ID: 626765
Sample Name: DN8slYDJr3.exe
Cookbook: default.jbs
Time: 05:53:17
Date: 15/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

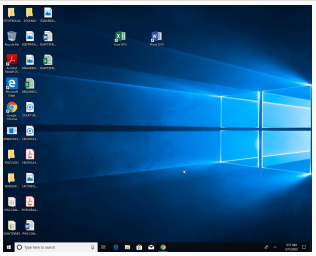
Windows Analysis Report

DN8slYDJr3.exe

Overview

General Information

Sample Name:	DN8slYDJr3.exe
Analysis ID:	626765
MD5:	a6fe8903e74115..
SHA1:	772e00c83eeae0..
SHA256:	63ad21733d5e1d.
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

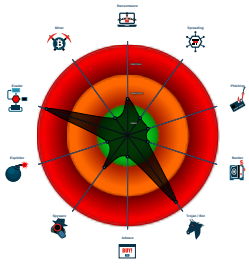
Nanocore

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 drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- DN8slYDJr3.exe (PID: 6440 cmdline: "C:\Users\user\Desktop\DN8slYDJr3.exe" MD5: A6FE8903E741154BC80352D0EE73EFFF)
  - powershell.exe (PID: 6788 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\lulEJNIqTKEFv.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6816 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lulEJNIqTKEFv" /XML "C:\Users\user\AppData\Local\Temp\tmp2ADE.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 7012 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "2dd75230-c203-4336-94aa-262a8b3e",
  "Group": "Mallow",
  "Domain1": "mallow.3utilities.com",
  "Domain2": "mallow2.3utilities.com",
  "Port": 83,
  "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": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000000.283747964.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000008.00000000.283747964.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000008.00000000.283747964.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000000.00000002.289573778.0000000004171000.00000004.00000800.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1a93b5:$x1: NanoCore.ClientPluginHost • 0x1a93f2:$x2: IClientNetworkHost • 0x1acf25:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.289573778.0000000004171000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 18 entries

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
8.3.RegSvcs.exe.1671486.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x39eb:$x1: NanoCore.ClientPluginHost • 0xb9eb:$x1: NanoCore.ClientPluginHost • 0x3a24:$x2: IClientNetworkHost • 0xba24:$x2: IClientNetworkHost
8.3.RegSvcs.exe.1671486.0.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x39eb:$x2: NanoCore.ClientPluginHost • 0xb9eb:$x2: NanoCore.ClientPluginHost • 0x3b36:$s4: PipeCreated • 0xbb36:$s4: PipeCreated • 0x3a05:$s5: IClientLoggingHost • 0xba05:$s5: IClientLoggingHost
8.3.RegSvcs.exe.1671486.0.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x3a8b:$x2: NanoCore.ClientPlugin • 0xba8b:$x2: NanoCore.ClientPlugin • 0x39eb:$x3: NanoCore.ClientPluginHost • 0xb9eb:$x3: NanoCore.ClientPluginHost • 0x3aa1:$i3: IClientNetwork • 0xbaa1:$i3: IClientNetwork • 0x3a43:$i5: IClientDataHost • 0xba43:$i5: IClientDataHost • 0x3a05:$i6: IClientLoggingHost • 0xba05:$i6: IClientLoggingHost • 0x3a24:$i7: IClientNetworkHost • 0xba24:$i7: IClientNetworkHost • 0x426c:$i9: IClientNameObjectCollection • 0xc26c:$i9: IClientNameObjectCollection • 0x3741:$s1: ClientPlugin • 0x3a94:$s1: ClientPlugin • 0xb741:$s1: ClientPlugin • 0xba94:$s1: ClientPlugin • 0x4680:$s2: EndPoint • 0xc680:$s2: EndPoint • 0x4371:$s3: IPAddress
0.2.DN8slYDJr3.exe.477a1c0.6.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.DN8slYDJr3.exe.477a1c0.6.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
Click to see the 49 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

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 109.248.150.171 −

Timestamp:	192.168.2.3109.248.150.17149771832816766 05/15/22-05:56:07.894508

SID:	2816766
Source Port:	49771
Destination Port:	83
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 109.248.150.171 - Destination IP: 192.168.2.3	
Timestamp:	109.248.150.171192.168.2.383497542841753 05/15/22-05:55:28.352765
SID:	2841753
Source Port:	83
Destination Port:	49754
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 109.248.150.171 - Destination IP: 192.168.2.3	
Timestamp:	109.248.150.171192.168.2.383497452841753 05/15/22-05:54:57.696804
SID:	2841753
Source Port:	83
Destination Port:	49745
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 109.248.150.171 - Destination IP: 192.168.2.3	
Timestamp:	109.248.150.171192.168.2.383497492841753 05/15/22-05:55:02.792533
SID:	2841753
Source Port:	83
Destination Port:	49749
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 109.248.150.171	
Timestamp:	192.168.2.3109.248.150.17149738832816766 05/15/22-05:54:43.813398
SID:	2816766
Source Port:	49738
Destination Port:	83
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 109.248.150.171	
Timestamp:	192.168.2.3109.248.150.17149751832816766 05/15/22-05:55:09.867717
SID:	2816766
Source Port:	49751
Destination Port:	83
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 109.248.150.171 - Destination IP: 192.168.2.3	
Timestamp:	109.248.150.171192.168.2.383497582841753 05/15/22-05:55:39.462032
SID:	2841753
Source Port:	83
Destination Port:	49758
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 109.248.150.171	
Timestamp:	192.168.2.3109.248.150.17149743832816766 05/15/22-05:54:52.689575
SID:	2816766
Source Port:	49743
Destination Port:	83
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 109.248.150.171	
Timestamp:	192.168.2.3109.248.150.17149770832816766 05/15/22-05:55:59.950651
SID:	2816766
Source Port:	49770
Destination Port:	83
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 109.248.150.171	
Timestamp:	192.168.2.3109.248.150.17149752832816766 05/15/22-05:55:15.941176
SID:	2816766
Source Port:	49752
Destination Port:	83
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 109.248.150.171 - Destination IP: 192.168.2.3	
Timestamp:	109.248.150.171192.168.2.383497692841753 05/15/22-05:55:51.676335
SID:	2841753
Source Port:	83
Destination Port:	49769
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 109.248.150.171	
Timestamp:	192.168.2.3109.248.150.17149753832816766 05/15/22-05:55:21.968753
SID:	2816766
Source Port:	49753
Destination Port:	83
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 109.248.150.171 - Destination IP: 192.168.2.3	
Timestamp:	109.248.150.171192.168.2.383498022841753 05/15/22-05:56:18.173297
SID:	2841753
Source Port:	83
Destination Port:	49802
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 109.248.150.171 - Destination IP: 192.168.2.3	
Timestamp:	109.248.150.171192.168.2.383497782841753 05/15/22-05:56:13.009421
SID:	2841753
Source Port:	83
Destination Port:	49778
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 109.248.150.171	
Timestamp:	192.168.2.3109.248.150.17149757832816766 05/15/22-05:55:34.302368
SID:	2816766
Source Port:	49757
Destination Port:	83
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 109.248.150.171 - Destination IP: 192.168.2.3	
Timestamp:	109.248.150.171192.168.2.383498202841753 05/15/22-05:56:28.052052

