ID: 623326
Sample Name:
e1f388b8a086e034b1fbd94ca7341008.exe
Cookbook: default.jbs
Time: 11:52:10
Date: 10/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

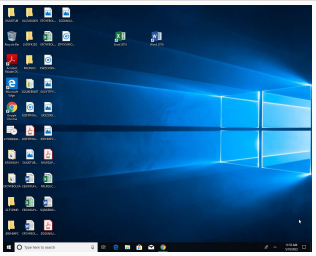
Windows Analysis Report

e1f388b8a086e034b1fbd94ca7341008.exe

Overview

General Information

Sample Name:	e1f388b8a086e034b1fbd94ca7341008.exe
Analysis ID:	623326
MD5:	916eb825989bc9..
SHA1:	e91e3a11ab3203.
SHA256:	6e5ce2c28b65e3..
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

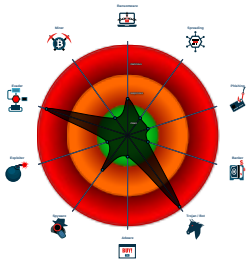
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Connects to many ports of the same…

Classification



Process Tree

- **System is w10x64**
- e1f388b8a086e034b1fbd94ca7341008.exe (PID: 6952 cmdline: "C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.exe" MD5: 916EB825989BC96A10EAB8916995C1E1)
  - powershell.exe (PID: 5508 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\QgGSCvPvvCY.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5204 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QgGSCvPvvCY" /XML "C:\Users\user\AppData\Local\Temp\tmp5BA5.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - e1f388b8a086e034b1fbd94ca7341008.exe (PID: 3312 cmdline: C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.exe MD5: 916EB825989BC96A10EAB8916995C1E1)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "a63bf89b-7de8-4696-9653-4f27004d",
  "Group": "APRILO",
  "Domain1": "ella666.duckdns.org",
  "Domain2": "mikeljack321.ddns.net",
  "Port": 31789,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "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": "ella666.duckdns.org"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.519250618.0000000003D81000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000008.00000002.515876792.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000008.00000002.515876792.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000008.00000002.515876792.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000000.00000002.293486073.0000000002DEB000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Click to see the 31 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.e1f388b8a086e034b1fbd94ca7341008.exe.5540000.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
8.2.e1f388b8a086e034b1fbd94ca7341008.exe.5540000.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
8.2.e1f388b8a086e034b1fbd94ca7341008.exe.5540000.5.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
8.2.e1f388b8a086e034b1fbd94ca7341008.exe.3d88a58.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
8.2.e1f388b8a086e034b1fbd94ca7341008.exe.3d88a58.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
Click to see the 78 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

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: 185.140.53.3

Timestamp:	192.168.2.3185.140.53.349767317892025019 05/10/22-11:54:04.775428
SID:	2025019
Source Port:	49767
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3

Timestamp:	192.168.2.3185.140.53.349778317892025019 05/10/22-11:54:18.335094
SID:	2025019
Source Port:	49778
Destination Port:	31789

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	
Timestamp:	192.168.2.3185.140.53.349826317892816766 05/10/22-11:54:42.317503
SID:	2816766
Source Port:	49826
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	
Timestamp:	192.168.2.3185.140.53.349867317892816766 05/10/22-11:55:08.482183
SID:	2816766
Source Port:	49867
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	
Timestamp:	192.168.2.3185.140.53.349868317892816766 05/10/22-11:55:15.380950
SID:	2816766
Source Port:	49868
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	
Timestamp:	192.168.2.3185.140.53.349843317892816766 05/10/22-11:54:56.333885
SID:	2816766
Source Port:	49843
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	
Timestamp:	192.168.2.3185.140.53.349762317892025019 05/10/22-11:53:57.886255
SID:	2025019
Source Port:	49762
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	
Timestamp:	192.168.2.3185.140.53.349758317892025019 05/10/22-11:53:52.880985
SID:	2025019
Source Port:	49758
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	
Timestamp:	192.168.2.3185.140.53.349782317892025019 05/10/22-11:54:25.487213
SID:	2025019
Source Port:	49782
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3

Timestamp:	192.168.2.3185.140.53.349771317892025019 05/10/22-11:54:11.319386
SID:	2025019
Source Port:	49771
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3

Timestamp:	192.168.2.3185.140.53.349750317892025019 05/10/22-11:53:37.365565
SID:	2025019
Source Port:	49750
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3

Timestamp:	192.168.2.3185.140.53.349752317892025019 05/10/22-11:53:45.193397
SID:	2025019
Source Port:	49752
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3

Timestamp:	192.168.2.3185.140.53.349750317892816766 05/10/22-11:53:38.950679
SID:	2816766
Source Port:	49750
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3

Timestamp:	192.168.2.3185.140.53.349782317892816766 05/10/22-11:54:26.713499
SID:	2816766
Source Port:	49782
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3

Timestamp:	192.168.2.3185.140.53.349762317892816766 05/10/22-11:53:59.504378
SID:	2816766
Source Port:	49762
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3

Timestamp:	192.168.2.3185.140.53.349771317892816766 05/10/22-11:54:13.062923
SID:	2816766
Source Port:	49771
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3

Timestamp:	192.168.2.3185.140.53.349837317892816766 05/10/22-11:54:49.300837
SID:	2816766
Source Port:	49837
Destination Port:	31789

