



ID: 623789
Sample Name: P2DIWOtpLf.exe
Cookbook: default.jbs
Time: 20:24:01
Date: 10/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report P2DIWOtpLf.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 6
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
AV Detection 7
E-Banking Fraud 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Snort Signatures 7
Joe Sandbox Signatures 8
AV Detection 8
Compliance 8
Networking 8
E-Banking Fraud 8
Operating System Destruction 8
System Summary 8
Data Obfuscation 8
Boot Survival 8
Hooking and other Techniques for Hiding and Protection 8
Malware Analysis System Evasion 8
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 9
Remote Access Functionality 9
Mitre Att&ck Matrix 9
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 12
URLs 12
Domains and IPs 13
Contacted Domains 13
URLs from Memory and Binaries 13
World Map of Contacted IPs 26
Public IPs 27
Private 27
General Information 27
Warnings 28
Simulations 28
Behavior and APIs 28
Joe Sandbox View / Context 28
IPs 28
Domains 28
ASNs 28
JA3 Fingerprints 28
Dropped Files 28
Created / dropped Files 29
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe 29
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier 29
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\P2DIWOtpLf.exe.log 29
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log 30
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 30
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hhukf3ev.kf3.psm1 30
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ifc2ygq5.uig.ps1 31
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mxlrk2j0.y2x.psm1 31
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ujntonns.a2o.ps1 31
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_w2dkegpy.3ku.psm1 31
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xpzwv1x0.mtv.ps1 32
C:\Users\user\AppData\Local\Temp\tmp3864.tmp 32
C:\Users\user\AppData\Local\Temp\tmp5E50.tmp 32
C:\Users\user\AppData\Local\Temp\tmp67E6.tmp 33
C:\Users\user\AppData\Local\Temp\tmpB218.tmp 33

Copyright Joe Security LLC 2022

C:\Users\user\AppData\Local\Temp\tmpD4F2.tmp 33
C:\Users\user\AppData\Local\Temp\tmpF53B.tmp 34
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 34
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat 34
C:\Users\user\AppData\Roaming\mjbsosItP.exe 35
C:\Users\user\AppData\Roaming\mjbsosItP.exe:Zone.Identifier 35
C:\Users\user\Documents\20220510\PowerShell_transcript.376483.n68wiFr5.20220510202612.txt 35
C:\Users\user\Documents\20220510\PowerShell_transcript.376483.rfYSk5DZ.20220510202541.txt 36
C:\Users\user\Documents\20220510\PowerShell_transcript.376483.tuCn2Xiy.20220510202621.txt 36
Static File Info 36
General 36
File Icon 37
Static PE Info 37
General 37
Entrypoint Preview 37
Data Directories 39
Sections 39
Resources 39
Imports 40
Version Infos 40
Network Behavior 40
Network Port Distribution 40
TCP Packets 40
UDP Packets 41
DNS Queries 41
DNS Answers 41
Statistics 41
Behavior 41
System Behavior 42
Analysis Process: P2DIWOtpLf.exePID: 6436, Parent PID: 3488 42
General 42
File Activities 42
File Created 42
File Deleted 43
File Written 43
File Read 44
Analysis Process: powershell.exePID: 6112, Parent PID: 6436 45
General 45
File Activities 45
File Created 45
File Deleted 46
File Written 46
File Read 47
Analysis Process: conhost.exePID: 3720, Parent PID: 6112 50
General 50
Analysis Process: schtasks.exePID: 3524, Parent PID: 6436 50
General 50
File Activities 51
File Read 51
Analysis Process: conhost.exePID: 5732, Parent PID: 3524 51
General 51
Analysis Process: P2DIWOtpLf.exePID: 5776, Parent PID: 6436 51
General 51
File Activities 52
File Created 52
File Deleted 53
File Written 53
File Read 55
Registry Activities 55
Key Value Created 55
Analysis Process: schtasks.exePID: 6840, Parent PID: 5776 55
General 56
File Activities 56
File Read 56
Analysis Process: conhost.exePID: 2368, Parent PID: 6840 56
General 56
Analysis Process: schtasks.exePID: 7112, Parent PID: 5776 56
General 56
File Activities 57
File Read 57
Analysis Process: P2DIWOtpLf.exePID: 7028, Parent PID: 696 57
General 57
File Activities 57
File Created 57
File Deleted 57
File Written 57
File Read 58
Analysis Process: conhost.exePID: 7104, Parent PID: 7112 58
General 58
Analysis Process: dhcpmon.exePID: 804, Parent PID: 696 59
General 59
Analysis Process: dhcpmon.exePID: 1320, Parent PID: 3688 59
General 59
Analysis Process: powershell.exePID: 6600, Parent PID: 7028 59
General 59
Analysis Process: conhost.exePID: 6512, Parent PID: 6600 60
General 60
Analysis Process: schtasks.exePID: 6500, Parent PID: 7028 60
General 60
Analysis Process: conhost.exePID: 6764, Parent PID: 6500 60
General 60

Analysis Process: powershell.exePID: 7080, Parent PID: 804 61
General 61
Analysis Process: conhost.exePID: 5672, Parent PID: 7080 61
General 61
Analysis Process: P2DIWOtpLf.exePID: 6108, Parent PID: 7028 61
General 61
Disassembly 62

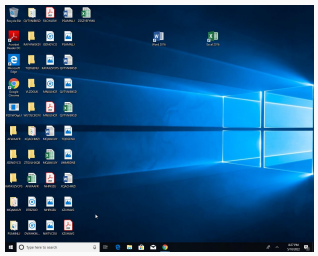
Windows Analysis Report

P2DIWOtpLf.exe

Overview

General Information

Sample Name:	P2DIWOtpLf.exe
Analysis ID:	623789
MD5:	3789175015481e.
SHA1:	500ccf71450ef91..
SHA256:	861bdb02b21024.
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

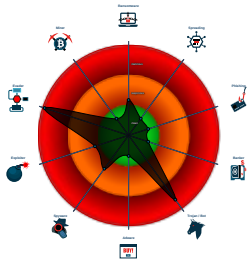
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Connects to many ports of the same…
- Protects its processes via BreakOn…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- P2DIWOtpLf.exe (PID: 6436 cmdline: "C:\Users\user\Desktop\P2DIWOtpLf.exe" MD5: 3789175015481EE123ABCBBFE83C3C16)
  - powershell.exe (PID: 6112 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\mjbsosItP.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 3524 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\mjbsosItP" /XML "C:\Users\user\AppData\Local\Temp\tmp3864.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - P2DIWOtpLf.exe (PID: 5776 cmdline: C:\Users\user\Desktop\P2DIWOtpLf.exe MD5: 3789175015481EE123ABCBBFE83C3C16)
    - schtasks.exe (PID: 6840 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp5E50.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 2368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 7112 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmp67E6.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 7104 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- P2DIWOtpLf.exe (PID: 7028 cmdline: C:\Users\user\Desktop\P2DIWOtpLf.exe 0 MD5: 3789175015481EE123ABCBBFE83C3C16)
  - powershell.exe (PID: 6600 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\mjbsosItP.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6512 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6500 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\mjbsosItP" /XML "C:\Users\user\AppData\Local\Temp\tmpB218.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - P2DIWOtpLf.exe (PID: 6108 cmdline: C:\Users\user\Desktop\P2DIWOtpLf.exe MD5: 3789175015481EE123ABCBBFE83C3C16)
- dhcpmon.exe (PID: 804 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 3789175015481EE123ABCBBFE83C3C16)
  - powershell.exe (PID: 7080 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\mjbsosItP.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 1984 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\mjbsosItP" /XML "C:\Users\user\AppData\Local\Temp\tmpD4F2.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5928 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6460 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 3789175015481EE123ABCBBFE83C3C16)
- dhcpmon.exe (PID: 1320 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 3789175015481EE123ABCBBFE83C3C16)
  - powershell.exe (PID: 6948 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\mjbsosItP.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6884 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\mjbsosItP" /XML "C:\Users\user\AppData\Local\Temp\tmpF53B.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