SID:	2841753
Source Port:	83
Destination Port:	49820
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 109.248.150.171	−
Timestamp:	192.168.2.3109.248.150.17149767832816766 05/15/22-05:55:46.492067
SID:	2816766
Source Port:	49767
Destination Port:	83
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 dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

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

Writes to foreign memory regions

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

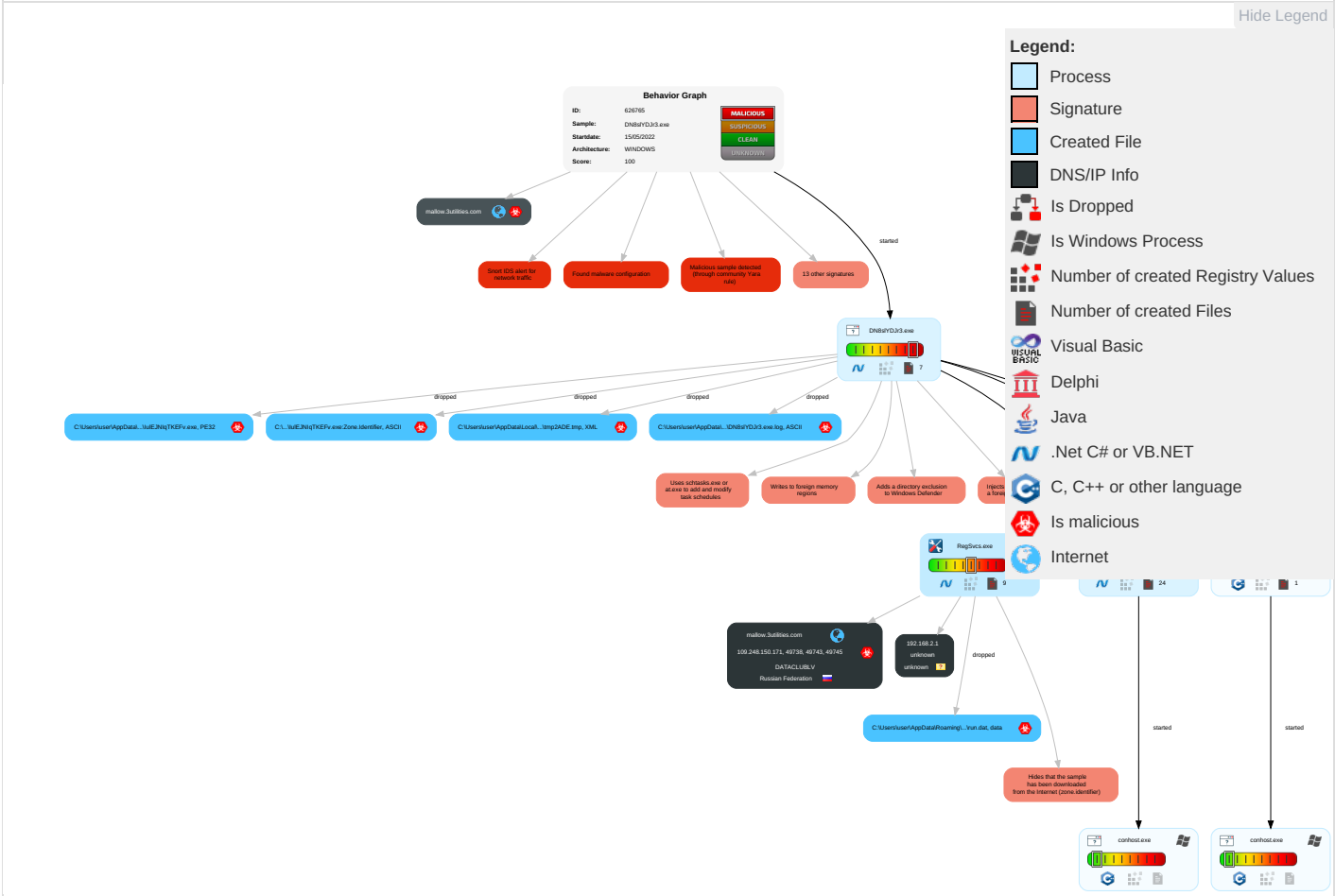
Detected Nanocore Rat

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	1 Windows Management Instrumentation	1 Scheduled Task/Job	2 1 1 Process Injection	1 Masquerading	1 Input Capture	2 1 1 Security Software Discovery	Remote Services	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	1 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	At (Linux)	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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 1 1 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	1 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	2 3 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
DN8slYDJr3.exe	56%	Virustotal		Browse
DN8slYDJr3.exe	63%	ReversingLabs	ByteCode-MSIL.Spyware.Negasteal	
DN8slYDJr3.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\lulEJNIqTKEFv.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\lulEJNIqTKEFv.exe	63%	ReversingLabs	ByteCode-MSIL.Spyware.Negasteal	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
8.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
mallow.3utilities.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/H	0%	URL Reputation	safe	
http://www.sajatypeworks.com;	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comivd	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
mallow.3utilities.com	3%	Virustotal		Browse
mallow.3utilities.com	100%	Avira URL Cloud	phishing	
http://www.founder.com.cn/cnH	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.founder.com.cn/cnB	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.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comueetd	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://www.galapagosdesign.com/JQ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0o	0%	Avira URL Cloud	safe	
http://www.fontbureau.com3	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.sajatypeworks.comaH	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0V	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com_	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/%	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.commr	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnr-cM	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsF1	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comgretao	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/r	0%	URL Reputation	safe	
http://en.wikipedia	0%	URL Reputation	safe	
http://www.sajatypeworks.come%	0%	Avira URL Cloud	safe	
mallow2.3utilities.com	100%	Avira URL Cloud	phishing	
http://www.founder.com.cn/cna-di	0%	Avira URL Cloud	safe	
http://www.fontbureau.commV	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.coma3	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comituV	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mallow.3utilities.com	109.248.150.171	true	true	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
mallow.3utilities.com	true	• 3%, Virustotal, Browse • Avira URL Cloud: phishing	unknown
mallow2.3utilities.com	true	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comI.TTF	DN8slYDJr3.exe, 00000000.00000003.250839452.0000000006128000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.250397967.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/H	DN8slYDJr3.exe, 00000000.00000003.245158910.000000000612B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.245071450.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com;	DN8slYDJr3.exe, 00000000.00000003.241147992.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.240973696.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241983094.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243249366.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.244612243.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241744081.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243416460.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241544747.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243092635.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241399274.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242884518.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243629445.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241508783.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243942870.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241924169.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242265504.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241318656.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.244093097.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243557493.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241016314.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242425287.000000000613B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comivd	DN8slYDJr3.exe, 00000000.00000003.241147992.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.240973696.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241983094.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243249366.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.244612243.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241744081.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243416460.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241544747.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243092635.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241399274.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242884518.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243629445.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241508783.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243942870.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241924169.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242265504.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243318656.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.244093097.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243557493.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241016314.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242425287.000000000613B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnH	DN8slYDJr3.exe, 00000000.00000003.242950568.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalsF	DN8slYDJr3.exe, 00000000.00000003.250839452.0000000006128000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnB	DN8slYDJr3.exe, 00000000.00000003.242950568.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/:	DN8slYDJr3.exe, 00000000.00000003.245158910.000000000612B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.245071450.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comueetd	DN8slYDJr3.exe, 00000000.00000003.250839452.0000000006128000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.250397967.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/3	DN8slYDJr3.exe, 00000000.00000003.245158910.000000000612B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.245071450.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/JQ	DN8slYDJr3.exe, 00000000.00000003.253233910.0000000006158000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.252988978.0000000006158000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.252858930.0000000006158000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.253034202.0000000006158000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.253083642.0000000006158000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0o	DN8slYDJr3.exe, 00000000.00000003.245158910.000000000612B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.245071450.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com3	DN8slYDJr3.exe, 00000000.00000003.250839452.0000000006128000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.250397967.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcom	DN8slYDJr3.exe, 00000000.00000003.250839452.0000000006128000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.250397967.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comaH	DN8slYDJr3.exe, 00000000.00000003.241147992.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.240973696.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241983094.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243249366.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.244612243.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241744081.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243416460.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241544747.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243092635.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241399274.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242884518.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243629445.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241508783.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243942870.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241924169.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242265504.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241318656.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.244093097.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243557493.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241016314.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242425287.000000000613B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0V	DN8slYDJr3.exe, 00000000.00000003.245158910.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