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	
Timestamp:	192.168.2.3185.140.53.349816317892816766 05/10/22-11:54:33.736622
SID:	2816766
Source Port:	49816
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	
Timestamp:	192.168.2.3185.140.53.349816317892025019 05/10/22-11:54:32.532276
SID:	2025019
Source Port:	49816
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	
Timestamp:	192.168.2.3185.140.53.349869317892025019 05/10/22-11:55:20.675127
SID:	2025019
Source Port:	49869
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.140.53.3 - Destination IP: 192.168.2.3	
Timestamp:	185.140.53.3192.168.2.331789498642841753 05/10/22-11:55:01.918437
SID:	2841753
Source Port:	31789
Destination Port:	49864
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	
Timestamp:	192.168.2.3185.140.53.349752317892816766 05/10/22-11:53:47.498984
SID:	2816766
Source Port:	49752
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 3 - Source IP: 185.140.53.3 - Destination IP: 192.168.2.3	
Timestamp:	185.140.53.3192.168.2.331789498692810451 05/10/22-11:55:45.875144
SID:	2810451
Source Port:	31789
Destination Port:	49869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	
Timestamp:	192.168.2.3185.140.53.349867317892025019 05/10/22-11:55:06.652869
SID:	2025019
Source Port:	49867
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3

Timestamp:	192.168.2.3185.140.53.349868317892025019 05/10/22-11:55:14.375651
SID:	2025019
Source Port:	49868
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	−
Timestamp:	192.168.2.3185.140.53.349767317892816766 05/10/22-11:54:06.037273
SID:	2816766
Source Port:	49767
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	−
Timestamp:	192.168.2.3185.140.53.349778317892816766 05/10/22-11:54:20.124819
SID:	2816766
Source Port:	49778
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.140.53.3 - Destination IP: 192.168.2.3	−
Timestamp:	185.140.53.3192.168.2.331789498692841753 05/10/22-11:55:45.875144
SID:	2841753
Source Port:	31789
Destination Port:	49869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 185.140.53.3 - Destination IP: 192.168.2.3	−
Timestamp:	185.140.53.3192.168.2.331789498692810290 05/10/22-11:55:23.881709
SID:	2810290
Source Port:	31789
Destination Port:	49869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	−
Timestamp:	192.168.2.3185.140.53.349826317892025019 05/10/22-11:54:39.732514
SID:	2025019
Source Port:	49826
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	−
Timestamp:	192.168.2.3185.140.53.349837317892025019 05/10/22-11:54:47.544258
SID:	2025019
Source Port:	49837
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	−
Timestamp:	192.168.2.3185.140.53.349771317892816718 05/10/22-11:54:13.062923
SID:	2816718
Source Port:	49771
Destination Port:	31789

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	−
Timestamp:	192.168.2.3185.140.53.349864317892025019 05/10/22-11:55:01.707210
SID:	2025019
Source Port:	49864
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.140.53.3 - Destination IP: 192.168.2.3	−
Timestamp:	185.140.53.3192.168.2.331789497582841753 05/10/22-11:53:53.093006
SID:	2841753
Source Port:	31789
Destination Port:	49758
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	−
Timestamp:	192.168.2.3185.140.53.349843317892025019 05/10/22-11:54:54.648860
SID:	2025019
Source Port:	49843
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 185.140.53.3	−
Timestamp:	192.168.2.3185.140.53.349868317892816718 05/10/22-11:55:15.380950
SID:	2816718
Source Port:	49868
Destination Port:	31789
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

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

Networking

Snort IDS alert for network traffic
Connects to many ports of the same IP (likely port scanning)
C2 URLs / IPs found in malware configuration
Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

