ID: 880328
Sample Name:
A1DB2JVWGG.CNT.exe
Cookbook: default.jbs
Time: 02:25:31
Date: 02/06/2023
Version: 37.1.0 Beryl

Table of Contents

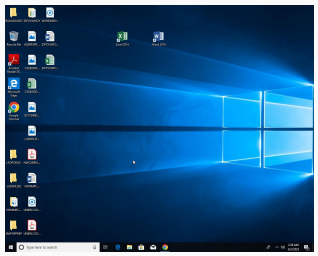
Windows Analysis Report

A1DB2JVWGG.CNT.exe

Overview

General Information

Sample Name:	A1DB2JVWGG.CNT.exe
Analysis ID:	880328
MD5:	a7817732eded…
SHA1:	e7e868e8a529…
SHA256:	95969e3e0c17…
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

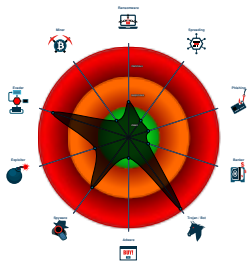
Nanocore, DarkComet

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

Signatures

- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected DarkComet
- Sigma detected: Scheduled temp fil…
- Multi AV Scanner detection for dom…

Classification



Process Tree

- **System is w10x64**
- A1DB2JVWGG.CNT.exe (PID: 7460 cmdline: C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe MD5: A7817732EDED62797B0C5E9DA109EDD7)
  - powershell.exe (PID: 7544 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7552 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 7640 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\JXayEzy.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7668 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 7660 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JXayEzy" /XML "C:\Users\user\AppData\Local\Temp\tmp12D0.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7688 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - A1DB2JVWGG.CNT.exe (PID: 7852 cmdline: C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe MD5: A7817732EDED62797B0C5E9DA109EDD7)
  - A1DB2JVWGG.CNT.exe (PID: 7908 cmdline: C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe MD5: A7817732EDED62797B0C5E9DA109EDD7)
  - A1DB2JVWGG.CNT.exe (PID: 7936 cmdline: C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe MD5: A7817732EDED62797B0C5E9DA109EDD7)
  - A1DB2JVWGG.CNT.exe (PID: 7948 cmdline: C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe MD5: A7817732EDED62797B0C5E9DA109EDD7)
    - cmd.exe (PID: 8032 cmdline: "C:\Windows\System32\cmd.exe" /k attrib "C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe" +s +h MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 8048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - attrib.exe (PID: 8096 cmdline: attrib "C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe" +s +h MD5: A5540E9F87D4CB083BDF8269DEC1CFF9)
    - cmd.exe (PID: 8040 cmdline: "C:\Windows\System32\cmd.exe" /k attrib "C:\Users\user\Desktop" +s +h MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 8064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - attrib.exe (PID: 8152 cmdline: attrib "C:\Users\user\Desktop" +s +h MD5: A5540E9F87D4CB083BDF8269DEC1CFF9)
    - JUNE STUB.EXE (PID: 8176 cmdline: "C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE" MD5: 4D9AC7D6E684CD3874B662971B6BC536)
    - notepad.exe (PID: 7292 cmdline: notepad MD5: D693F13FE3AA2010B854C4C60671B8E2)
    - msdcsc.exe (PID: 5860 cmdline: "C:\Users\user\Documents\MSDCSC\msdcsc.exe" MD5: A7817732EDED62797B0C5E9DA109EDD7)
      - powershell.exe (PID: 2680 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Documents\MSDCSC\msdcsc.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - conhost.exe (PID: 4404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 7672 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\JXayEzy.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - conhost.exe (PID: 7732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 7688 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JXayEzy" /XML "C:\Users\user\AppData\Local\Temp\tmp5A49.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 2100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - msdcsc.exe (PID: 6284 cmdline: C:\Users\user\Documents\MSDCSC\msdcsc.exe MD5: A7817732EDED62797B0C5E9DA109EDD7)
      - msdcsc.exe (PID: 6288 cmdline: C:\Users\user\Documents\MSDCSC\msdcsc.exe MD5: A7817732EDED62797B0C5E9DA109EDD7)

- JUNE STUB.EXE (PID: 8152 cmdline: "C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE" MD5: 4D9AC7D6E684CD3874B662971B6BC536)
- notepad.exe (PID: 1340 cmdline: notepad MD5: D693F13FE3AA2010B854C4C60671B8E2)

- JXayEzy.exe (PID: 7808 cmdline: C:\Users\user\AppData\Roaming\JXayEzy.exe MD5: A7817732EDED62797B0C5E9DA109EDD7)
- msdcsc.exe (PID: 7264 cmdline: "C:\Users\user\Documents\MSDCSC\msdcsc.exe" MD5: A7817732EDED62797B0C5E9DA109EDD7)
  - schtasks.exe (PID: 7804 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JXayEzy" /XML "C:\Users\user\AppData\Local\Temp\tmp9C72.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - msdcsc.exe (PID: 5840 cmdline: C:\Users\user\Documents\MSDCSC\msdcsc.exe MD5: A7817732EDED62797B0C5E9DA109EDD7)
- dhcpmon.exe (PID: 6384 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 4D9AC7D6E684CD3874B662971B6BC536)
- msdcsc.exe (PID: 7432 cmdline: "C:\Users\user\Documents\MSDCSC\msdcsc.exe" MD5: A7817732EDED62797B0C5E9DA109EDD7)
  - schtasks.exe (PID: 7612 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JXayEzy" /XML "C:\Users\user\AppData\Local\Temp\tmpE34F.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5304 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - msdcsc.exe (PID: 5100 cmdline: C:\Users\user\Documents\MSDCSC\msdcsc.exe MD5: A7817732EDED62797B0C5E9DA109EDD7)
  - msdcsc.exe (PID: 5236 cmdline: C:\Users\user\Documents\MSDCSC\msdcsc.exe MD5: A7817732EDED62797B0C5E9DA109EDD7)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Nanocore RAT, NanoCore	Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.	• APT33 • The Gorgon Group	**http://** https://assets.virustotal.com/reports/2021trends.pdfhttps://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/https://blog.morphisec.com/syk-crypter-discord	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.nanocore

Name	Description	Attribution	Blogpost URLs	Link
DarkComet	DarkComet is one of the most famous RATs, developed by Jean-Pierre Lesueur in 2008. After being used in the Syrian civil war in 2011, Lesuer decided to stop developing the trojan. Indeed, DarkComet is able to enable control over a compromised system through use of a simple graphic user interface. Experts think that this user friendliness is the key of its mass success.	• APT33 • Lazarus Group • Operation C-Major	**http://** contagiodump.blogspot.com/2012/06/rat-samples-from-syrian-targeted.htmlhttps://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-1-darkcomet/https://blog.malwarebytes.com/threat-analysis/2012/10/dark-comet-2-electric-boogaloo/https://blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.htmlhttps://blog.talosintelligence.com/2022/06/avoslocker-new-arsenal.html	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.darkcomet

Malware Configuration

Threatname: DarkComet

```
{
  "MUTEX": "DC_MUTEX-75NC51J",
  "SID": "JUNE 2023",
  "FWB": "0",
  "NETDATA": [
    "timmy08.ddns.net:39399"
  ],
  "GENCODE": "l2V3BCJaaFmA",
  "INSTALL": "1",
  "COMBOPATH": "7",
  "EDTPATH": "MSDCSC\\msdcsc.exe",
  "KEYNAME": "chrome",
  "EDTDATE": "16/04/2007",
  "PERSINST": "1",
  "MELT": "1",
  "CHANGEDATE": "0",
  "DIRATTRIB": "6",
  "FILEATTRIB": "6",
  "SH1": "1",
  "SH3": "1",
  "SH7": "1",
  "SH8": "1",
  "SH9": "1",
  "CHIDEF": "1",
  "CHIDED": "1",
  "PERS": "1",
  "OFFLINEK": "1",
  "BIND": "1",
  "MULTIBIND": "1"
}
```


Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "29684d78-e3d5-43d3-a123-9a499c31",
  "Group": "JUNE 2023",
  "Domain1": "timmy08.ddns.net",
  "Domain2": "timmy06.ddns.net",
  "Port": 28289,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	0xff05:$x1: NanoCore Client.exe 0x1018d:$x2: NanoCore.ClientPluginHost 0x117c6:$s1: PluginCommand 0x117ba:$s2: FileCommand 0x1266b:$s3: PipeExists 0x18422:$s4: PipeCreated 0x101b7:$s5: IClientLoggingHost
C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	0xfef5:$x1: NanoCore Client 0xff05:$x1: NanoCore Client 0x1014d:$x2: NanoCore.ClientPlugin 0x1018d:$x3: NanoCore.ClientPluginHost 0x10142:$i1: IClientApp 0x10163:$i2: IClientData 0x1016f:$i3: IClientNetwork 0x1017e:$i4: IClientAppHost 0x101a7:$i5: IClientDataHost 0x101b7:$i6: IClientLoggingHost 0x101ca:$i7: IClientNetworkHost 0x101dd:$i8: IClientUIHost 0x101eb:$i9: IClientNameObjectCollection 0x10207:$i10: IClientReadOnlyNameObjectCollection 0xff54:$s1: ClientPlugin 0x10156:$s1: ClientPlugin 0x1064a:$s2: EndPoint 0x10653:$s3: IPAddress 0x1065d:$s4: IPEndPoint 0x12093:$s6: get_ClientSettings 0x12637:$s7: get_Connected
C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xfef5:$a: NanoCore 0xff05:$a: NanoCore 0x10139:$a: NanoCore 0x1014d:$a: NanoCore 0x1018d:$a: NanoCore 0xff54:$b: ClientPlugin 0x10156:$b: ClientPlugin 0x10196:$b: ClientPlugin 0x1007b:$c: ProjectData 0x10a82:$d: DESCrypto 0x1844e:$e: KeepAlive 0x1643c:$g: LogClientMessage 0x12637:$i: get_Connected 0x10db8:$j: #=q 0x10de8:$j: #=q 0x10e04:$j: #=q 0x10e34:$j: #=q 0x10e50:$j: #=q 0x10e6c:$j: #=q 0x10e9c:$j: #=q 0x10eb8:$j: #=q

Click to see the 7 entries

Memory Dumps

Source	Rule	Description	Author	Strings
00000020.00000002.622990283.0000000002C81000.00000004.00001000.00020000.00000000.sdmp	DarkComet_2	DarkComet	Jean-Philippe Teissier / @Jipe_	0xf58:$b: #EOF DARKCOMET DATA -- 0xfd7:$c: DC_MUTEX-
00000027.00000002.468665185.0000000002E81000.00000004.00001000.00020000.00000000.sdmp	DarkComet_2	DarkComet	Jean-Philippe Teissier / @Jipe_	0xf08:$a: #BEGIN DARKCOMET DATA -- 0xfd0:$a: #BEGIN DARKCOMET DATA -- 0xee0:$b: #EOF DARKCOMET DATA -- 0xfaf:$c: DC_MUTEX-
00000027.00000002.468665185.0000000002E7A000.00000004.00001000.00020000.00000000.sdmp	DarkComet_2	DarkComet	Jean-Philippe Teissier / @Jipe_	0x948:$c: DC_MUTEX-
00000013.00000002.639756642.0000000006C60000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	0x5b0b:$x1: NanoCore.ClientPluginHost 0x5b44:$x2: IClientNetworkHost
00000013.00000002.639756642.0000000006C60000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	0x5b0b:$x2: NanoCore.ClientPluginHost 0x5c0f:$s4: PipeCreated 0x5b25:$s5: IClientLoggingHost