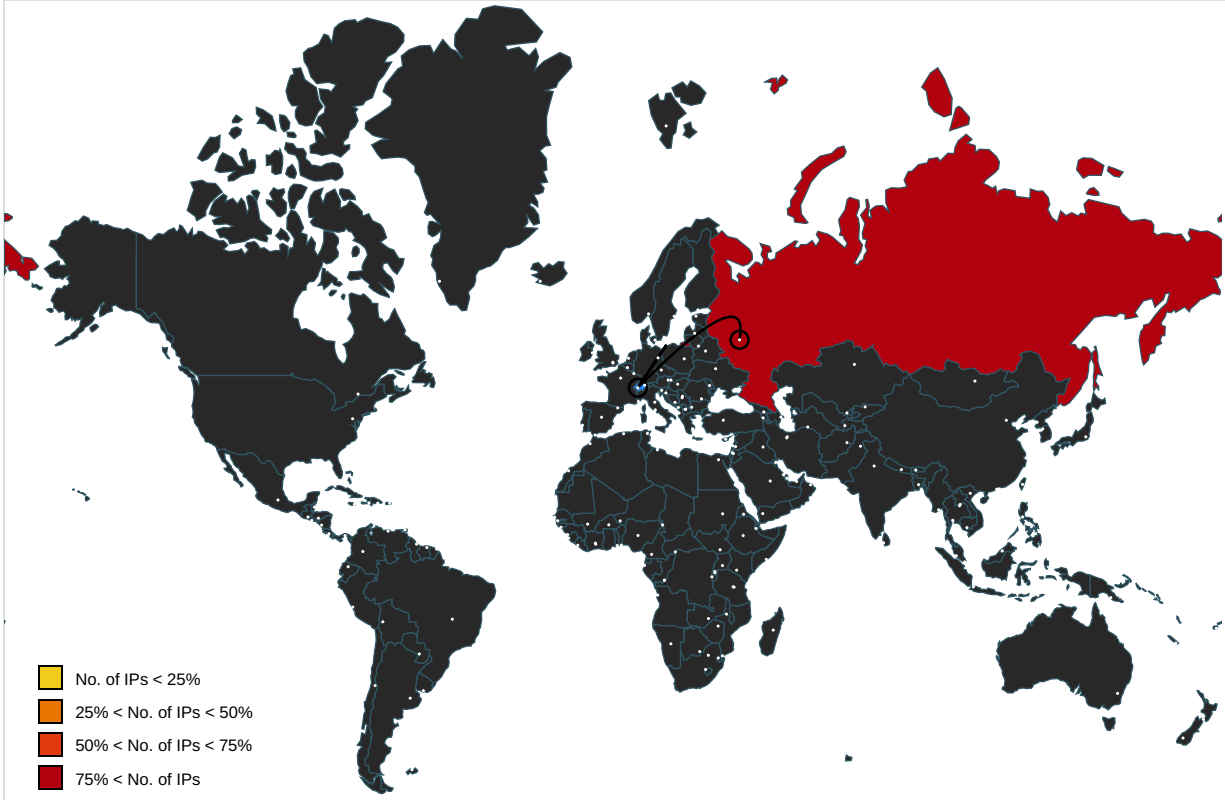
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com_	DN8slYDJr3.exe, 00000000.00000003.241147992.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.240973696.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241983094.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243249366.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.244612243.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241744081.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243416460.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241544747.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243092635.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241399274.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242884518.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243629445.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241508783.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243942870.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241924169.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242265504.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241318656.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.244093097.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243557493.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241016314.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242425287.000000000613B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fonts.com	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/%	DN8slYDJr3.exe, 00000000.00000003.245158910.000000000612B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.245071450.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kr	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	DN8slYDJr3.exe, 00000000.00000002.287530312.0000000003171000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.commr	DN8slYDJr3.exe, 00000000.00000003.250839452.0000000006128000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.250397967.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnr-cM	DN8slYDJr3.exe, 00000000.00000003.242950568.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comalsF1	DN8slYDJr3.exe, 00000000.00000003.250397967.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	DN8slYDJr3.exe, 00000000.00000003.250839452.0000000006128000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.250397967.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	DN8slYDJr3.exe, 00000000.00000003.252858930.0000000006158000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgretao	DN8slYDJr3.exe, 00000000.00000003.285353913.0000000006120000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.257046421.000000000612A000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000002.296409775.0000000006120000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/r	DN8slYDJr3.exe, 00000000.00000003.245158910.000000000612B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.245071450.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.wikipedia	DN8slYDJr3.exe, 00000000.00000003.240622717.0000000006143000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.240647322.0000000006142000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.come%	DN8slYDJr3.exe, 00000000.00000003.241147992.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.240973696.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241983094.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243249366.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.244612243.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241744081.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243416460.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241544747.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243092635.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241399274.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242884518.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243629445.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241508783.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243942870.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241924169.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242265504.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241318656.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.244093097.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.243557493.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.241016314.000000000613B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242425287.000000000613B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cna-di	DN8slYDJr3.exe, 00000000.00000003.242745769.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.commV	DN8slYDJr3.exe, 00000000.00000003.285353913.0000000006120000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.257046421.000000000612A000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000002.296409775.0000000006120000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	DN8slYDJr3.exe, 00000000.00000003.245158910.000000000612B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.245071450.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	DN8slYDJr3.exe, 00000000.00000003.250839452.0000000006128000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.250397967.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	DN8slYDJr3.exe, 00000000.00000003.241072805.0000000006126000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.coma3	DN8slYDJr3.exe, 00000000.00000003.285353913.0000000006120000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.257046421.000000000612A000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000002.296409775.0000000006120000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	DN8slYDJr3.exe, 00000000.00000003.242899291.0000000006128000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.242745769.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	DN8slYDJr3.exe, 00000000.00000003.245071450.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	DN8slYDJr3.exe, 00000000.00000002.296539257.0000000007332000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comituV	DN8slYDJr3.exe, 00000000.00000003.250839452.0000000006128000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.250397967.0000000006127000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/d	DN8slYDJr3.exe, 00000000.00000003.245158910.000000000612B000.00000004.00000800.00020000.00000000.sdmp, DN8slYDJr3.exe, 00000000.00000003.245071450.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.248.150.171	mallow.3utilities.com	Russian Federation		52048	DATACLUBLV	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626765
Start date and time: 15/05/202205:53:17	2022-05-15 05:53:17 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DN8slYDJr3.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:	34
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@9/12@17/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 60.1% • Quality standard deviation: 38.5%
HCA Information:	• Successful, ratio: 88% • 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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, go.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.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 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
05:55:14	API Interceptor	1x Sleep call for process: DN8slYDJr3.exe modified
05:55:23	API Interceptor	40x Sleep call for process: powershell.exe modified
05:55:28	API Interceptor	844x Sleep call for process: RegSvcs.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\DN8slYDJr3.exe.log