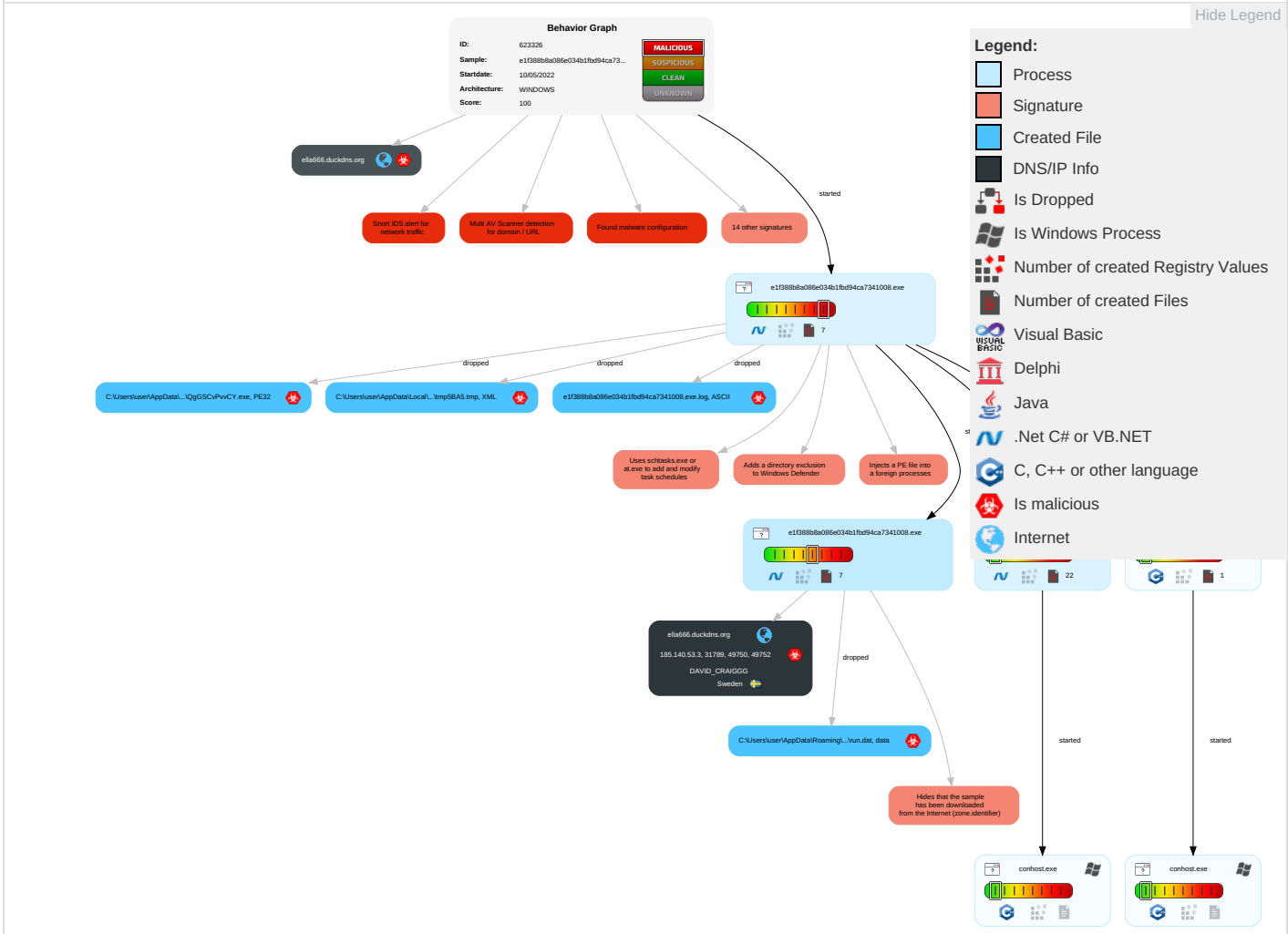
Yara detected Nanocore RAT

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	2 Command and Scripting Interpreter	1 Scheduled Task/Job	1 1 2 Process Injection	1 Masquerading	2 1 Input Capture	2 1 Security Software Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Native API	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	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	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	Network Sniffing	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	1 2 Software Packing	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

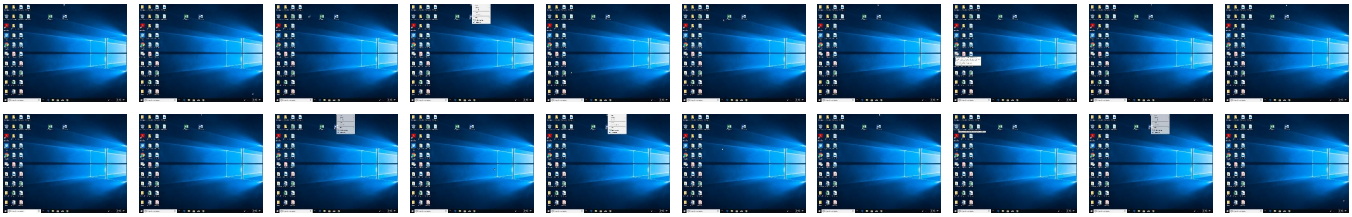
Behavior Graph



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
e1f388b8a086e034b1fbd94ca7341008.exe	22%	Virustotal		Browse
e1f388b8a086e034b1fbd94ca7341008.exe	24%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\QgGSCvPvvCY.exe	25%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\QgGSCvPvvCY.exe	24%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.e1f388b8a086e034b1fbd94ca7341008.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.e1f388b8a086e034b1fbd94ca7341008.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.e1f388b8a086e034b1fbd94ca7341008.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.e1f388b8a086e034b1fbd94ca7341008.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.e1f388b8a086e034b1fbd94ca7341008.exe.57f0000.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File
8.0.e1f388b8a086e034b1fbd94ca7341008.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.e1f388b8a086e034b1fbd94ca7341008.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
ella666.duckdns.org	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
ella666.duckdns.org	12%	Virustotal		Browse
ella666.duckdns.org	100%	Avira URL Cloud	malware	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
mikeljack321.ddns.net	7%	Virustotal		Browse
mikeljack321.ddns.net	0%	Avira URL Cloud	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ella666.duckdns.org	185.140.53.3	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation

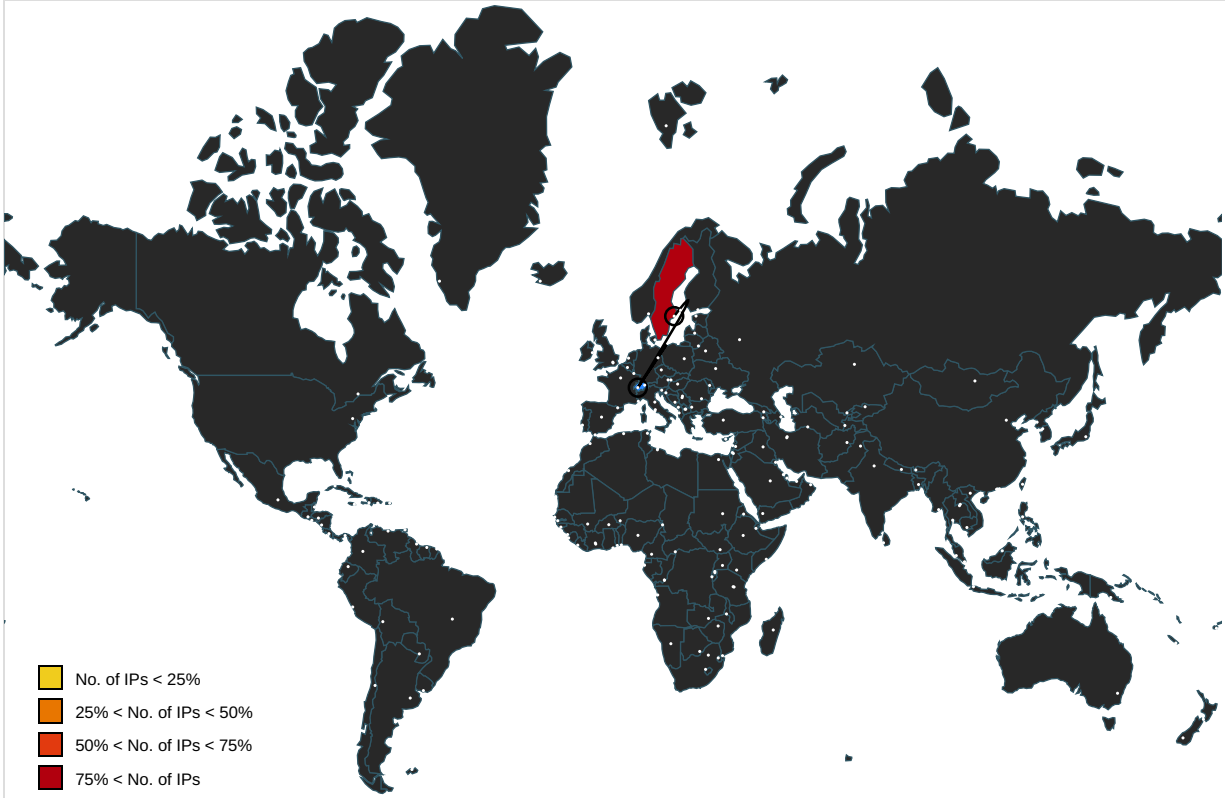
Name	Malicious	Antivirus Detection	Reputation
ella666.duckdns.org	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
mikeljack321.ddns.net	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.292557381.0000000001457000.00000004.00000020.00020000.00000000.sdmp, e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.292920833.0000000002C31000.00000004.00000800.00020000.00000000.sdmp, e1f388b8a086e034b1fbd94ca7341008.exe, 00000008.00000002.518021079.0000000002D21000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	e1f388b8a086e034b1fbd94ca7341008.exe, 00000000.00000002.297515280.0000000006D12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.3	ella666.duckdns.org	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	623326
Start date and time: 10/05/202211:52:10	2022-05-10 11:52:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 34s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	e1f388b8a086e034b1fbd94ca7341008.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/10@16/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- 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
11:53:22	API Interceptor	865x Sleep call for process: e1f388b8a086e034b1fbd94ca7341008.exe modified
11:53:29	API Interceptor	35x Sleep call for process: powershell.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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\e1f388b8a086e034b1fbd94ca7341008.exe.log