Copyright Joe Security LLC 2022

- dhcpmon.exe (PID: 5600 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 3789175015481EE123ABCBBFE83C3C16)

- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000001A.00000000.523160689.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001A.00000000.523160689.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001A.00000000.523160689.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
0000001A.00000000.520325919.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001A.00000000.520325919.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 118 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
19.2.dhcpmon.exe.4cb9300.8.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x447ad:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x447ea:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x4831d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
19.2.dhcpmon.exe.4cb9300.8.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x44525:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x447ad:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x45de6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x45dda:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x46c8b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x4ca42:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost • 0x447d7:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
19.2.dhcpmon.exe.4cb9300.8.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
19.2.dhcpmon.exe.4cb9300.8.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x44515:$x1: NanoCore Client • 0x44525:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x4476d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x447ad:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x44762:$i1: IClientApp • 0x10163:$i2: IClientData • 0x44783:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x4478f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x4479e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x447c7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x447d7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost
19.2.dhcpmon.exe.4cb9300.8.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0x44515:$a: NanoCore • 0x44525:$a: NanoCore • 0x44759:$a: NanoCore • 0x4476d:$a: NanoCore • 0x447ad:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x44574:$b: ClientPlugin • 0x44776:$b: ClientPlugin • 0x447b6:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x4469b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x450a2:$d: DESCrypto • 0x1844e:$e: KeepAlive
Click to see the 225 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

No Snort rule has matched

Copyright Joe Security LLC 2022

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance



Detected unpacking (overwrites its own PE header)

Networking



Connects to many ports of the same IP (likely port scanning)

E-Banking Fraud



Yara detected Nanocore RAT

Operating System Destruction



Protects its processes via BreakOnTermination flag

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

Boot Survival



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

Hooking and other Techniques for Hiding and Protection



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

Malware Analysis System Evasion



Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion



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



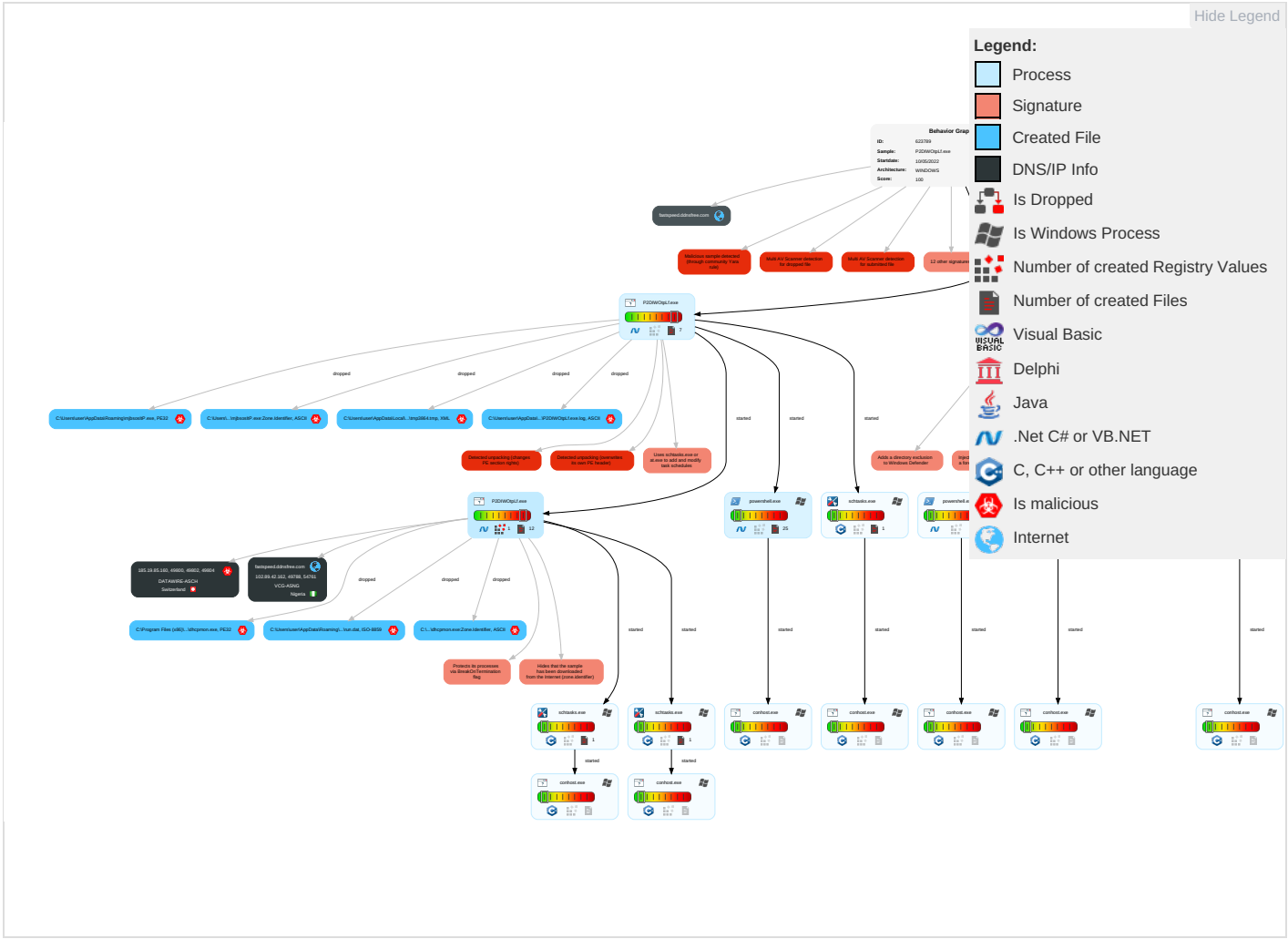
Detected Nanocore Rat

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 Scheduled Task/Job	1 Scheduled Task/Job	1 1 2 Process Injection	2 Masquerading	2 1 Input Capture	1 Query Registry	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 1 Security Software 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 Process Discovery	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)	1 1 2 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	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 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	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 Remote System 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	3 Obfuscated Files or Information	DCSync	1 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 3 Software Packing	Proc Filesystem	1 2 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