Process:	C:\Users\user\Desktop\DN8slYDJr3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4FsXE8:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHJ
MD5:	EA78C102145ED608EF0E407B978AF339
SHA1:	66C9179ED9675B9271A97AB1FC878077E09AB731
SHA-256:	8BF01E0C445BD07C0B4EDC7199B7E17DAF1CA55CA52D4A6EAC4EF211C2B1A73E
SHA-512:	8C04139A1FC3C3BDACB680EC443615A43EB18E73B5A0CFCA644CB4A5E71746B275B3E238DD1A5A205405313E457BB75F9BBB93277C67AFA5D78DCFA30E5DA02B
Malicious:	**true**
Reputation:	moderate, 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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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=b77a

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):	22272
Entropy (8bit):	5.6012805385595374
Encrypted:	false
SSDEEP:	384:3tMjDsh0mVQr5S7m3eOYSBKnwjultI+b7Y9gcSJ3xOT1MR7ZlbAV7gBwKZBDI+iB:GUQ5kwY4KwClth7ccUChfwcVo
MD5:	4D79D8CB401FDFC04F9E03CA87ED2C7A
SHA1:	821F58E4D01AFC06AE97561C1C184CDB65FD6692
SHA-256:	A2024CA244F691E72EA043DBCD704DA31F9AF33AD673FA181271AD7762D1B6AE
SHA-512:	93B187C634803B41B072E69777CB7439C30B7E7FC3D9C6D0C1043B378408D43B21963928480B015291A2F20606966B2866ADDF1D81A9EA4EB56B2F0875C28580

Malicious:	false
Reputation:	low
Preview:	@...e.....y.....h.".E.<.9.....I.....@.....H.....<@.^.L."My...:X..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.. .....'....L..}.....System.Numerics.4.....Zg5..:O..g..q.....System.Xml..@.....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.....Sy stem.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_jhkev1fh.4vf.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_m2k5xmri.aaz.psm1

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

C:\Users\user\AppData\Local\Temp\tmp2ADE.tmp

Process:	C:\Users\user\Desktop\DN8slYDJr3.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1600
Entropy (8bit):	5.159339618769527
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNt9xvn:cge4MYrFdOFzOzN33ODOiDdKrsuTDv
MD5:	5D6452ACB55BD8182F9E3BEE2FDA460D
SHA1:	27AD05A72FCC6E63D3AB0AFAF614D7AC5F8A78B7
SHA-256:	ACE22EF71978C4709786CAF11262D33D5C7E6E4ED2E8609315333321900803DA
SHA-512:	0F19187CFC9331F373412EA98D7C467C762B11F9211B02A4F2DA0296A1AA2E9866923A5994687CCBB74249D1A912F88610959F3D0CB7F03CF9BACF5D93791733
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>2014-1 0-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Princip al id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Vs:G
MD5:	D6C06BC5AAD8EF66419EDE04C8C3E9D1
SHA1:	8C188D1109D036BA2C7B7801AC0A74CF00077D37
SHA-256:	AA56215F55E0D18F8793F6EC5B4390EF8324856B27479B4E57A26908D75BFB12
SHA-512:	F2794281A41F7C7942A3EAFECD3C1A541D8EDB2484A988B75B1B8A7FAED80B91B604AF3CFA4380CB155ABEB3114BBBA6CDB9A3018F41AA8BD6E37C9E884D6147
Malicious:	**true**
Preview:	.U./r6.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	327928
Entropy (8bit):	**7.9994709860950985**
Encrypted:	**true**
SSDEEP:	6144:EV615H8mrxOdiCllSG0fG4DWvsN24t17uyyHAg5TGbgQYZ3CifoqiI9FQvLib8:4615cmrx8fSHfG0Wvs71yHAgRGgzV5K5
MD5:	FAFF7BD1824C990ACE96C5385AE54073
SHA1:	2C14D468D0C8116B448E65D791D3409DC254785D