Process:	C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
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):	22240
Entropy (8bit):	5.601926797997156
Encrypted:	false
SSDEEP:	384:4jtCDLq0hX3AcoATY4KnwjultIt27Y9gNSJ3xWT1MaLZlbAV7ia23ZBDI+iaE:44X3474KwCltSyNckCafwQVU
MD5:	07C4587984660ADA43BA12DE61D64EEF
SHA1:	897D5E48E0516C17830E2C09ED3A8F5FCA5FE5E6
SHA-256:	4BCFB8127C63B308F026A42EB8795AAFE832FD05B65E3288E23BB8A7940BE95B
SHA-512:	BF4A65E900E7201916391CE8F0C620EC296A42D59F38EB6BBC4D5D5361BE4B17FF9E79B223CA4B2C086157C07D32814C17880358FC3FBD4D9D44FCA5B8BD68F
Malicious:	false
Reputation:	low
Preview:	@...e.....p.....h...W.N.K.....y...H.....@.....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__PSScriptPolicyTest_axfdujok.0nl.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ryl20vvq.5q2.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp5BA5.tmp

Process:	C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1598
Entropy (8bit):	5.158943217736509
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNttXxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTrv
MD5:	75F7A3F0883E114F65B5970F1FCD4CF2
SHA1:	24DF87D295A023E8F73C69E312DBB504288BD914
SHA-256:	8A965519AAF417D139A3F1E5D44129DF65CACA48A9E1C174CA6F3026CD9B40D0
SHA-512:	8EA192A569456D1CB1102BB9AF9D13CC4CB1E81317A55C110CC66A5106D29F255916112F89131621AEA22824D8FE5F1F11B7D51472F180D21E8A7A265C470546
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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.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:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35(A5
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\Desktop\e1f388b8a086e034b1fbd94ca7341008.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:mln:ml
MD5:	E578BDC4870935A8ED87C86290D526C2
SHA1:	A238F1F66DDEB7F15E3438B2020D9699B236907D
SHA-256:	73DC67D9CA00AFEC69D033CA24EAC73F73F4EA97B678794A91A1F970EFADC81B
SHA-512:	8BAB6343B110F99E148426F23B0D9CD17E2257BD1042F445FC5A0F1D256AC3B32DB44EDAC364E9F53E12B5DA72D16E3265B5C25B8FC253E7185B20990E53779
Malicious:	**true**
Preview:	...c.2.H

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

Process:	C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1159168
Entropy (8bit):	7.014675929913691
Encrypted:	false
SSDEEP:	12288:zzODfxt7J0n9QnXZObXEbA3OBGr0IUfV4p4ifhTdVx5tLaN6lZFm+t5rCQJG/kez:3E2n9QXZOkAeUFUSnRz5tm6bFme2
MD5:	916EB825989BC96A10EAB8916995C1E1
SHA1:	E91E3A11AB3203C912B5D756C5F22E620760EDF9
SHA-256:	6E5CE2C28B65E3F50C89EE799DE9C047C07EC4C27B4D4B8B6F4F202B1E8D557A
SHA-512:	E3AED0247856EC0D976032467921989708FC9F8A64580444788A6C9871C092C6C28D440E5D77DFAD7B1DFC84835D681959173C3A291100D167EC713075A5E381
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 25%, Browse • Antivirus: ReversingLabs, Detection: 24%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.../.zb.....0..T...Z.....r.. .....@.. ....@.....r..O.....W..... ....H.....text....R... ...T..... ..`.rsrc....W.....X...V.....@..@.rel oc.....@..B.....r.....H.....h...$.....-. .:....*..{)...*..{*...*V.(+.....}).....}*...*. ....)UU.Z(,....{)...o0...X)UU.Z(.....{*...o1.. .X*&...(4...*B.(.....}....*^..}.....(5.....(.....*&..(.....*>...(....(.....*..(B...*..oC...*..oD...*..o....*..o....*..oE...*.sF...*.sG...*.sH...*.sI...*.sJ...*..oK...*..(K...*..oL...*"..oM...*"..oN...*"..oO ...*"..oP...*"..oQ...*"..oR...*"..oS...*"..oT...*"..oU...*"..oV...*"..oW...*"..oX...*"..oY...*"..oZ.