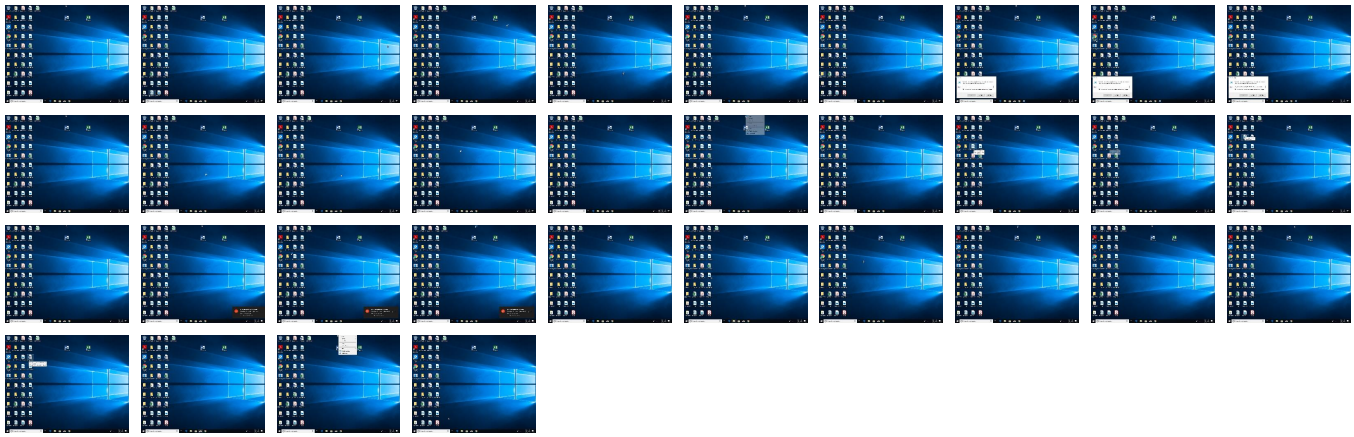
Behavior Graph



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
P2DIWOtpLf.exe	40%	Virustotal		Browse
P2DIWOtpLf.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
P2DIWOtpLf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\mjbsosItP.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\mjbsosItP.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
16.2.P2DIWOtpLf.exe.6e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
9.0.P2DIWOtpLf.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.P2DIWOtpLf.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.P2DIWOtpLf.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
26.0.P2DIWOtpLf.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
26.0.P2DIWOtpLf.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
26.0.P2DIWOtpLf.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.P2DIWOtpLf.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
26.0.P2DIWOtpLf.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.P2DIWOtpLf.exe.6340000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
26.0.P2DIWOtpLf.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.P2DIWOtpLf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.P2DIWOtpLf.exe.b70000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
18.2.dhcpmon.exe.be0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
26.2.P2DIWOtpLf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.P2DIWOtpLf.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.2.dhcpmon.exe.d00000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comFU	0%	Avira URL Cloud	safe	
http://fontfabrik.comX	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fonts.com(	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/H	0%	URL Reputation	safe	
http://www.founder.com.cn/cnu-eA	0%	Avira URL Cloud	safe	
http://www.urwpp.deett	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/xor	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnC	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cno	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comD	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/l	0%	URL Reputation	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/&	0%	URL Reputation	safe	
http://www.carterandcone.comue4	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comN	0%	URL Reputation	safe	
http://www.carterandcone.comb	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/~	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Z	0%	URL Reputation	safe	
http://www.carterandcone.comf	0%	URL Reputation	safe	
http://www.fontbureau.comasoml	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cndnl	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/T	0%	URL Reputation	safe	
http://www.carterandcone.comX	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnu-r	0%	Avira URL Cloud	safe	
http://www.fontbureau.comW.TTF	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnm	0%	URL Reputation	safe	
http://www.carterandcone.comv	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/obz	0%	Avira URL Cloud	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.carterandcone.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/C	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.comm	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.comk	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnva	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/$	0%	Avira URL Cloud	safe	
http://www.urwpp.den	0%	Avira URL Cloud	safe	
http://www.fontbureau.commaU	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.urwpp.de.Ti	0%	Avira URL Cloud	safe	
http://www.urwpp.deu	0%	Avira URL Cloud	safe	
http://www.fonts.com0	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/g	0%	URL Reputation	safe	
http://www.fontbureau.comdsed	0%	URL Reputation	safe	
http://www.fontbureau.com~	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fastspeed.ddnsfree.com	102.89.42.162	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comFU	P2DIWOtpLf.exe, 00000000.00000003.393476650.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394245132.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394168094.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.393633510.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394482605.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394307830.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394410040.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394010406.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.393402662.000000000834C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fontfabrik.comX	P2DIWOtpLf.exe, 00000000.00000003.383843099.0000000008375000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com(	P2DIWOtpLf.exe, 00000000.00000003.383172870.0000000008375000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/jp/H	P2DIWOtpLf.exe, 00000000.00000003.388774743.0000000008344000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389481709.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388301602.0000000008345000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389066705.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389569000.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388753507.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389226808.000000000834A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnu-eA	P2DIWOtpLf.exe, 00000000.00000003.385682403.000000000834B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deett	P2DIWOtpLf.exe, 00000000.00000003.392550924.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.392621877.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.392374489.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	P2DIWOtpLf.exe, 00000000.00000003.393402662.000000000834C000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/xor	P2DIWOtpLf.exe, 00000000.00000003.388774743.0000000008344000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389481709.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388301602.0000000008345000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389066705.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389569000.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388753507.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389226808.000000000834A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	P2DIWOtpLf.exe, 00000000.00000003.387224652.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnC	P2DIWOtpLf.exe, 00000000.00000003.385682403.000000000834B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/~	P2DIWOtpLf.exe, 00000000.00000003.387799705.0000000008343000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388774743.0000000008344000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388301602.0000000008345000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388753507.000000000834A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cno	P2DIWOtpLf.exe, 00000000.00000003.385957942.000000000836E000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.385771041.000000000836F000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.385896289.000000000836F000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386062891.000000000836E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	P2DIWOtpLf.exe, 00000000.00000003.397452438.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.397037094.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.397218992.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.397576502.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.396998132.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.397344668.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.396958498.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.397690766.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comD	P2DIWOtpLf.exe, 00000000.00000003.387188620.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387337670.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386976947.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387100157.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387030788.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387203737.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387322435.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387250123.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387355333.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387137073.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387163223.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387265802.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387224652.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comB.TTF	P2DIWOtpLf.exe, 00000000.00000003.394892694.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394482605.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394410040.000000000834C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmlP	P2DIWOtpLf.exe, 00000000.00000003.394262342.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comcom	P2DIWOtpLf.exe, 00000000.00000003.393476650.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394245132.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394168094.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.393633510.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394482605.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394307830.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394410040.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394010406.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.393402662.000000000834C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/l	P2DIWOtpLf.exe, 00000000.00000003.388774743.0000000008344000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388301602.0000000008345000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389066705.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388753507.000000000834A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	P2DIWOtpLf.exe, 00000000.00000003.389481709.000000000834B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	P2DIWOtpLf.exe, 00000000.00000003.383336328.0000000008375000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.383382845.0000000008375000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.383212554.0000000008375000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/&	P2DIWOtpLf.exe, 00000000.00000003.387799705.0000000008343000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388774743.0000000008344000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389481709.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388301602.0000000008345000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389066705.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389569000.0000000008334B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388753507.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389226808.000000000834A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comue4	P2DIWOtpLf.exe, 00000000.00000003.387337670.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387203737.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387322435.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387250123.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387355333.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387265802.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387224652.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersz	P2DIWOtpLf.exe, 00000000.00000003.393476650.000000000834C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.urwpp.de	P2DIWOtpLf.exe, 00000000.00000003.395675410.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.392550924.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.392374489.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	P2DIWOtpLf.exe, 00000000.00000003.386592271.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386703883.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	P2DIWOtpLf.exe, 00000000.00000002.451037709.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000010.00000002.529814220.0000000002AA1000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000012.00000002.574049078.0000000003021000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000013.00000002.593612504.00000000030A1000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.como.	P2DIWOtpLf.exe, 00000000.00000003.387188620.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387337670.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386976947.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387100157.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387030788.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387203737.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387322435.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387250123.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387355333.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387137073.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387163223.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387265802.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387224652.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	P2DIWOtpLf.exe, 00000000.00000003.389569000.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comN	P2DIWOtpLf.exe, 00000000.00000003.387337670.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387322435.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387250123.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387355333.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387265802.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comb	P2DIWOtpLf.exe, 00000000.00000003.387188620.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387337670.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386836555.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386976947.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387100157.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387030788.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387203737.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387322435.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387250123.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386856885.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387355333.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387137073.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386775920.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386703883.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387163223.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386930256.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387265802.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387224652.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/~	P2DIWOtpLf.exe, 00000000.00000003.389066705.000000000834A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Z	P2DIWOtpLf.exe, 00000000.00000003.389936787.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388774743.0000000008344000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.391100510.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390241062.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390514907.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389815916.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390629031.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389877155.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390883210.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389481709.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390754279.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388301602.0000000008345000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389066705.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390148181.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389975419.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389569000.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390953030.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388753507.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390377451.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389226808.000000000834A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comf	P2DIWOtpLf.exe, 00000000.00000003.387188620.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387337670.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387100157.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387030788.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387203737.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387322435.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387250123.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387355333.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387137073.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387163223.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387265802.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387224652.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comasoml	P2DIWOtpLf.exe, 00000000.00000002.465840522.0000000008340000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.449097558.0000000008340000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cndnl	P2DIWOtpLf.exe, 00000000.00000003.385682403.000000000834B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/T	P2DIWOtpLf.exe, 00000000.00000003.389936787.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388774743.0000000008344000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389815916.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389877155.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389481709.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388301602.0000000008345000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389066705.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389975419.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389569000.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388753507.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389226808.000000000834A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comX	P2DIWOtpLf.exe, 00000000.00000003.386976947.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387100157.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387030788.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386856885.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387137073.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387163223.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386930256.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnu-r	P2DIWOtpLf.exe, 00000000.00000003.386836555.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386592271.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386856885.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386775920.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386703883.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comW.TTF	P2DIWOtpLf.exe, 00000000.00000003.393476650.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394245132.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394168094.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.393633510.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394482605.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394307830.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394410040.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394010406.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.393402662.000000000834C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnm	P2DIWOtpLf.exe, 00000000.00000003.386592271.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comv	P2DIWOtpLf.exe, 00000000.00000003.387337670.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387322435.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387250123.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387355333.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387265802.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387224652.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/obz	P2DIWOtpLf.exe, 00000000.00000003.385957942.000000000836E000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.385896289.000000000836F000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386062891.000000000836E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comlic	P2DIWOtpLf.exe, 00000000.00000003.387355333.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comt	P2DIWOtpLf.exe, 00000000.00000003.386775920.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/C	P2DIWOtpLf.exe, 00000000.00000003.389936787.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389815916.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389877155.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389481709.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389066705.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389975419.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389569000.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389226808.000000000834A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/	P2DIWOtpLf.exe, 00000000.00000003.391795637.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389936787.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.391379562.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388774743.0000000008344000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.391100510.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390241062.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.392040029.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390514907.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389815916.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.391300929.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390629031.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.392476219.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389877155.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390883210.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389481709.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.391591212.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390754279.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388301602.000000000834500.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389066705.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390148181.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389975419.000000000834B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	P2DIWOtpLf.exe, 00000000.00000003.394892694.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394482605.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394307830.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394410040.000000000834C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comm	P2DIWOtpLf.exe, 00000000.00000003.387188620.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386836555.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386976947.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387100157.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387030788.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387203737.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386856885.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387137073.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386775920.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386703883.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387163223.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386930256.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387224652.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comk	P2DIWOtpLf.exe, 00000000.00000003.387188620.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387337670.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387203737.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387322435.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387250123.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387265802.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387224652.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	P2DIWOtpLf.exe, 00000000.00000003.385682403.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	P2DIWOtpLf.exe, 00000000.00000003.394262342.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cnva	P2DIWOtpLf.exe, 00000000.00000003.386836555.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386976947.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387100157.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.387030788.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386592271.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386856885.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386775920.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386703883.0000000008370000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386930256.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/$	P2DIWOtpLf.exe, 00000000.00000003.385957942.000000000836E000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.385896289.000000000836F000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.386062891.000000000836E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.den	P2DIWOtpLf.exe, 00000000.00000003.392374489.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.commaU	P2DIWOtpLf.exe, 00000000.00000002.465840522.0000000008340000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.449097558.0000000008340000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	P2DIWOtpLf.exe, 00000000.00000003.388753507.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.390377451.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.391929355.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389226808.000000000834A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de.Ti	P2DIWOtpLf.exe, 00000000.00000003.395675410.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deu	P2DIWOtpLf.exe, 00000000.00000003.392374489.0000000008370000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	P2DIWOtpLf.exe, 00000000.00000003.394482605.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394410040.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000002.466085741.0000000009552000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com0	P2DIWOtpLf.exe, 00000000.00000003.383336328.0000000008375000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.383382845.0000000008375000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/g	P2DIWOtpLf.exe, 00000000.00000003.389936787.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388774743.0000000008344000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389815916.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389877155.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389481709.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388301602.0000000008345000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389066705.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389975419.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389569000.000000000834B000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.388753507.000000000834A000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.389226808.000000000834A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comdsed	P2DIWOtpLf.exe, 00000000.00000003.393476650.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394245132.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394168094.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.393633510.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394307830.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394010406.000000000834C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com~	P2DIWOtpLf.exe, 00000000.00000003.393476650.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394245132.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394168094.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.393218978.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.393633510.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.393128030.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394307830.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.393009068.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.394010406.000000000834C000.00000004.00000800.00020000.00000000.sdmp, P2DIWOtpLf.exe, 00000000.00000003.393402662.000000000834C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
102.89.42.162	fastspeed.ddnsfree.com	Nigeria		29465	VCG-ASNG	false
185.19.85.160	unknown	Switzerland		48971	DATAWIRE-ASCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	623789
Start date and time: 10/05/202220:24:01	2022-05-10 20:24:01 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	P2DIWOtpLf.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:	41
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