Click to see the 199 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
19.2.JUNE STUB.EXE.6c40000.16.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	0x16e3:$x1: NanoCore.ClientPluginHost 0x171c:$x2: IClientNetworkHost
19.2.JUNE STUB.EXE.6c40000.16.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	0x16e3:$x2: NanoCore.ClientPluginHost 0x1800:$s4: PipeCreated 0x16fd:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
19.2.JUNE STUB.EXE.6c40000.16.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x175f:$x2: NanoCore.ClientPlugin • 0x16e3:$x3: NanoCore.ClientPluginHost • 0x1775:$i3: IClientNetwork • 0x16fd:$i6: IClientLoggingHost • 0x171c:$i7: IClientNetworkHost • 0x1491:$s1: ClientPlugin • 0x1768:$s1: ClientPlugin
19.2.JUNE STUB.EXE.6c40000.16.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x16e3:$a1: NanoCore.ClientPluginHost • 0x175f:$a2: NanoCore.ClientPlugin • 0x16fd:$b9: IClientLoggingHost
19.2.JUNE STUB.EXE.6ce0000.23.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
Click to see the 344 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230

Timestamp:	192.168.2.35.252.165.23049702282892025019 06/02/23-02:26:44.385767
SID:	2025019
Source Port:	49702
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN DarkComet-RAT init connection 2 - Source IP: 5.252.165.230 - Destination IP: 192.168.2.3

Timestamp:	5.252.165.230192.168.2.339399497042806577 06/02/23-02:27:01.218517
SID:	2806577
Source Port:	39399
Destination Port:	49704
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230

Timestamp:	192.168.2.35.252.165.23049711282892025019 06/02/23-02:27:54.203652

SID:	2025019
Source Port:	49711
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230

Timestamp:	192.168.2.35.252.165.23049713282892025019 06/02/23-02:28:03.961219
SID:	2025019
Source Port:	49713
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230

Timestamp:	192.168.2.35.252.165.23049705282892025019 06/02/23-02:27:16.433852
SID:	2025019
Source Port:	49705
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230

Timestamp:	192.168.2.35.252.165.23049712282892025019 06/02/23-02:27:59.459924
SID:	2025019
Source Port:	49712
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230

Timestamp:	192.168.2.35.252.165.23049716282892025019 06/02/23-02:28:22.359438
SID:	2025019
Source Port:	49716
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230

Timestamp:	192.168.2.35.252.165.23049706282892025019 06/02/23-02:27:24.140871
SID:	2025019
Source Port:	49706
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230

Timestamp:	192.168.2.35.252.165.23049708282892025019 06/02/23-02:27:35.526983
SID:	2025019
Source Port:	49708
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230

Timestamp:	192.168.2.35.252.165.23049707282892025019 06/02/23-02:27:28.447502
SID:	2025019
Source Port:	49707
Destination Port:	28289
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049713282892816718 06/02/23-02:28:05.016410
SID:	2816718
Source Port:	49713
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049702282892816718 06/02/23-02:26:45.935768
SID:	2816718
Source Port:	49702
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049710282892025019 06/02/23-02:27:47.888873
SID:	2025019
Source Port:	49710
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049708282892816766 06/02/23-02:27:36.099395
SID:	2816766
Source Port:	49708
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049707282892816766 06/02/23-02:27:29.300655
SID:	2816766
Source Port:	49707
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049709282892816766 06/02/23-02:27:43.508322
SID:	2816766
Source Port:	49709
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049706282892816766 06/02/23-02:27:24.211225
SID:	2816766
Source Port:	49706
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049716282892816766 06/02/23-02:28:25.005929

SID:	2816766
Source Port:	49716
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049709282892025019 06/02/23-02:27:41.004326
SID:	2025019
Source Port:	49709
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN DarkComet-RAT server join acknowledgement 2 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049704393992806578 06/02/23-02:27:01.218732
SID:	2806578
Source Port:	49704
Destination Port:	39399
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN DarkComet-RAT activity - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049704393992807821 06/02/23-02:28:23.003919
SID:	2807821
Source Port:	49704
Destination Port:	39399
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049710282892816766 06/02/23-02:27:48.244529
SID:	2816766
Source Port:	49710
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049711282892816766 06/02/23-02:27:54.312190
SID:	2816766
Source Port:	49711
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 5.252.165.230 - Destination IP: 192.168.2.3	
Timestamp:	5.252.165.230192.168.2.328289497142841753 06/02/23-02:28:11.405336
SID:	2841753
Source Port:	28289
Destination Port:	49714
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049702282892816766 06/02/23-02:26:46.881522
SID:	2816766
Source Port:	49702
Destination Port:	28289
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049712282892816766 06/02/23-02:27:59.647498
SID:	2816766
Source Port:	49712
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049713282892816766 06/02/23-02:28:06.982149
SID:	2816766
Source Port:	49713
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 5.252.165.230 - Destination IP: 192.168.2.3	
Timestamp:	5.252.165.230192.168.2.328289497062810290 06/02/23-02:27:24.236176
SID:	2810290
Source Port:	28289
Destination Port:	49706
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 5.252.165.230 - Destination IP: 192.168.2.3	
Timestamp:	5.252.165.230192.168.2.328289497032841753 06/02/23-02:27:02.943535
SID:	2841753
Source Port:	28289
Destination Port:	49703
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049714282892816766 06/02/23-02:28:11.424790
SID:	2816766
Source Port:	49714
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049715282892816766 06/02/23-02:28:17.957593
SID:	2816766
Source Port:	49715
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049703282892816766 06/02/23-02:27:05.840215
SID:	2816766
Source Port:	49703
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049705282892816766 06/02/23-02:27:18.414247

SID:	2816766
Source Port:	49705
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 5.252.165.230 - Destination IP: 192.168.2.3	
Timestamp:	5.252.165.230192.168.2.328289497122841753 06/02/23-02:27:59.490400
SID:	2841753
Source Port:	28289
Destination Port:	49712
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 5.252.165.230 - Destination IP: 192.168.2.3	
Timestamp:	5.252.165.230192.168.2.328289497102841753 06/02/23-02:27:47.915148
SID:	2841753
Source Port:	28289
Destination Port:	49710
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 5.252.165.230 - Destination IP: 192.168.2.3	
Timestamp:	5.252.165.230192.168.2.328289497112841753 06/02/23-02:27:54.245563
SID:	2841753
Source Port:	28289
Destination Port:	49711
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 5.252.165.230 - Destination IP: 192.168.2.3	
Timestamp:	5.252.165.230192.168.2.328289497062841753 06/02/23-02:27:24.193892
SID:	2841753
Source Port:	28289
Destination Port:	49706
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 5.252.165.230 - Destination IP: 192.168.2.3	
Timestamp:	5.252.165.230192.168.2.328289497072841753 06/02/23-02:27:28.477912
SID:	2841753
Source Port:	28289
Destination Port:	49707
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 5.252.165.230 - Destination IP: 192.168.2.3	
Timestamp:	5.252.165.230192.168.2.328289497082841753 06/02/23-02:27:35.555003
SID:	2841753
Source Port:	28289
Destination Port:	49708
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049715282892025019 06/02/23-02:28:16.130201
SID:	2025019
Source Port:	49715
Destination Port:	28289
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049703282892025019 06/02/23-02:26:52.916534
SID:	2025019
Source Port:	49703
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 5.252.165.230	
Timestamp:	192.168.2.35.252.165.23049714282892025019 06/02/23-02:28:11.375206
SID:	2025019
Source Port:	49714
Destination Port:	28289
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Yara detected Nanocore RAT
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- Snort IDS alert for network traffic
- Uses dynamic DNS services
- C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

- Installs a global keyboard hook

E-Banking Fraud

- Yara detected Nanocore RAT

System Summary

- Malicious sample detected (through community Yara rule)
- Yara detected DarkComet

Data Obfuscation

.NET source code contains potential unpacker

Persistence and Installation Behavior

Uses cmd line tools excessively to alter registry or file data

Drops PE files to the document folder of the user

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Creates a thread in another existing process (thread injection)

Adds a directory exclusion to Windows Defender

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings

Changes security center settings (notifications, updates, antivirus, firewall)

Disables the Windows task manager (taskmgr)

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

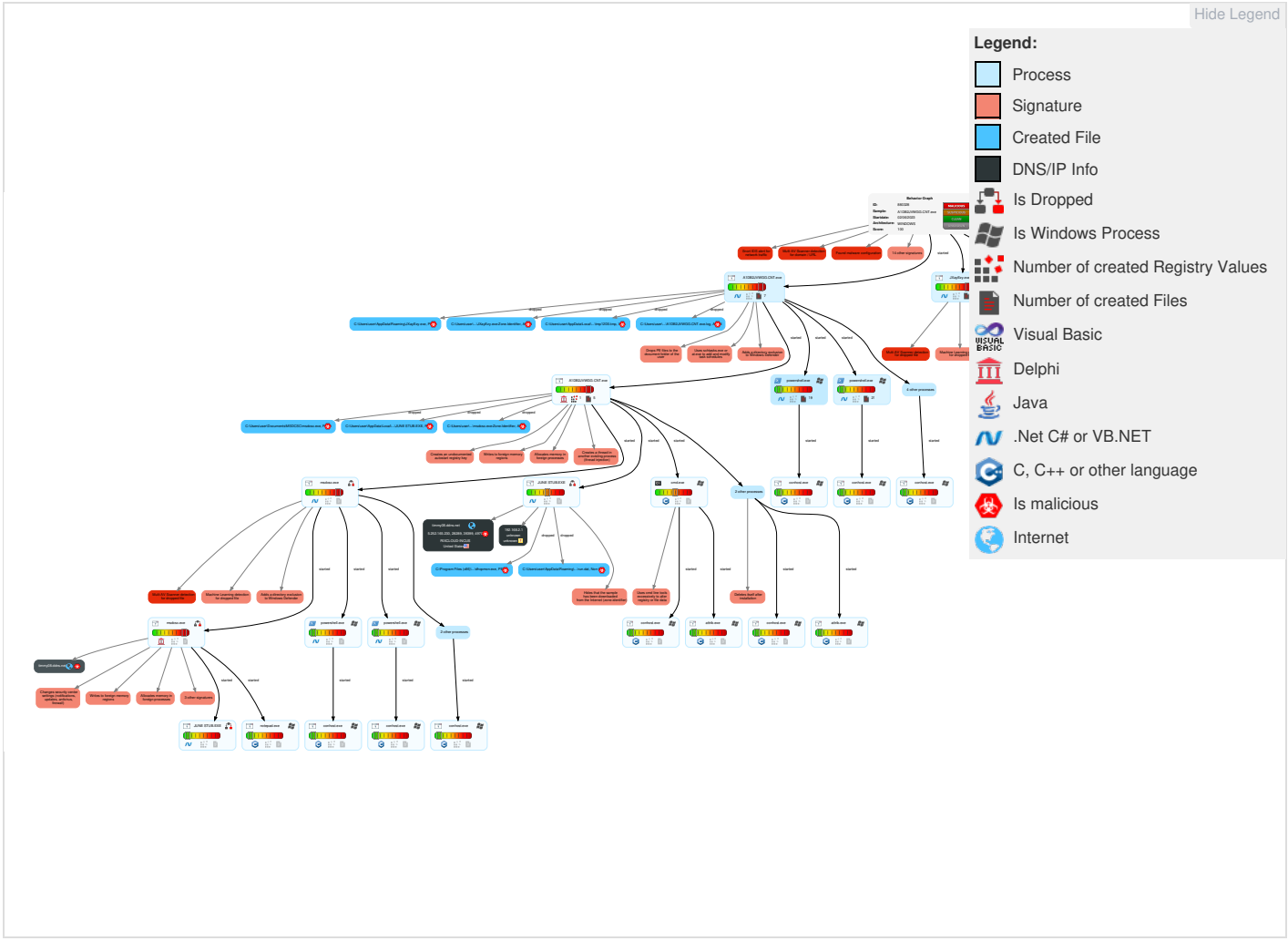
Yara detected Nanocore RAT

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
Valid Accounts	1 Windows Management Instrumentation	1 LSASS Driver	1 LSASS Driver	3 1 Disable or Modify Tools	1 2 1 Input Capture	1 2 File and Directory Discovery	Remote Services	1 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	1 Command and Scripting Interpreter	1 DLL Side-Loading	1 DLL Side-Loading	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	2 2 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 Scheduled Task/Job	1 Windows Service	1 Access Token Manipulation	4 Obfuscated Files or Information	Security Account Manager	1 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 2 1 Input Capture	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	1 Scheduled Task/Job	1 Windows Service	1 3 Software Packing	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	1 1 Registry Run Keys / Startup Folder	4 1 2 Process Injection	1 DLL Side-Loading	LSA Secrets	2 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	1 Scheduled Task/Job	1 File Deletion	Cached Domain Credentials	1 Application Window 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	1 1 Registry Run Keys / Startup Folder	2 Masquerading	DCSync	1 Remote System Discovery	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	Network Service Scanning	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)	1 Access Token Manipulation	/etc/passwd and /etc/shadow	System Network Connections 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)	4 1 2 Process Injection	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 Hidden Files and Directories	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

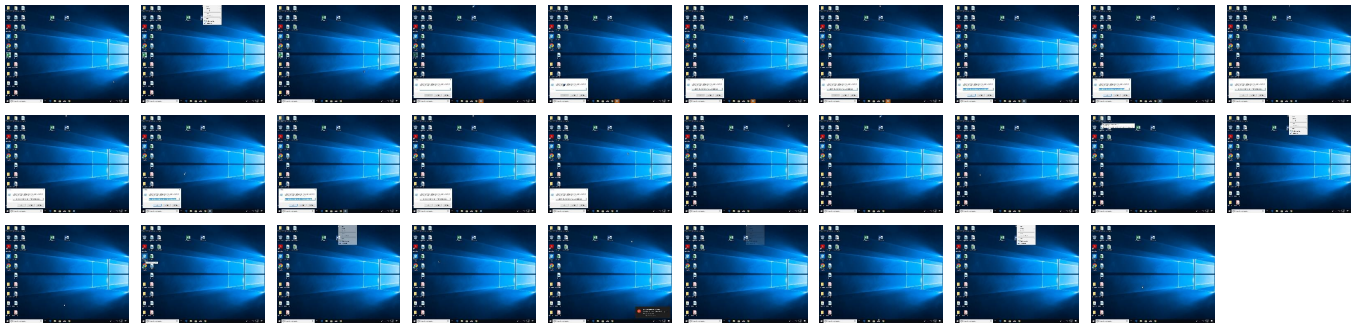
Behavior Graph



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
A1DB2JVWGG.CNT.exe	22%	ReversingLabs	Win32.Trojan.Generic	
A1DB2JVWGG.CNT.exe	30%	Virustotal		Browse
A1DB2JVWGG.CNT.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\Documents\MSDCSC\msdcsc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\JXayEzy.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\JXayEzy.exe	27%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\Documents\MSDCSC\msdcsc.exe	27%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
timmy08.ddns.net	13%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnK	0%	URL Reputation	safe	
http://www.founder.com.cn/cnK	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/H	0%	URL Reputation	safe	
http://www.founder.com.cn/cnU	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://www.founder.com.cn/cnw	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/m	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.carterandcone.comtig	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/A	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://en.wikip	0%	URL Reputation	safe	
http://www.carterandcone.comto	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn-	0%	URL Reputation	safe	
http://www.founder.com.cn/cn9	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/_	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/_	0%	URL Reputation	safe	
http://www.fontbureau.comceu3	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/r-f	0%	Avira URL Cloud	safe	
timmy06.ddns.net	100%	Avira URL Cloud	malware	
timmy08.ddns.net	100%	Avira URL Cloud	malware	
timmy08.ddns.net	13%	Virustotal		Browse
http://www.jiyu-kobo.co.jp/r-f	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
timmy08.ddns.net	5.252.165.230	true	true	• 13%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
timmy08.ddns.net	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
timmy06.ddns.net	true	• Avira URL Cloud: malware	unknown

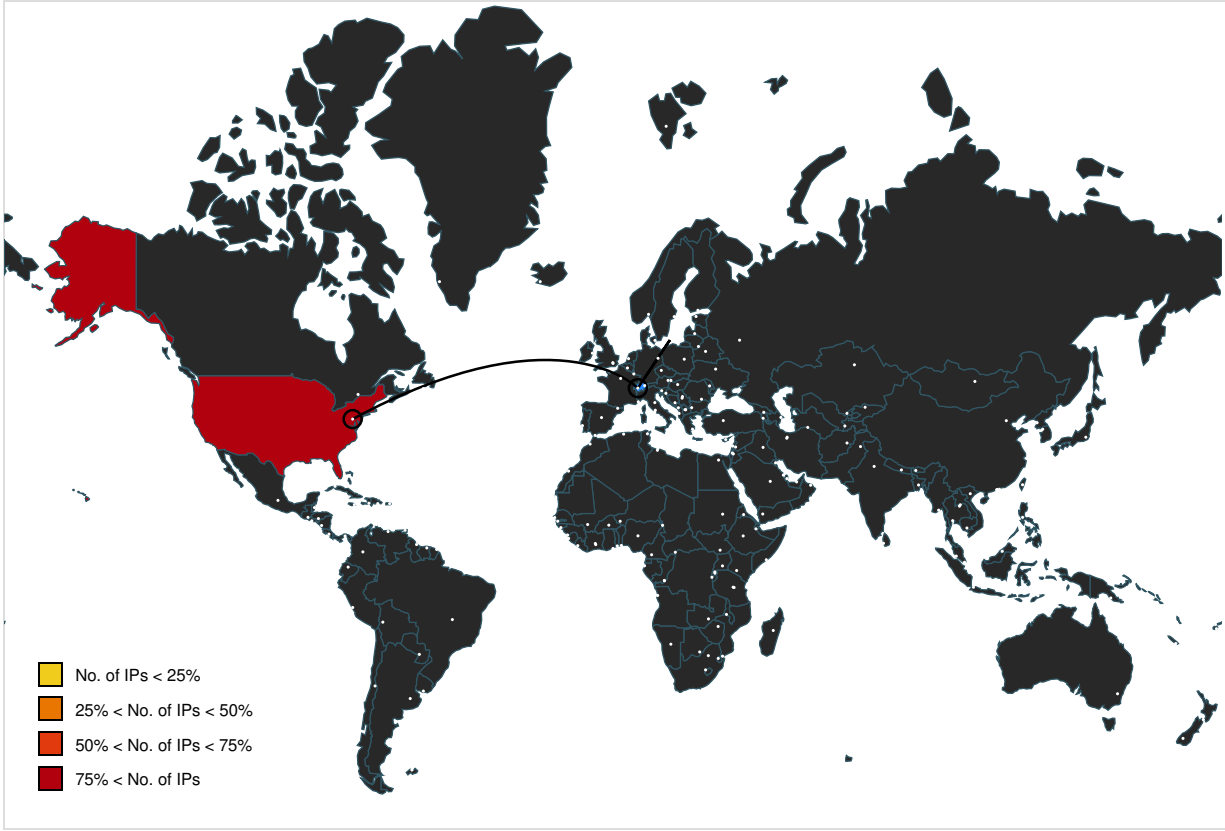
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnK	A1DB2JVWGG.CNT.exe, 00000000.00000003.358248155.0000000005DBC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comceu3	A1DB2JVWGG.CNT.exe, 00000000.00000003.384541193.0000000005DB0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/H	A1DB2JVWGG.CNT.exe, 00000000.00000003.359124042.0000000005DB7000.00000004.00000020.00020000.00000000.sdmp, A1DB2JVWGG.CNT.exe, 00000000.00000003.359247918.0000000005DB7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnU	A1DB2JVWGG.CNT.exe, 00000000.00000003.358248155.0000000005DBC000.00000004.00000020.00020000.00000000.sdmp, A1DB2JVWGG.CNT.exe, 00000000.00000003.358336012.0000000005DBC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com	JUNE STUB.EXE, 00000013.00000002.625066874.00000000033FB000.00000004.00000800.00020000.00000000.sdmp, JUNE STUB.EXE, 00000013.00000002.640195396.0000000006CA0000.00000004.08000000.00040000.00000000.sdmp	false		high
http://www.sajatypeworks.com	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	A1DB2JVWGG.CNT.exe, 00000000.00000002.44 1824981.0000000006EC2000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/3	A1DB2JVWGG.CNT.exe, 00000000.00000003.35 9124042.0000000005DB7000.00000004.000000 20.00020000.00000000.sdmp, A1DB2JVWGG.CN T.exe, 00000000.00000003.359247918.00000 00005DB7000.00000004.00000020.00020000.0 0000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/r-f	A1DB2JVWGG.CNT.exe, 00000000.00000003.35 9124042.0000000005DB7000.00000004.000000 20.00020000.00000000.sdmp, A1DB2JVWGG.CN T.exe, 00000000.00000003.359247918.00000 00005DB7000.00000004.00000020.00020000.0 0000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnw	A1DB2JVWGG.CNT.exe, 00000000.00000003.35 8248155.0000000005DBC000.00000004.000000 20.00020000.00000000.sdmp, A1DB2JVWGG.CN T.exe, 00000000.00000003.358336012.00000 00005DBC000.00000004.00000020.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/m	A1DB2JVWGG.CNT.exe, 00000000.00000003.35 9124042.0000000005DB7000.00000004.000000 20.00020000.00000000.sdmp, A1DB2JVWGG.CN T.exe, 00000000.00000003.359247918.00000 00005DB7000.00000004.00000020.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	A1DB2JVWGG.CNT.exe, 00000000.00000002.44 1824981.0000000006EC2000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	A1DB2JVWGG.CNT.exe, 00000000.00000002.44 1824981.0000000006EC2000.00000004.000008 00.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/%	A1DB2JVWGG.CNT.exe, 00000000.00000003.35 9124042.0000000005DB7000.00000004.000000 20.00020000.00000000.sdmp, A1DB2JVWGG.CN T.exe, 00000000.00000003.359247918.00000 00005DB7000.00000004.00000020.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kr	A1DB2JVWGG.CNT.exe, 00000000.00000002.44 1824981.0000000006EC2000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	A1DB2JVWGG.CNT.exe, 00000000.00000002.44 1824981.0000000006EC2000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	A1DB2JVWGG.CNT.exe, 00000000.00000002.44 1824981.0000000006EC2000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/nam e	A1DB2JVWGG.CNT.exe, 00000000.00000002.39 2562881.0000000002F01000.00000004.000008 00.00020000.00000000.sdmp, msdcsc.exe, 0 0000015.00000002.442690195.0000000002F21 000.00000004.00000800.00020000.00000000.sdmp, msdcsc.exe, 00000016.00000002.475372371.0000 0000033B7000.00000004.00000800.00020000. 00000000.sdmp, msdcsc.exe, 00000024.0000 0002.512029267.0000000003097000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	A1DB2JVWGG.CNT.exe, 00000000.00000002.44 1824981.0000000006EC2000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnd	A1DB2JVWGG.CNT.exe, 00000000.00000003.35 8248155.0000000005DBC000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comtig	A1DB2JVWGG.CNT.exe, 00000000.00000003.35 8704115.0000000005DB3000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	A1DB2JVWGG.CNT.exe, 00000000.00000002.44 1824981.0000000006EC2000.00000004.000008 00.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	A1DB2JVWGG.CNT.exe, 00000000.00000002.44 1824981.0000000006EC2000.00000004.000008 00.00020000.00000000.sdmp, A1DB2JVWGG.CN T.exe, 00000000.00000003.384541193.00000 00005DB0000.00000004.00000020.00020000.0 0000000.sdmp	false		high
http://www.founder.com.cn/cn/H	A1DB2JVWGG.CNT.exe, 00000000.00000003.35 8336012.0000000005DBC000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/A	A1DB2JVWGG.CNT.exe, 00000000.00000003.359124042.0000000005DB7000.00000004.00000020.00020000.00000000.sdmp, A1DB2JVWGG.CNT.exe, 00000000.00000003.359247918.00000005DB7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	A1DB2JVWGG.CNT.exe, 00000000.00000003.359124042.0000000005DB7000.00000004.00000020.00020000.00000000.sdmp, A1DB2JVWGG.CNT.exe, 00000000.00000003.359247918.00000005DB7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.wikip	A1DB2JVWGG.CNT.exe, 00000000.00000003.358071188.0000000005DBE000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comto	A1DB2JVWGG.CNT.exe, 00000000.00000003.358704115.0000000005DB3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	A1DB2JVWGG.CNT.exe, 00000000.00000003.358248155.0000000005DBC000.00000004.00000020.00020000.00000000.sdmp, A1DB2JVWGG.CNT.exe, 00000000.00000003.358336012.00000005DBC000.00000004.00000020.00020000.00000000.sdmp, A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn-	A1DB2JVWGG.CNT.exe, 00000000.00000003.358248155.0000000005DBC000.00000004.00000020.00020000.00000000.sdmp, A1DB2JVWGG.CNT.exe, 00000000.00000003.358336012.00000005DBC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn9	A1DB2JVWGG.CNT.exe, 00000000.00000003.358248155.0000000005DBC000.00000004.00000020.00020000.00000000.sdmp, A1DB2JVWGG.CNT.exe, 00000000.00000003.358336012.00000005DBC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comm	A1DB2JVWGG.CNT.exe, 00000000.00000002.441627539.0000000005DB8000.00000004.00000020.00020000.00000000.sdmp, A1DB2JVWGG.CNT.exe, 00000000.00000003.384541193.00000005DB0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	A1DB2JVWGG.CNT.exe, 00000000.00000003.359124042.0000000005DB7000.00000004.00000020.00020000.00000000.sdmp, A1DB2JVWGG.CNT.exe, 00000000.00000003.359247918.00000005DB7000.00000004.00000020.00020000.00000000.sdmp, A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	A1DB2JVWGG.CNT.exe, 00000000.00000002.441824981.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/_	A1DB2JVWGG.CNT.exe, 00000000.00000003.359124042.0000000005DB7000.00000004.00000020.00020000.00000000.sdmp, A1DB2JVWGG.CNT.exe, 00000000.00000003.359247918.00000005DB7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.252.165.230	timmy08.ddns.net	United States		64271	RIXCLOUD-INCUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	880328
Start date and time:	2023-06-02 02:25:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	46
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
Sample file name:	A1DB2JVWGG.CNT.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@67/28@15/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 90.6%) • Quality average: 72.7% • Quality standard deviation: 31.8%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
02:26:28	API Interceptor	2x Sleep call for process: A1DB2JVWGG.CNT.exe modified
02:26:32	Task Scheduler	Run new task: JXayEzy path: C:\Users\user\AppData\Roaming\JXayEzy.exe
02:26:32	API Interceptor	131x Sleep call for process: powershell.exe modified
02:26:39	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run chrome C:\Users\user\Documents\MSDCSC\msdcsc.exe
02:26:41	API Interceptor	459x Sleep call for process: JUNE STUB.EXE modified
02:26:46	API Interceptor	752x Sleep call for process: msdcsc.exe modified
02:26:47	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
02:26:57	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run chrome C:\Users\user\Documents\MSDCSC\msdcsc.exe
02:27:03	API Interceptor	1x Sleep call for process: JXayEzy.exe modified

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:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.448476558203999
Encrypted:	false
SSDEEP:	6144:gLV6Bta6dtJmakIM5W4w9QT09e8iCp1Tz5kl7:gLV6BtpmkjIlc8iCp1P5kl7
MD5:	4D9AC7D6E684CD3874B662971B6BC536
SHA1:	726CD96B680082910EBC451D7741A2D6934ED339
SHA-256:	48987956556721DFB5F988683693BEBC094B5965F6BD58EEFF928FD7C6BA9330
SHA-512:	27DDC60B921ED3B6B9223321EA310FA6CE9A3F4D0CB1B96899FC8FB08556D73F92FB3EC7DA93A60DE046105129B1B128828D5AB57869160749A5F7F2A7A8AB71
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. ..... .....8...W.... ...]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc....]... ...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....- (&s8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0 ..$.....~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\JUNE STUB.EXE.log

Process:	C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06

Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\A1DB2JVWGG.CNT.exe.log

Process:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1302
Entropy (8bit):	5.3499841584777394
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84bE4Ks:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	4664C2114894A4BFC1E657FC08C72FF4
SHA1:	95A1E14E2AD65BCA561261DA3899074BF5276AED
SHA-256:	6E36229D13672B4304C696812B365F2E5657875DD0E11F13AE010566CC87607A
SHA-512:	4E7862716D5C0BC2174E819BAB329A2974FE83A36D5417EE732AB2F3D77D95620B3D462A1C9608F5FE90A48030140DE53DB642F8C370CD8E191BDBE83C638CA1
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Users\user\AppData\Roaming\JXayEzy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1302
Entropy (8bit):	5.3499841584777394
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84bE4Ks:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	4664C2114894A4BFC1E657FC08C72FF4
SHA1:	95A1E14E2AD65BCA561261DA3899074BF5276AED
SHA-256:	6E36229D13672B4304C696812B365F2E5657875DD0E11F13AE010566CC87607A
SHA-512:	4E7862716D5C0BC2174E819BAB329A2974FE83A36D5417EE732AB2F3D77D95620B3D462A1C9608F5FE90A48030140DE53DB642F8C370CD8E191BDBE83C638CA1
Malicious:	false

Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	21860
Entropy (8bit):	5.5972826889109575
Encrypted:	false
SSDEEP:	384:WtCRLq0DKA7vZF+0oj8nYSBxouleWiJ9glSJ3uyzSv0ZqbAVrd3sffBT+iRYc:5V0diY4iuleOlcuBs4wk+c
MD5:	0053A5FE80C85D084F9273222792DE1C
SHA1:	E9518C301A6C283676FF55B86C23831F40AF019E
SHA-256:	22B5F051CEE4CC570A86DB41F8F1ADADEF798462A25C27A8B7B7AA382288881A
SHA-512:	3BC8313C2DBE0AF84FB75700F85E81A79BD58F65AB9694DA7D09B5FC392CC8316F779036E242658BF691BC5752F980881763DBC3A9D58C5350A95668D6347012
Malicious:	false
Preview:	@...e.....c.f.....D.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE

Process:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	207360
Entropy (8bit):	7.448476558203999
Encrypted:	false
SSDEEP:	6144:gLV6Bta6dtJmakIM5W4w9QT09e8iCp1Tz5kl7:gLV6BtpmkjIlc8iCp1P5kl7
MD5:	4D9AC7D6E684CD3874B662971B6BC536
SHA1:	726CD96B680082910EBC451D7741A2D6934ED339
SHA-256:	48987956556721DFB5F988683693BEBC094B5965F6BD58EEFF928FD7C6BA9330
SHA-512:	27DDC60B921ED3B6B9223321EA310FA6CE9A3F4D0CB1B96899FC8FB08556D73F92FB3EC7DA93A60DE046105129B1B128828D5AB57869160749A5F7F2A7A8AB71
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. .....8...W.... ...]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc....]...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$.....~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2dokkkyb.5a3.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U

MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ccef3fwz.eck.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_d5tgwwwd.pky.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hzblhftc.ghg.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kq5n4yzc.iw1.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)

Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qo2objni.hng.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uzgv2wkw.yz4.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wdxwza43.sz1.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp12D0.tmp	
Process:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1594
Entropy (8bit):	5.151574547335532
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtSxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTWv
MD5:	B8801377A791997FBC93D3EDC361C57F
SHA1:	CBC782BC13AAD45C48C7DE025F1478F065FF38BB
SHA-256:	EBBCB00843283918F69415DF2D0FE78D7239527A592F03E65F296EEE3F9FB4E4
SHA-512:	4A68B1BED4CEDE648A1AD0BE535DB587844AE8D69E742C49DA0F3EE0B01F3F983E96F21F77CE9CE69BC3204F57AA91B289253E25FF118B74FCDC1329A4004C49
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmp5A49.tmp	
Process:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1594
Entropy (8bit):	5.151574547335532
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtSxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTWv
MD5:	B8801377A791997FBC93D3EDC361C57F
SHA1:	CBC782BC13AAD45C48C7DE025F1478F065FF38BB
SHA-256:	EBBCB00843283918F69415DF2D0FE78D7239527A592F03E65F296EEE3F9FB4E4
SHA-512:	4A68B1BED4CEDE648A1AD0BE535DB587844AE8D69E742C49DA0F3EE0B01F3F983E96F21F77CE9CE69BC3204F57AA91B289253E25FF118B74FCDC1329A4004C49
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmp9C72.tmp	
Process:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1594
Entropy (8bit):	5.151574547335532
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtSxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTWv
MD5:	B8801377A791997FBC93D3EDC361C57F
SHA1:	CBC782BC13AAD45C48C7DE025F1478F065FF38BB
SHA-256:	EBBCB00843283918F69415DF2D0FE78D7239527A592F03E65F296EEE3F9FB4E4
SHA-512:	4A68B1BED4CEDE648A1AD0BE535DB587844AE8D69E742C49DA0F3EE0B01F3F983E96F21F77CE9CE69BC3204F57AA91B289253E25FF118B74FCDC1329A4004C49
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmpE34F.tmp	
Process:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1594
Entropy (8bit):	5.151574547335532
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOilQRvh7hwrgXuNtSxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTWv
MD5:	B8801377A791997FBC93D3EDC361C57F
SHA1:	CBC782BC13AAD45C48C7DE025F1478F065FF38BB
SHA-256:	EBBCB00843283918F69415DF2D0FE78D7239527A592F03E65F296EEE3F9FB4E4
SHA-512:	4A68B1BED4CEDE648A1AD0BE535DB587844AE8D69E742C49DA0F3EE0B01F3F983E96F21F77CE9CE69BC3204F57AA91B289253E25FF118B74FCDC1329A4004C49
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:eWt:eWt
MD5:	628DD28222B41ED590BE807455B900F4
SHA1:	B2D20B6D905CDFA73EE48A63D68CDBC2CB95544E
SHA-256:	F55D454E585D202858EA0F2DC330BC6D72C2A80B89E8D307C1CDD1D007FDAA9B
SHA-512:	8FA90F6F764BD6504218CF1DC312B0CA15423B83386339D3030CEA23D33966B5C3F638A27D38DA418767BDC765EA9D409BE340D9DF76D726878BF85EA95C0AE
Malicious:	**true**
Preview:	m.qyKc.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false

SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat

Process:	C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE
File Type:	data
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2C
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.l'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`']..Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...."..bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9..j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\JXayEzy.exe

Process:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2223104
Entropy (8bit):	7.68131929551722
Encrypted:	false
SSDEEP:	24576:tA74/4qimDN0nixgBQcZ+WtGsK0i+CqBRCJcbpaa4S7qeL7pjhlyIy6Vs6wGpYUa:tA74/t6FQcZ+WRs+BRL4ShjTyIF
MD5:	A7817732EDED62797B0C5E9DA109EDD7
SHA1:	E7E868E8A529CDD6BD32B4FA3711EFF0C9029DBB
SHA-256:	95969E3E0C1793E6177D5C5D20C9A667C9F28BB64907AD489682C41668EFC29D
SHA-512:	3664953E0E5C601E8D8123C0B9F3F43D727BF6F48F81A93FED051D6F0D275728CEDA92ECEF201E4CDCEAC29C17CE66B46820A43A6DAC9FD4B77B6D54F226D01
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...F.xd.....0..F.....e... .....@.. .....`".....@.....<e..O.....,.....@".....\&..T..... ..... ..H.....text....E... ...F..... ..`.rsrc...,.....H.....@..@.reloc.....@".....!.....@..B.....pe.....H.....K..$.....$...8/.....0..).....{.....{....t.....|.....(...+...3.*....0..).....{.....{....t.....|.....(...+...3.*...}.....}.....(.....{.....{....o....&*.0..$.....r...pr7..p.. (.....,..(.....*.0.....{....o....&.{.....o.....{....(...o!....{....(...o!....{....(...o!....{....(...o!....{....(...o!....{....(...o!....{....(...o!....{....(...o!....*...0..-.....{....o".....,..{.....o.....+..{...

C:\Users\user\AppData\Roaming\JXayEzy.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309

SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\MSDCSC\msdcsc.exe

Process:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2223104
Entropy (8bit):	7.68131929551722
Encrypted:	false
SSDEEP:	24576:tA74/4qimDN0nixgBQcZ+WtGsK0i+CqBRCJcbpaa4S7qeL7pjhlyIy6Vs6wGpYUa:tA74/t6FQcZ+WRs+BRL4ShjTyIF
MD5:	A7817732EDED62797B0C5E9DA109EDD7
SHA1:	E7E868E8A529CDD6BD32B4FA3711EFF0C9029DBB
SHA-256:	95969E3E0C1793E6177D5C5D20C9A667C9F28BB64907AD489682C41668EFC29D
SHA-512:	3664953E0E5C601E8D8123C0B9F3F43D727BF6F48F81A93FED051D6F0D275728CEDA92ECEF201E4CDCEAC29C17CE66B46820A43A6DAC9FD4B77B6D54F226DB01
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...F.xd.....0..F.....e... .....@.. .....`".....@.....<e..O.....,.....@".....\&..T..... ..... ..H.....text....E... ...F..... ..`.rsrc...,.....H.....@..@.reloc.....@".....!.....@..B.....pe.....H.....K..$.....$...8/.....0..).....{.....(....t.....\|.....(...+...3.*....0..).....{.....(....t.....\|.....(...+...3.*...}.....}.....(.....(.....{....o....&*.0..$.....r...pr7..p.. (.....,..(.....*.0.....{....o....&.{.....o.....{....(...o!.....{....(...o!.....{....(...o!.....{....(...o!.....{....(...o!.....{....(...o!.....{....(...o!....*...0..-.....{....o".....,..{.....o.....+..{...

C:\Users\user\Documents\MSDCSC\msdcsc.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.68131929551722
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	A1DB2JVWGG.CNT.exe
File size:	2223104
MD5:	a7817732eded62797b0c5e9da109edd7
SHA1:	e7e868e8a529cdd6bd32b4fa3711eff0c9029dbb
SHA256:	95969e3e0c1793e6177d5c5d20c9a667c9f28bb64907ad489682c41668efc29d
SHA512:	3664953e0e5c601e8d8123c0b9f3f43d727bf6f48f81a93fed051d6f0d275728ceda92ecef201e4cdceac29c17ce66b46820a43a6dac9fd4b77b6d54f226db01
SSDEEP:	24576:tA74/4qimDN0nixgBQcZ+WtGsK0i+CqBRCJcbpaa4S7qeL7pjhlyIy6Vs6wGpYUa:tA74/t6FQcZ+WRs+BRL4ShjTyIF

TLSH:	FDA5D000DABBCDDCC4760E780034163116B79F62586FE3C8997579B9E8787C2A684E7B
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...F.xd..............0..F...........e... ....@.. ....`"...........@................................

File Icon

Icon Hash:	cfc3ce4cccccc74f

Static PE Info

General

Entrypoint:	0x5b658e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6478F346 [Thu Jun 1 19:36:38 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1b653c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1b8000	0x6a02c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x224000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1b265c	0x54	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1b4594	0x1b4600	False	0.9364711266470925	data	7.897532048001292	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x1b8000	0x6a02c	0x6a200	False	0.2072359945524146	data	5.854806072192783	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x224000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1b82b0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024		
RT_ICON	0x1b8718	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304		
RT_ICON	0x1b90a0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096		
RT_ICON	0x1ba148	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216		
RT_ICON	0x1bc6f0	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384		
RT_ICON	0x1c0918	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736		
RT_ICON	0x1c5da0	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1cf248	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536		
RT_ICON	0x1dfa70	0x42028	Device independent bitmap graphic, 256 x 512 x 32, image size 262144		
RT_GROUP_ICON	0x221a98	0x84	data		
RT_VERSION	0x221b1c	0x324	data		
RT_MANIFEST	0x221e40	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

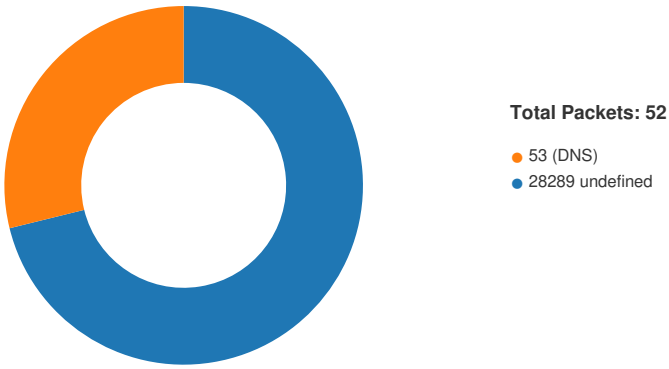
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.35.252.165.230 49702282892025019 06/02/23-02:26:44.385767	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49702	28289	192.168.2.3	5.252.165.230
5.252.165.230192.168.2.3 39399497042806577 06/02/23-02:27:01.218517	TCP	2806577	ETPRO TROJAN DarkComet-RAT init connection 2	39399	49704	5.252.165.230	192.168.2.3
192.168.2.35.252.165.230 49711282892025019 06/02/23-02:27:54.203652	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49711	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49713282892025019 06/02/23-02:28:03.961219	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49713	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49705282892025019 06/02/23-02:27:16.433852	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49712282892025019 06/02/23-02:27:59.459924	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49712	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49716282892025019 06/02/23-02:28:22.359438	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49716	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49706282892025019 06/02/23-02:27:24.140871	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49708282892025019 06/02/23-02:27:35.526983	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49708	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49707282892025019 06/02/23-02:27:28.447502	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49707	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49713282892816718 06/02/23-02:28:05.016410	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49713	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49702282892816718 06/02/23-02:26:45.935768	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49702	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49710282892025019 06/02/23-02:27:47.888873	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49710	28289	192.168.2.3	5.252.165.230

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.35.252.165.230 49708282892816766 06/02/23-02:27:36.099395	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49708	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49707282892816766 06/02/23-02:27:29.300655	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49707	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49709282892816766 06/02/23-02:27:43.508322	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49709	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49706282892816766 06/02/23-02:27:24.211225	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49706	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49716282892816766 06/02/23-02:28:25.005929	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49716	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49709282892025019 06/02/23-02:27:41.004326	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49704393992806578 06/02/23-02:27:01.218732	TCP	2806578	ETPRO TROJAN DarkComet-RAT server join acknowledgement 2	49704	39399	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49704393992807821 06/02/23-02:28:23.003919	TCP	2807821	ETPRO TROJAN DarkComet-RAT activity	49704	39399	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49710282892816766 06/02/23-02:27:48.244529	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49710	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49711282892816766 06/02/23-02:27:54.312190	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49711	28289	192.168.2.3	5.252.165.230
5.252.165.230192.168.2.3 28289497142841753 06/02/23-02:28:11.405336	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	28289	49714	5.252.165.230	192.168.2.3
192.168.2.35.252.165.230 49702282892816766 06/02/23-02:26:46.881522	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49712282892816766 06/02/23-02:27:59.647498	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49712	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49713282892816766 06/02/23-02:28:06.982149	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49713	28289	192.168.2.3	5.252.165.230
5.252.165.230192.168.2.3 28289497062810290 06/02/23-02:27:24.236176	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	28289	49706	5.252.165.230	192.168.2.3
5.252.165.230192.168.2.3 28289497032841753 06/02/23-02:27:02.943535	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	28289	49703	5.252.165.230	192.168.2.3
192.168.2.35.252.165.230 49714282892816766 06/02/23-02:28:11.424790	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49714	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49715282892816766 06/02/23-02:28:17.957593	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49715	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49703282892816766 06/02/23-02:27:05.840215	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	28289	192.168.2.3	5.252.165.230

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.35.252.165.230 49705282892816766 06/02/23-02:27:18.414247	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49705	28289	192.168.2.3	5.252.165.230
5.252.165.230192.168.2.3 28289497122841753 06/02/23-02:27:59.490400	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	28289	49712	5.252.165.230	192.168.2.3
5.252.165.230192.168.2.3 28289497102841753 06/02/23-02:27:47.915148	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	28289	49710	5.252.165.230	192.168.2.3
5.252.165.230192.168.2.3 28289497112841753 06/02/23-02:27:54.245563	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	28289	49711	5.252.165.230	192.168.2.3
5.252.165.230192.168.2.3 28289497062841753 06/02/23-02:27:24.193892	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	28289	49706	5.252.165.230	192.168.2.3
5.252.165.230192.168.2.3 28289497072841753 06/02/23-02:27:28.477912	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	28289	49707	5.252.165.230	192.168.2.3
5.252.165.230192.168.2.3 28289497082841753 06/02/23-02:27:35.555003	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	28289	49708	5.252.165.230	192.168.2.3
192.168.2.35.252.165.230 49715282892025019 06/02/23-02:28:16.130201	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49715	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49703282892025019 06/02/23-02:26:52.916534	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49703	28289	192.168.2.3	5.252.165.230
192.168.2.35.252.165.230 49714282892025019 06/02/23-02:28:11.375206	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49714	28289	192.168.2.3	5.252.165.230

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 02:26:44.151659012 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.176666975 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.176943064 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.385766983 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.461059093 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.461219072 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.531969070 CEST	28289	49702	5.252.165.230	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 02:26:44.532335043 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.558764935 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.572933912 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.648416996 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.648534060 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.719214916 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.719274998 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.719321966 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.719372988 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.719436884 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.719438076 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.724944115 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.744440079 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.744507074 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.744559050 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.744612932 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.744642973 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.744677067 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.744725943 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.744774103 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.744795084 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.744831085 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.744859934 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.744911909 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.744962931 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.769788980 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.769835949 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.769870043 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.769901991 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.769927025 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.769962072 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.769975901 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.770009041 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.770039082 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.770071030 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.770088911 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.770116091 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.770131111 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.770160913 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.770190954 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.770222902 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.770237923 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.770268917 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.770301104 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.770313978 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.770344019 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.770356894 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.770387888 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.770431042 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.795751095 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.795823097 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.795876980 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.795927048 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.795958042 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.795983076 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.796030998 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796077967 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796125889 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796173096 CEST	28289	49702	5.252.165.230	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 02:26:44.796192884 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.796240091 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796293020 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.796338081 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796387911 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796437979 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.796461105 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796509027 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796560049 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.796577930 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796622992 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.796643972 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796694040 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796741962 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.796760082 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796808004 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796852112 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.796874046 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796926022 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.796972036 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.797019005 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.797039032 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.797086000 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.797133923 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.797152996 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.797183037 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.797218084 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.797266006 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.797318935 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.797332048 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.797379017 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.797429085 CEST	49702	28289	192.168.2.3	5.252.165.230
Jun 2, 2023 02:26:44.797446012 CEST	28289	49702	5.252.165.230	192.168.2.3
Jun 2, 2023 02:26:44.797494888 CEST	28289	49702	5.252.165.230	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 02:26:44.097316027 CEST	52387	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:26:44.140640974 CEST	53	52387	8.8.8.8	192.168.2.3
Jun 2, 2023 02:26:52.799304008 CEST	56924	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:26:52.834667921 CEST	53	56924	8.8.8.8	192.168.2.3
Jun 2, 2023 02:27:01.122903109 CEST	60625	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:27:01.157489061 CEST	53	60625	8.8.8.8	192.168.2.3
Jun 2, 2023 02:27:13.448749065 CEST	49302	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:27:13.469129086 CEST	53	49302	8.8.8.8	192.168.2.3
Jun 2, 2023 02:27:24.085566044 CEST	53975	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:27:24.114435911 CEST	53	53975	8.8.8.8	192.168.2.3
Jun 2, 2023 02:27:28.394402027 CEST	51139	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:27:28.415224075 CEST	53	51139	8.8.8.8	192.168.2.3
Jun 2, 2023 02:27:35.480336905 CEST	52955	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:27:35.500720978 CEST	53	52955	8.8.8.8	192.168.2.3
Jun 2, 2023 02:27:40.942588091 CEST	60582	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:27:40.977518082 CEST	53	60582	8.8.8.8	192.168.2.3
Jun 2, 2023 02:27:47.830245018 CEST	57134	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:27:47.858867884 CEST	53	57134	8.8.8.8	192.168.2.3
Jun 2, 2023 02:27:54.156784058 CEST	62050	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:27:54.177257061 CEST	53	62050	8.8.8.8	192.168.2.3
Jun 2, 2023 02:27:59.039582968 CEST	56042	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 02:27:59.075484037 CEST	53	56042	8.8.8.8	192.168.2.3
Jun 2, 2023 02:28:03.900932074 CEST	59636	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:28:03.929716110 CEST	53	59636	8.8.8.8	192.168.2.3
Jun 2, 2023 02:28:11.316447020 CEST	55638	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:28:11.342737913 CEST	53	55638	8.8.8.8	192.168.2.3
Jun 2, 2023 02:28:16.073724031 CEST	57704	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:28:16.102108955 CEST	53	57704	8.8.8.8	192.168.2.3
Jun 2, 2023 02:28:22.290910006 CEST	65320	53	192.168.2.3	8.8.8.8
Jun 2, 2023 02:28:22.325861931 CEST	53	65320	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 2, 2023 02:26:44.097316027 CEST	192.168.2.3	8.8.8.8	0xa280	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:26:52.799304008 CEST	192.168.2.3	8.8.8.8	0x2563	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:01.122903109 CEST	192.168.2.3	8.8.8.8	0x3b25	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:13.448749065 CEST	192.168.2.3	8.8.8.8	0x72f6	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:24.085566044 CEST	192.168.2.3	8.8.8.8	0x5786	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:28.394402027 CEST	192.168.2.3	8.8.8.8	0x5f2c	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:35.480336905 CEST	192.168.2.3	8.8.8.8	0xfe7f	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:40.942588091 CEST	192.168.2.3	8.8.8.8	0x25e1	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:47.830245018 CEST	192.168.2.3	8.8.8.8	0x554	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:54.156784058 CEST	192.168.2.3	8.8.8.8	0x7d9a	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:59.039582968 CEST	192.168.2.3	8.8.8.8	0x1fe3	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:28:03.900932074 CEST	192.168.2.3	8.8.8.8	0x9445	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:28:11.316447020 CEST	192.168.2.3	8.8.8.8	0xae54	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:28:16.073724031 CEST	192.168.2.3	8.8.8.8	0x33e2	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:28:22.290910006 CEST	192.168.2.3	8.8.8.8	0xd8e	Standard query (0)	timmy08.ddns.net	A (IP address)	IN (0x0001)	false

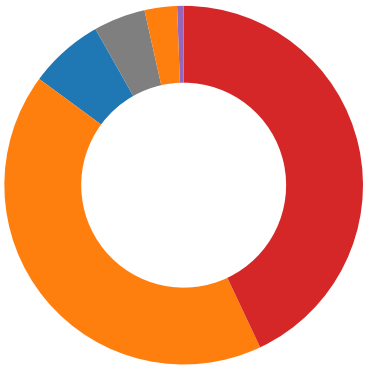
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 2, 2023 02:26:44.140640974 CEST	8.8.8.8	192.168.2.3	0xa280	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:26:52.834667921 CEST	8.8.8.8	192.168.2.3	0x2563	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:01.157489061 CEST	8.8.8.8	192.168.2.3	0x3b25	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:13.469129086 CEST	8.8.8.8	192.168.2.3	0x72f6	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:24.114435911 CEST	8.8.8.8	192.168.2.3	0x5786	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:28.415224075 CEST	8.8.8.8	192.168.2.3	0x5f2c	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:35.500720978 CEST	8.8.8.8	192.168.2.3	0xfe7f	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 2, 2023 02:27:40.977518082 CEST	8.8.8.8	192.168.2.3	0x25e1	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:47.858867884 CEST	8.8.8.8	192.168.2.3	0x554	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:54.177257061 CEST	8.8.8.8	192.168.2.3	0x7d9a	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:27:59.075484037 CEST	8.8.8.8	192.168.2.3	0x1fe3	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:28:03.929716110 CEST	8.8.8.8	192.168.2.3	0x9445	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:28:11.342737913 CEST	8.8.8.8	192.168.2.3	0xae54	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:28:16.102108955 CEST	8.8.8.8	192.168.2.3	0x33e2	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false
Jun 2, 2023 02:28:22.325861931 CEST	8.8.8.8	192.168.2.3	0xd8e	No error (0)	timmy08.ddns.net		5.252.165.230	A (IP address)	IN (0x0001)	false

Statistics

Behavior



- A1DB2JVWGG.CNT.exe
- powershell.exe
- conhost.exe
- powershell.exe
- schtasks.exe
- conhost.exe
- conhost.exe
- JXayEzy.exe
- A1DB2JVWGG.CNT.exe
- A1DB2JVWGG.CNT.exe
- A1DB2JVWGG.CNT.exe
- A1DB2JVWGG.CNT.exe
- cmd.exe
- cmd.exe
- conhost.exe
- conhost.exe
- attrib.exe
- attrib.exe
- JUNE STUB.EXE
- notepad.exe
- msdcsc.exe
- msdcsc.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- msdcsc.exe
- msdcsc.exe
- dhcpmon.exe
- JUNE STUB.EXE
- notepad.exe
- msdcsc.exe
- schtasks.exe
- conhost.exe
- msdcsc.exe
- schtasks.exe
- conhost.exe
- msdcsc.exe
- msdcsc.exe

Click to jump to process

System Behavior

Analysis Process: A1DB2JVWGG.CNT.exe PID: 7460, Parent PID: 3452

General

Target ID:	0
Start time:	02:26:22
Start date:	02/06/2023
Path:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
Imagebase:	0x970000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.399195409.0000000004886000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: RAT_DarkComet, Description: Detects DarkComet RAT, Source: 00000000.00000002.399195409.0000000004886000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DarkCometRat, Description: Yara detected DarkComet, Source: 00000000.00000002.399195409.0000000004886000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.399195409.0000000004886000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000000.00000002.399195409.0000000004886000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000000.00000002.399195409.0000000004886000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.399195409.0000000004886000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: DarkComet_1, Description: DarkComet RAT, Source: 00000000.00000002.399195409.0000000004886000.00000004.00000800.00020000.00000000.sdmp, Author: botherder https://github.com/botherder • Rule: DarkComet_3, Description: unknown, Source: 00000000.00000002.399195409.0000000004886000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: DarkComet_4, Description: unknown, Source: 00000000.00000002.399195409.0000000004886000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Darkcomet_1df27bcc, Description: unknown, Source: 00000000.00000002.399195409.0000000004886000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.399195409.0000000004886000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000000.00000002.392562881.0000000002F01000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.399195409.0000000004105000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: RAT_DarkComet, Description: Detects DarkComet RAT, Source: 00000000.00000002.399195409.0000000004105000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DarkCometRat, Description: Yara detected DarkComet, Source: 00000000.00000002.399195409.0000000004105000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.399195409.0000000004105000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000000.00000002.399195409.0000000004105000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000000.00000002.399195409.0000000004105000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.399195409.0000000004105000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: DarkComet_1, Description: DarkComet RAT, Source: 00000000.00000002.399195409.0000000004105000.00000004.00000800.00020000.00000000.sdmp, Author: botherder https://github.com/botherder • Rule: DarkComet_3, Description: unknown, Source: 00000000.00000002.399195409.0000000004105000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: DarkComet_4, Description: unknown, Source: 00000000.00000002.399195409.0000000004105000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Darkcomet_1df27bcc, Description: unknown, Source: 00000000.00000002.399195409.0000000004105000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.399195409.0000000004105000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

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	7299CF06	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	7299CF06	unknown
C:\Users\user\AppData\Roaming\JXayEzy.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	717EDD66	CopyFileW
C:\Users\user\AppData\Roaming\JXayEzy.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	717EDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp12D0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	717E7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\A1DB2JVWGG.CNT.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp12D0.tmp	success or wait	1	717E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\JXayEzy.exe	0	524288	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 46 fd 78 64 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 46 1b 00 00 fd 06 00 00 00 00 00 fd 65 1b 00 00 20 00 00 00 fd 1b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 22 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELFxd0Fe @ `" @	success or wait	5	717EDD66	CopyFileW
C:\Users\user\AppData\Roaming\JXayEzy.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	717EDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp12D0.tmp	0	1594	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationInfo>	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\A1DB2JVWGG.CNT.exe.log	0	1302	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 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 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 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	72CAC907	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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: powershell.exe PID: **7544**, Parent PID: **7460**

General

Target ID:	1
Start time:	02:26:30
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
Imagebase:	0xd60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kq5n4yzc.iw1.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qo2objni.hng.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
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	7299CF06	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	7299CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kq5n4yzc.iw1.ps1	success or wait	1	717E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qo2objni.hng.psm1	success or wait	1	717E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kq5n4yzc.iw1.ps1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qo2objni.hng.psm1	0	1	31	1	success or wait	1	717E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 12 14 00 00 18 00 00 00 63 0d 66 05 fd 07 fd 07 fd 07 00 00 fd 00 fd 00 0c 00 44 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00	@ecfD@	success or wait	1	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@BMDmEEMqqS%n4&5&7&	success or wait	11	72C676FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72981F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22372	success or wait	1	7298203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	104	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	73	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: conhost.exe PID: **7552**, Parent PID: **7544**

General

Target ID:	2
Start time:	02:26:30
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: powershell.exe PID: **7640**, Parent PID: **7460**

General

Target ID:	3
Start time:	02:26:31
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\JXayEzy.exe
Imagebase:	0xd60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71745B28	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71745B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_d5tgwwwd.pky.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ccef3fwz.eck.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
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	7299CF06	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	7299CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_d5tgwwwd.pky.ps1	success or wait	1	717E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ccef3fwz.eck.psm1	success or wait	1	717E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_d5tgwwwd.pky.ps1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ccef3fwz.eck.psm1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 12 14 00 00 18 00 00 00 63 0d 66 05 fd 07 fd 07 fd 07 00 00 fd 00 fd 00 0c 00 44 0d 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00	@ecfD@	success or wait	1	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	72C676FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@BMDmEEMqqS%n4&5&7&	success or wait	11	72C676FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72981F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22372	success or wait	1	7298203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: schtasks.exe PID: **7660**, Parent PID: **7460**

General	
Target ID:	4
Start time:	02:26:31
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JXayEzy" /XML "C:\Users\user\AppData\Local\Temp\tmp12D0.tmp
Imagebase:	0x1f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp12D0.tmp	unknown	2	success or wait	1	1FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp12D0.tmp	unknown	1595	success or wait	1	1FABD9	ReadFile

Analysis Process: conhost.exe PID: **7668**, Parent PID: **7640**

General	
Target ID:	5
Start time:	02:26:31
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: conhost.exe PID: **7688**, Parent PID: **7660**

General	
Target ID:	6
Start time:	02:26:31
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: JXayEzy.exe PID: **7808**, Parent PID: **1080**

General

Target ID:	7
Start time:	02:26:32
Start date:	02/06/2023
Path:	C:\Users\user\AppData\Roaming\JXayEzy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\JXayEzy.exe
Imagebase:	0x9d0000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 27%, ReversingLabs
Reputation:	low

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	7299CF06	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	7299CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JXayEzy.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	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\JXayEzy.exe.log	0	1216	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 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 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 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	72CAC907	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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: A1DB2JVWGG.CNT.exe PID: **7852**, Parent PID: **7460**

General

Target ID:	8
Start time:	02:26:34
Start date:	02/06/2023
Path:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
Imagebase:	0x3e0000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

Analysis Process: A1DB2JVWGG.CNT.exe PID: **7908**, Parent PID: **7460**

General	
Target ID:	10
Start time:	02:26:35
Start date:	02/06/2023
Path:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
Imagebase:	0x160000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: A1DB2JVWGG.CNT.exe PID: **7936**, Parent PID: **7460**

General	
Target ID:	11
Start time:	02:26:35
Start date:	02/06/2023
Path:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
Imagebase:	0x4c0000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: A1DB2JVWGG.CNT.exe PID: **7948**, Parent PID: **7460**

General	
Target ID:	12
Start time:	02:26:35
Start date:	02/06/2023
Path:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe
Imagebase:	0xce0000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: DarkComet_2, Description: DarkComet, Source: 0000000C.00000002.400104178.0000000003096000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_ • Rule: Malware_QA_update, Description: VT Research QA uploaded malware - file update.exe, Source: 0000000C.00000002.397292430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: RAT_DarkComet, Description: Detects DarkComet RAT, Source: 0000000C.00000002.397292430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DarkCometRat, Description: Yara detected DarkComet, Source: 0000000C.00000002.397292430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 0000000C.00000002.397292430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_DarkComet, Description: Detects DarkComet, Source: 0000000C.00000002.397292430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: DarkComet_1, Description: DarkComet RAT, Source: 0000000C.00000002.397292430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: botherder https://github.com/botherder • Rule: DarkComet_3, Description: unknown, Source: 0000000C.00000002.397292430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: DarkComet_4, Description: unknown, Source: 0000000C.00000002.397292430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Darkcomet_1df27bcc, Description: unknown, Source: 0000000C.00000002.397292430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: DarkComet_2, Description: DarkComet, Source: 0000000C.00000002.400104178.000000000306C000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_ • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 0000000C.00000002.397292430.000000000049D000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: DarkComet_2, Description: DarkComet, Source: 0000000C.00000002.400104178.00000000030BA000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_ • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.397292430.00000000004A4000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.397292430.00000000004A4000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.397292430.00000000004A4000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.397292430.00000000004A4000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: DarkComet_2, Description: DarkComet, Source: 0000000C.00000002.400104178.00000000030C1000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\MSDCSC	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40A85E	CreateDirectoryA
C:\Users\user\Documents\MSDCSC\msdcsc.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	48FD57	CopyFileA
C:\Users\user\Documents\MSDCSC \msdcsc.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	48FD57	CopyFileA
C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	48BE47	CreateFileA

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\Documents\MSDCSC \msdcsc.exe	0	524288	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 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 46 fd 78 64 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 46 1b 00 00 fd 06 00 00 00 00 00 fd 65 1b 00 00 20 00 00 00 fd 1b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 22 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELFxd0Fe @ `" @	success or wait	5	48FD57	CopyFileA
C:\Users\user\Documents\MSDCSC \msdcsc.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	48FD57	CopyFileA
C:\Users\user\AppData\Local\Te mp\JUNE STUB.EXE	0	207360	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 27 fd 54 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 fd 01 00 00 60 01 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 00 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL'T` @	success or wait	1	48BE6D	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\DC3_FEXEC	success or wait	1	421884	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	chrome	unicode	C:\Users\user\Documents\MSDCSC\msdcsc.exe	success or wait	1	4851CB	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	UserInit	unicode	C:\Windows\system32\userinit.exe,	C:\Windows\system32\userinit.exe,C:\Users\user\Documents\MSDCSC\msdcsc.exe	success or wait	1	4221BF	RegSetValueExA

Analysis Process: cmd.exe PID: **8032**, Parent PID: **7948**

General

Target ID:	13
Start time:	02:26:36
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /k attrib "C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe" +s +h
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **8040**, Parent PID: **7948**

General

Target ID:	14
Start time:	02:26:37
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /k attrib "C:\Users\user\Desktop" +s +h
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **8048**, Parent PID: **8032**

General

Target ID:	15
Start time:	02:26:37
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **8064**, Parent PID: **8040**

General	
Target ID:	16
Start time:	02:26:37
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: attrib.exe PID: **8096**, Parent PID: **8032**

General	
Target ID:	17
Start time:	02:26:38
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\attrib.exe
Wow64 process (32bit):	true
Commandline:	attrib "C:\Users\user\Desktop\A1DB2JVWGG.CNT.exe" +s +h
Imagebase:	0x1220000
File size:	19456 bytes
MD5 hash:	A5540E9F87D4CB083BDF8269DEC1CFF9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: attrib.exe PID: **8152**, Parent PID: **8040**

General	
Target ID:	18
Start time:	02:26:38
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\attrib.exe
Wow64 process (32bit):	true
Commandline:	attrib "C:\Users\user\Desktop" +s +h
Imagebase:	0x1220000
File size:	19456 bytes
MD5 hash:	A5540E9F87D4CB083BDF8269DEC1CFF9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: JUNE STUB.EXE PID: **8176**, Parent PID: **7948**

General

Target ID:	19
Start time:	02:26:38
Start date:	02/06/2023
Path:	C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE"
Imagebase:	0xcc0000
File size:	207360 bytes
MD5 hash:	4D9AC7D6E684CD3874B662971B6BC536
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.639756642.0000000006C60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.639756642.0000000006C60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.639756642.0000000006C60000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.639756642.0000000006C60000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.640582585.0000000006CE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.640582585.0000000006CE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.640582585.0000000006CE0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.640582585.0000000006CE0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.640822750.0000000006D00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.640822750.0000000006D00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.640822750.0000000006D00000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.640822750.0000000006D00000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.639572623.0000000006C40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.639572623.0000000006C40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.639572623.0000000006C40000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.639572623.0000000006C40000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.639327601.0000000006C10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.639327601.0000000006C10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.639327601.0000000006C10000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.639327601.0000000006C10000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.640048341.0000000006C80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.640048341.0000000006C80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.640048341.0000000006C80000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.640048341.0000000006C80000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.625066874.00000000033FB000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.625066874.00000000033FB000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.391419117.0000000000CC2000.00000002.00000001.01000000.0000000A.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.391419117.0000000000CC2000.00000002.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.391419117.0000000000CC2000.00000002.00000001.01000000.0000000A.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000000.391419117.0000000000CC2000.00000002.00000001.01000000.0000000A.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.640453706.0000000006CD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.640453706.0000000006CD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.640453706.0000000006CD0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen

	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.640453706.0000000006CD0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.639417055.0000000006C20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.639417055.0000000006C20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.639417055.0000000006C20000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.639417055.0000000006C20000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.640195396.0000000006CA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.640195396.0000000006CA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.640195396.0000000006CA0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.640195396.0000000006CA0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.640312728.0000000006CB0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.640312728.0000000006CB0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.640312728.0000000006CB0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.640312728.0000000006CB0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.640130436.0000000006C90000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.640130436.0000000006C90000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.640130436.0000000006C90000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.640130436.0000000006C90000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.637176007.0000000005D10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.637176007.0000000005D10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.637176007.0000000005D10000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.637176007.0000000005D10000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.637176007.0000000005D10000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.631531483.0000000004515000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.641220331.0000000006D30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.641220331.0000000006D30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.641220331.0000000006D30000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.641220331.0000000006D30000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.631531483.000000000441F000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.636982367.0000000005A80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.636982367.0000000005A80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000013.00000002.636982367.0000000005A80000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.636982367.0000000005A80000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.625066874.00000000033A1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

Analysis Process: notepad.exe PID: 7292, Parent PID: 7948

General

Target ID:	20
Start time:	02:26:40
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\notepad.exe

Wow64 process (32bit):	true
Commandline:	notepad
Imagebase:	0xdd0000
File size:	236032 bytes
MD5 hash:	D693F13FE3AA2010B854C4C60671B8E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: msdcsc.exe PID: **5860**, Parent PID: **7948**

General

Target ID:	21
Start time:	02:26:41
Start date:	02/06/2023
Path:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Documents\MSDCSC\msdcsc.exe"
Imagebase:	0x940000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.470317430.0000000004126000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.470317430.0000000004126000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.470317430.0000000004126000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000002.470317430.0000000004126000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000015.00000002.442690195.000000000319D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.470317430.0000000004AAC000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: RAT_DarkComet, Description: Detects DarkComet RAT, Source: 00000015.00000002.470317430.0000000004AAC000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DarkCometRat, Description: Yara detected DarkComet, Source: 00000015.00000002.470317430.0000000004AAC000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.470317430.0000000004AAC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000015.00000002.470317430.0000000004AAC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000015.00000002.470317430.0000000004AAC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.470317430.0000000004AAC000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: DarkComet_1, Description: DarkComet RAT, Source: 00000015.00000002.470317430.0000000004AAC000.00000004.00000800.00020000.00000000.sdmp, Author: botherder https://github.com/botherder • Rule: DarkComet_3, Description: unknown, Source: 00000015.00000002.470317430.0000000004AAC000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: DarkComet_4, Description: unknown, Source: 00000015.00000002.470317430.0000000004AAC000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Darkcomet_1df27bcc, Description: unknown, Source: 00000015.00000002.470317430.0000000004AAC000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000002.470317430.0000000004AAC000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 27%, ReversingLabs

Analysis Process: msdcsc.exe PID: **7264**, Parent PID: **3452**

General

Target ID:	22
Start time:	02:26:47
Start date:	02/06/2023
Path:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\Documents\MSDCSC\msdcsc.exe"
Imagebase:	0xd80000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000016.00000002.475372371.00000000033B7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.486347814.0000000005049000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.486347814.0000000005049000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.486347814.0000000005049000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000016.00000002.486347814.0000000005049000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: powershell.exe PID: **2680**, Parent PID: **5860**

General	
Target ID:	23
Start time:	02:26:49
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Documents\MSDCSC\msdcsc.exe
Imagebase:	0xd60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **4404**, Parent PID: **2680**

General	
Target ID:	24
Start time:	02:26:49
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **7672**, Parent PID: **5860**

General	
Target ID:	25
Start time:	02:26:49
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\JXayEzy.exe

Imagebase:	0xd60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **7732**, Parent PID: **7672**

General	
Target ID:	26
Start time:	02:26:49
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **7688**, Parent PID: **5860**

General	
Target ID:	27
Start time:	02:26:49
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JXayEzy" /XML "C:\Users\user\AppData\Local\Temp\tmp5A49.tmp
Imagebase:	0x1f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2100**, Parent PID: **7688**

General	
Target ID:	28
Start time:	02:26:49
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: msdcsc.exe PID: **6284**, Parent PID: **5860**

General	
Target ID:	31
Start time:	02:26:55
Start date:	02/06/2023
Path:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
Imagebase:	0x100000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: msdcsc.exe PID: **6288**, Parent PID: **5860**

General	
Target ID:	32
Start time:	02:26:55
Start date:	02/06/2023
Path:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
Imagebase:	0x800000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: DarkComet_2, Description: DarkComet, Source: 00000020.00000002.622990283.0000000002C81000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_ • Rule: DarkComet_2, Description: DarkComet, Source: 00000020.00000002.622990283.0000000002C2C000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_ • Rule: DarkComet_2, Description: DarkComet, Source: 00000020.00000002.622990283.0000000002C7A000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_

Analysis Process: dhcpmon.exe PID: **6384**, Parent PID: **3452**

General	
Target ID:	33
Start time:	02:26:57
Start date:	02/06/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x1f0000
File size:	207360 bytes
MD5 hash:	4D9AC7D6E684CD3874B662971B6BC536
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000002.456486839.00000000039D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.456486839.00000000039D1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000021.00000002.456486839.00000000039D1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000002.454672045.00000000029D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.454672045.00000000029D1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000021.00000002.454672045.00000000029D1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

Analysis Process: JUNE STUB.EXE PID: **8152**, Parent PID: **6288**

General

Target ID:	34
Start time:	02:26:59
Start date:	02/06/2023
Path:	C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\JUNE STUB.EXE"
Imagebase:	0x7f0000
File size:	207360 bytes
MD5 hash:	4D9AC7D6E684CD3874B662971B6BC536
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000022.00000002.459239135.0000000002ED1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000022.00000002.459239135.0000000002ED1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000022.00000002.459239135.0000000002ED1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: notepad.exe PID: **1340**, Parent PID: **6288**

General

Target ID:	35
Start time:	02:26:59
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\notepad.exe
Wow64 process (32bit):	true
Commandline:	notepad
Imagebase:	0xdd0000
File size:	236032 bytes
MD5 hash:	D693F13FE3AA2010B854C4C60671B8E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: msdcsc.exe PID: **7432**, Parent PID: **3452**

General

Target ID:	36

Start time:	02:27:06
Start date:	02/06/2023
Path:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Documents\MSDCSC\msdcsc.exe"
Imagebase:	0xb60000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: schtasks.exe PID: **7804**, Parent PID: **7264**

General	
Target ID:	37
Start time:	02:27:07
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JXayEzy" /XML "C:\Users\user\AppData\Local\Temp\tmp9C72.tmp
Imagebase:	0x1f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **7772**, Parent PID: **7804**

General	
Target ID:	38
Start time:	02:27:07
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: msdcsc.exe PID: **5840**, Parent PID: **7264**

General	
Target ID:	39
Start time:	02:27:11
Start date:	02/06/2023
Path:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
Imagebase:	0x900000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: DarkComet_2, Description: DarkComet, Source: 00000027.00000002.468665185.0000000002E81000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_ • Rule: DarkComet_2, Description: DarkComet, Source: 00000027.00000002.468665185.0000000002E7A000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_ • Rule: DarkComet_2, Description: DarkComet, Source: 00000027.00000002.468665185.0000000002E56000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_ • Rule: DarkComet_2, Description: DarkComet, Source: 00000027.00000002.468665185.0000000002E2C000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_

Analysis Process: schtasks.exe PID: **7612**, Parent PID: **7432**

General

Target ID:	40
Start time:	02:27:26
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JXayEzy" /XML "C:\Users\user\AppData\Local\Temp\tmpE34F.tmp
Imagebase:	0x1f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5304**, Parent PID: **7612**

General

Target ID:	41
Start time:	02:27:26
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: msdcsc.exe PID: **5100**, Parent PID: **7432**

General

Target ID:	42
Start time:	02:27:28
Start date:	02/06/2023
Path:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
Imagebase:	0x100000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Analysis Process: msdcsc.exe PID: **5236**, Parent PID: **7432**

General

Target ID:	43
Start time:	02:27:30
Start date:	02/06/2023
Path:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Documents\MSDCSC\msdcsc.exe
Imagebase:	0x640000
File size:	2223104 bytes
MD5 hash:	A7817732EDED62797B0C5E9DA109EDD7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: DarkComet_2, Description: DarkComet, Source: 0000002B.00000002.507022400.0000000002ACA000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_ • Rule: DarkComet_2, Description: DarkComet, Source: 0000002B.00000002.507022400.0000000002AA6000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_ • Rule: DarkComet_2, Description: DarkComet, Source: 0000002B.00000002.507022400.0000000002A7C000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_ • Rule: DarkComet_2, Description: DarkComet, Source: 0000002B.00000002.507022400.0000000002AD1000.00000004.00001000.00020000.00000000.sdmp, Author: Jean-Philippe Teissier / @Jipe_

Disassembly

No disassembly