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

Process:	C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.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:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220510\PowerShell_transcript.284992.KzD+VzNg.20220510115327.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5793
Entropy (8bit):	5.423338801980799
Encrypted:	false
SSDEEP:	96:BZWhUN7qDo1ZRZbuhUN7qDo1Zja0yjZihUN7qDo1ZczCCajZ8a:O
MD5:	229A9A51D89E599FC053B83B450DBF0F
SHA1:	855A0E98DBB6EA5C17C1332D6DA6AD729F0CE5E1
SHA-256:	558143EEDE6ED094BEDC9268C81C9506EEE016326E7175DDE197915EEAB2127E
SHA-512:	426CE8347969D30A990F062251CAC8311CC5407EAE6DDF8C8E19B27F83E8E0F783F27F32AA625EA5DFB80C850EAF67330E9F14A3D35C8516833752B31A4DE1D
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220510115328..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\QgGSCvPvvCY.exe..Process ID: 5508..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220510115328..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\QgGSCvPvvCY.exe..**********..Windows PowerShell transcript start..Start time: 20220510115647..Username: computer\user..RunAs User: computer\ha

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.014675929913691
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:	e1f388b8a086e034b1fbd94ca7341008.exe
File size:	1159168
MD5:	916eb825989bc96a10eab8916995c1e1
SHA1:	e91e3a11ab3203c912b5d756c5f22e620760edf9
SHA256:	6e5ce2c28b65e3f50c89ee799de9c047c07ec4c27b4d4b8b6f4f202b1e8d557a
SHA512:	e3aed0247856ec0d976032467921989708fc9f8a64580444788a6c9871c092c6c28d440e5d77dfad7b1dfc84835d681959173c3a291100d167ec713075a5e381
SSDEEP:	12288:zzODfxt7J0n9QnXZObXEbA3OBGr0IUfV4p4ifhTdVx5tLaN6lZFm+t5rCQJG/kez:3E2n9QXZOkAeUFUSnRz5tm6bFme2
TLSH:	5A3528987254F9DEC85BD071CA685CF0AA207C6AC31B820B50173D9EB97DB83DF215A7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.../.zb.....0..T...Z.....r... .....@.. .....@.....

File Icon

Icon Hash:	f274fec6b6c2e00c

Static PE Info

General

Entrypoint:	0x5072de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627A172F [Tue May 10 07:41:35 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10728c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x108000	0x15708	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x11e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x1052e4	0x105400	False	0.644225665371	data	7.15323039057	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x108000	0x15708	0x15800	False	0.151560228924	data	4.00261840431	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x11e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1081d8	0x8a8	data		
RT_ICON	0x108a80	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x108fe8	0x10828	data		
RT_ICON	0x119810	0x25a8	data		
RT_ICON	0x11bdb8	0x10a8	data		
RT_ICON	0x11ce60	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x11d2c8	0x5a	data		
RT_VERSION	0x11d324	0x3e4	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2011 BASeCamp Software Solutions
Assembly Version	1.4.8.0
InternalName	MRMWrapperDiction.exe
FileVersion	1.4.8.0
CompanyName	BASeCamp Software Solutions
LegalTrademarks	
Comments	
ProductName	BASeCamp JobClock
ProductVersion	1.4.8.0
FileDescription	JobClock Administration Applet
OriginalFilename	MRMWrapperDiction.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3185.140.53.349767317892025019 05/10/22-11:54:04.775428	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49767	31789	192.168.2.3	185.140.53.3

