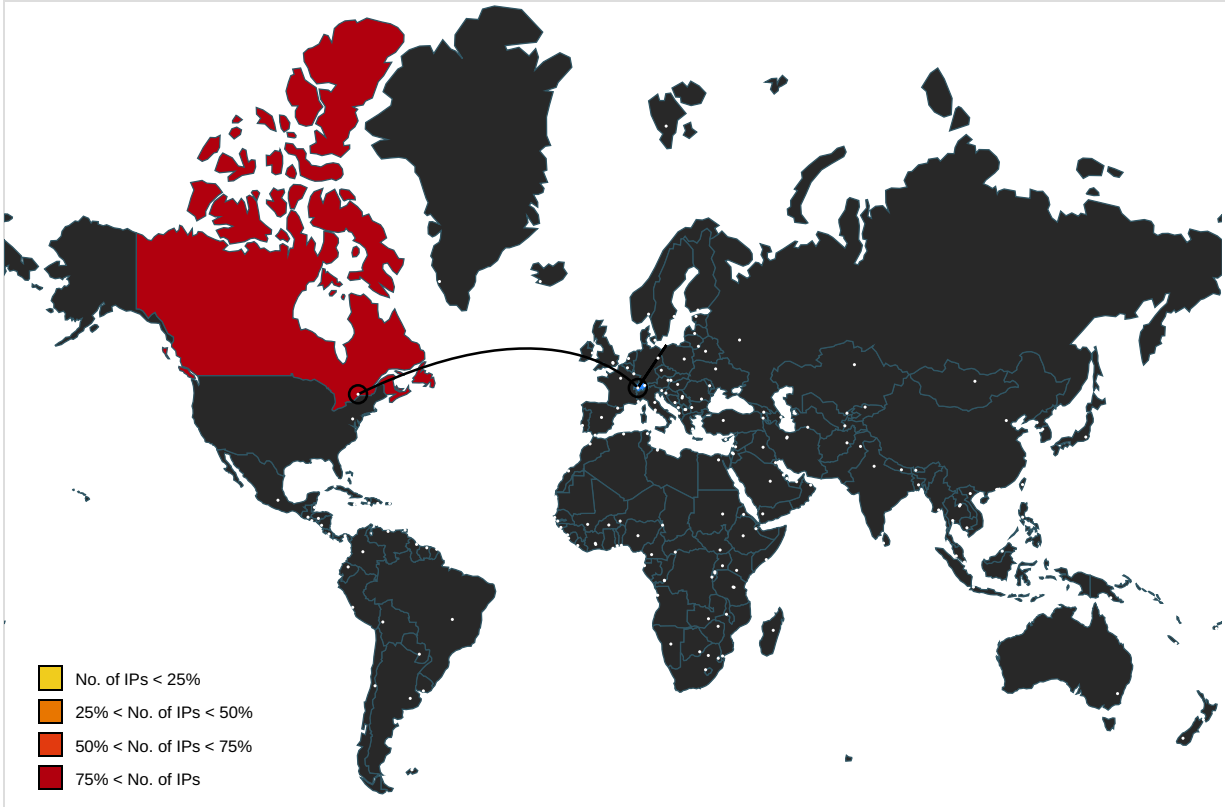
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
njlove.duckdns.org	66.154.111.162	true	true	• 2%, Virustotal, Browse	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.154.111.162	njlove.duckdns.org	Canada		46562	TOTAL-SERVER-SOLUTIONSUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562521
Start date:	29.01.2022
Start time:	00:10:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.MSIL.Kryptik.AECS.24576.13236 (renamed file extension from 13236 to msi)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	39
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winMSI@36/35@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.3%) • Quality average: 43.1% • Quality standard deviation: 42.2%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 2.20.157.220
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

Time	Type	Description
00:11:53	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 040b20e882d013c0c9f6ceff16d97f7a "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" ..
00:12:02	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run 040b20e882d013c0c9f6ceff16d97f7a "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" ..
00:12:04	API Interceptor	30x Sleep call for process: RegSvcs.exe modified
00:12:11	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 040b20e882d013c0c9f6ceff16d97f7a "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" ..

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Config.Msi\6537bf.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	8093
Entropy (8bit):	5.4465567087908475
Encrypted:	false
SSDEEP:	96:Ymr07+63C9wQeiJYScU0+eD2JtZCsvVDeU0+eD2JtZC6jYPBQAvVDvQGqg5qZW9B:Nr7BeI38C387cUmpq
MD5:	F0C5ADEFCF329EBB98333F599A1A8BAE
SHA1:	D8B9759FA6E1E207DB6E50F80E5E2FFAC4BA92F8
SHA-256:	E3F306A54970543F1287CBE35FA41BCA21BE33A87439736ECBDEEFEB4EF36D8C
SHA-512:	47DB1FDFEBB4FC1A64B487D78218782DB4F5358F60F8103D44B609BE0E1CCA0EC23F44E9906DB508712D1767E58F18B4FA7FF3716A6FA421F2D46E2197A38D8
Malicious:	false
Preview:	...@IXOS.@.....@z.=T.@.....@.....@.....@.....@.....@.....&.{8291D67C-2E0B-4E71-B034-09AFE03383E8}X.M.i.c.r.o.s.o.f.t... .V.i.s.u.a.l. .S.t.u.d.i.o... .-. .U.N.R.E.G.I.S.T.E.R.E.D. .-. .W.r.a.p.p.e.d. .u.s.i.n.g. .M.S.I. .W.r.a.p.p.e.r. .f.r.o.m. .w.w.w...e.x.e.m.s.i...c.o.m.,.SecuriteInfo.com.MSIL.Kryptik.AECS.24576.msi.@.....@.....@.....@.....&.{49C681E5-45C4-4467-92EE-456F1E355C5F}.....@.....@.....@.....@.....@.....@.....@.....@....X.M.i.c.r.o.s.o.f.t... .V.i.s.u.a.l. .S.t.u.d.i.o... .-. .U.N.R.E.G.I.S.T.E.R.E.D. .-. .W.r.a.p.p.e.d. .u.s.i.n.g. .M.S.I. .W.r.a.p.p.e.r. .f.r.o.m. .w.w.w...e.x.e.m.s.i...c.o.m.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{EDE10F6C-30F4-42CA-B5C7-ADB905E45BFC}&.{8291D67C-2E0B-4E71-B034-09AFE03383E8}.@.....WriteRegistryValues..Writing system registry values..Key: [1], Name: [2], Value: [3]$..@....*.SOFTWARE\EXEMSI.COM\MSI Wrapper\Installed\..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1141
Entropy (8bit):	5.340874572595606
Encrypted:	false
SSDEEP:	24:MLzayE4gayE47mE4K5E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:M3ayHgayH7mHK5HKXwYHKhQnoPtHoxHe
MD5:	DB2EF3BD59C93968A627D15CC207CBF4
SHA1:	F0C61B1D05A79EDBB9EBB6FFB8C8E217F2BDD62A
SHA-256:	31D645F0A9462B5632F184DF6D131C28ADEA6777C7E42AF8E91643E47447E4C8
SHA-512:	55EC90EE78C75E817F888197CE289202FF8973348DD992DAA4AB791261732AB4006E56F84A4DA449F71A69B7A2F6BD91B4A6D16521AD0CB6D3A4A531851A8F5

Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Transactions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, Public

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\server.exe.log

Process:	C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files\server.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.348034597186669
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat92n4M6:ML9E4Ks2wKDE4KhK3VZ9pKhg84j
MD5:	07FC10473CB7F0DEC42EE8079EB0DF28
SHA1:	90FA6D0B604991B3E5E8F6DB041651B10FD4284A
SHA-256:	A42B61DFB4AF366D05CE1815C88E2392C7C4AA9B6B17604234BEB7A7DADA7E4C
SHA-512:	D7240EE88D207E631990907AFA96C8384FB51729A16247BD4BDB96CBA3C4CDB9A68ADCD07819B2242A0F395690AD831B1B547EC91E988CBE39398F472055D56F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files.cab

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	Microsoft Cabinet archive data, 669935 bytes, 1 file
Category:	dropped
Size (bytes):	669935
Entropy (8bit):	7.957969373333579
Encrypted:	false
SSDEEP:	12288:nkKSpNcjNXmpYpNLKAKMYzh5E4OGF9+AxUH5tXT0rHo7sv0yxYElXXyoZhTUGL:kTNcjk8LKAj6h5E4Z9+SgzDOo7sv0yxX
MD5:	262E1B25CAAB9FABDED95EECFDCB28EB
SHA1:	966B778B45CF788F3F3D34C841D137F8C22AA997
SHA-256:	B17D933378BB378797102613EE8034BEC9B7E73E4540EFA2E48D4B90CB7494D9
SHA-512:	0A5562D3C41657BE46A657C62ECF2D5FF013D559621AB81734B53025F2F76E1F88B39BBCE65B669EC20677A9EB66D3674A048FFF7DAA4D531C6A13F096AF181E
Malicious:	false
Preview:	MSCF.....8.....,.....G.....8.....<TW. .server.exe...3.....MZ.....@.....!..L.!This program cannot be run in DOS mode....$ .....PE..L....b).....0.@,.....:L.. ...`....@.. .....`.....0K..J....`.....zK..8..... ..... ..H..... .....text...@,... ..... ..`.rsrc.....`.....0.....@..@.reloc.....6.....@..@.....`K.....H..... ...Xb.....xJ.....e`:C).... ..0.&.....Ndq.t28q..W.z..X.....V...{.("....N.5...V.Z....l...kf..'..".6..`m....`8.).].....z5.:[5....Amy.b.....k..n.Q.N..&....\...../ ..;fsp.B...*.....[@..A..h.d.....h..-n...ynT...=...$.Ns A....7....^.. ....].,.A....L...E...HI#.a.#....DA.=n.....U1@...>?%....|r..0...o.L.[9#.."4..m..QW.04A.,.e.&z