Copyright Joe Security LLC 2022

Classification:	mal100.troj.evad.winEXE@42/24@4/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 2% (good quality ratio 1.1%) • Quality average: 33.6% • Quality standard deviation: 35.7%
HCA Information:	• Successful, ratio: 90% • 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

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.35.236.56
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing behavior and disassembly information.
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many 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
20:25:29	API Interceptor	590x Sleep call for process: P2DIWOtpLf.exe modified
20:25:44	API Interceptor	134x Sleep call for process: powershell.exe modified
20:26:00	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\P2DIWOtpLf.exe" s>$(Arg0)
20:26:00	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
20:26:03	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
20:26:09	API Interceptor	4x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\P2DIWOtpLf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	670208
Entropy (8bit):	7.742892435183354
Encrypted:	false
SSDEEP:	12288:KxjoxTdLDVXj6TKJfO2J7uE2ezRvfqFlfVX3xLJOrabQudntH:qjoxhETDfE9zRvyCt
MD5:	3789175015481EE123ABCBBFE83C3C16
SHA1:	500CCF71450EF911B6A431E25DA230742CA8BF65
SHA-256:	861BDB02B21024B41ACC04AC63D0CA3455F47DDA85B3D46DFD02D1F63855B796
SHA-512:	659831E3ED3CE843A9D574C19E6B21C2D5BC1844377142DFA25F0B868B1EAFBF46E9196756BDF404339E7ACE61F7830B1861121F4146D4205D414A53272F5FD9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Qhxb.....0..0.....>O... ...`....@.. ..... .....@.....N..O...`..... ....H.....text...D/... ...0..... ..`.rsrc.....`.....2..... ..@..@.reloc.....8.....@..B..... O.....H.....l_.....u...z.....].....Z.....[.R$6.|X8L.R..t ....t*.X....i.:>j.=...w....\...u.P.....J.=.v....R.. ..`4xz"....3.Ty.)....)+...z.acZuE...A.].-.[>5...Q....?.P;E..z...*=Vtd.,(G.o..."..I:.....G..,f..m...t...C...S.6c}....(f..R..V.YGWl...1.....<\r~....M....}E@N..8Y...>....xm.T.j..%j<D<A..T.y. .\z..'O-t`.....,...7X..q.Gh..si.....y...A.N..;.....#g.... ..M...{..[i@?.VJ..':._.).H?.t5.V.{9...R.}h

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

Process:	C:\Users\user\Desktop\P2DIWOtpLf.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**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\P2DIWOtpLf.exe.log

Process:	C:\Users\user\Desktop\P2DIWOtpLf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	unknown

Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22188
Entropy (8bit):	5.601485346416237
Encrypted:	false
SSDEEP:	384:ntCDLq0JVqTZa3om0sOBrd5SBKnojultIA4paeQCv3g3hlnAML+6fmAV7k/OqRZd:Vl3omTOp4KoClt7Qatg667Kepc/+8
MD5:	55F0D7D2DBE97721D80F2A7FC65B82C0
SHA1:	9C59597D8EAE1157F5CC28ED11FCD7E3BDB1374E
SHA-256:	073C9D37478A2DDC9F81D0E05AE137585EC1722DF63A7E3790717BB4E9358E96
SHA-512:	451A52848057DF5820EAD3CE137C5C1F2CB8918B0D8BEFEDB41206938B23D28FA09091D5CAD4049EEDEDE07CDD165F0A088A14AC0BF48C2CA52ACEC51622321B
Malicious:	false
Reputation:	unknown
Preview:	@...e.....d.....o.{.....z.....O.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hhukf3ev.kf3.psm1

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

SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ifc2ygq5.uig.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mxlrk2j0.y2x.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ujntonns.a2o.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_w2dkegpy.3ku.psm1

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

File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xpzwv1x0.mtv.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp3864.tmp

Process:	C:\Users\user\Desktop\P2DIWOtpLf.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1608
Entropy (8bit):	5.112901951806503
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtLrLxvn:cgea6YrFdOFzOzN33ODOiDdKrsuTVv
MD5:	88AA601F9B38D4A8E15CE1206E119A78
SHA1:	C2BDCBBFCAC423AA0EE896FCFF53DC0EB388CCA2
SHA-256:	8D1D2180C05375699EA716A5D57E815CD276F6DF0E83E5E0763DF4314AB1E54F
SHA-512:	96B15BF23449EC28AC580791BFA7DA5DAD52E4D47FFB68DFDB3C42810B1451FD140E1204124A756F451954FDC3993FE428BDCF00AB1C6D9D977536CC809A214
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailab

C:\Users\user\AppData\Local\Temp\tmp5E50.tmp

Process:	C:\Users\user\Desktop\P2DIWOtpLf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1303
Entropy (8bit):	5.097337447692703
Encrypted:	false

SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Vrxtn:cbk4oL600QydbQxIYODOLedq3Uj
MD5:	C34011DA8F37A9F3447EA8F62B8C593F
SHA1:	89A47BFD18B4B11AE83A00B7E7F37FF7AB268950
SHA-256:	A60E7630AA3760F1E3E0A65C3C83C39FCB7E9C4702AD9700FBB2B7291D104CEA
SHA-512:	9AED82D72015E61F16A5DED7C9D320AD6B329D1314E59A53870E56896A9845B604251E342303C79325FA1593E9344507B45E0ACDB0498E6CA245AE6197E5FEA(
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Princi pals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoing OnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyI fNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunO nlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp67E6.tmp

Process:	C:\Users\user\Desktop\P2DIWOtpLf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733 4
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Princi pals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoing OnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyI fNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunO nlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpB218.tmp

Process:	C:\Users\user\Desktop\P2DIWOtpLf.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1608
Entropy (8bit):	5.112901951806503
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtLrLxvn:cgea6YrFdOFzOzN33ODOiDdKrsuTVv
MD5:	88AA601F9B38D4A8E15CE1206E119A78
SHA1:	C2BDCBBFCAC423AA0EE896FCFF53DC0EB388CCA2
SHA-256:	8D1D2180C05375699EA716A5D57E815CD276F6DF0E83E5E0763DF4314AB1E54F
SHA-512:	96B15BF23449EC28AC580791BFA7DA5DAD52E4D47FFB68DFDB3C42810B1451FD140E1204124A756F451954FDC3993FE428BDCF00AB1C6D9D977536CC809A21 4
Malicious:	false
Reputation:	unknown
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</StartWhenAvailab

C:\Users\user\AppData\Local\Temp\tmpD4F2.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1608

Entropy (8bit):	5.112901951806503
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtLrLxvn:cgea6YrFdOFzOzN33ODOiDdKrsuTVv
MD5:	88AA601F9B38D4A8E15CE1206E119A78
SHA1:	C2BDCBBFCAC423AA0EE896FCFF53DC0EB388CCA2
SHA-256:	8D1D2180C05375699EA716A5D57E815CD276F6DF0E83E5E0763DF4314AB1E54F
SHA-512:	96B15BF23449EC28AC580791BFA7DA5DAD52E4D47FFB68DFDB3C42810B1451FD140E1204124A756F451954FDC3993FE428BDCF00AB1C6D9D977536CC809A214
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailab

C:\Users\user\AppData\Local\Temp\tmpF53B.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1608
Entropy (8bit):	5.112901951806503
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtLrLxvn:cgea6YrFdOFzOzN33ODOiDdKrsuTVv
MD5:	88AA601F9B38D4A8E15CE1206E119A78
SHA1:	C2BDCBBFCAC423AA0EE896FCFF53DC0EB388CCA2
SHA-256:	8D1D2180C05375699EA716A5D57E815CD276F6DF0E83E5E0763DF4314AB1E54F
SHA-512:	96B15BF23449EC28AC580791BFA7DA5DAD52E4D47FFB68DFDB3C42810B1451FD140E1204124A756F451954FDC3993FE428BDCF00AB1C6D9D977536CC809A214
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailab

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

Process:	C:\Users\user\Desktop\P2DIWOtpLf.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:a/ln:ad
MD5:	1A0D28D985B3AEFA84693C40D0AB6E52
SHA1:	DB1A8F262ABC0B223D91129FC6D383309E4C3985
SHA-256:	D784A482679364A60950E3AEC7F25ABE0E993490ED308BF267B031AA18160B68
SHA-512:	5CDB2B726881D43635792ED177289492CD0B7E036881FAA1FBA225CF28FE29D123C4F4C8A07FC86788E931E2C2D0A561234D484CD88593D28B8CF3D69A5301A
Malicious:	**true**
Reputation:	unknown
Preview:	.....2.H

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

Process:	C:\Users\user\Desktop\P2DIWOtpLf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	40
Entropy (8bit):	4.261768795973195
Encrypted:	false

SSDEEP:	3:oNN2+W1XhK9:oNN2Rjy
MD5:	CAB55ACDB8D7DAB3A5C46A4D8ADCFC79
SHA1:	F0279FDD19C5A93879DA5A874912C224307859A3
SHA-256:	57F9ADBE872F564744EFD85AC6731C5218B9FCEB9F4EB1CCDFA31A9582949289
SHA-512:	12D7EE61887D06EEAD3ADF71BB71B6272D35287A93680BCA263BD3112ABECA22F5CF1C87DDD071A18BBB6CDEB4D0A46696EFF86391E452D608B4F949B4FBD D70
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\P2DIWOtpLf.exe

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

Process:	C:\Users\user\Desktop\P2DIWOtpLf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	670208
Entropy (8bit):	7.742892435183354
Encrypted:	false
SSDEEP:	12288:KxjoxTdLDVXj6TKJfO2J7uE2ezRvfqFlfVX3xLJOrabQudntH:qjoxhETDfE9zRvyCt
MD5:	3789175015481EE123ABCBBFE83C3C16
SHA1:	500CCF71450EF911B6A431E25DA230742CA8BF65
SHA-256:	861BDB02B21024B41ACC04AC63D0CA3455F47DDA85B3D46DFD02D1F63855B796
SHA-512:	659831E3ED3CE843A9D574C19E6B21C2D5BC1844377142DFA25F0B868B1EAFBF46E9196756BDF404339E7ACE61F7830B1861121F4146D4205D414A53272F5FD9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Qhxb.....0..0.....>O... ...`....@.. ..... .....@.....N..O....`..... ....H.....text...D/... ...0..... ..`.rsrc.....`.....2..... ..@..@.reloc.....8.....@..B..... O.....H.....l_.....u...z.....].....Z.....[.R$6.|X8L.R..t ....t*.X....i.:>j.=...w....\...u.P.....J.=.v....R.. ..`4xz"....3.Ty.)....)+...z.acZuE...A.].-.[>5...Q....?.P;E..z...*=Vtd.,(G.o..".l:.....G..,f..m...t...C...S.6c}....(f..R..V.YGWl...1.....<\r~....M....}E@N..8Y...>....xm.T.j..%j<D<A..T.y. .\z..'O-t`.....,...7X..q.Gh..si.....y...A.N..;.....#g.... ..M...{..[i@?.VJ..':._.).H?.t5.V.{9...R.}h