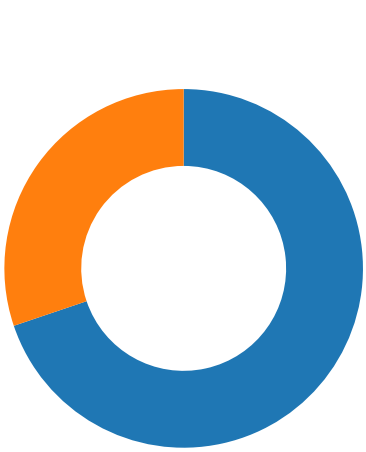
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3185.140.53.349778317892025019 05/10/22-11:54:18.335094	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349826317892816766 05/10/22-11:54:42.317503	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49826	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349867317892816766 05/10/22-11:55:08.482183	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49867	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349868317892816766 05/10/22-11:55:15.380950	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49868	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349843317892816766 05/10/22-11:54:56.333885	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49843	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349762317892025019 05/10/22-11:53:57.886255	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349758317892025019 05/10/22-11:53:52.880985	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349782317892025019 05/10/22-11:54:25.487213	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349771317892025019 05/10/22-11:54:11.319386	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349750317892025019 05/10/22-11:53:37.365565	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349752317892025019 05/10/22-11:53:45.193397	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349750317892816766 05/10/22-11:53:38.950679	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49750	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349782317892816766 05/10/22-11:54:26.713499	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49782	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349762317892816766 05/10/22-11:53:59.504378	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49762	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349771317892816766 05/10/22-11:54:13.062923	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49771	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349837317892816766 05/10/22-11:54:49.300837	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49837	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349816317892816766 05/10/22-11:54:33.736622	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49816	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349816317892025019 05/10/22-11:54:32.532276	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49816	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.349869317892025019 05/10/22-11:55:20.675127	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49869	31789	192.168.2.3	185.140.53.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
185.140.53.3192.168.2.33 1789498642841753 05/10/22-11:55:01.918437	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	31789	49864	185.140.53.3	192.168.2.3
192.168.2.3185.140.53.34 9752317892816766 05/10/22-11:53:47.498984	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49752	31789	192.168.2.3	185.140.53.3
185.140.53.3192.168.2.33 1789498692810451 05/10/22-11:55:45.875144	TCP	2810451	ETPRO TROJAN NanoCore RAT Keepalive Response 3	31789	49869	185.140.53.3	192.168.2.3
192.168.2.3185.140.53.34 9867317892025019 05/10/22-11:55:06.652869	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49867	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.34 9868317892025019 05/10/22-11:55:14.375651	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49868	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.34 9767317892816766 05/10/22-11:54:06.037273	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49767	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.34 9778317892816766 05/10/22-11:54:20.124819	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49778	31789	192.168.2.3	185.140.53.3
185.140.53.3192.168.2.33 1789498692841753 05/10/22-11:55:45.875144	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	31789	49869	185.140.53.3	192.168.2.3
185.140.53.3192.168.2.33 1789498692810290 05/10/22-11:55:23.881709	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	31789	49869	185.140.53.3	192.168.2.3
192.168.2.3185.140.53.34 9826317892025019 05/10/22-11:54:39.732514	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49826	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.34 9837317892025019 05/10/22-11:54:47.544258	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49837	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.34 9771317892816718 05/10/22-11:54:13.062923	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49771	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.34 9864317892025019 05/10/22-11:55:01.707210	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49864	31789	192.168.2.3	185.140.53.3
185.140.53.3192.168.2.33 1789497582841753 05/10/22-11:53:53.093006	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	31789	49758	185.140.53.3	192.168.2.3
192.168.2.3185.140.53.34 9843317892025019 05/10/22-11:54:54.648860	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49843	31789	192.168.2.3	185.140.53.3
192.168.2.3185.140.53.34 9868317892816718 05/10/22-11:55:15.380950	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49868	31789	192.168.2.3	185.140.53.3

Network Port Distribution

Total Packets: 53

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 11:53:37.110084057 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:37.303845882 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:37.304080009 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:37.365565062 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:37.653333902 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:37.668632984 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:37.879831076 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:37.939357996 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:38.355535984 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:38.355720043 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:38.605391979 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:38.605454922 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:38.605638981 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:38.805238008 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:38.805272102 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:38.805288076 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:38.805382967 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:38.807291031 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:38.809726000 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:38.950679064 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.014911890 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.014954090 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.014977932 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.015104055 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.015157938 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.016700983 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.017688036 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.017786980 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.017833948 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.017862082 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.021110058 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.021997929 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.022931099 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.023113966 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.211493015 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.212590933 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.212636948 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.212661982 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.215523958 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.215563059 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.215579033 CEST	31789	49750	185.140.53.3	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 11:53:39.215610981 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.215642929 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.217804909 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.219566107 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.219583988 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.219633102 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.221483946 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.221529007 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.221549034 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.222563028 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.222616911 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.226156950 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.226175070 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.226191044 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.226237059 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.227515936 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.227587938 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.414208889 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.414334059 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.414391041 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.415216923 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.415285110 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.415319920 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.415322065 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.415399075 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.415435076 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.417263031 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.417573929 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.417612076 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.417612076 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.419213057 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.419253111 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.419264078 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.420223951 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.420264006 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.420334101 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.421292067 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.421333075 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.421366930 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.422338009 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.422455072 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.422480106 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.433501959 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.433630943 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.433648109 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.433720112 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.433741093 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.435477972 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.435518026 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.435544968 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.436760902 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.436780930 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.436810970 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.436851025 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.436868906 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.436888933 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.438604116 CEST	31789	49750	185.140.53.3	192.168.2.3
May 10, 2022 11:53:39.438669920 CEST	49750	31789	192.168.2.3	185.140.53.3
May 10, 2022 11:53:39.438672066 CEST	31789	49750	185.140.53.3	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 11:53:36.991666079 CEST	58116	53	192.168.2.3	8.8.8.8
May 10, 2022 11:53:37.100851059 CEST	53	58116	8.8.8.8	192.168.2.3
May 10, 2022 11:53:44.852917910 CEST	65358	53	192.168.2.3	8.8.8.8
May 10, 2022 11:53:44.961446047 CEST	53	65358	8.8.8.8	192.168.2.3
May 10, 2022 11:53:52.551485062 CEST	53802	53	192.168.2.3	8.8.8.8
May 10, 2022 11:53:52.658183098 CEST	53	53802	8.8.8.8	192.168.2.3
May 10, 2022 11:53:57.567101002 CEST	49327	53	192.168.2.3	8.8.8.8
May 10, 2022 11:53:57.677052021 CEST	53	49327	8.8.8.8	192.168.2.3
May 10, 2022 11:54:04.547096014 CEST	63146	53	192.168.2.3	8.8.8.8
May 10, 2022 11:54:04.564308882 CEST	53	63146	8.8.8.8	192.168.2.3
May 10, 2022 11:54:11.105657101 CEST	58625	53	192.168.2.3	8.8.8.8
May 10, 2022 11:54:11.122956991 CEST	53	58625	8.8.8.8	192.168.2.3
May 10, 2022 11:54:18.103682995 CEST	55151	53	192.168.2.3	8.8.8.8
May 10, 2022 11:54:18.123296022 CEST	53	55151	8.8.8.8	192.168.2.3
May 10, 2022 11:54:25.232455015 CEST	64996	53	192.168.2.3	8.8.8.8
May 10, 2022 11:54:25.250078917 CEST	53	64996	8.8.8.8	192.168.2.3
May 10, 2022 11:54:32.229193926 CEST	50450	53	192.168.2.3	8.8.8.8
May 10, 2022 11:54:32.337620974 CEST	53	50450	8.8.8.8	192.168.2.3
May 10, 2022 11:54:39.297074080 CEST	50608	53	192.168.2.3	8.8.8.8
May 10, 2022 11:54:39.405493975 CEST	53	50608	8.8.8.8	192.168.2.3
May 10, 2022 11:54:47.325944901 CEST	54096	53	192.168.2.3	8.8.8.8
May 10, 2022 11:54:47.343204021 CEST	53	54096	8.8.8.8	192.168.2.3
May 10, 2022 11:54:54.328751087 CEST	57829	53	192.168.2.3	8.8.8.8
May 10, 2022 11:54:54.437845945 CEST	53	57829	8.8.8.8	192.168.2.3
May 10, 2022 11:55:01.386909962 CEST	63326	53	192.168.2.3	8.8.8.8
May 10, 2022 11:55:01.495198011 CEST	53	63326	8.8.8.8	192.168.2.3
May 10, 2022 11:55:06.434148073 CEST	57442	53	192.168.2.3	8.8.8.8
May 10, 2022 11:55:06.453212023 CEST	53	57442	8.8.8.8	192.168.2.3
May 10, 2022 11:55:13.546652079 CEST	51557	53	192.168.2.3	8.8.8.8
May 10, 2022 11:55:13.654952049 CEST	53	51557	8.8.8.8	192.168.2.3
May 10, 2022 11:55:20.432488918 CEST	65334	53	192.168.2.3	8.8.8.8
May 10, 2022 11:55:20.449237108 CEST	53	65334	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 10, 2022 11:53:36.991666079 CEST	192.168.2.3	8.8.8.8	0x5c6	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:53:44.852917910 CEST	192.168.2.3	8.8.8.8	0x8e0f	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:53:52.551485062 CEST	192.168.2.3	8.8.8.8	0xa59f	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:53:57.567101002 CEST	192.168.2.3	8.8.8.8	0xd93a	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:54:04.547096014 CEST	192.168.2.3	8.8.8.8	0xa2cc	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:54:11.105657101 CEST	192.168.2.3	8.8.8.8	0x945f	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:54:18.103682995 CEST	192.168.2.3	8.8.8.8	0xc9e	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:54:25.232455015 CEST	192.168.2.3	8.8.8.8	0x9285	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:54:32.229193926 CEST	192.168.2.3	8.8.8.8	0xe093	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:54:39.297074080 CEST	192.168.2.3	8.8.8.8	0x1de0	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:54:47.325944901 CEST	192.168.2.3	8.8.8.8	0x4064	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:54:54.328751087 CEST	192.168.2.3	8.8.8.8	0x7337	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:55:01.386909962 CEST	192.168.2.3	8.8.8.8	0x3081	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)