C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files\02f017f8dcfd4885887fe1ceb996bbc7dpx.tmp\cfa11b188d32074992aa4060114f8638.tmp

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	669696
Entropy (8bit):	7.958276686942886
Encrypted:	false
SSDEEP:	12288:EkKSarcjMXmuYpN0KAKMSzhFE4OUF94Ax/m5GXT0rao7Ev0ixYElXtyoLhTUGe:dQrcjXv0KAjUhFE4794SOMD7o7Ev0ixm
MD5:	CD4D919B4FC88C9D6F03C864A181E40F
SHA1:	F0E56473DEBCF2DFD121E0249908828FE36EA621
SHA-256:	7E6B89DBF95819AC599FF79ACD6CB50DE2A53EE135B51E37DAF00AF7313CE8D6
SHA-512:	3E70ADBDDF558F24349896DD2CD82FCA8A4FA3C732E0966B6A2A16EAD57FB7EBABB810F5C9870C7C928C7C09F365F28C5AD0EBD1B7C0EE6279F7E85B4108D0A8
Malicious:	**true**

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 16%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....b).....0.@,.....:L.. ...`....@.. ..... ..`.....0K..J....`.....zK..8..... ..... ..H.....text...@,... ..... ..`.rsrc.....`.....0.....@..@.rel oc.....6.....@..@.....`K.....H..... ...Xb.....xJ.....e`:C).....0.&.....Ndq.t28q..W.z..X.....V...{.("....N.5...V.Z....I...kf..'...".6. .`m....`8.).]....z5.:[5....Amy.b.....:k..n.Q.N..&....\...../ ..;fsp.B...*.....[@..A..h.d.....h..-n...ynT...=...$.NsA....7....^.. ....]..,.A....L...E...Hl#.a.#....DA.=n.....U1@...>?%....|r..0...o.L. [9#.."4..m..QW.04A.,.e.&z*l.?PR.p4^..M.o..F<.uFyaw.....>..s-X..-\.(....f...bT>A{.P..us....2..J.m.n.$

C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files\server.exe (copy)

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	669696
Entropy (8bit):	7.958276686942886
Encrypted:	false
SSDEEP:	12288:EkKSarcjMXmuYpN0KAKMSzhFE4OUF94Ax/m5GXT0rao7Ev0ixYElXtyoLhTUGe:dQrcjXv0KAjUhFE4794SOMD7o7Ev0ixm
MD5:	CD4D919B4FC88C9D6F03C864A181E40F
SHA1:	F0E56473DEBCF2DFD121E0249908828FE36EA621
SHA-256:	7E6B89DBF95819AC599FF79ACD6CB50DE2A53EE135B51E37DAF00AF7313CE8D6
SHA-512:	3E70ADBDDF558F24349896DD2CD82FCA8A4FA3C732E0966B6A2A16EAD57FB7EBABB810F5C9870C7C928C7C09F365F28C5AD0EBD1B7C0EE6279F7E85B4108D 0A8
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 16%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....b).....0.@,.....:L.. ...`....@.. ..... ..`.....0K..J....`.....zK..8..... ..... ..H.....text...@,... ..... ..`.rsrc.....`.....0.....@..@.rel oc.....6.....@..@.....`K.....H..... ...Xb.....xJ.....e`:C).....0.&.....Ndq.t28q..W.z..X.....V...{.("....N.5...V.Z....I...kf..'...".6. .`m....`8.).]....z5.:[5....Amy.b.....:k..n.Q.N..&....\...../ ..;fsp.B...*.....[@..A..h.d.....h..-n...ynT...=...$.NsA....7....^.. ....]..,.A....L...E...Hl#.a.#....DA.=n.....U1@...>?%....|r..0...o.L. [9#.."4..m..QW.04A.,.e.&z*l.?PR.p4^..M.o..F<.uFyaw.....>..s-X..-\.(....f...bT>A{.P..us....2..J.m.n.$

C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	1426
Entropy (8bit):	3.6464727035070923
Encrypted:	false
SSDEEP:	24:f3dX8DW8dfj+vQD+AMKcDNESrF393IFUlSaz93IFUlSaay293IFUlSaOUxlFnal3:fe6K+NJF393I8193I8YI93I8VxlQl
MD5:	7CB5DE5993EE769767AC0E19369684CE
SHA1:	1E2183C28ABAAAD558631D6867178A3E12EE997F
SHA-256:	2ED222CF66CBD694BA3744EC49E63534D2EA9532C822BDB11D5A3FF46909E142
SHA-512:	6F486BBE7C3A6A9E86943008C47F02F1FB1DB33320D01A9CC5FDAB39303D85823F3E7A12EA4CE0962D309F35546765EC1FADD12748EE10BCB445B16CF7BF11(E
Malicious:	false
Preview:	W.r.a.p.p.e.d.A.p.p.l.i.c.a.t.i.o.n.I.d.=...W.r.a.p.p.e.d.R.e.g.i.s.t.r.a.t.i.o.n.=.H.i.d.d.e.n...I.n.s.t.a.l.l.S.u.c.c.e.s.s.C.o.d.e.s.=.0...E.l.e.v.a.t.i.o.n.M.o.d.e.=.a.d.m.i.n.i.s.t.r.a. t.o.r.s...B.a.s.e.N.a.m.e.=.s.e.r.v.e.r...e.x.e...C.a.b.H.a.s.h.=.b.1.7.d.9.3.3.3.7.8.b.b.3.7.8.7.9.7.1.0.2.6.1.3.e.e.8.0.3.4.b.e.c.9.b.7.e.7.3.e.4.5.4.0.e.f.a.2.e.4.8.d.4.b.9.0.c. b.7.4.9.4.d.9...S.e.t.u.p.P.a.r.a.m.e.t.e.r.s.=...W.o.r.k.i.n.g.D.i.r.=...C.u.r.r.e.n.t.D.i.r.=.*.S.O.U.R.C.E.D.I.R.*...U.I.L.e.v.e.l.=.5...F.o.c.u.s.=.y.e.s...S.e.s.s.i.o.n.D.i.r.=.C.:\.U. s.e.r.s.\.j.o.n.e.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.7.1.3.2.2.5.7.0.-.7.0.0.8.-.4.6.b.5.-.b.b.7.3.-.7.7.0.9.8.a.f.1.b.7.5.2.\...F.i.l.e.s.D.i.r.=.C.:.\.U.s.e.r.s.\.j.o.n.e.s.\. A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.7.1.3.2.2.5.7.0.-.7.0.0.8.-.4.6.b.5.-.b.b.7.3.-.7.7.0.9.8.a.f.1.b.7.5.2.\.f.i.l.e.s.\...R.u.n.B.e.f.o.r.e.I.n.s.t.a.l.l.F.i.l.e.=...R.u.n.B.e.f.o. r.e.I.n.s.t.a.l.l.P.a.r.a.m.e.t.e.r.s.=...R.u.n.A.f.t.e.r.I.

C:\Windows\Installer\6537be.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Microsoft Visual Studio - UNREGISTERED - W rapped using MSI Wrapper from www.exemsi.com 16.6.255.35071, Subject: Microsoft Visual Studio - UNREGISTERED - Wrapped using MSI Wrapper from www.exem si.com, Author: Microsoft Corporation, Keywords: Installer, Template: x64;1033, Revision Number: {49C681E5-45C4-4467-92EE-456F1E355C5F}, Create Time/Date: Sun Feb 7 22:37:14 2021, Last Saved Time/Date: Sun Feb 7 22:37:14 2021, Number of Pages: 200, Number of Words: 2, Name of Creating Application: MSI Wrapper (10.0.50.0), Security: 2
Category:	dropped
Size (bytes):	921600
Entropy (8bit):	7.70038526988355
Encrypted:	false
SSDEEP:	24576:StZcpVJ78TNcjk8LKAj6h5E4Z9+SgzDOo7sv0yx3FXyoUc:Rpz78OI/i4nhgzDOo3yLC+
MD5:	1D59589778C525AADCB645270CEE737C
SHA1:	AD4584C1B7734854939C59674CBBF22A99618285
SHA-256:	1F95063441E9D231E0E2B15365A8722C5136C2A6FE2716F3653C260093026354

SHA-512:	11D4394566EFE3BC75336D90371017EA0E4E9EDC556736E2537201AFB648E9C2167BEB82CA87C3CC4A4B23603D49EB19BFC403C782858F0E781BB127771109D
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\6537c0.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Microsoft Visual Studio - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 16.6.255.35071, Subject: Microsoft Visual Studio - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft Corporation, Keywords: Installer, Template: x64;1033, Revision Number: {49C681E5-45C4-4467-92EE-456F1E355C5F}, Create Time/Date: Sun Feb 7 22:37:14 2021, Last Saved Time/Date: Sun Feb 7 22:37:14 2021, Number of Pages: 200, Number of Words: 2, Name of Creating Application: MSI Wrapper (10.0.50.0), Security: 2
Category:	dropped
Size (bytes):	921600
Entropy (8bit):	7.70038526988355
Encrypted:	false
SSDEEP:	24576:StZcpVJ78TNcjk8LKAj6h5E4Z9+SgzDOo7sv0yx3FXyoUc:Rpz78OI/i4nhgzDOo3yLC+
MD5:	1D59589778C525AADCB645270CEE737C
SHA1:	AD4584C1B7734854939C59674CBBF22A99618285
SHA-256:	1F95063441E9D231E0E2B15365A8722C5136C2A6FE2716F3653C260093026354
SHA-512:	11D4394566EFE3BC75336D90371017EA0E4E9EDC556736E2537201AFB648E9C2167BEB82CA87C3CC4A4B23603D49EB19BFC403C782858F0E781BB127771109D
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\MSI3B77.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.513495229990427
Encrypted:	false
SSDEEP:	3072:9spAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLu2loHUvU1yGxr5nqM2a8:/tOdiRQYpgjpjew5JWyGxJqo8
MD5:	D8AD3B90E6F172C97F1A95678EC8E1A4
SHA1:	C33402EDEB359044309E01B2E8C4D1694B48C5E1
SHA-256:	2D4AFDF54F3CB2E602A23CD22F7223199F0E483D556CC8DF7A8DA72C7FE1336A
SHA-512:	64A2DC66A0056740BCF03065522962FFF847307F12545256817A7481A00025ECA9F0C097ECF660C17045729666D663137DEDC1B42E2FD14B587CEE242CCBE54F
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p....p..../.p.....p...q.%.p.....p....p.....p.Rich..p... .....PE..L....k `.....!.....h.....K.....@.....P...]..... P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)..`..*.....@..B..... ....