SHA-256:	1120219B5C6646F6A910CE2A556385DCA8F6C551D0FB05F719D07FE2061932AA
SHA-512:	C5D48611DD5BA55A998C94FD5245BA7FA78F351F0677990F0512CFC2B803310C9B07EFA77A9ABE2FF4ECA25DE054E0860EEB6C89E022BC7689665C42BACCC7D5
Malicious:	false
Preview:	..,!..LJy..5<...9....!..?.AJ.._I..Px.9g..._t..].....t./...a.k.Z3.H...o..>.6.x.E.....hBu*.#.Z..v..).#..x...hI..e...B-<.J0...o...]....%.....51.h..G{.u.|*r..xs.d..#....).&.e.3..6.V+....d.....!..v...)Y.....pe...c.mW.....O.X...>.[.....w^.0.&Z.^5se.(..1 Zq.....G.`y.F.f..T[k.^.fj.o.~...t.=..[...zU8_..b...%.....J.6._..._!{.c... .8...^.....^.,|...7T.c._X/n..Fd.M>.=..Cmwd.%N.S.-..jk!.B.q>S...7.h....?sa.S@..3...G.B.M..Q.f..b....j..0y.i&..$...LIq}&..8F.....m.....=..5O.g...}"4.....z.q.b.Am.A1."]"".....C..F..9.2.u.DL..s.=^.s.@..k.c>.u...rw.W.E....Jn.....$...C...0../.l.M...D._.K.d.2...|...T....1.....g.-x.....U$.I.n...e..|J...AVU.v.I..3.7%&.6.....)....@f.....}TR...g]W8x..."...{.H.....gS,..@.).....L...K7.'V.42...~.b..q.j.V.1...V..`.NW*].l6A...c.<..5..'..u...i...*...L..'..!.cD..m...3~....As.@+....'&..\4_...6..t.jq2lK.K.2..E&.K..wi9...enm.7...0.EVG.Ab....S...(%.of.b.?.J..;."0....0u.%.M....(a...A.LEn....P.z.x.3.8....G.....MT.:

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

Process:	C:\Users\user\Desktop\DN8slYDJr3.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	884736
Entropy (8bit):	7.874267720295541
Encrypted:	false
SSDEEP:	24576:p7DOlquevT6sh7g2781m7U+0aGmBwlt3prONe:p7D8Dev2Mg+IgUoG7lt3Ae
MD5:	A6FE8903E741154BC80352D0EE73EFFF
SHA1:	772E00C83EEAE03EA4C7433F737B8D6A1D8B967E
SHA-256:	63AD21733D5E1DB06FAA9C863422889AE1F185116E02B45A50259E286EE42E50
SHA-512:	1C984A4E72726E2EE01D5A0F14D5E4DB66B72C5B1F5C087CB3599B7FAC2AF726992CDACC2302B4830383B13CC0861E41F36A7A054C4690A25A0404ECE060761B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 63%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z|b.....0.. ...@.....#... ...@....@.. ... .@.....".."..O...@.....`.....|!..... ..... ..H.....text..... ... ... ..... ..`.rsrc.....@... ...@.....@..@.reloc.....`... ...`.....@..B..... .....

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

Process:	C:\Users\user\Desktop\DN8slYDJr3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220515\PowerShell_transcript.347688.VGMBSiq0.20220515055521.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):	5801
Entropy (8bit):	5.433137009420185
Encrypted:	false
SSDEEP:	96:BZYh8NEqDo1ZnZih8NEqDo1ZN4GQjZzh8NEqDo1Zid5ggJZ6:Nq
MD5:	32B4DF8F09E0D13DD9F54D51916A0C88
SHA1:	7C7DCA62D7E5235D69F3CA1E56C84EF60D36592C
SHA-256:	35376FA680A3616E5FEDAC3D0AA1F5908BF36E820872317620C27ED1B54FA126
SHA-512:	4C70233BEFD8BB93FE71B7EBB142E1FE6C9246CBAC5B4D00F01E9CD9CF43B3BA2821167D9EBDAE60BE942ED659B789E5529230F9918E7DC7BFD9101F97504298
Malicious:	false

Preview:	.**********..Windows PowerShell transcript start..Start time: 20220515055522..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 347688 (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\lulEJNIqTKEFv.exe..Process ID: 6788..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: 20220515055522..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\lulEJNIqTKEFv.exe..**********..Windows PowerShell transcript start..Start time: 20220515055902..Username: computer\user..RunAs User: DESKTOP-716T77

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.874267720295541
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	DN8slYDJr3.exe
File size:	884736
MD5:	a6fe8903e741154bc80352d0ee73efff
SHA1:	772e00c83eeae03ea4c7433f737b8d6a1d8b967e
SHA256:	63ad21733d5e1db06faa9c863422889ae1f185116e02b45a50259e286ee42e50
SHA512:	1c984a4e72726e2ee01d5a0f14d5e4db66b72c5b1f5c087cb3599b7fac2af726992cdacc2302b4830383b13cc0861e41f36a7a054c4690a25a0404ece060761b
SSDEEP:	24576:p7DOlquevT6sh7g2781m7U+0aGmBwlt3prONe:p7D8Dev2Mg+IgUoG7lt3Ae
TLSH:	65152338272C2336E81BC7B6CF00E3DDA7B87DA41D00E60F5D9879CCA675B45869256B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z|b.....0.. ...@.....#... ...@....@.. ... .@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d2306
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:	0x627C5AB0 [Thu May 12 00:54:08 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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0xd22b4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd4000	0x5f4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd217c	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd030c	0xd2000	False	0.964989071801	data	7.95859467732	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd4000	0x5f4	0x2000	False	0.0838623046875	data	1.09899540351	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd6000	0xc	0x2000	False	0.0050048828125	data	0.00881485270734	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd4090	0x364	data		
RT_MANIFEST	0xd4404	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2013
Assembly Version	0.0.1.0
InternalName	DynamicAssemblyFl.exe
FileVersion	0.0.1.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	PagedOptionsDialog
ProductVersion	0.0.1.0
FileDescription	PagedOptionsDialog
OriginalFilename	DynamicAssemblyFl.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3109.248.150.17149771832816766 05/15/22-05:56:07.894508	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49771	83	192.168.2.3	109.248.150.171
109.248.150.171192.168.2.383497542841753 05/15/22-05:55:28.352765	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	83	49754	109.248.150.171	192.168.2.3
109.248.150.171192.168.2.383497452841753 05/15/22-05:54:57.696804	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	83	49745	109.248.150.171	192.168.2.3
109.248.150.171192.168.2.383497492841753 05/15/22-05:55:02.792533	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	83	49749	109.248.150.171	192.168.2.3
192.168.2.3109.248.150.17149738832816766 05/15/22-05:54:43.813398	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49738	83	192.168.2.3	109.248.150.171
192.168.2.3109.248.150.17149751832816766 05/15/22-05:55:09.867717	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49751	83	192.168.2.3	109.248.150.171