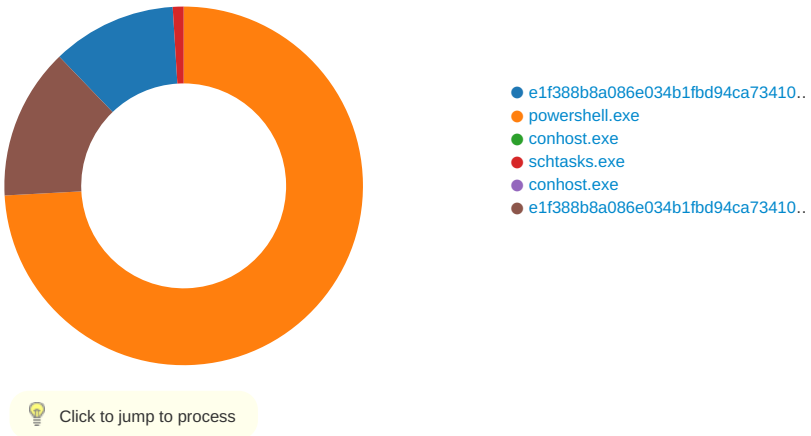
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 10, 2022 11:55:06.434148073 CEST	192.168.2.3	8.8.8.8	0xf36d	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:55:13.546652079 CEST	192.168.2.3	8.8.8.8	0x5962	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)
May 10, 2022 11:55:20.432488918 CEST	192.168.2.3	8.8.8.8	0xc1a8	Standard query (0)	ella666.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2022 11:53:37.100851059 CEST	8.8.8.8	192.168.2.3	0x5c6	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:53:44.961446047 CEST	8.8.8.8	192.168.2.3	0x8e0f	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:53:52.658183098 CEST	8.8.8.8	192.168.2.3	0xa59f	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:53:57.677052021 CEST	8.8.8.8	192.168.2.3	0xd93a	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:54:04.564308882 CEST	8.8.8.8	192.168.2.3	0xa2cc	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:54:11.122956991 CEST	8.8.8.8	192.168.2.3	0x945f	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:54:18.123296022 CEST	8.8.8.8	192.168.2.3	0xc9e	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:54:25.250078917 CEST	8.8.8.8	192.168.2.3	0x9285	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:54:32.337620974 CEST	8.8.8.8	192.168.2.3	0xe093	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:54:39.405493975 CEST	8.8.8.8	192.168.2.3	0x1de0	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:54:47.343204021 CEST	8.8.8.8	192.168.2.3	0x4064	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:54:54.437845945 CEST	8.8.8.8	192.168.2.3	0x7337	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:55:01.495198011 CEST	8.8.8.8	192.168.2.3	0x3081	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:55:06.453212023 CEST	8.8.8.8	192.168.2.3	0xf36d	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:55:13.654952049 CEST	8.8.8.8	192.168.2.3	0x5962	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)
May 10, 2022 11:55:20.449237108 CEST	8.8.8.8	192.168.2.3	0xc1a8	No error (0)	ella666.duckdns.org		185.140.53.3	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: e1f388b8a086e034b1fbd94ca7341008.exe PID: **6952**, Parent PID: **160**