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

Process:	C:\Users\user\Desktop\P2DIWOtpLf.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220510\PowerShell_transcript.376483.n68wiFr5.20220510202612.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):	5815
Entropy (8bit):	5.3698784748721335
Encrypted:	false
SSDEEP:	96:BZ8TLxNuaqDo1ZFZZTLxNuaqDo1ZZI+wjZwTLxNuaqDo1Z25AAjZQ:Y
MD5:	D4E77CCFAA4C8ABD46B90989B46DED73
SHA1:	781DE920B3E4EBBF8249C76B85A822ACFADD6133
SHA-256:	E9DE8674BCB6A21D3955FB4353987F173187C031EF6AF6081B782FA81EBB662B

SHA-512:	7AD4720EF2CC5FDC2AF12E4D3B9FCBFB702520F4C57CF73A643863095E4085C443797CBD8FB44DCF02B8BD73B0E33EBD136C66276C8B6D260A4D4145962082A
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220510202617..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 376483 (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\mjbsosItP.exe..Process ID: 6600..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: 20220510202617..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\mjbsosItP.exe..**********..Windows PowerShell transcript start..Start time: 20220510202953..Username: computer\user..RunAs User: DESKTOP

C:\Users\user\Documents\20220510\PowerShell_transcript.376483.rfYSk5DZ.20220510202541.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):	5815
Entropy (8bit):	5.368433643341428
Encrypted:	false
SSDEEP:	96:BZYTLxNrqDo1ZFZtTLxNrqDo1ZXI+wjZW2TLxNrqDo1ZJ5AAZZi:I
MD5:	90F237585489DF92A3631D638F472E37
SHA1:	B4AF5FCDCCFA3217FAF0B7407B5B67BA277A1D51
SHA-256:	5B3EEB3843F62BDF490285F5DF45601296D0E2AD1AC8F64842DFC1D30371C141
SHA-512:	0BD0B0D2D3C80CCFC30711998A75BC55E51D13320EA42D74E8A8E75CFD3B47177FF7E5B10813275828003C732DE0BB26A9B08263FA4144C196AF97904753CFA
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220510202543..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 376483 (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\mjbsosItP.exe..Process ID: 6112..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: 20220510202543..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\mjbsosItP.exe..**********..Windows PowerShell transcript start..Start time: 20220510202957..Username: computer\user..RunAs User: DESKTOP

C:\Users\user\Documents\20220510\PowerShell_transcript.376483.tuCn2Xiy.20220510202621.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):	5815
Entropy (8bit):	5.3663742154888014
Encrypted:	false
SSDEEP:	96:BZSTLxNgqDo1Z/ZNTLxNgqDo1ZLI+wjZOTLxNgqDo1ZU5AAtZ2:r
MD5:	0D8C48DB96DD23E99D662100718F7F1D
SHA1:	A585729E1C8B734980BFE4AE8BCE688EA5584FAE
SHA-256:	B6F375C4686C1F643C7D9E4E41744E3B9C24CEF3896AFB8DBB6ECE883C2AA24B
SHA-512:	542A87C92DCD101DDA0E19D07E5175A9FCB0589EE31DAFF6AB3C020221F2B752A4519CED24AA179E98F596A066DB3B7B0CB4713D9AC8A146587B390709F3B4F5
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220510202624..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 376483 (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\mjbsosItP.exe..Process ID: 7080..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: 20220510202624..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\mjbsosItP.exe..**********..Windows PowerShell transcript start..Start time: 20220510203020..Username: computer\user..RunAs User: DESKTOP

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.742892435183354

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	P2DIWOtpLf.exe
File size:	670208
MD5:	3789175015481ee123abcbbfe83c3c16
SHA1:	500ccf71450ef911b6a431e25da230742ca8bf65
SHA256:	861bdb02b21024b41acc04ac63d0ca3455f47dda85b3d46dfd02d1f63855b796
SHA512:	659831e3ed3ce843a9d574c19e6b21c2d5bc1844377142dfa25f0b868b1eafbf46e9196756bdf404339e7ace61f7830b1861121f4146d4205d414a53272f5fd9
SSDEEP:	12288:KxjoxTdLDVXj6TKJfO2J7uE2ezRvfqFlfVX3xLJOrabQudntH:qjoxhETDfE9zRvyCt
TLSH:	FCE4AD9C765075EFC857CC76DAA82C64EA6074BB530BD203A46316ED9A0DA8BCF141F3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Qhxb.....0..0.....>O... ...`....@.. .....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a4f3e
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:	0x62786851 [Mon May 9 01:03:13 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Instruction
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa4eec	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa6000	0x5c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
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	0xa2f44	0xa3000	False	0.860415967696	data	7.7499144591	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa6000	0x5c0	0x600	False	0.42578125	data	4.10658701877	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa8000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa60a0	0x334	data		
RT_MANIFEST	0xa63d4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Copyright Joe Security LLC 2022

Imports

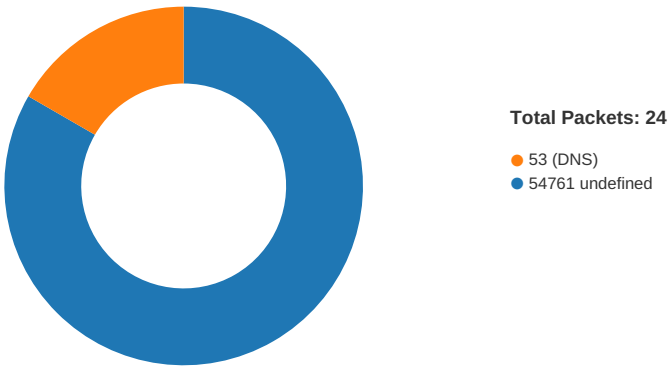
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014
Assembly Version	1.0.0.0
InternalName	SendOrPostCallb.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Oversikt
ProductVersion	1.0.0.0
FileDescription	Oversikt
OriginalFilename	SendOrPostCallb.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 20:26:04.762273073 CEST	49780	54761	192.168.2.6	102.89.42.162
May 10, 2022 20:26:07.800924063 CEST	49780	54761	192.168.2.6	102.89.42.162
May 10, 2022 20:26:13.801299095 CEST	49780	54761	192.168.2.6	102.89.42.162
May 10, 2022 20:26:30.984358072 CEST	49788	54761	192.168.2.6	102.89.42.162
May 10, 2022 20:26:34.006028891 CEST	49788	54761	192.168.2.6	102.89.42.162
May 10, 2022 20:26:34.146702051 CEST	54761	49788	102.89.42.162	192.168.2.6
May 10, 2022 20:26:34.146877050 CEST	49788	54761	192.168.2.6	102.89.42.162
May 10, 2022 20:26:39.670906067 CEST	49788	54761	192.168.2.6	102.89.42.162
May 10, 2022 20:26:47.196285009 CEST	49790	54761	192.168.2.6	102.89.42.162
May 10, 2022 20:26:50.370172977 CEST	49790	54761	192.168.2.6	102.89.42.162
May 10, 2022 20:26:56.479660034 CEST	49790	54761	192.168.2.6	102.89.42.162
May 10, 2022 20:27:12.553906918 CEST	49800	54761	192.168.2.6	185.19.85.160
May 10, 2022 20:27:12.581156015 CEST	54761	49800	185.19.85.160	192.168.2.6
May 10, 2022 20:27:13.106061935 CEST	49800	54761	192.168.2.6	185.19.85.160
May 10, 2022 20:27:13.124330044 CEST	54761	49800	185.19.85.160	192.168.2.6
May 10, 2022 20:27:13.809268951 CEST	49800	54761	192.168.2.6	185.19.85.160