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
109.248.150.171192.168.2.383497582841753 05/15/22-05:55:39.462032	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	83	49758	109.248.150.171	192.168.2.3
192.168.2.3109.248.150.17149743832816766 05/15/22-05:54:52.689575	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49743	83	192.168.2.3	109.248.150.171
192.168.2.3109.248.150.17149770832816766 05/15/22-05:55:59.950651	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49770	83	192.168.2.3	109.248.150.171
192.168.2.3109.248.150.17149752832816766 05/15/22-05:55:15.941176	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49752	83	192.168.2.3	109.248.150.171
109.248.150.171192.168.2.383497692841753 05/15/22-05:55:51.676335	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	83	49769	109.248.150.171	192.168.2.3
192.168.2.3109.248.150.17149753832816766 05/15/22-05:55:21.968753	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49753	83	192.168.2.3	109.248.150.171
109.248.150.171192.168.2.383498022841753 05/15/22-05:56:18.173297	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	83	49802	109.248.150.171	192.168.2.3
109.248.150.171192.168.2.383497782841753 05/15/22-05:56:13.009421	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	83	49778	109.248.150.171	192.168.2.3
192.168.2.3109.248.150.17149757832816766 05/15/22-05:55:34.302368	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49757	83	192.168.2.3	109.248.150.171
109.248.150.171192.168.2.383498202841753 05/15/22-05:56:28.052052	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	83	49820	109.248.150.171	192.168.2.3
192.168.2.3109.248.150.17149767832816766 05/15/22-05:55:46.492067	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49767	83	192.168.2.3	109.248.150.171

Network Port Distribution

Total Packets: 54

- 53 (DNS)
- 83 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 15, 2022 05:54:42.494297028 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:42.522737980 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:42.522900105 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:42.603166103 CEST	49738	83	192.168.2.3	109.248.150.171

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 15, 2022 05:54:42.680036068 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:42.827708006 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:42.905734062 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:43.707685947 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:43.723180056 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:43.751591921 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:43.813397884 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:43.898201942 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.023403883 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.059678078 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.059747934 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.059787035 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.059815884 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.059825897 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.059866905 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.059906960 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.059912920 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.059947968 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.059961081 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.059988976 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.060029030 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.060069084 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.060075998 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.060488939 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.087606907 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.087675095 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.087713957 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.087754011 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.087752104 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.087794065 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.087805986 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.087836027 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.087877989 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.087903976 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.087915897 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.087958097 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.087997913 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.088011026 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.088037968 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.088080883 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.088093042 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.088123083 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.088162899 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.088181973 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.088205099 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.088243961 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.088275909 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.088285923 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.088303089 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.088326931 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.090013027 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.090070963 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.090104103 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.090130091 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.115858078 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.115926027 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116087914 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116133928 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116174936 CEST	83	49738	109.248.150.171	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 15, 2022 05:54:44.116214037 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116252899 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116292000 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116333961 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116378069 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116416931 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116457939 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116533041 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116575956 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116609097 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.116615057 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116652012 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.116657019 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116697073 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116728067 CEST	83	49738	109.248.150.171	192.168.2.3
May 15, 2022 05:54:44.116761923 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.116796017 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:44.958950996 CEST	49738	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:50.035624027 CEST	49743	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:50.063533068 CEST	83	49743	109.248.150.171	192.168.2.3
May 15, 2022 05:54:50.063818932 CEST	49743	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:50.183475018 CEST	49743	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:50.257505894 CEST	83	49743	109.248.150.171	192.168.2.3
May 15, 2022 05:54:50.326814890 CEST	83	49743	109.248.150.171	192.168.2.3
May 15, 2022 05:54:50.373653889 CEST	49743	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:51.360863924 CEST	49743	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:51.425935984 CEST	83	49743	109.248.150.171	192.168.2.3
May 15, 2022 05:54:51.510365009 CEST	49743	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:51.576093912 CEST	49743	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:51.644898891 CEST	83	49743	109.248.150.171	192.168.2.3
May 15, 2022 05:54:51.777121067 CEST	49743	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:51.867172003 CEST	83	49743	109.248.150.171	192.168.2.3
May 15, 2022 05:54:51.974879980 CEST	83	49743	109.248.150.171	192.168.2.3
May 15, 2022 05:54:52.040430069 CEST	49743	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:52.068775892 CEST	83	49743	109.248.150.171	192.168.2.3
May 15, 2022 05:54:52.112411976 CEST	49743	83	192.168.2.3	109.248.150.171
May 15, 2022 05:54:52.183248997 CEST	83	49743	109.248.150.171	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 15, 2022 05:54:42.462292910 CEST	57851	53	192.168.2.3	8.8.8.8
May 15, 2022 05:54:42.482404947 CEST	53	57851	8.8.8.8	192.168.2.3
May 15, 2022 05:54:50.014200926 CEST	49316	53	192.168.2.3	8.8.8.8
May 15, 2022 05:54:50.034410954 CEST	53	49316	8.8.8.8	192.168.2.3
May 15, 2022 05:54:57.621617079 CEST	56417	53	192.168.2.3	8.8.8.8
May 15, 2022 05:54:57.638111115 CEST	53	56417	8.8.8.8	192.168.2.3
May 15, 2022 05:55:02.713583946 CEST	57723	53	192.168.2.3	8.8.8.8
May 15, 2022 05:55:02.731678009 CEST	53	57723	8.8.8.8	192.168.2.3
May 15, 2022 05:55:07.622051001 CEST	57421	53	192.168.2.3	8.8.8.8
May 15, 2022 05:55:07.638731003 CEST	53	57421	8.8.8.8	192.168.2.3
May 15, 2022 05:55:14.887804031 CEST	65358	53	192.168.2.3	8.8.8.8
May 15, 2022 05:55:14.906346083 CEST	53	65358	8.8.8.8	192.168.2.3
May 15, 2022 05:55:21.222600937 CEST	49873	53	192.168.2.3	8.8.8.8
May 15, 2022 05:55:21.241132021 CEST	53	49873	8.8.8.8	192.168.2.3
May 15, 2022 05:55:28.258460045 CEST	53802	53	192.168.2.3	8.8.8.8
May 15, 2022 05:55:28.278736115 CEST	53	53802	8.8.8.8	192.168.2.3
May 15, 2022 05:55:33.341849089 CEST	63332	53	192.168.2.3	8.8.8.8
May 15, 2022 05:55:33.359914064 CEST	53	63332	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 15, 2022 05:55:39.376532078 CEST	63548	53	192.168.2.3	8.8.8.8
May 15, 2022 05:55:39.396401882 CEST	53	63548	8.8.8.8	192.168.2.3
May 15, 2022 05:55:44.618705988 CEST	61380	53	192.168.2.3	8.8.8.8
May 15, 2022 05:55:44.635627031 CEST	53	61380	8.8.8.8	192.168.2.3
May 15, 2022 05:55:51.591789007 CEST	63146	53	192.168.2.3	8.8.8.8
May 15, 2022 05:55:51.610121012 CEST	53	63146	8.8.8.8	192.168.2.3
May 15, 2022 05:55:57.830147028 CEST	52985	53	192.168.2.3	8.8.8.8
May 15, 2022 05:55:57.848510981 CEST	53	52985	8.8.8.8	192.168.2.3
May 15, 2022 05:56:06.463772058 CEST	58625	53	192.168.2.3	8.8.8.8
May 15, 2022 05:56:06.484291077 CEST	53	58625	8.8.8.8	192.168.2.3
May 15, 2022 05:56:12.925609112 CEST	59390	53	192.168.2.3	8.8.8.8
May 15, 2022 05:56:12.943950891 CEST	53	59390	8.8.8.8	192.168.2.3
May 15, 2022 05:56:18.048286915 CEST	50152	53	192.168.2.3	8.8.8.8
May 15, 2022 05:56:18.066441059 CEST	53	50152	8.8.8.8	192.168.2.3
May 15, 2022 05:56:22.961030006 CEST	54960	53	192.168.2.3	8.8.8.8
May 15, 2022 05:56:22.977479935 CEST	53	54960	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 15, 2022 05:54:42.462292910 CEST	192.168.2.3	8.8.8.8	0xe2e6	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:54:50.014200926 CEST	192.168.2.3	8.8.8.8	0xec48	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:54:57.621617079 CEST	192.168.2.3	8.8.8.8	0x3669	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:55:02.713583946 CEST	192.168.2.3	8.8.8.8	0xa052	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:55:07.622051001 CEST	192.168.2.3	8.8.8.8	0xe481	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:55:14.887804031 CEST	192.168.2.3	8.8.8.8	0x2fa2	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:55:21.222600937 CEST	192.168.2.3	8.8.8.8	0xc35d	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:55:28.258460045 CEST	192.168.2.3	8.8.8.8	0x15f4	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:55:33.341849089 CEST	192.168.2.3	8.8.8.8	0x976f	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:55:39.376532078 CEST	192.168.2.3	8.8.8.8	0x1771	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:55:44.618705988 CEST	192.168.2.3	8.8.8.8	0x713	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:55:51.591789007 CEST	192.168.2.3	8.8.8.8	0xd62e	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:55:57.830147028 CEST	192.168.2.3	8.8.8.8	0xf8c2	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:56:06.463772058 CEST	192.168.2.3	8.8.8.8	0xbf8f	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:56:12.925609112 CEST	192.168.2.3	8.8.8.8	0xded1	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:56:18.048286915 CEST	192.168.2.3	8.8.8.8	0x8431	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)
May 15, 2022 05:56:22.961030006 CEST	192.168.2.3	8.8.8.8	0xdecd	Standard query (0)	mallow.3utilities.com	A (IP address)	IN (0x0001)