C:\Windows\Installer\MSIAA7E.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	1940
Entropy (8bit):	5.458968263899004
Encrypted:	false
SSDEEP:	48:pLr07+psbs7YD8SMyaeU9nMgxuDGLEVltayiCq:pLr07+6g7wnaecMgwDGLEPYyBq
MD5:	4E8344A5DC2DBCC8A862436792F50965
SHA1:	6DC315CA22D243D3F5686EE3D9B165A08C6C2562
SHA-256:	80077465795E5449E2F746283252A42A9870DBFBE0F277FAE88787EBA32E42DE
SHA-512:	595EEF87EED89AB8F227A416103F0B484F3A67E3B38E20693315950144C97707152C0EBAEA112CF24F7C1717B48BC49C2DF5A0E3B4C4CF9984B7C517104A1B17
Malicious:	false

Preview:	...@IXOS.@.....@y.=T.@.....@.....@.....@.....@.....@.....&.{8291D67C-2E0B-4E71-B034-09AFE03383E8}X.M.i.c.r.o.s.o.f.t... .V.i.s.u.a.l. .S.t.u.d.i.o... .-. .U.N.R.E.G.I.S. T.E.R.E.D. .-. .W.r.a.p.p.e.d. .u.s.i.n.g. .M.S.I. .W.r.a.p.p.e.r. .f.r.o.m. .w.w.w...e.x.e.m.s.i...c.o.m.,.SecuriteInfo.com.MSIL.Kryptik.AECS.24576.msi.@.....@.....@.....@..... &.{49C681E5-45C4-4467-92EE-456F1E355C5F}.....@.....@.....@.....@.....@.....@.....@.....@....X.M.i.c.r.o.s.o.f.t... .V.i.s.u.a.l. .S.t.u.d.i.o... .-. .U.N.R.E.G.I.S.T.E.R.E.D. . -. .W.r.a.p.p.e.d. .u.s.i.n.g. .M.S.I. .W.r.a.p.p.e.r. .f.r.o.m. .w.w.w...e.x.e.m.s.i...c.o.m.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]...@.....@.....@.....ProcessComponents..Updating component registration.....@.....@.....@.]....&.{EDE10F6C-30F4-42CA-B5C7-ADB905E45BFC}7.22:\SOFT WARE\EXEMSI.COM\MSI Wrapper\Installed\LogonUser.@.....@.....@.....@.....WriteRegistryValues..Writing system registry values..Key: [1],

C:\Windows\Installer\MSIAA7F.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.513495229990427
Encrypted:	false
SSDEEP:	3072:9spAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLu2loHUvU1yGxr5nqM2a8:/tOdiRQYpgjpjew5JWyGxJqo8
MD5:	D8AD3B90E6F172C97F1A95678EC8E1A4
SHA1:	C33402EDEB359044309E01B2E8C4D1694B48C5E1
SHA-256:	2D4AFDF54F3CB2E602A23CD22F7223199F0E483D556CC8DF7A8DA72C7FE1336A
SHA-512:	64A2DC66A0056740BCF03065522962FFF847307F12545256817A7481A00025ECA9F0C097ECF660C17045729666D663137DEDC1B42E2FD14B587CEE242CCBE54F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p.....p..../.p.....p...q.%.p.....p.....p.....p.Rich..p... .....PE..L....k `.....!.....h.....K.....@.....P...]....P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`...*.....@..B..... ....

C:\Windows\Installer\MSIBF62.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	212992
Entropy (8bit):	6.513495229990427
Encrypted:	false
SSDEEP:	3072:9spAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLu2loHUvU1yGxr5nqM2a8:/tOdiRQYpgjpjew5JWyGxJqo8
MD5:	D8AD3B90E6F172C97F1A95678EC8E1A4
SHA1:	C33402EDEB359044309E01B2E8C4D1694B48C5E1
SHA-256:	2D4AFDF54F3CB2E602A23CD22F7223199F0E483D556CC8DF7A8DA72C7FE1336A
SHA-512:	64A2DC66A0056740BCF03065522962FFF847307F12545256817A7481A00025ECA9F0C097ECF660C17045729666D663137DEDC1B42E2FD14B587CEE242CCBE54F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p.....p..../.p.....p...q.%.p.....p.....p.....p.Rich..p... .....PE..L....k `.....!.....h.....K.....@.....P...]....P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`...*.....@..B..... ....

C:\Windows\Installer\SourceHash{8291D67C-2E0B-4E71-B034-09AFE03383E8}

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.1819271031136984
Encrypted:	false
SSDEEP:	12:JSbX72Fje5TliAGiLIlHVRp/h/77777777777777777777777vDHFun7gTriwV:JUTiQl57YiX8F
MD5:	6B8E60B59582EEC45CB1BE8561409AF8
SHA1:	B382E4CCA80B7BC1F8B5A60A3232D380F5E1BBD8
SHA-256:	E4A3C6060A3C2A97E6B2DEE4B0373EBA33A22929760934BC492342B77CD81D1D
SHA-512:	9CE17DEC719FB406ECF86DC5C582684BFB4F083C8E47BC4C116004E2D23BBB6CED1B88C29CE32D933E96B18675E1F446B3C3BA531C6CF8CC8E99AC8AFEE4 BBC
Malicious:	false

Preview:	.....>..... ....

C:\Windows\Installer\inprogressinstallinfo.ipi	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.551188796700849
Encrypted:	false
SSDEEP:	48:GfO8PhBuRc06WX44nT5mvYpHAuesdASronfrXfdASB21r0Pyt:qBhB1InTWuq9qq9P
MD5:	3BE07B0E6ABD6F1380F26C49D20B4010
SHA1:	40F7AFCA7262E9823EF28D2FD5DDA8A71B943C67
SHA-256:	A54ECBCCC12DBB9710C4FED1EF5BFBB611B226C3C617C66C01331795C315BA5D
SHA-512:	C96A08F4DBC55BB2E2E81CCDE987B91CA5278012DC16C0DC0C56F2B1B5F79AE4FC5D7393FD0C52BEFE3C47E3266FE3A25A8719D74F0EEBA032FA1CC61B54A6E4
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Logs\DPX\setupact.log	
Process:	C:\Windows\SysWOW64\expand.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	933929
Entropy (8bit):	4.385952864024072
Encrypted:	false
SSDEEP:	192:kKcKnKcKqKcKnKcKqKcKnKcKqKcKnKcKqKcKnKcKqKcKnKcKqKcKnKco:V
MD5:	FE27DC7691051218EA3D3E176EED977B
SHA1:	4E57DDC06C68966ADDFAD989F9EA2626AA4E1BF6
SHA-256:	4423838CB5079083E9649DD599ED8CE122851D8A5B339DFAA0480F160ECC8F39
SHA-512:	0AD274632DEAC3CE8836E23242DB6D3AAE27E2BBAD3235C74413179FE38CAD17BB816A337759E528DB64D209499D9C43617FFA5E7436E42155656F6DCCE6695
Malicious:	false
Preview:	.2019-06-27 00:56:09, Info DPX Started DPX phase: Resume and Download Job..2019-06-27 00:56:09, Info DPX Started DPX phase: Apply Deltas Provided In File..2019-06-27 00:56:09, Info DPX Ended DPX phase: Apply Deltas Provided In File..2019-06-27 00:56:09, Info DPX Started DPX phase: Apply Deltas Provided In File..2019-06-27 00:56:09, Info DPX Ended DPX phase: Apply Deltas Provided In File..2019-06-27 00:56:09, Info DPX CJob::Resume completed with status: 0x0..2019-06-27 00:56:09, Info DPX Ended DPX phase: Resume and Download Job..2019-06-27 00:56:09, Info DPX Started DPX phase: Resume and Download Job..2019-06-27 00:56:09, Info DPX Started DPX phase: Apply Deltas Provided In File..2019-06-27 00:56:09, Info DPX Ended DPX phase: Apply Deltas Provided In File..2019-06-27 00:56:09, Info

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	
Process:	C:\Windows\System32\msiexec.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	79122
Entropy (8bit):	5.282115154928446
Encrypted:	false
SSDEEP:	192:jmXs969ozNSkk3peTBYeHt0tfoI9qsjl0urmwYyim:yXs9UogeWeH29qclhmwYyim
MD5:	66FE9B41903AB5D0184B35D63FC1621B
SHA1:	5E255F22B8783E489363A17C7268994DE2134197
SHA-256:	6F6D2465A3A3C067379B316FA13DF65D14BA30F7F11BA2721CDBF2BFA2A999E2
SHA-512:	B23059DB85693E64C2833DA7B5CCD02821381A84F0C677A30F7EC9E047040A9F18BEDCAE47718B31658CE6FCA36FCF9090F4CFA3995066EA3BAAE0BD5E43D93B
Malicious:	false

Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..07/23/2020 03:22:38.143 [320]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Outlook, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.159 [320]: ngen returning 0x00000000..07/23/2020 03:22:38.222 [3748]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Word, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.237 [3748]: ngen returning 0x00000000..07/23/2020 03:22:38.284 [64]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Common.Implementation, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.300 [64]:

C:\Windows\System32\MsDtc\Trace\dtctrace.log

Process:	C:\Windows\System32\msdtc.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.32056240596048735
Encrypted:	false
SSDEEP:	6:QKt3dEX8ta/ygA5UMclSqlPMclX/7EJRD/tz8gYbOCzE5Zm3n+SkSJkJIOcuCjHF:zaX80y52xX/7En7q6CzE5Z2+fqjFhl
MD5:	7A141E48D07008633F69DE5A0962C3D7
SHA1:	427889058B5A3401D1F3028EACDA31BD8F88C0A7
SHA-256:	CFDDD10FED936C66EB0DA9D65478D057B26E6095976976CA95D85C1113A61FE7
SHA-512:	534413FB19E57EBA818C170EFAF5164A095A38D7A5948D329A315C90E3C199294ED1238EAC015FA16A6656B8161BA045F12B834223061DF15C04559AA0C21D07
Malicious:	false
Preview:	.@..X...X.....X...I.....5._-.....@.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.3.2.2.....@.t.z.r.e.s...d.l.l.,.-.3.2.1.....:..... .....w.....M.S.D.T.C._.T.R.A.C.E._.S.E.S.S.I.O.N...C.:.\.W.i.n.d.o.w.s.\.s.y.s.t.e.m.3.2.\.M.S.D.t.c.\.t.r.a.c.e.\.d.t.c.t.r.a.c.e...l.o.g.....P.P.....5._-.....

C:\Windows\Temp\~DF03391F73031C0A34.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	

C:\Windows\Temp\~DF22D398DA2AC0F842.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	

C:\Windows\Temp\~DF25DC81189B88B007.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DF4B4630A3D90165FC.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.242111497633235
Encrypted:	false
SSDEEP:	48:2rA5upM+xFX4fT5gvYpHAuesdASronfrXfdASB21r0Pyt:2k5g8Touq9qq9P
MD5:	F947EC28BEE2D39A680021C0B666F034
SHA1:	83BBC3BA11BFE26D02ED764182CE1D046F3B7B81
SHA-256:	43F8A107692C45C619F0C6C7EE744833367441ABF09F73E47E3DC2B19E65DA10
SHA-512:	9E7B3C9D85141DD4B65DD13CDB179E1C3E3D8A2FCD9FD0CB7C36B783F7C7AD33B63325D8107412E3588B5DEA96DFF6ED0032EE6D10217B40C0A98D63F7BA5390
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DF51AB674798AB773E.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.551188796700849
Encrypted:	false
SSDEEP:	48:GfO8PhBuRc06WX44nT5mvYpHAuesdASronfrXfdASB21r0Pyt:qBhB1InTWuq9qq9P
MD5:	3BE07B0E6ABD6F1380F26C49D20B4010
SHA1:	40F7AFCA7262E9823EF28D2FD5DDA8A71B943C67
SHA-256:	A54ECBCCC12DBB9710C4FED1EF5BFBB611B226C3C617C66C01331795C315BA5D
SHA-512:	C96A08F4DBC55BB2E2E81CCDE987B91CA5278012DC16C0DC0C56F2B1B5F79AE4FC5D7393FD0C52BEFE3C47E3266FE3A25A8719D74F0EEBA032FA1CC61B54A6E4
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DF580A4C0E4BCBE8F6.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.13764522655708583
Encrypted:	false
SSDEEP:	24:8NctbPtwY+QJfAebfdAipV72XdAipVJV2BwGtplrkg9SkUn+IpHA0n:ntbPNrfdASB2XdASronfrXUnFpHA0n

MD5:	991167EEA182FCFB993E4E260943D1C5
SHA1:	0C4DCB947F0C06990A29C420A7B64193BFE0B5A8
SHA-256:	CFEFCB870FFC06DEF2042612E91FB61DF8FACDB1BA17A564B1FA4D3F96110BB9
SHA-512:	FB9013D258C8CDC5F63612F6033B4EB106E1D462E77D16990260A28A2D0D4811E37BE0437FC0E94E4040F58623DC876A25D3A18FF87734B9FE33FDC6BA4056E
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF5D4C48B55B4BFC19.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.242111497633235
Encrypted:	false
SSDEEP:	48:2rA5upM+xFX4fT5gvYpHAuesdASronfrXfdASB21r0Pyt:2k5g8Touq9qq9P
MD5:	F947EC28BEE2D39A680021C0B666F034
SHA1:	83BBC3BA11BFE26D02ED764182CE1D046F3B7B81
SHA-256:	43F8A107692C45C619F0C6C7EE744833367441ABF09F73E47E3DC2B19E65DA10
SHA-512:	9E7B3C9D85141DD4B65DD13CDB179E1C3E3D8A2FCD9FD0CB7C36B783F7C7AD33B63325D8107412E3588B5DEA96DFF6ED0032EE6D10217B40C0A98D63F7BA5 390
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF6CC46065D10C7A25.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.08454305645594185
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOuUV6GQ3I2rQpTrTs14Vky6lwt/:2F0i8n0itFzDHFun7gTriw1
MD5:	C1ACC1C2E59C0C4C69DE5DAB0C357421
SHA1:	656C5B8159572325A6657AB1C62A424EB5AEBF47
SHA-256:	C394492BEE24556C4BD45CD20090CE5DD6E9AFFD84330D9066A3FF7B497EAA87
SHA-512:	B5E818E035671A5660C98EDCB1C1C791C4C8570E161C1E39EC03DAD8BE97B39B1CA56DDB31482AD664D234987AE85410E229A84DE8CD28216AEDC8618B6D2 35
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFB5C2126B1B76E891.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false

Preview:	.....

C:\Windows\Temp\~DFC6CBD75861280262.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.551188796700849
Encrypted:	false
SSDEEP:	48:GfO8PhBuRc06WX44nT5mvYpHAuesdASronfrXfdASB21r0Pyt:qBhB1InTWuq9qq9P
MD5:	3BE07B0E6ABD6F1380F26C49D20B4010
SHA1:	40F7AFCA7262E9823EF28D2FD5DDA8A71B943C67
SHA-256:	A54ECBCCC12DBB9710C4FED1EF5BFBB611B226C3C617C66C01331795C315BA5D
SHA-512:	C96A08F4DBC55BB2E2E81CCDE987B91CA5278012DC16C0DC0C56F2B1B5F79AE4FC5D7393FD0C52BEFE3C47E3266FE3A25A8719D74F0EEBA032FA1CC61B54A6E4
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DFCF309A9E155014E3.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DFFCD8D26BF9AB481A.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.242111497633235
Encrypted:	false
SSDEEP:	48:2rA5upM+xFX4fT5gvYpHAuesdASronfrXfdASB21r0Pyt:2k5g8Touq9qq9P
MD5:	F947EC28BEE2D39A680021C0B666F034
SHA1:	83BBC3BA11BFE26D02ED764182CE1D046F3B7B81
SHA-256:	43F8A107692C45C619F0C6C7EE744833367441ABF09F73E47E3DC2B19E65DA10
SHA-512:	9E7B3C9D85141DD4B65DD13CDB179E1C3E3D8A2FCD9FD0CB7C36B783F7C7AD33B63325D8107412E3588B5DEA96DFF6ED0032EE6D10217B40C0A98D63F7BA5390
Malicious:	false
Preview:	.....>.....

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF, LF line terminators

Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.058268497021542
Encrypted:	false
SSDEEP:	12:zKLLDkOA4BFNY1RI5gYXH8fvfKwZGRrsTACF7Bjmpv:zKLXkb4DO1RGTcSwZursMCrmB
MD5:	6D96D5AD1A844AE8D1CBA8B2D0D3AEED
SHA1:	1FE3C841A8B52C534D5BD7375B2427E13BBEBF76
SHA-256:	81ECD2B22E988559B583F2A5D1389B9036CC325F8BF97BDBA7B6D81137366E20
SHA-512:	8841FF1E18A425AAE729330DB74BEA5E24339296D3DF2F76EF8DAF024ED790496E03FB0B2EF1736A66779F4C9714014BAFD2C909B111200BC88F0BD2FED01B34
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....An unknown exception occurred during installation:..1: System.IO.FileLoadException - Could not load file or assembly 'C:\\Windows\\Microsoft.NET\\Framework' or one of its dependencies. The given assembly name or codebase was invalid. (Exception from HRESULT: 0x80131047)..

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Microsoft Visual Studio - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 16.6.255.35071, Subject: Microsoft Visual Studio - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft Corporation, Keywords: Installer, Template: x64;1033, Revision Number: {49C681E5-45C4-4467-92EE-456F1E355C5F}, Create Time/Date: Sun Feb 7 22:37:14 2021, Last Saved Time/Date: Sun Feb 7 22:37:14 2021, Number of Pages: 200, Number of Words: 2, Name of Creating Application: MSI Wrapper (10.0.50.0), Security: 2
Entropy (8bit):	7.70038526988355
TrID:	• Microsoft Windows Installer (77509/1) 90.64% • Generic OLE2 / Multistream Compound File (8008/1) 9.36%
File name:	SecuriteInfo.com.MSIL.Kryptik.AECS.24576.msi
File size:	921600
MD5:	1d59589778c525aadcb645270cee737c
SHA1:	ad4584c1b7734854939c59674cbbf22a99618285
SHA256:	1f95063441e9d231e0e2b15365a8722c5136c2a6fe2716f3653c260093026354
SHA512:	11d4394566efe3bc75336d90371017ea0e4e9edc556736e2537201afb648e9c2167beb82ca87c3cc4a4b23603d49eb19bfc403c782858f0e781bb127771109d9
SSDEEP:	24576:StZcpVJ78TNcjk8LKAj6h5E4Z9+SgzDOo7sv0yx3FXyoUc:Rpz78OI/i4nhgzDOo3yLC+
File Content Preview:	.....>.....