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 20:27:13.827147961 CEST	54761	49800	185.19.85.160	192.168.2.6
May 10, 2022 20:27:17.891681910 CEST	49802	54761	192.168.2.6	185.19.85.160
May 10, 2022 20:27:17.915910959 CEST	54761	49802	185.19.85.160	192.168.2.6
May 10, 2022 20:27:18.512868881 CEST	49802	54761	192.168.2.6	185.19.85.160
May 10, 2022 20:27:18.561018944 CEST	54761	49802	185.19.85.160	192.168.2.6
May 10, 2022 20:27:19.106645107 CEST	49802	54761	192.168.2.6	185.19.85.160
May 10, 2022 20:27:19.128591061 CEST	54761	49802	185.19.85.160	192.168.2.6
May 10, 2022 20:27:23.140638113 CEST	49804	54761	192.168.2.6	185.19.85.160
May 10, 2022 20:27:23.158305883 CEST	54761	49804	185.19.85.160	192.168.2.6
May 10, 2022 20:27:23.669464111 CEST	49804	54761	192.168.2.6	185.19.85.160
May 10, 2022 20:27:23.687640905 CEST	54761	49804	185.19.85.160	192.168.2.6
May 10, 2022 20:27:24.200735092 CEST	49804	54761	192.168.2.6	185.19.85.160
May 10, 2022 20:27:24.218380928 CEST	54761	49804	185.19.85.160	192.168.2.6
May 10, 2022 20:27:28.413501978 CEST	49806	54761	192.168.2.6	102.89.42.162

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 20:26:04.567907095 CEST	56550	53	192.168.2.6	8.8.8.8
May 10, 2022 20:26:04.737948895 CEST	53	56550	8.8.8.8	192.168.2.6
May 10, 2022 20:26:30.582058907 CEST	57037	53	192.168.2.6	8.8.8.8
May 10, 2022 20:26:30.752882004 CEST	53	57037	8.8.8.8	192.168.2.6
May 10, 2022 20:26:47.177160025 CEST	54529	53	192.168.2.6	8.8.8.8
May 10, 2022 20:26:47.194267988 CEST	53	54529	8.8.8.8	192.168.2.6
May 10, 2022 20:27:28.235871077 CEST	53829	53	192.168.2.6	8.8.8.8
May 10, 2022 20:27:28.412312984 CEST	53	53829	8.8.8.8	192.168.2.6

DNS Queries

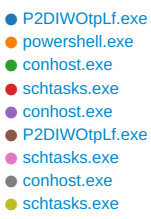
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 10, 2022 20:26:04.567907095 CEST	192.168.2.6	8.8.8.8	0xdc78	Standard query (0)	fastspeed.ddnsfree.com	A (IP address)	IN (0x0001)
May 10, 2022 20:26:30.582058907 CEST	192.168.2.6	8.8.8.8	0xbd80	Standard query (0)	fastspeed.ddnsfree.com	A (IP address)	IN (0x0001)
May 10, 2022 20:26:47.177160025 CEST	192.168.2.6	8.8.8.8	0xc54	Standard query (0)	fastspeed.ddnsfree.com	A (IP address)	IN (0x0001)
May 10, 2022 20:27:28.235871077 CEST	192.168.2.6	8.8.8.8	0xc589	Standard query (0)	fastspeed.ddnsfree.com	A (IP address)	IN (0x0001)

DNS Answers

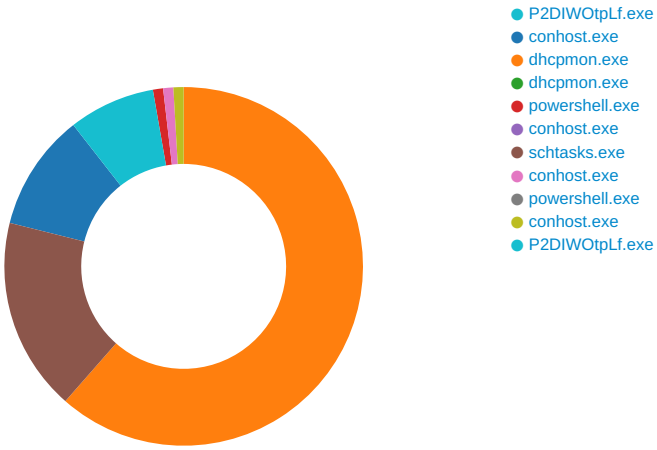
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2022 20:26:04.737948895 CEST	8.8.8.8	192.168.2.6	0xdc78	No error (0)	fastspeed.ddnsfree.com		102.89.42.162	A (IP address)	IN (0x0001)
May 10, 2022 20:26:30.752882004 CEST	8.8.8.8	192.168.2.6	0xbd80	No error (0)	fastspeed.ddnsfree.com		102.89.42.162	A (IP address)	IN (0x0001)
May 10, 2022 20:26:47.194267988 CEST	8.8.8.8	192.168.2.6	0xc54	No error (0)	fastspeed.ddnsfree.com		102.89.42.162	A (IP address)	IN (0x0001)
May 10, 2022 20:27:28.412312984 CEST	8.8.8.8	192.168.2.6	0xc589	No error (0)	fastspeed.ddnsfree.com		102.89.42.162	A (IP address)	IN (0x0001)

Statistics

Behavior



Copyright Joe Security LLC 2022



System Behavior

Analysis Process: P2DIWOtpLf.exe PID: **6436**, Parent PID: **3488**

General

Target ID:	0
Start time:	20:25:17
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\P2DIWOtpLf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\P2DIWOtpLf.exe"
Imagebase:	0xb70000
File size:	670208 bytes
MD5 hash:	3789175015481EE123ABCBBFE83C3C16
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.451037709.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.459586189.0000000004B4E000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.459586189.0000000004B4E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.459586189.0000000004B4E000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D9DCF06	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	6D9DCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\mjbsosItP.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	6C82DD66	CopyFileW
C:\Users\user\AppData\Roaming\mjbsosItP.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C82DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp3864.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C827038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\P2DIWOtpLf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DCEC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3864.tmp	success or wait	1	6C826A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\mjbsosItP.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3864.tmp	0	1608	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 65 6e 67 69 6e 65 65 72 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	<?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	6C821B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\P2DIWOtpLf.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	6DCEC907	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	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D9B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D9BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D9B5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C821B4F	ReadFile

Analysis Process: powershell.exe PID: **6112**, Parent PID: **6436**

General

Target ID:	5
Start time:	20:25:39
Start date:	10/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\mjbsosItP.exe
Imagebase:	0xf10000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D9DCF06	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	6D9DCF06	unknown
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	6C785B28	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	6C785B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xpzwv1x0.mtv.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C821E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hhukf3ev.kf3.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C821E60	CreateFileW
C:\Users\user\Documents\20220510	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C82BEFF	CreateDirectoryW
C:\Users\user\Documents\20220510\PowerShell_transcript.376483.rfYSk5DZ.20220510202541.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C821E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xpzwv1x0.mtv.ps1	success or wait	1	6C826A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hhukf3ev.kf3.psm1	success or wait	1	6C826A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xpzwv1x0.mtv.ps1	0	1	31	1	success or wait	1	6C821B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hhukf3ev.kf3.psm1	0	1	31	1	success or wait	1	6C821B4F	WriteFile
C:\Users\user\Documents\20220510\PowerShell_transcript.376483.rfYSk5DZ.20220510202541.txt	0	3	ff		success or wait	1	6C821B4F	WriteFile
C:\Users\user\Documents\20220510\PowerShell_transcript.376483.rfYSk5DZ.20220510202541.txt	3	685	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 31 30 32 30 32 35 34 33 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 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 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 37 36 34 38 33 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	**********Windows PowerShell transcript startStart time: 20220510202543Username: computer\userRunAsUser: computer\userConfiguration Name: Machine: 376483 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	44	6C821B4F	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 64 14 00 00 18 00 00 00 6f 0c 7b 04 fd 07 fd 07 fd 07 00 00 7a 01 fd 00 1b 00 4f 0c 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@edo{zO@	success or wait	1	6DCA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	6DCA76FC	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	6DCA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DCA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DCA76FC	WriteFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@BMDmEEMqqS%n4&5&7&	success or wait	11	6DCA76FC	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	6D9B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D9B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D9BCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D9BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D9BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D9B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D9B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D9B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D9B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D9B5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D9C1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	6D9C203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9103DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C821B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C821B4F	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D9B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D9B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C821B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D9B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D9B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C821B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	2	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C821B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C821B4F	ReadFile