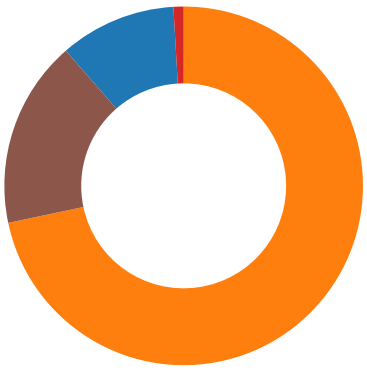
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 15, 2022 05:54:42.482404947 CEST	8.8.8.8	192.168.2.3	0xe2e6	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:54:50.034410954 CEST	8.8.8.8	192.168.2.3	0xec48	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:54:57.638111115 CEST	8.8.8.8	192.168.2.3	0x3669	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:55:02.731678009 CEST	8.8.8.8	192.168.2.3	0xa052	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 15, 2022 05:55:07.638731003 CEST	8.8.8.8	192.168.2.3	0xe481	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:55:14.906346083 CEST	8.8.8.8	192.168.2.3	0x2fa2	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:55:21.241132021 CEST	8.8.8.8	192.168.2.3	0xc35d	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:55:28.278736115 CEST	8.8.8.8	192.168.2.3	0x15f4	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:55:33.359914064 CEST	8.8.8.8	192.168.2.3	0x976f	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:55:39.396401882 CEST	8.8.8.8	192.168.2.3	0x1771	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:55:44.635627031 CEST	8.8.8.8	192.168.2.3	0x713	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:55:51.610121012 CEST	8.8.8.8	192.168.2.3	0xd62e	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:55:57.848510981 CEST	8.8.8.8	192.168.2.3	0xf8c2	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:56:06.484291077 CEST	8.8.8.8	192.168.2.3	0xbf8f	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:56:12.943950891 CEST	8.8.8.8	192.168.2.3	0xded1	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:56:18.066441059 CEST	8.8.8.8	192.168.2.3	0x8431	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)
May 15, 2022 05:56:22.977479935 CEST	8.8.8.8	192.168.2.3	0xdecd	No error (0)	mallow.3utilities.com		109.248.150.171	A (IP address)	IN (0x0001)

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: DN8slYDJr3.exe PID: **6440**, Parent PID: **2044**

General

Target ID:	0
Start time:	05:55:03
Start date:	15/05/2022
Path:	C:\Users\user\Desktop\DN8slYDJr3.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DN8slYDJr3.exe"
Imagebase:	0xdc0000