File Icon

Icon Hash:	a2a0b496b2caca72

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.MSIL.Kryptik.AECS.24576.msi"

Indicators

Has Summary Info:	True
Application Name:	MSI Wrapper (10.0.50.0)
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary	
Code Page:	1252
Title:	Microsoft Visual Studio - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 16.6.255.35071
Subject:	Microsoft Visual Studio - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com
Author:	Microsoft Corporation
Keywords:	Installer
Template:	x64;1033
Revion Number:	{49C681E5-45C4-4467-92EE-456F1E355C5F}
Create Time:	2021-02-07 22:37:14
Last Saved Time:	2021-02-07 22:37:14
Number of Pages:	200
Number of Words:	2
Creating Application:	MSI Wrapper (10.0.50.0)
Security:	2

Document Summary	
Document Code Page:	1252
Company:	Microsoft Corporation

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 136

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	136
Entropy:	3.23907469015
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . X . . . . . (. . . . . 0 . . . . . 8 . . . . . M i c r o o f t C o r p o r a t i o n . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 58 00 00 00 03 00 00 00 01 00 00 00 28 00 00 00 00 00 00 80 30 00 00 00 0f 00 00 00 38 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 e4 04 00 00 13 00 00 00 09 04 00 00 1e 00 00 00 16 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 588

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	588
Entropy:	4.89141384854
Base64 Encoded:	True
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . x . . . . . (. . . . . I n s t a l l e r . . . . . x 6 4 ; 1 0 3 3 . . . . . ' . . . { 4 9 C 6 8 1 E 5 4 5 C 4 - 4 4 6 7 - 9 2 E E - 4 5 6 F 1 E 3
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 1c 02 00 00 0d 00 00 00 01 00 00 00 78 00 00 00 02 00 00 00 28 01 00 00 03 00 00 00 98 01 00 00 04 00 00 00 08 01 00 00 05 00 00 00 80 00 00 00 07 00 00 00 94 00 00 00 09 00 00 00 a8 00 00 00 0c 00 00 00 d8 00 00 00 0d 00 00 00 e4 00 00 00

Stream Path: \x17163\x16689\x18229\x16766\x18365\x17760\x17636\x16947\x16167\x17896\x17656\x17753\x17074\x16693\x18480, File Type: Microsoft Cabinet archive data, 669935 bytes, 1 file, Stream Size: 669935

General	
Stream Path:	\x17163\x16689\x18229\x16766\x18365\x17760\x17636\x16947\x16167\x17896\x17656\x17753\x17074\x16693\x18480
File Type:	Microsoft Cabinet archive data, 669935 bytes, 1 file
Stream Size:	669935
Entropy:	7.95796937333
Base64 Encoded:	True
Data ASCII:	M S C F . . . . . 8 . . . . . , ... G . . . . . 8 . . . . . < T W . . s e r v e r . e x e . . . 3 . . . . . M Z . . . . . @ . . . . . ! . . L . ! T h i s p r o g r a m c a n n o t b e r u n i n D O S m o d e . . . . $ . . . . . P E . . L . . . . b) . . . . . 0 . @ , ... : L . . . . .
Data Raw:	4d 53 43 46 00 00 00 00 ef 38 0a 00 00 00 00 00 2c 00 00 00 00 00 00 00 03 01 01 00 01 00 00 00 9b 8e 00 00 47 00 00 00 15 00 00 00 00 00 38 0a 00 00 00 00 00 00 00 3c 54 57 80 20 00 73 65 72 76 65 72 2e 65 78 65 00 99 0a 33 f0 00 80 00 80 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x17163\x16689\x18229\x16766\x18365\x17932\x17910\x17458\x16778\x17207\x17522\x17357\x18479, File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, Stream Size: 212992

General	
Stream Path:	\x17163\x16689\x18229\x16766\x18365\x17932\x17910\x17458\x16778\x17207\x17522\x17357\x18479
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Stream Size:	212992
Entropy:	6.51349522999
Base64 Encoded:	True
Data ASCII:	M Z . . . . . @ . . . . . ! . . L . ! T h i s p r o g r a m c a n n o t b e r u n i n D O S m o d e . . . . $ . . . . . p . . . p . . . p . . . . . p . . . . . p . . . . . / . p . . . . . p . . . q . % . p . . . . . p . . . . . p . . . . . p . R i c h . . p . . . . . P E . . L . . . . k ` . . . .
Data Raw:	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00

Stream Path: \x18496\x15167\x17394\x17464\x17841, File Type: data, Stream Size: 672	
General	
Stream Path:	\x18496\x15167\x17394\x17464\x17841
File Type:	data
Stream Size:	672
Entropy:	4.76447414203
Base64 Encoded:	False
Data ASCII:	. . . . . " . " .) .) . * . * . * . + . + . / . / . / . / . / . 5 . 5 . 5 . = . = . = . = . M . M . M . M . M . M . M . M . \\ . \\ . a . a . a . a . a . a . a . a . a . o . o . r . r . r . s . s . s . t . t . w . w . w . w . w . w . . . . .
Data Raw:	06 00 06 00 06 00 06 00 06 00 06 00 06 00 06 00 06 00 22 00 22 00 22 00 29 00 29 00 29 00 2a 00 2a 00 2a 00 2b 00 2b 00 2f 00 2f 00 2f 00 2f 00 2f 00 35 00 35 00 35 00 3d 00 3d 00 3d 00 3d 00 3d 00 4d 00 4d 00 4d 00 4d 00 4d 00 4d 00 4d 00 4d 00 5c 00 5c 00 61 00 61 00 61 00 61 00 61 00 61 00 61 00 6f 00 6f 00 72 00 72 00 72 00 73 00 73 00 73 00 74 00 74 00 77 00

Stream Path: \x18496\x16191\x17783\x17516\x15210\x17892\x18468, File Type: ISO-8859 text, with very long lines, with no line terminators, Stream Size: 8555	
General	
Stream Path:	\x18496\x16191\x17783\x17516\x15210\x17892\x18468
File Type:	ISO-8859 text, with very long lines, with no line terminators
Stream Size:	8555
Entropy:	5.07763841758
Base64 Encoded:	True
Data ASCII:	N a m e T a b l e T y p e C o l u m n _ V a l i d a t i o n V a l u e N P r o p e r t y I d _ S u m m a r y I n f o r m a t i o n D e s c r i p t i o n S e t C a t e g o r y K e y C o l u m n M a x V a l u e N u l l a b l e K e y T a b l e M i n V a l u e I d e n t i f i e r N a m e o f t a b l e N a m e o f c o l u m n Y ; N W h e t h e r t h e c o l u m n i s n u l l a b l e Y M i n i m u m v a l u e a l l o w e d M a x i m u m v a l u e a l l o w e d F o r f o r e i g n k e y
Data Raw:	4e 61 6d 65 54 61 62 6c 65 54 79 70 65 43 6f 6c 75 6d 6e 5f 56 61 6c 69 64 61 74 69 6f 6e 56 61 6c 75 65 4e 50 72 6f 70 65 72 74 79 49 64 5f 53 75 6d 6d 61 72 79 49 6e 66 6f 72 6d 61 74 69 6f 6e 44 65 73 63 72 69 70 74 69 6f 6e 53 65 74 43 61 74 65 67 6f 72 79 4b 65 79 43 6f 6c 75 6d 6e 4d 61 78 56 61 6c 75 65 4e 75 6c 6c 61 62 6c 65 4b 65 79 54 61 62 6c 65 4d 69 6e 56 61 6c 75 65

Stream Path: \x18496\x16191\x17783\x17516\x15978\x17586\x18479, File Type: data, Stream Size: 1216	
General	
Stream Path:	\x18496\x16191\x17783\x17516\x15978\x17586\x18479
File Type:	data
Stream Size:	1216
Entropy:	3.08768728885
Base64 Encoded:	False
Data ASCII:	. . . . . , ... * . . . . . 6 . . . $ . . . . . B . . . . . o . . . . . ' . . . . . ; . . . . . > . . . . . ' . . . . . S . . . ^ . . .
Data Raw:	00 00 00 00 04 00 06 00 05 00 02 00 00 00 00 00 04 00 02 00 06 00 02 00 0b 00 15 00 05 00 05 00 01 00 2c 00 0a 00 01 00 13 00 02 00 0b 00 06 00 03 00 02 00 08 00 02 00 09 00 02 00 08 00 02 00 08 00 02 00 08 00 02 00 08 00 02 00 0a 00 19 00 0d 00 01 00 0e 00 01 00 03 00 01 00 1e 00 01 00 01 00 2a 00 15 00 01 00 15 00 01 00 36 00 01 00 24 00 01 00 f5 00 01 00 0f 00 01 00 04 00 09 00

Stream Path: \x18496\x16255\x16740\x16943\x18486, File Type: data, Stream Size: 38	
General	
Stream Path:	\x18496\x16255\x16740\x16943\x18486
File Type:	data
Stream Size:	38
Entropy:	3.12396375672
Base64 Encoded:	False
Data ASCII:	. . " .) . * . + . / . 5 . = . M . \\ . a . o . r . s . t . w . . . . .
Data Raw:	06 00 22 00 29 00 2a 00 2b 00 2f 00 35 00 3d 00 4d 00 5c 00 61 00 6f 00 72 00 73 00 74 00 77 00 82 00 86 00 90 00