Analysis Process: conhost.exe PID: **3720**, Parent PID: **6112**

General

Target ID:	6
Start time:	20:25:40
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: **3524**, Parent PID: **6436**

General

Target ID:	7
Start time:	20:25:40
Start date:	10/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\mjbsosItP" /XML "C:\Users\user\AppData\Local\Temp\tmp3864.tmp
Imagebase:	0xc80000
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\tmp3864.tmp	unknown	2	success or wait	1	C8AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3864.tmp	unknown	1609	success or wait	1	C8ABD9	ReadFile

Analysis Process: conhost.exe PID: **5732**, Parent PID: **3524**

General

Target ID:	8
Start time:	20:25:42
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: P2DIWOtpLf.exe PID: **5776**, Parent PID: **6436**

General

Target ID:	9
Start time:	20:25:46
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\P2DIWOtpLf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\P2DIWOtpLf.exe
Imagebase:	0x840000
File size:	670208 bytes
MD5 hash:	3789175015481EE123ABCBBFE83C3C16
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: 00000009.00000002.651685390.0000000005640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.651685390.0000000005640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000009.00000002.651685390.0000000005640000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.444632787.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.444632787.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.444632787.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.650081379.0000000003C19000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.650081379.0000000003C19000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.647846914.0000000002C11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.447407809.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.447407809.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.447407809.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.651959106.0000000006340000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.651959106.0000000006340000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.651959106.0000000006340000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000009.00000002.651959106.0000000006340000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.645899723.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.645899723.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.645899723.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.446080328.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.446080328.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.446080328.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.651668684.0000000005630000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.651668684.0000000005630000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000009.00000002.651668684.0000000005630000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.446663860.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.446663860.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.446663860.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D9DCF06	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	6D9DCF06	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	6C82BEFF	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	6C821E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C82BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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	6C82DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C82DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp5E50.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C827038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C821E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp67E6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C827038	GetTempFileNameW
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	6C82BEFF	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	6C82BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5E50.tmp	success or wait	1	6C826A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp67E6.tmp	success or wait	1	6C826A95	DeleteFileW
C:\Users\user\Desktop\P2DIWOtpLf.exe:Zone.Identifier	success or wait	1	6C7A2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd fd fd fd fd 32 fd 48	2H	success or wait	1	6C821B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp67E6.tmp	0	1310	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 0d 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 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	6C821B4F	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	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D9B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D9BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C821B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D99D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D99D72F	unknown
C:\Users\user\Desktop\P2DIWOtpLf.exe	unknown	4096	success or wait	1	6D99D72F	unknown
C:\Users\user\Desktop\P2DIWOtpLf.exe	unknown	512	success or wait	1	6D99D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6C82646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **6840**, Parent PID: **5776**

General	
Target ID:	12
Start time:	20:25:58
Start date:	10/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp5E50.tmp
Imagebase:	0xc80000
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\tmp5E50.tmp	unknown	2	success or wait	1	C8AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp5E50.tmp	unknown	1304	success or wait	1	C8ABD9	ReadFile

Analysis Process: conhost.exe PID: **2368**, Parent PID: **6840**

General	
Target ID:	13
Start time:	20:25:59
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: **7112**, Parent PID: **5776**

General	
Target ID:	15
Start time:	20:26:00
Start date:	10/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp67E6.tmp
Imagebase:	0xc80000
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\tmp67E6.tmp	unknown	2	success or wait	1	C8AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp67E6.tmp	unknown	1311	success or wait	1	C8ABD9	ReadFile

Analysis Process: P2DIWOtpLf.exe PID: **7028**, Parent PID: **696**

General

Target ID:	16
Start time:	20:26:01
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\P2DIWOtpLf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\P2DIWOtpLf.exe 0
Imagebase:	0x6e0000
File size:	670208 bytes
MD5 hash:	3789175015481EE123ABCBBFE83C3C16
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: 00000010.00000002.563478498.000000000464E000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.563478498.000000000464E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.563478498.000000000464E000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000010.00000002.529814220.0000000002AA1000.00000004.00000800.00020000.00000000.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	6D9DCF06	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	6D9DCF06	unknown
C:\Users\user\AppData\Local\Temp\tmpB218.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C827038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB218.tmp	success or wait	1	6C826A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB218.tmp	0	1608	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 65 6e 67 69 6e 65 65 72 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	<?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	6C821B4F	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	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D9B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D9BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D9B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C821B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C821B4F	ReadFile

Analysis Process: conhost.exe PID: **7104**, Parent PID: **7112**

General

Target ID:	17
Start time:	20:26:01
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: dhcpmon.exe PID: **804**, Parent PID: **696**

General

Target ID:	18
Start time:	20:26:03
Start date:	10/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xbe0000
File size:	670208 bytes
MD5 hash:	3789175015481EE123ABCBBFE83C3C16
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: 00000012.00000002.585593634.0000000004BCE000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.585593634.0000000004BCE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.585593634.0000000004BCE000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000012.00000002.574049078.0000000003021000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 63%, ReversingLabs

Analysis Process: dhcpmon.exe PID: **1320**, Parent PID: **3688**

General

Target ID:	19
Start time:	20:26:08
Start date:	10/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xd00000
File size:	670208 bytes
MD5 hash:	3789175015481EE123ABCBBFE83C3C16
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000013.00000002.593612504.00000000030A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.600335778.0000000004C4E000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.600335778.0000000004C4E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.600335778.0000000004C4E000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: powershell.exe PID: **6600**, Parent PID: **7028**

General

Target ID:	20
Start time:	20:26:10
Start date:	10/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\mjbsosItP.exe
Imagebase:	0xf10000

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

Analysis Process: conhost.exe PID: **6512**, Parent PID: **6600**

General

Target ID:	21
Start time:	20:26:11
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **6500**, Parent PID: **7028**

General

Target ID:	22
Start time:	20:26:11
Start date:	10/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\mjbsosItP" /XML "C:\Users\user\AppData\Local\Temp\tmpB218.tmp
Imagebase:	0xc80000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6764**, Parent PID: **6500**

General

Target ID:	23
Start time:	20:26:16
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **7080**, Parent PID: **804**

General	
Target ID:	24
Start time:	20:26:19
Start date:	10/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\mjbsosItP.exe
Imagebase:	0xf10000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **5672**, Parent PID: **7080**

General	
Target ID:	25
Start time:	20:26:20
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: P2DIWOtpLf.exe PID: **6108**, Parent PID: **7028**

General	
Target ID:	26
Start time:	20:26:20
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\P2DIWOtpLf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\P2DIWOtpLf.exe
Imagebase:	0xc00000
File size:	670208 bytes
MD5 hash:	3789175015481EE123ABCBBFE83C3C16
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: 0000001A.00000000.523160689.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000000.523160689.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000000.523160689.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000000.520325919.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000000.520325919.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000000.520325919.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000002.568084479.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.568084479.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.568084479.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.574248700.0000000003021000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.574248700.0000000003021000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.574448013.0000000004029000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.574448013.0000000004029000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000000.525271678.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000000.525271678.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000000.525271678.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000000.519784779.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000000.519784779.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000000.519784779.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

No disassembly