File size:	884736 bytes
MD5 hash:	A6FE8903E741154BC80352D0EE73EFFF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.289573778.0000000004171000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.289573778.0000000004171000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.289573778.0000000004171000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.294913817.00000000046FF000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.294913817.00000000046FF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.294913817.00000000046FF000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.287530312.0000000003171000.00000004.00000800.00020000.00000000.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	6DBCCF06	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	6DBCCF06	unknown
C:\Users\user\AppData\Roaming\IulEJNIqTKEFv.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	6CA1DD66	CopyFileW
C:\Users\user\AppData\Roaming\IulEJNIqTKEFv.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CA1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2ADE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CA17038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DN8slYDJr3.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEDC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2ADE.tmp	success or wait	1	6CA16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\IulEJNIqTKEFv.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 fd 5a 7c 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 20 0d 00 00 40 00 00 00 00 00 00 06 23 0d 00 00 20 00 00 00 40 0d 00 00 00 40 00 00 20 00 00 00 20 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0d 00 00 20 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.$PELZ|b0 @# @@ @	success or wait	4	6CA1DD66	CopyFileW
C:\Users\user\AppData\Roaming\IulEJNIqTKEFv.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	6CA1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2ADE.tmp	0	1600	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	6CA11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DN8slYDJr3.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	6DEDC907	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	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA11B4F	ReadFile

Analysis Process: powershell.exe PID: **6788**, Parent PID: **6440**

General

Target ID:	4
Start time:	05:55:17
Start date:	15/05/2022
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\lulEJNIqTKEFv.exe
Imagebase:	0x8c0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C975B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C975B28	unknown
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	6DBCCF06	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	6DBCCF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jhkev1fh.4vf.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CA11E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m2k5xmri.aaz.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CA11E60	CreateFileW
C:\Users\user\Documents\20220515	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA1BEFF	CreateDirectoryW
C:\Users\user\Documents\20220515\PowerShell_transcript.347688.VGMBSiq0.20220515055521.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CA11E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jhkev1fh.4vf.ps1	success or wait	1	6CA16A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m2k5xmri.aaz.psm1	success or wait	1	6CA16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jhkev1fh.4vf.ps1	0	1	31	1	success or wait	1	6CA11B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m2k5xmri.aaz.psm1	0	1	31	1	success or wait	1	6CA11B4F	WriteFile
C:\Users\user\Documents\20220515\PowerShell_transcript.347688.VGMBSiq0.20220515055521.txt	0	3	ff		success or wait	1	6CA11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220515\PowerShell_transcript.347688.VGMBSiq0.20220515055521.txt	3	680	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 35 30 35 35 35 32 32 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 33 34 37 36 38 38 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: 20220515055522Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 347688 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6CA11B4F	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 79 14 00 00 18 00 00 00 68 0d 22 04 45 09 3c 09 39 09 00 00 fd 00 fd 00 0c 00 49 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eyh"E<9I@	success or wait	1	6DE976FC	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 58 00 00 00 0e 00 20 00	H<@^L"My:X	success or wait	17	6DE976FC	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	6DE976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DE976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DE976FC	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 fd 01 40 00 5b 01 40 00 4e 54 40 01 55 00 40 00 48 54 40 01 47 00 40 00 fd 53 40 01 56 00 40 00 fd 01 40 00 fd 00 40 00 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 fd 67 40 01 fd 01 40 00 fd 00 40 00 42 4d 40 01 fd 44 40 01 6d 45 40	T@>@@V@H@X@@[@NT@U@HT@G@S@ V@@@ 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@g@@@BM@D@ mE@	success or wait	11	6DE976FC	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	6DBA5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBACA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBA5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBA5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DBB1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6DBB203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB003DE	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	6CA11B4F	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	6CA11B4F	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	6CA11B4F	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	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	136	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CA11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBA5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	6	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBA5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	69	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	11	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CA11B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CA11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CA11B4F	ReadFile

Analysis Process: conhost.exe PID: **6808**, Parent PID: **6788**

General

Target ID:	5
Start time:	05:55:18
Start date:	15/05/2022
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: **6816**, Parent PID: **6440**

General

Target ID:	6
Start time:	05:55:18
Start date:	15/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\IulEJNIqTKEFv" /XML "C:\Users\user\AppData\Local\Temp\tmp2ADE.tmp
Imagebase:	0xc0000
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\tmp2ADE.tmp	unknown	2	success or wait	1	CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2ADE.tmp	unknown	1601	success or wait	1	CABD9	ReadFile

Analysis Process: conhost.exe PID: **6964**, Parent PID: **6816**

General	
Target ID:	7
Start time:	05:55:21
Start date:	15/05/2022
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: RegSvcs.exe PID: **7012**, Parent PID: **6440**

General	
Target ID:	8
Start time:	05:55:23
Start date:	15/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xfb0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.283747964.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.283747964.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.283747964.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.282381940.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.282381940.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.282381940.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.284049855.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.284049855.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.284049855.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.283054100.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.283054100.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.283054100.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.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	6DBCCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBCCF06	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	6CA1BEFF	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	6CA11E60	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	6CA1BEFF	CreateDirectoryW
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	6CA1BEFF	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	13	6CA11E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CA11E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CA11E60	CreateFileW

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	18 55 fd 2f 72 36 fd 48	U/r6H	success or wait	1	6CA11B4F	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	9	6CA11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327928	fd fd 2c 21 fd 3c 4c 4a 79 fd fd 35 3c fd 01 fd 39 fd fd fd fd 21 fd 1d 3f ff 41 4a fd 14 5f 6c fd fd 50 78 fd 39 67 fd fd fd 5f 74 fd fd 03 5d fd 0c 0b fd fd 74 fd fd 2f fd fd 1b 61 fd 6b fd 5a 33 fd 48 fd fd fd 6f fd 0f 3e fd 36 fd 78 fd 45 02 fd fd fd fd 68 42 75 2a 10 23 ac 5a 0a fd 76 fd fd 29 cd 23 fd fd 78 10 fd fd 68 49 fd 12 65 fd fd fd 42 2d 3c 11 4a 30 fd fd 6e 6f 12 06 fd 5d fd fd fd fd 25 fd fd fd cc fd fd 35 31 fd 68 fd d1 47 7b fd 75 16 7c 2a 72 10 fd 78 73 fd 64 fd fd 23 fd fd dd fd 29 fa 26 fd 65 fd 33 2e fd 36 fd 56 2b fd fd 0a fd 64 fd fd fd 07 fd 00 21 fd 4a 76 fd fd fd 29 59 fd 0e fd fd fd 7f 70 65 fd fd b0 63 03 6d 57 fd fd fd fd fd 4f fd 58 fd fd fd 3e 1f 5b fd fd fd 0d fd fd 77 5e fd	,!LJy5<9!? AJ_lPx9g_t]t/akZ3Ho> 6xEhBu*#Zv)#xhIeB-<J0o]%51hG{u |*rxsd#)&e3.6V+d!v)YpecmWOX>[w^	success or wait	1	6CA11B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	6CA11B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DBACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DBACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	4096	success or wait	1	6DB8D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	512	success or wait	1	6DB8D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DBA5705	unknown

Disassembly

No disassembly