Stream Path: \x18496\x16383\x17380\x16876\x17892\x17580\x18481, File Type: data, Stream Size: 2064	
General	
Stream Path:	\x18496\x16383\x17380\x16876\x17892\x17580\x18481
File Type:	data
Stream Size:	2064
Entropy:	2.38126922111
Base64 Encoded:	False
Data ASCII:	. . . . . "." ." .) .) . * . * . * . + . + . / . / . / . / . / . 5 . 5 . 5 . = . = . = . = . = . M . M . M . M . M . M . M . M . M . \\ . \\ . a . a . a . a . a a . a . a . o . o . r . r . r . s . s . s . t . t . w . w . w . w . w . w . . . . . # . % . ' . # . % . ' . # . % . . . - . % . / . 1 . 4 . 7 . : . 5 . I . K . . . # . @ . C . F . . . 4 . 7 . M . O .
Data Raw:	06 00 06 00 06 00 06 00 06 00 06 00 06 00 06 00 06 00 0a 00 0a 00 22 00 22 00 22 00 29 00 29 00 29 00 2a 00 2a 00 2a 00 2b 00 2b 00 2f 00 2f 00 2f 00 2f 00 2f 00 2f 00 35 00 35 00 35 00 3d 00 3d 00 3d 00 3d 00 3d 00 4d 00 4d 00 4d 00 4d 00 4d 00 4d 00 4d 00 4d 00 4d 00 5c 00 5c 00 61 00 61 00 61 00 61 00 61 00 61 00 61 00 6f 00 6f 00 72 00 72 00 72 00 73 00 73 00 73 00 74 00

Stream Path: \x18496\x16661\x17528\x17126\x17548\x16881\x17900\x17580\x18481, File Type: data, Stream Size: 4	
General	
Stream Path:	\x18496\x16661\x17528\x17126\x17548\x16881\x17900\x17580\x18481
File Type:	data
Stream Size:	4
Entropy:	1.5
Base64 Encoded:	False
Data ASCII:	. . . .
Data Raw:	e1 00 e2 00

Stream Path: \x18496\x16842\x17200\x15281\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 48	
General	
Stream Path:	\x18496\x16842\x17200\x15281\x16955\x17958\x16951\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	48
Entropy:	3.06842109407
Base64 Encoded:	False
Data ASCII:	. . . . . x . . . < . . . . .
Data Raw:	9d 00 9e 00 9f 00 a0 00 a1 00 a2 00 a3 00 a4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 78 85 dc 85 3c 8f a0 8f c8 99

Stream Path: \x18496\x16842\x17200\x16305\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 24	
General	
Stream Path:	\x18496\x16842\x17200\x16305\x16146\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	24
Entropy:	2.59436093777
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	9d 00 9e 00 9f 00 a5 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 14 85

Stream Path: \x18496\x16842\x17913\x18126\x16808\x17912\x16168\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 42	
General	
Stream Path:	\x18496\x16842\x17913\x18126\x16808\x17912\x16168\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	42
Entropy:	2.9135675273
Base64 Encoded:	False
Data ASCII:	. . . . . x . . . . .
Data Raw:	9d 00 9f 00 a0 00 a1 00 a4 00 a6 00 a7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 83 e8 83 78 85 dc 85 c8 99 9c 98 00 99

Stream Path: \x18496\x16911\x17892\x17784\x15144\x17458\x17587\x16945\x17905\x18486, File Type: data, Stream Size: 4	
General	
Stream Path:	\x18496\x16911\x17892\x17784\x15144\x17458\x17587\x16945\x17905\x18486
File Type:	data
Stream Size:	4
Entropy:	1.5
Base64 Encoded:	False
Data ASCII:	. . . .

General	
Data Raw:	cc 00 aa 00

Stream Path: \x18496\x16911\x17892\x17784\x18472, File Type: 386 compact demand paged pure executable, Stream Size: 16	
General	
Stream Path:	\x18496\x16911\x17892\x17784\x18472
File Type:	386 compact demand paged pure executable
Stream Size:	16
Entropy:	1.9197367178
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	cc 00 00 00 cd 00 00 00 02 80 01 80 00 00 00 80

Stream Path: \x18496\x16918\x17191\x18468, File Type: MIPSEB Ucode, Stream Size: 14	
General	
Stream Path:	\x18496\x16918\x17191\x18468
File Type:	MIPSEB Ucode
Stream Size:	14
Entropy:	0.946372935985
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	01 80 00 00 00 80 00 00 00 00 00 00 00 00

Stream Path: \x18496\x16923\x17194\x17910\x18229, File Type: data, Stream Size: 60	
General	
Stream Path:	\x18496\x16923\x17194\x17910\x18229
File Type:	data
Stream Size:	60
Entropy:	3.52924126798
Base64 Encoded:	False
Data ASCII:	. . . . " . % . (. . . . . . . # . & .) . . . ! . $. ' . * . . . . .
Data Raw:	ad 00 1f 01 22 01 25 01 28 01 ff 7f ff 7f ff 7f ff 7f ff 7f 1c 01 1c 01 1c 01 1c 01 1c 01 1d 01 20 01 23 01 26 01 29 01 1e 01 21 01 24 01 27 01 2a 01 aa 00 aa 00 aa 00 aa 00 aa 00

Stream Path: \x18496\x17163\x16689\x18229, File Type: data, Stream Size: 8	
General	
Stream Path:	\x18496\x17163\x16689\x18229
File Type:	data
Stream Size:	8
Entropy:	1.75
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	a8 00 a9 00 01 00 01 00

Stream Path: \x18496\x17165\x16949\x17894\x17778\x18492, File Type: data, Stream Size: 18	
General	
Stream Path:	\x18496\x17165\x16949\x17894\x17778\x18492
File Type:	data
Stream Size:	18
Entropy:	2.10218717095
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	ac 00 c7 00 c9 00 c7 00 c9 00 00 00 c8 00 ca 00 cb 00

Stream Path: \x18496\x17490\x17910\x17380\x15279\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 216	
General	
Stream Path:	\x18496\x17490\x17910\x17380\x15279\x16955\x17958\x16951\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	216
Entropy:	4.29485555194
Base64 Encoded:	False

General	
Data ASCII:	. . . . . x . . . . . d . . . . . @ . . . (. . . p . . . ! . y . . .
Data Raw:	9d 00 9e 00 9f 00 a0 00 a1 00 a3 00 a4 00 a6 00 a7 00 ae 00 b0 00 b1 00 b4 00 b6 00 b7 00 b9 00 ba 00 bb 00 bd 00 bf 00 c0 00 c2 00 c3 00 cf 00 d0 00 d1 00 d2 00 d3 00 d4 00 d5 00 d6 00 d7 00 d8 00 d9 00 db 00 df 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 dc 00 dc 00 dc 00 de 00 de 00 de 00 de 00 da 00 dd 00 dd 00 dd 00 dd 00 dd 00 00 00 00 00 00 00 00 00 00

Stream Path: \x18496\x17490\x17910\x17380\x16303\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 48	
General	
Stream Path:	\x18496\x17490\x17910\x17380\x16303\x16146\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	48
Entropy:	3.11008776073
Base64 Encoded:	False
Data ASCII:	. . . . . d . . . . .
Data Raw:	9d 00 9e 00 9f 00 a5 00 cf 00 d0 00 d1 00 d2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 14 85 19 80 64 80 bc 82 b0 84

Stream Path: \x18496\x17548\x17648\x17522\x17512\x18487, File Type: Dyalog APL aplcore version 171.0, Stream Size: 12	
General	
Stream Path:	\x18496\x17548\x17648\x17522\x17512\x18487
File Type:	Dyalog APL aplcore version 171.0
Stream Size:	12
Entropy:	2.29248125036
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	aa 00 ab 00 ac 00 04 81 00 00 ad 00

Stream Path: \x18496\x17630\x17770\x16868\x18472, File Type: data, Stream Size: 32	
General	
Stream Path:	\x18496\x17630\x17770\x16868\x18472
File Type:	data
Stream Size:	32
Entropy:	2.1983911108
Base64 Encoded:	False
Data ASCII:	/ . / . . . - . - . . . . .
Data Raw:	2f 01 2f 01 00 00 2d 01 2d 01 00 00 00 00 00 00 01 00 00 80 02 00 00 80 00 00 00 00 19 01 18 01

Stream Path: \x18496\x17753\x17650\x17768\x18231, File Type: data, Stream Size: 80	
General	
Stream Path:	\x18496\x17753\x17650\x17768\x18231
File Type:	data
Stream Size:	80
Entropy:	3.89623018849
Base64 Encoded:	False
Data ASCII:	. . . . . / . . . . . - . . .
Data Raw:	91 00 e3 00 e5 00 e6 00 f1 00 f3 00 f6 00 f7 00 f9 00 fb 00 fd 00 ff 00 01 01 03 01 10 01 11 01 13 01 15 01 17 01 1a 01 2f 01 e4 00 e4 00 e4 00 02 01 f4 00 f0 00 f8 00 fa 00 fc 00 fe 00 00 01 02 01 02 01 2e 01 12 01 14 01 16 01 2d 01 1b 01