General

Target ID:	0
Start time:	11:53:14
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.exe"
Imagebase:	0x760000
File size:	1159168 bytes
MD5 hash:	916EB825989BC96A10EAB8916995C1E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.293486073.0000000002DEB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.292920833.0000000002C31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.294855459.0000000003DDF000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.294855459.0000000003DDF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.294855459.0000000003DDF000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
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	6DBDCF06	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	6DBDCF06	unknown
C:\Users\user\AppData\Roaming\QgGSCvPvvCY.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	6CB2DD66	CopyFileW
C:\Users\user\AppData\Roaming\QgGSCvPvvCY.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CB2DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp5BA5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB27038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\e1f388b8a086e034b1fbd94ca7341008.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEEC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5BA5.tmp	success or wait	1	6CB26A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QgGSCvPvvCY.exe	0	262144	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 2f 17 7a 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 54 10 00 00 5a 01 00 00 00 00 00 fd 72 10 00 00 20 00 00 00 fd 10 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 00 12 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.$PEL/zb0TZr @ @	success or wait	5	6CB2DD66	CopyFileW
C:\Users\user\AppData\Roaming\QgGSCvPvvCY.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	6CB2DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp5BA5.tmp	0	1598	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	6CB21B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\e1f388b8a086e034b1fbd94ca734108.exe.log	0	1308	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	6DEEC907	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	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB21B4F	ReadFile

Analysis Process: powershell.exe PID: **5508**, Parent PID: **6952**

General

Target ID:	4
Start time:	11:53:26
Start date:	10/05/2022
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\QgGSCvPvvCY.exe
Imagebase:	0x870000
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBDCF06	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	6DBDCF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ryl20vvq.5q2.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CB21E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_axfdujok.0nl.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CB21E60	CreateFileW
C:\Users\user\Documents\20220510	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB2BEFF	CreateDirectoryW
C:\Users\user\Documents\20220510\PowerShell_transcript.284992.KzD+VzNg.20220510115327.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CB21E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ryl20vvq.5q2.ps1	success or wait	1	6CB26A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_axfdujok.0nl.psm1	success or wait	1	6CB26A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ryl20vvq.5q2.ps1	0	1	31	1	success or wait	1	6CB21B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_axfdujok.0nl.psm1	0	1	31	1	success or wait	1	6CB21B4F	WriteFile
C:\Users\user\Documents\20220510\PowerShell_transcript.284992.KzD+VzNg.20220510115327.txt	0	3	ff		success or wait	1	6CB21B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220510\PowerShell_transcript.284992.KzD+VzNg.20220510115327.txt	3	678	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 31 30 31 31 35 33 32 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 38 34 39 39 32 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220510115328Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 284992 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6CB21B4F	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 70 14 00 00 19 00 00 00 68 0d 10 05 57 08 4e 08 4b 08 00 00 fd 00 79 00 0b 00 48 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@ephWNKyH@	success or wait	1	6DEA76FC	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	6DEA76FC	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	6DEA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DEA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DEA76FC	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 40 01 fd 44 40 01 6d 45 40 01 45 4d 40 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@BM@D@mE@EM@qqS%n4&5&7&	success or wait	11	6DEA76FC	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	6DBB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBBCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBBCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBB5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DBC1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23196	success or wait	1	6DBC203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB103DE	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	6CB21B4F	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	6CB21B4F	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	6CB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	138	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CB21B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CB21B4F	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	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	3	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	68	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CB21B4F	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	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	15	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	2	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CB21B4F	ReadFile

Analysis Process: conhost.exe PID: **5144**, Parent PID: **5508**

General

Target ID:	5
Start time:	11:53:26
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: schtasks.exe PID: **5204**, Parent PID: **6952**

General

Target ID:	6
Start time:	11:53:26
Start date:	10/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QgGSCvPvvCY" /XML "C:\Users\user\AppData\Local\Temp\tmp5BA5.tmp
Imagebase:	0x9b0000
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\tmp5BA5.tmp	unknown	2	success or wait	1	9BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp5BA5.tmp	unknown	1599	success or wait	1	9BABD9	ReadFile

Analysis Process: conhost.exe PID: **6292**, Parent PID: **5204**

General

Target ID:	7
Start time:	11:53:27
Start date:	10/05/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: e1f388b8a086e034b1fbd94ca7341008.exe PID: **3312**, Parent PID: **6952**

General

Target ID:	8
Start time:	11:53:29
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.exe
Imagebase:	0x840000
File size:	1159168 bytes
MD5 hash:	916EB825989BC96A10EAB8916995C1E1
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: 00000008.00000002.519250618.0000000003D81000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.515876792.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.515876792.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.515876792.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.288319319.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.288319319.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.288319319.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.289425663.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.289425663.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.289425663.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.520324734.0000000005540000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.520324734.0000000005540000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.520324734.0000000005540000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.286410609.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.286410609.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.286410609.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.288866971.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.288866971.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.288866971.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.520506917.00000000057F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.520506917.00000000057F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.520506917.00000000057F0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.520506917.00000000057F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.518021079.0000000002D21000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	6DBDCF06	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	6DBDCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB2BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CB21E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB2BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB2BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	11	6CB21E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.exe:Zone.Identifier	success or wait	1	52F7C7E	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd 0f 00 63 fd 32 fd 48	c2H	success or wait	1	6CB21B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	12	6CB21B4F	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	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.exe	unknown	4096	success or wait	1	6DB9D72F	unknown
C:\Users\user\Desktop\e1f388b8a086e034b1fbd94ca7341008.exe	unknown	512	success or wait	1	6DB9D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6DB9D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DB9D72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DB9D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DB9D72F	unknown

Disassembly

No disassembly