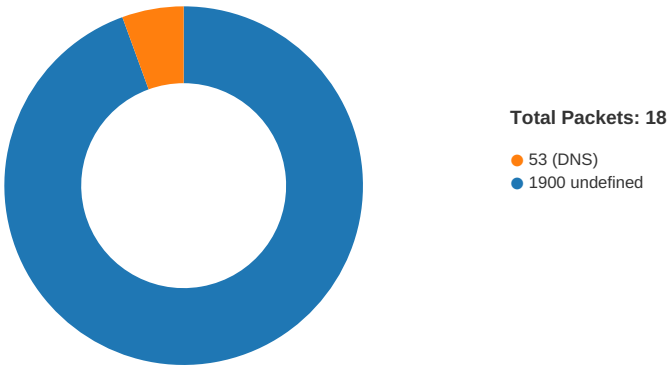
Stream Path: \x18496\x17932\x17910\x17458\x16778\x17207\x17522, File Type: data, Stream Size: 180	
General	
Stream Path:	\x18496\x17932\x17910\x17458\x16778\x17207\x17522
File Type:	data
Stream Size:	180
Entropy:	2.77261833239
Base64 Encoded:	False
Data ASCII:	. . . . . 3 . . . . . 3 . . . 3 . . . . . 3 . . . 3 . . . . .
Data Raw:	ae 00 b0 00 b1 00 b4 00 b6 00 b7 00 b9 00 ba 00 bb 00 bd 00 bf 00 c0 00 c2 00 c3 00 c5 00 01 80 33 80 01 80 01 80 33 80 01 8c 33 80 01 8c 01 80 01 80 33 80 01 8c 33 80 01 84 01 80 a9 00 b1 00 a9 00 a9 00 b7 00 a9 00 ba 00 a9 00 a9 00 a9 00 c0 00 a9 00 c3 00 a9 00 a9 00 af 00 b2 00 b3 00 b5 00 b2 00 b8 00 b2 00 b3 00 bc 00 be 00 b2 00 c1 00 b2 00 c4 00 c6 00 00 00 00 00 00 00 00 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/29/22-00:11:56.214088	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62389	8.8.8.8	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2022 00:11:56.219197989 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:11:56.417572021 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:11:56.418525934 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:11:57.600756884 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:11:57.966366053 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:11:57.966490030 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:11:58.366198063 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:02.634665012 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:02.637063026 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:12:02.980595112 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:03.211981058 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:12:03.480596066 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:11.634632111 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:12:11.980432034 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:19.760725021 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:12:20.168732882 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:20.777785063 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:20.780415058 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:12:21.172262907 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:36.795154095 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:12:37.167376041 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:38.889597893 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:38.890038967 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:12:39.168204069 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:45.340825081 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:12:45.666985989 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:53.466917038 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:12:53.879239082 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:56.972980976 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:12:56.973484993 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:12:57.270128012 CET	1900	49775	66.154.111.162	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2022 00:13:09.939162970 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:13:10.182445049 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:13:15.037537098 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:13:15.038743019 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:13:15.365333080 CET	1900	49775	66.154.111.162	192.168.2.4
Jan 29, 2022 00:13:18.064316988 CET	49775	1900	192.168.2.4	66.154.111.162
Jan 29, 2022 00:13:18.365268946 CET	1900	49775	66.154.111.162	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2022 00:11:56.106125116 CET	62389	53	192.168.2.4	8.8.8.8
Jan 29, 2022 00:11:56.214087963 CET	53	62389	8.8.8.8	192.168.2.4

DNS Queries

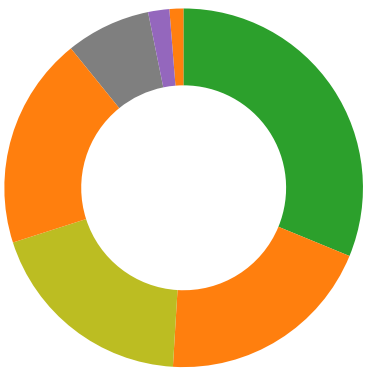
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 29, 2022 00:11:56.106125116 CET	192.168.2.4	8.8.8.8	0x7081	Standard query (0)	njlove.duc kdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2022 00:11:56.214087963 CET	8.8.8.8	192.168.2.4	0x7081	No error (0)	njlove.duc kdns.org		66.154.111.162	A (IP address)	IN (0x0001)

Statistics

Behavior



- msiexec.exe
- msiexec.exe
- msiexec.exe
- icacls.exe
- conhost.exe
- expand.exe
- conhost.exe
- server.exe
- AddInProcess.exe
- InstallUtil.exe
- AddInProcess.exe
- RegSvcs.exe
- icacls.exe
- conhost.exe
- netsh.exe
- conhost.exe
- cmd.exe
- conhost.exe
- RegSvcs.exe
- conhost.exe
- msdtc.exe
- RegSvcs.exe
- conhost.exe
- RegSvcs.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: msiexec.exe PID: 6712, Parent PID: 6112

General

Target ID:	0

Start time:	00:11:19
Start date:	29/01/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\SecuriteInfo.com.MSIL.Kryptik.AECS.24576.msi"
Imagebase:	0x7ff777c90000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **6128**, Parent PID: **568**

General

Target ID:	2
Start time:	00:11:19
Start date:	29/01/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff777c90000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	79028	94	30 31 2f 32 39 2f 32 30 32 32 20 30 30 3a 31 31 3a 32 30 2e 39 34 34 20 5b 36 31 32 38 5d 3a 20 53 65 74 74 69 6e 67 20 4d 53 49 20 68 61 6e 64 6c 65 2c 20 69 6e 73 74 61 6c 6c 20 6c 6f 67 67 69 6e 67 20 77 69 6c 6c 20 67 6f 20 69 6e 74 6f 20 74 68 65 20 4d 53 49 20 6c 6f 67 0d 0a	01/29/2022 00:11:20.944 [6128]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FFA95A9BEF0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	unknown	3	success or wait	1	7FFA95A9BBC6	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **6992**, Parent PID: **6128**

General

Target ID:	5
Start time:	00:11:21
Start date:	29/01/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 8427D5518DE818285DF2E5650B3C2701
Imagebase:	0x200000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E0A05E1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E099D24	CreateFileW
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files.cab	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E09BD84	CreateFileW
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E0A05E1	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files\server.exe	success or wait	1	699A049F	DeleteFileW
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	success or wait	1	699A049F	DeleteFileW
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files.cab	success or wait	1	699A049F	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	182	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=admini	success or wait	1	6E099D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	236	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=administratorsBaseName=server.ex	success or wait	1	6E099D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	280	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=administratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	338	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	378	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files.cab	0	1000	4d 53 43 46 00 00 00 00 fd 38 0a 00 00 00 00 00 2c 00 00 00 00 00 00 00 03 01 01 00 01 00 00 00 fd fd 00 00 47 00 00 00 15 00 00 00 00 38 0a 00 00 00 00 00 00 00 3c 54 57 fd 20 00 73 65 72 76 65 72 2e 65 78 65 00 fd 0a 33 fd 00 fd 00 fd 4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 62 29 fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 40 2c 0a 00 fd 04 00 00 00 00 00 00 3a 4c 0a 00 00 20 00 00	MSCF8,G8<TW server.exe3MZ@!L!This program cannot be run in DOS mode.$PELb)0@,:L	success or wait	670	6E09BDFE	WriteFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	524	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRe gistration=HiddenInstallS ucces sCodes=0ElevationMode =administ ratorsBaseName=server. exeCabHash=	success or wait	1	6E099D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	558	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	582	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	628	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	648	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	668	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	840	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	1020	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	1064	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	1120	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	1162	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRegistration=HiddenInstallSuccesCodes=0ElevationMode=administratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	1216	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRe gistration=HiddenInstallSucces sCodes=0ElevationMode=administ ratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	0	1426	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 61 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00 72 00 61 00 74 00 6f 00 72 00 73 00 0a 00 42 00 61 00 73 00 65 00 4e 00 61 00 6d 00 65 00 3d 00 73 00 65 00 72 00 76 00 65 00 72 00 2e 00 65 00 78 00 65 00 0a 00 43 00 61 00 62 00 48 00 61 00 73 00 68 00 3d	WrappedApplicationId=WrappedRe gistration=HiddenInstallSucces sCodes=0ElevationMode=administ ratorsBaseName=server.exeCabHash=	success or wait	1	6E099D7F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
unknown	unknown	4294967295	object type mismatch	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	182	success or wait	16	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files.cab	unknown	1000	success or wait	670	6E09BA34	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1216	success or wait	1	6E0999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1426	success or wait	1	6F3699C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1426	success or wait	1	6F3699C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1426	success or wait	1	699999C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\msiwrapper.ini	unknown	1426	success or wait	1	699999C9	ReadFile

Analysis Process: icacls.exe PID: **5596**, Parent PID: **6992**

General

Target ID:	6
Start time:	00:11:26
Start date:	29/01/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\." /SETINTEGRITYLEVEL (CI)(OI)HIGH
Imagebase:	0x1220000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5520**, Parent PID: **5596**

General

Target ID:	8
Start time:	00:11:26
Start date:	29/01/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: expand.exe PID: **4552**, Parent PID: **6992**

General

Target ID:	9
Start time:	00:11:27
Start date:	29/01/2022
Path:	C:\Windows\SysWOW64\expand.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files
Imagebase:	0xd70000
File size:	52736 bytes
MD5 hash:	8F8C20238C1194A428021AC62257436D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6740**, Parent PID: **4552**

General

Target ID:	10
Start time:	00:11:28
Start date:	29/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: server.exe PID: **7028**, Parent PID: **6992**

General

Target ID:	11
Start time:	00:11:31
Start date:	29/01/2022
Path:	C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files\server.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files\server.exe"
Imagebase:	0xeb0000
File size:	669696 bytes
MD5 hash:	CD4D919B4FC88C9D6F03C864A181E40F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 0000000B.00000002.721799355.0000000005A51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 0000000B.00000002.721299654.00000000045A6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000B.00000002.720255310.0000000003695000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 0000000B.00000002.720255310.0000000003695000.00000004.00000800.00020000.00000000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 0000000B.00000002.720255310.0000000003695000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.721129681.0000000004371000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 0000000B.00000002.721129681.0000000004371000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.721342787.0000000004613000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 0000000B.00000002.721342787.0000000004613000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.721704181.0000000005720000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 0000000B.00000002.721704181.0000000005720000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_DisableWinDefender, Description: Detects executables containing artifcats associated with disabling Widnows Defender, Source: 0000000B.00000002.721704181.0000000005720000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCMD, Description: Detects Windows exceutables bypassing UAC using CMSTP utility, command line and INF, Source: 0000000B.00000002.721704181.0000000005720000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM, Description: Detects executables embedding command execution via IExecuteCommand COM object, Source: 0000000B.00000002.721704181.0000000005720000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste, Description: Detects executables potentially checking for WinJail sandbox window, Source: 0000000B.00000002.721704181.0000000005720000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000B.00000002.717043543.0000000003371000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 0000000B.00000002.717043543.0000000003371000.00000004.00000800.00020000.00000000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 0000000B.00000002.717043543.0000000003371000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\server.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBEC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\server.exe.log	0	522	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6DBEC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D8B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess.exe	unknown	42080	success or wait	2	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	unknown	41064	success or wait	1	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_state.exe	unknown	47208	success or wait	1	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	45152	success or wait	1	6C721B4F	ReadFile

Analysis Process: AddInProcess.exe PID: **6312**, Parent PID: **7028**

General

Target ID:	12
Start time:	00:11:39
Start date:	29/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess.exe
Imagebase:	0x1f195890000
File size:	42080 bytes
MD5 hash:	11D8A500C4C0FBAF20EBDB8CDF6EA452
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: InstallUtil.exe PID: **6304**, Parent PID: **7028**

General	
Target ID:	13
Start time:	00:11:39
Start date:	29/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x2d0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: AddInProcess.exe PID: **7104**, Parent PID: **7028**

General	
Target ID:	14
Start time:	00:11:40
Start date:	29/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess.exe
Imagebase:	0x24a101b0000
File size:	42080 bytes
MD5 hash:	11D8A500C4C0FBAF20EBDB8CDF6EA452
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegSvcs.exe PID: **7148**, Parent PID: **7028**

General	
Target ID:	15
Start time:	00:11:41
Start date:	29/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x9a0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000F.00000000.709022701.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 0000000F.00000000.709022701.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 0000000F.00000000.709022701.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000F.00000000.708532058.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 0000000F.00000000.708532058.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 0000000F.00000000.708532058.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000F.00000000.709256674.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 0000000F.00000000.709256674.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 0000000F.00000000.709256674.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000F.00000000.708790888.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 0000000F.00000000.708790888.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 0000000F.00000000.708790888.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000F.00000002.927280027.0000000002CDE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000F.00000002.926559345.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 0000000F.00000002.926559345.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 0000000F.00000002.926559345.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D8DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D8DCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D8B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D8BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D8BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C721B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D8B5705	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\software\040b20e882d013c0c9f6ceff16d97f7a	success or wait	1	6C725F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\040 b20e882d013c0c9f6ceff16d97f7a	hp	unicode	bmpsb3ZlLmR1Y2tkbnMub3JnOjE5MDAs	success or wait	1	6C72646A	RegSetValueExW
HKEY_CURRENT_USER\Software\040 b20e882d013c0c9f6ceff16d97f7a	i	unicode	!	success or wait	1	6C72646A	RegSetValueExW
HKEY_CURRENT_USER	di	unicode	!	success or wait	1	6C72646A	RegSetValueExW
HKEY_CURRENT_USER\Environment	SEE_MASK_NOZONECHECKS	unicode	1	success or wait	1	6C72646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	040b20e882d013c0c9f6ceff16d97f7a	unicode	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" ..	success or wait	1	6C72646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	040b20e882d013c0c9f6ceff16d97f7a	unicode	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" ..	success or wait	1	6C72646A	RegSetValueExW
HKEY_CURRENT_USER\Software\040 b20e882d013c0c9f6ceff16d97f7a	kl	unicode	rr	success or wait	1	6C72646A	RegSetValueExW

Analysis Process: icacls.exe PID: 5164, Parent PID: 6992

General

Target ID:	18
Start time:	00:11:48
Start date:	29/01/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\." /SETINTEGRITYLEVEL (CI)(OI)LOW
Imagebase:	0x1220000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5576, Parent PID: 5164

General

Target ID:	19
Start time:	00:11:49
Start date:	29/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: netsh.exe PID: **6520**, Parent PID: **7148**

General

Target ID:	20
Start time:	00:11:51
Start date:	29/01/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	netsh firewall add allowedprogram "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" "RegSvcs.exe" ENABLE
Imagebase:	0x9f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	306	306	4f 6b 2e 0d 0a 0d 0a	Ok.	success or wait	1	9F7B1B	WriteFile
\Device\ConDrv	311	5	0d 0a		success or wait	1	9F7B1B	WriteFile
\Device\ConDrv	313	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	9F7B1B	WriteFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **2092**, Parent PID: **6520**

General

Target ID:	21
Start time:	00:11:52
Start date:	29/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5568**, Parent PID: **6992**

General

Target ID:	22
Start time:	00:11:55
Start date:	29/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c rd /s /q "C:\Users\user\AppData\Local\Temp\MW-71322570-7008-46b5-bb73-77098af1b752\files"
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5632**, Parent PID: **5568**

General

Target ID:	23
Start time:	00:11:56
Start date:	29/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: **3848**, Parent PID: **3424**

General

Target ID:	24
Start time:	00:12:03
Start date:	29/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" ..
Imagebase:	0xdf0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D8DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D8DCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBEC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C721B4F	WriteFile
\Device\ConDrv	141	141	0a 41 6e 20 75 6e 6b 6e 6f 77 6e 20 65 78 63 65 70 74 69 6f 6e 20 6f 63 63 75 72 72 65 64 20 64 75 72 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 3a 0d 0a 31 3a 20 53 79 73 74 65 6d 2e 49 4f 2e 46 69 6c 65 4c 6f 61 64 45 78 63 65 70 74 69 6f 6e 20 2d 20 43 6f 75 6c 64 20 6e 6f 74 20 6c 6f 61 64 20 66 69 6c 65 20 6f 72 20 61 73 73 65 6d 62 6c 79 20 27 43 3a 5c 5c 57 69 6e 64 6f 77 73 5c 5c 4d 69 63 72 6f 73 6f 66 74	An unknown exception occurred during installation:1: System. IO.FileLoadException - Could not load file or assembly 'C:\\ Windows\\Microsoft	success or wait	1	6C721B4F	WriteFile
\Device\ConDrv	194	53	31 3a 20 53 79 73 74 65 6d 2e 49 4f 2e 46 69 6c 65 4c 6f 61 64 45 78 63 65 70 74 69 6f 6e 20 2d 20 43 6f 75 6c 64 20 6e 6f 74 20 6c 6f 61 64 20 66 69 6c 65 20	1: System.IO.FileLoadException - Could not load file	success or wait	1	6C721B4F	WriteFile
\Device\ConDrv	414	220	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C721B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	0	1141	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 54 72 61	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",02,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",02,"System.Tra	success or wait	1	6DBEC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D8B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D8BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D8BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\System.EnterpriseServices\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.EnterpriseServices.dll	unknown	4096	success or wait	1	6D89D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\System.EnterpriseServices\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.EnterpriseServices.dll	unknown	512	success or wait	1	6D89D72F	unknown

Analysis Process: conhost.exe PID: 6048, Parent PID: 3848

General

Target ID:	25

Start time:	00:12:03
Start date:	29/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: msdtc.exe PID: **6320**, Parent PID: **568**

General

Target ID:	26
Start time:	00:12:06
Start date:	29/01/2022
Path:	C:\Windows\System32\msdtc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\msdtc.exe
Imagebase:	0x7ff739d10000
File size:	148480 bytes
MD5 hash:	9A94F32C1DC90A7E5A35D0F820A8FB1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegSvcs.exe PID: **6972**, Parent PID: **3424**

General

Target ID:	28
Start time:	00:12:11
Start date:	29/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" ..
Imagebase:	0x6c0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D8DCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D8DCF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C721B4F	WriteFile
\Device\ConDrv	141	141	0a 41 6e 20 75 6e 6b 6e 6f 77 6e 20 65 78 63 65 70 74 69 6f 6e 20 6f 63 63 75 72 72 65 64 20 64 75 72 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 3a 0d 0a 31 3a 20 53 79 73 74 65 6d 2e 49 4f 2e 46 69 6c 65 4c 6f 61 64 45 78 63 65 70 74 69 6f 6e 20 2d 20 43 6f 75 6c 64 20 6e 6f 74 20 6c 6f 61 64 20 66 69 6c 65 20 6f 72 20 61 73 73 65 6d 62 6c 79 20 27 43 3a 5c 5c 57 69 6e 64 6f 77 73 5c 5c 4d 69 63 72 6f 73 6f 66 74	An unknown exception occurred during installation:1: System. IO.FileLoadException - Could not load file or assembly 'C:\\ Windows\\Microsoft	success or wait	1	6C721B4F	WriteFile
\Device\ConDrv	194	53	31 3a 20 53 79 73 74 65 6d 2e 49 4f 2e 46 69 6c 65 4c 6f 61 64 45 78 63 65 70 74 69 6f 6e 20 2d 20 43 6f 75 6c 64 20 6e 6f 74 20 6c 6f 61 64 20 66 69 6c 65 20	1: System.IO.FileLoadException - Could not load file	success or wait	1	6C721B4F	WriteFile
\Device\ConDrv	414	220	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C721B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D8B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D8BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D8BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	6D8103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C721B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D8B5705	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\System.EnterpriseSe rvices\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.EnterpriseServices.dll	unknown	4096	success or wait	1	6D89D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\System.EnterpriseSe rvices\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.EnterpriseServices.dll	unknown	512	success or wait	1	6D89D72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_32\System.EnterpriseServices\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.EnterpriseServices.dll	unknown	512	success or wait	1	6D89D72F	unknown

Analysis Process: conhost.exe PID: **7020**, Parent PID: **6972**

General

Target ID:	29
Start time:	00:12:13
Start date:	29/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: **984**, Parent PID: **3424**

General

Target ID:	30
Start time:	00:12:19
Start date:	29/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" ..
Imagebase:	0xa40000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **6148**, Parent PID: **984**

General

Target ID:	31
Start time:	00:12:20
Start date:	29/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly