ID: 357426
Sample Name:
cp573oYDUX.exe
Cookbook: default.jbs
Time: 16:09:26
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

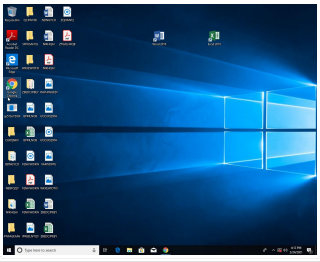
Analysis Report cp573oYDUX.exe

Overview

General Information

Sample Name:	cp573oYDUX.exe
Analysis ID:	357426
MD5:	33cf3af09d2a178..
SHA1:	ffe606addd56944..
SHA256:	8da32ea516feb3b.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

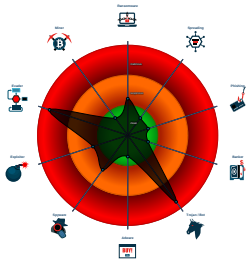
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Connects to many ports of the same…

Classification



Startup

- **System is w10x64**
- cp573oYDUX.exe (PID: 7012 cmdline: 'C:\Users\user\Desktop\cp573oYDUX.exe' MD5: 33CF3AF09D2A1789A2BBAD009A43EDD5)
  - schtasks.exe (PID: 3800 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eVEWVTvFLGVU' /XML 'C:\Users\user\AppData\Local\Temp\tmp53F8.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 2264 cmdline: {path} MD5: 71369277D09DA0830C8C59F9E22BB23A)
    - schtasks.exe (PID: 6632 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpFC43.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6620 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5996 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpFF61.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 5692 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 5684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5680 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6916 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 7144 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 7116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "572eb7a9-aedf-4b39-8669-f7563dab8a38",
  "Group": "GREAT",
  "Domain1": "strongodss.ddns.net",
  "Domain2": "79.134.225.43",
  "Port": 58103,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8009,
  "BufferSize": "02000100",
  "MaxPacketSize": "",
  "GCThreshold": "",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.600652707.000000000503 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000007.00000002.600652707.000000000503 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000007.00000002.594405865.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000007.00000002.594405865.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000007.00000002.594405865.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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

Click to see the 14 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.RegSvcs.exe.5030000.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
7.2.RegSvcs.exe.5030000.7.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
7.2.RegSvcs.exe.3daec9e.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x4083:$x1: NanoCore.ClientPluginHost
7.2.RegSvcs.exe.3daec9e.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x4083:$x2: NanoCore.ClientPluginHost • 0x4161:$s4: PipeCreated • 0x409d:$s5: IClientLoggingHost
7.2.RegSvcs.exe.3db9511.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 44 entries				

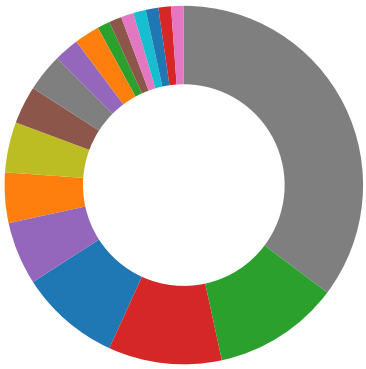
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Operating System Destruction
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

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

Uses dynamic DNS services

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:

.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 AntiVM_3

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

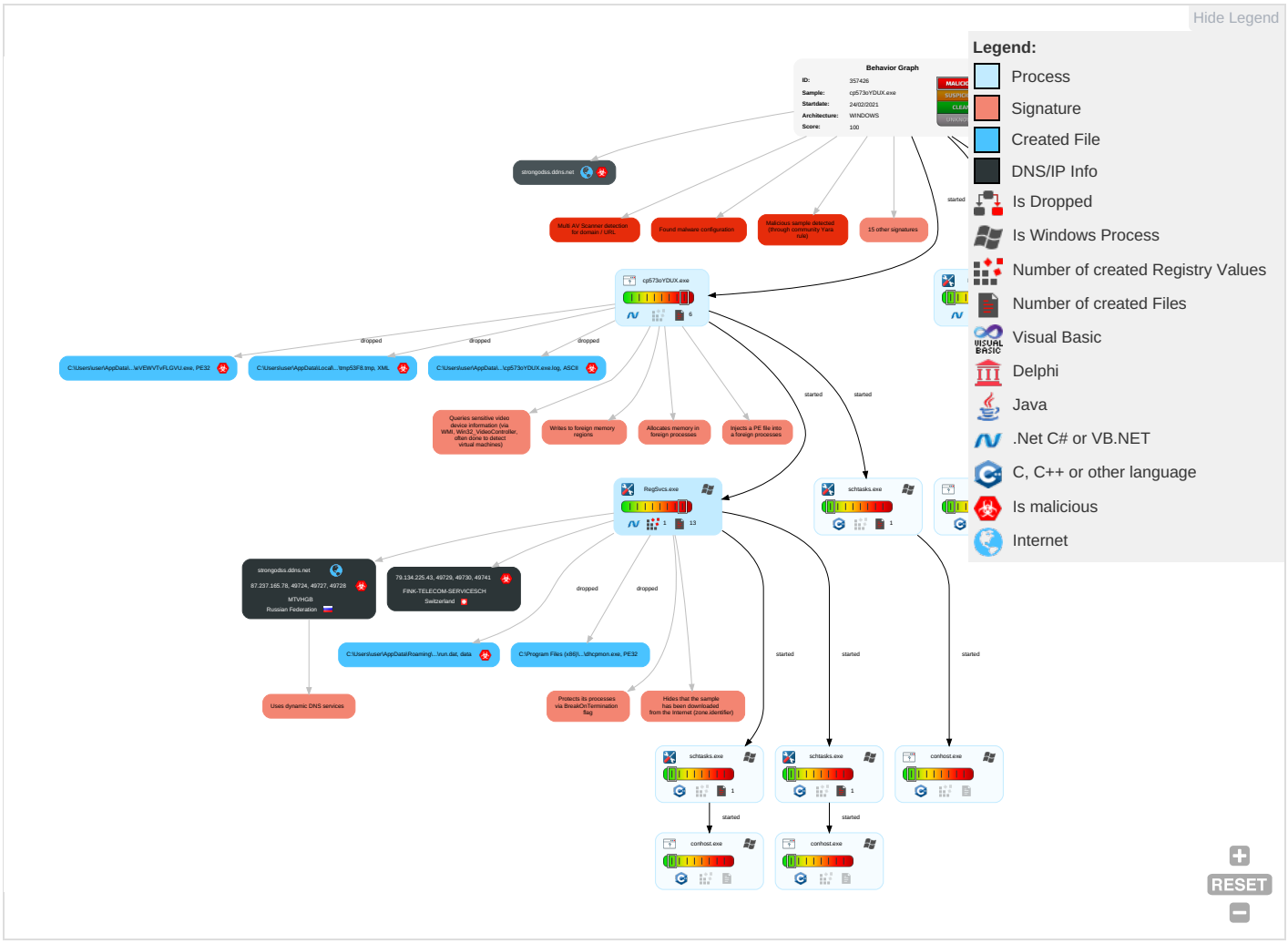
Detected Nanocore Rat

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
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 2 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

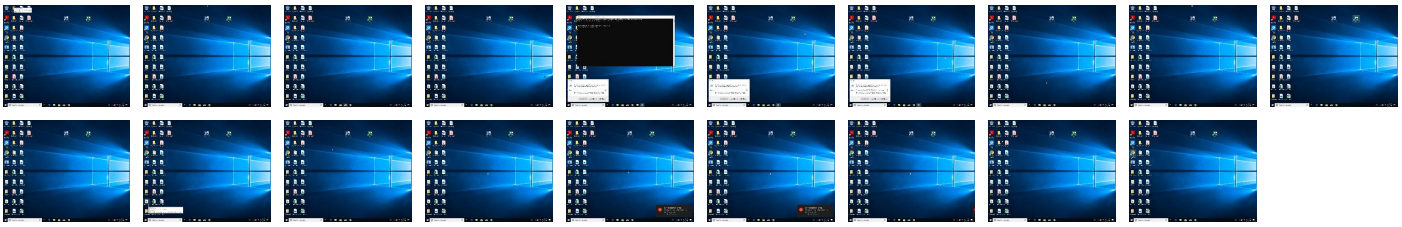
Behavior Graph



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
cp573oYDUX.exe	33%	Virustotal		Browse
cp573oYDUX.exe	31%	ReversingLabs	Win32.Trojan.AgentTesla	
cp573oYDUX.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\eVEWVTvFLGVU.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\eVEWVTvFLGVU.exe	31%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.RegSvcs.exe.59a0000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
strongodss.ddns.net	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
79.134.225.43	1%	Virustotal		Browse
79.134.225.43	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.fontbureau.comitudF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/F	0%	Avira URL Cloud	safe	
http://www.carterandcone.comams	0%	Avira URL Cloud	safe	
http://www.carterandcone.comal	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.sandoll.co.kr-h	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com(	0%	Avira URL Cloud	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/_	0%	Avira URL Cloud	safe	
http://www.fonts.comont	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//typ	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.sandoll.co.krproductW	0%	Avira URL Cloud	safe	
http://www.carterandcone.comEac	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnhy/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.carterandcone.comuct	0%	Avira URL Cloud	safe	
http://www.fontbureau.comrsiv	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.carterandcone.comic	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr:	0%	Avira URL Cloud	safe	
http://www.urwpp.deX	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krx	0%	Avira URL Cloud	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0P	0%	Avira URL Cloud	safe	
http://www.fontbureau.comonyF	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.sandoll.co.krIns	0%	Avira URL Cloud	safe	
http://www.carterandcone.comtig55E	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.fontbureau.comdi	0%	Avira URL Cloud	safe	
strongodss.ddns.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
strongodss.ddns.net	87.237.165.78	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
79.134.225.43	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
strongodss.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false		high

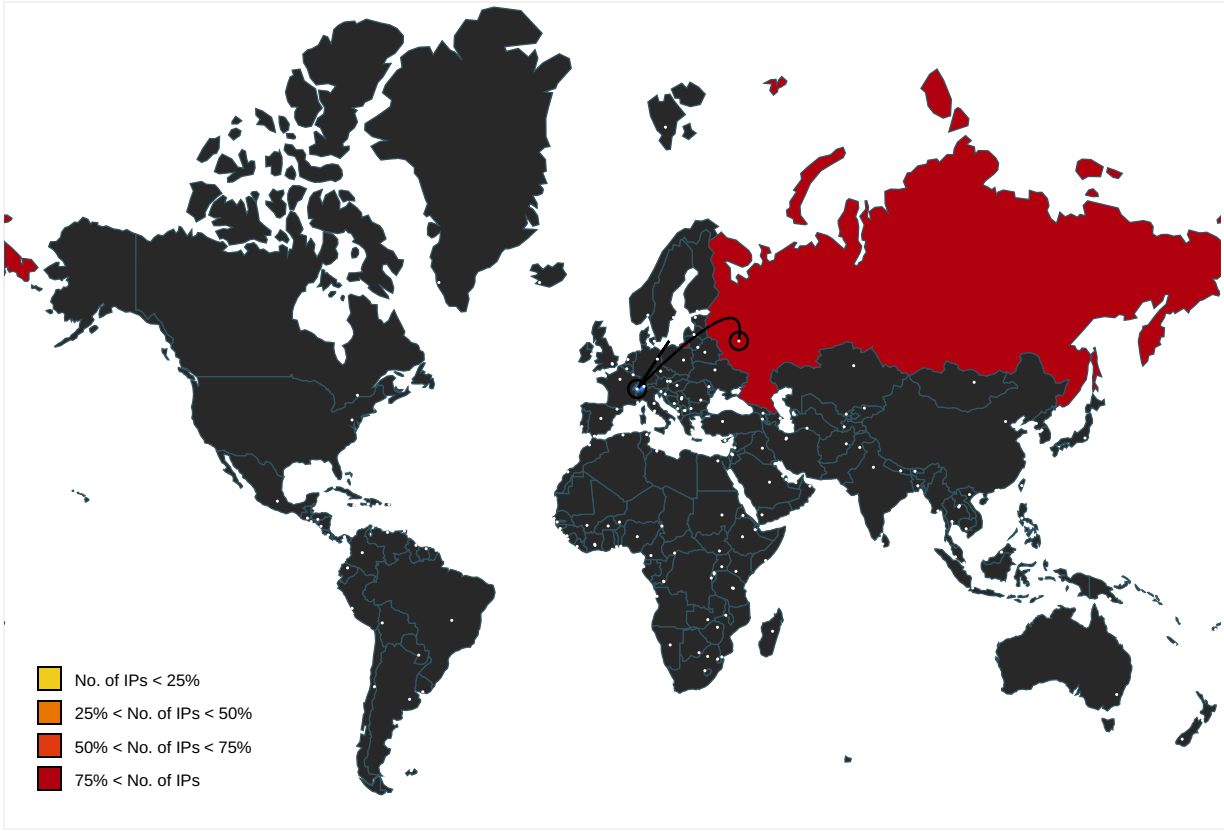
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comn-u	cp573oYDUX.exe, 00000000.00000003.329047446.0000000005281000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comitudF	cp573oYDUX.exe, 00000000.00000003.332598799.000000000525A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/F	cp573oYDUX.exe, 00000000.00000003.330163656.000000000525A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comams	cp573oYDUX.exe, 00000000.00000003.329047446.0000000005281000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comal	cp573oYDUX.exe, 00000000.00000003.329047446.0000000005281000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp, cp573oYDUX.exe, 00000000.00000003.333338294.000000000525A000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr-h	cp573oYDUX.exe, 00000000.00000003.328160873.000000000525E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	cp573oYDUX.exe, 00000000.00000003.329047446.0000000005281000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com(	cp573oYDUX.exe, 00000000.00000003.329047446.0000000005281000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.com.	cp573oYDUX.exe, 00000000.00000003.329047446.0000000005281000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/_	cp573oYDUX.exe, 00000000.00000003.330163656.000000000525A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comont	cp573oYDUX.exe, 00000000.00000003.326989499.000000000116C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//typ	cp573oYDUX.exe, 00000000.00000003.329818359.0000000005259000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krproductW	cp573oYDUX.exe, 00000000.00000003.328160873.000000000525E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersa	cp573oYDUX.exe, 00000000.00000003.332247018.000000000525A000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comEac	cp573oYDUX.exe, 00000000.00000003.329047446.0000000005281000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnhy/	cp573oYDUX.exe, 00000000.00000003.328391063.000000000527D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comgrito	cp573oYDUX.exe, 00000000.00000003.331556678.000000000525A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comuct	cp573oYDUX.exe, 00000000.00000003.329047446.0000000005281000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comrsiv	cp573oYDUX.exe, 00000000.00000003.333160694.000000000525A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	cp573oYDUX.exe, 00000000.00000003.327285488.0000000005285000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	cp573oYDUX.exe, 00000000.00000003.333449545.000000000525A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	cp573oYDUX.exe, 00000000.00000003.328825494.0000000005280000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com=	cp573oYDUX.exe, 00000000.00000003.333160694.000000000525A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comic	cp573oYDUX.exe, 00000000.00000003.329047446.0000000005281000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersr	cp573oYDUX.exe, 00000000.00000003.333160694.000000000525A000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr:	cp573oYDUX.exe, 00000000.00000003.328160873.000000000525E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deX	cp573oYDUX.exe, 00000000.00000003.333507582.000000000525A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	cp573oYDUX.exe, 00000000.00000003.328781426.000000000527F000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	cp573oYDUX.exe, 00000000.00000003.331677577.000000000525A000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/_	cp573oYDUX.exe, 00000000.00000003.332897804.000000000525A000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.krx	cp573oYDUX.exe, 00000000.00000003.328160873.000000000525E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.agfamonotype.	cp573oYDUX.exe, 00000000.00000003.337101264.0000000005281000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlp	cp573oYDUX.exe, 00000000.00000003.332869924.0000000005281000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comTC	cp573oYDUX.exe, 00000000.00000003.329047446.0000000005281000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0P	cp573oYDUX.exe, 00000000.00000003.330163656.000000000525A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comonyF	cp573oYDUX.exe, 00000000.00000003.331677577.000000000525A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/F	cp573oYDUX.exe, 00000000.00000003.329395807.0000000005253000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	cp573oYDUX.exe, 00000000.00000003.330299816.000000000525A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krlns	cp573oYDUX.exe, 00000000.00000003.328160873.000000000525E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comtig55E	cp573oYDUX.exe, 00000000.00000003.329047446.0000000005281000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma	cp573oYDUX.exe, 00000000.00000002.374558524.0000000005250000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.w	cp573oYDUX.exe, 00000000.00000003.329395807.0000000005253000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comdi	cp573oYDUX.exe, 00000000.00000003.331677577.000000000525A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.krnyis	cp573oYDUX.exe, 00000000.00000003.328160873.000000000525E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html8p(	cp573oYDUX.exe, 00000000.00000003.332131926.0000000005281000.00000004.00000001.sdmp	false		high
http://www.urwpp.deeg	cp573oYDUX.exe, 00000000.00000003.333449545.000000000525A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	cp573oYDUX.exe, 00000000.00000003.328672332.000000000527F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/RJG	cp573oYDUX.exe, 00000000.00000003.329818359.0000000005259000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comiond	cp573oYDUX.exe, 00000000.00000003.331677577.000000000525A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	cp573oYDUX.exe, 00000000.00000003.332131926.0000000005281000.00000004.00000001.sdmp, cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comfacG5w	cp573oYDUX.exe, 00000000.00000003.329047446.0000000005281000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	cp573oYDUX.exe, 00000000.00000003.332932000.0000000005281000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comt	cp573oYDUX.exe, 00000000.00000003.333160694.000000000525A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	cp573oYDUX.exe, 00000000.00000003.330299816.000000000525A000.00000004.00000001.sdmp, cp573oYDUX.exe, 00000000.00000003.330044302.000000000525A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comona	cp573oYDUX.exe, 00000000.00000003.329047446.0000000005281000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/i	cp573oYDUX.exe, 00000000.00000003.329939920.000000000525A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	cp573oYDUX.exe, 00000000.00000002.374864091.00000000053C0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comueikM	cp573oYDUX.exe, 00000000.00000003.332897804.000000000525A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comals	cp573oYDUX.exe, 00000000.00000003.333507582.000000000525A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/s-c	cp573oYDUX.exe, 00000000.00000003.329395807.0000000005253000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/b	cp573oYDUX.exe, 00000000.00000003.330044302.000000000525A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/_	cp573oYDUX.exe, 00000000.00000003.329818359.0000000005259000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
87.237.165.78	unknown	Russian Federation		49967	MTVHGB	true
79.134.225.43	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357426
Start date:	24.02.2021
Start time:	16:09:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cp573oYDUX.exe

Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@18/13@12/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.9% (good quality ratio 2.1%) • Quality average: 53.3% • Quality standard deviation: 40%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.42.151.234, 23.54.113.53, 13.64.90.137, 52.255.188.83, 51.11.168.160, 52.155.217.156, 23.0.174.187, 23.0.174.185, 20.54.26.129, 51.103.5.159, 23.10.249.25, 23.10.249.26, 95.100.54.203 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
16:10:21	API Interceptor	1x Sleep call for process: cp573oYDUX.exe modified
16:10:37	API Interceptor	853x Sleep call for process: RegSvcs.exe modified
16:10:38	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe" s>$(Arg0)
16:10:38	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
16:10:40	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
87.237.165.78	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	
	M5QDAaK9yM.exe	Get hash	malicious	Browse	
	TdX45jQWjj.exe	Get hash	malicious	Browse	
79.134.225.43	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	
	TdX45jQWjj.exe	Get hash	malicious	Browse	
	JfRbEbUkpV39K4L.exe	Get hash	malicious	Browse	
	Dachser Consulta de cliente saliente no. 000150849 - SKBMT03082020-0012-IMG0149.exe	Get hash	malicious	Browse	
	290453721.xls	Get hash	malicious	Browse	
	nUo0FukkVO.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
strongodss.ddns.net	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	• 87.237.165.78
	M5QDAaK9yM.exe	Get hash	malicious	Browse	• 87.237.165.78
	TdX45jQWjj.exe	Get hash	malicious	Browse	• 87.237.165.78

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MTVHGB	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	• 87.237.165.78
	M5QDAaK9yM.exe	Get hash	malicious	Browse	• 87.237.165.78
	TdX45jQWjj.exe	Get hash	malicious	Browse	• 87.237.165.78
	QUOTATION 19 01 2021.exe	Get hash	malicious	Browse	• 87.237.165.162
FINK-TELECOM-SERVICESCH	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	• 79.134.225.43
	xF7GogN7tM.exe	Get hash	malicious	Browse	• 79.134.225.120
	TZgGVyMJYF.exe	Get hash	malicious	Browse	• 79.134.225.74
	ilpbALnKbE.exe	Get hash	malicious	Browse	• 79.134.225.103
	Documents.exe	Get hash	malicious	Browse	• 79.134.225.87
	SWcNyi2YBj.exe	Get hash	malicious	Browse	• 79.134.225.103
	Confirmation Transfer Note Ref Number0002636.exe	Get hash	malicious	Browse	• 79.134.225.8
	TdX45jQWjj.exe	Get hash	malicious	Browse	• 79.134.225.43
	e92b274943f4a3a557881ee0dd57772d.exe	Get hash	malicious	Browse	• 79.134.225.105
	WxTm2cWLHF.exe	Get hash	malicious	Browse	• 79.134.225.71
	Payment Confirmation.exe	Get hash	malicious	Browse	• 79.134.225.30
	rjHlt1zz28.exe	Get hash	malicious	Browse	• 79.134.225.49
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 79.134.225.49
	document.exe	Get hash	malicious	Browse	• 79.134.225.122
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 79.134.225.105
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 79.134.225.105
	256ec8f8f67b59c5e085b0bb63afcd13.exe	Get hash	malicious	Browse	• 79.134.225.105
	JOIN.exe	Get hash	malicious	Browse	• 79.134.225.30
	Delivery pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 79.134.225.105

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	receipt.exe	Get hash	malicious	Browse	
	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	
	M5QDAaK9yM.exe	Get hash	malicious	Browse	
	oMWv1Zof2y.exe	Get hash	malicious	Browse	
	TdX45jQWjj.exe	Get hash	malicious	Browse	
	QTxFuxF5NQ.exe	Get hash	malicious	Browse	
	a34b93ef-dea2-45f8-a5bf-4f6b0b5291c7.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	3fcd8c19-af88-4cd9-87e7-0bfea1de01a1.exe	Get hash	malicious	Browse	
	Vietnam Order.exe	Get hash	malicious	Browse	
	Dhl Shipping Document.exe	Get hash	malicious	Browse	
	PO-WJO-001, pdf.exe	Get hash	malicious	Browse	
	byWuWAR5FD.exe	Get hash	malicious	Browse	
	parcel_images.exe	Get hash	malicious	Browse	
	0712020.exe	Get hash	malicious	Browse	
	JfRbEbUkpV39K4L.exe	Get hash	malicious	Browse	
	DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe	Get hash	malicious	Browse	
	DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe	Get hash	malicious	Browse	
	zC3edqmNNt.exe	Get hash	malicious	Browse	
	Shipping Document.pdf..exe	Get hash	malicious	Browse	
	PPR & CPR_HEA_DECEMBER 4 2020.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7515815714465193
Encrypted:	false
SSDEEP:	384:BOj9Y8/gS7SDriLGKq1MHR5U4Ag6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgWSW72uw:B+gSAdN1MH3HAFRJngW2u
MD5:	71369277D09DA0830C8C59F9E22BB23A
SHA1:	37F9781314F0F6B7E9CB529A573F2B1C8DE9E93F
SHA-256:	D4527B7AD2FC4778CC5BE8709C95AEA44EAC0568B367EE14F7357D72898C3698
SHA-512:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB7
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: receipt.exe, Detection: malicious, Browse • Filename: YoWPu2BQzA9FeDd.exe, Detection: malicious, Browse • Filename: M5QDAaK9yM.exe, Detection: malicious, Browse • Filename: oMWv1Zof2y.exe, Detection: malicious, Browse • Filename: TdX45jQWjj.exe, Detection: malicious, Browse • Filename: QTxFuxF5NQ.exe, Detection: malicious, Browse • Filename: a34b93ef-dea2-45f8-a5bf-4f6b0b5291c7.exe, Detection: malicious, Browse • Filename: 3fcd8c19-af88-4cd9-87e7-0bfea1de01a1.exe, Detection: malicious, Browse • Filename: Vietnam Order.exe, Detection: malicious, Browse • Filename: Dhl Shipping Document.exe, Detection: malicious, Browse • Filename: PO-WJO-001, pdf.exe, Detection: malicious, Browse • Filename: byWuWAR5FD.exe, Detection: malicious, Browse • Filename: parcel_images.exe, Detection: malicious, Browse • Filename: 0712020.exe, Detection: malicious, Browse • Filename: JfRbEbUkpV39K4L.exe, Detection: malicious, Browse • Filename: DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe, Detection: malicious, Browse • Filename: DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe, Detection: malicious, Browse • Filename: zC3edqmNNt.exe, Detection: malicious, Browse • Filename: Shipping Document.pdf..exe, Detection: malicious, Browse • Filename: PPR & CPR_HEA_DECEMBER 4 2020.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....P... .....k... .....@.. .....[.. ..@.....k..K..... k..... ....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\cp573oYDUX.exe.log	
Process:	C:\Users\user\Desktop\cp573oYDUX.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	655
Entropy (8bit):	5.273171405160065
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9t0U2WUXBQav:MLF20NaL329hJ5g522rWz2p29XBT
MD5:	2703120C370FBB4A8BA08C6D1754039E
SHA1:	EC0DB47BF00A4A828F796147619386C0BBEA66A1
SHA-256:	F95566974BC44F3A757CAFB1456D185D8F333AC84775089DE18310B90C18B1BC
SHA-512:	BC05A2A1BE5B122FC6D3DEA66EF4258522F13351B9754378395AAD019631E312CFD3BC990F3E3D5C7BB0BDBA1EAD54A2B34A96DEE2FCCD703721E98F6192EE 48
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\4de9980 4c29261edb63c93616550f034\System.Management.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmp53F8.tmp	
Process:	C:\Users\user\Desktop\cp573oYDUX.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1657
Entropy (8bit):	5.169379230727161
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3yPtn:cbha7JlNQV/rydbz9l3YODOLNdq3a
MD5:	441C63E7DAD6297B2955622DAB7933C3
SHA1:	51158143E133CBCD60214C98416436E6E64344EA
SHA-256:	86B3D194F04436CA2A2AF48AD2670ED72F5CAC647A95323B9A8965E0172D7749
SHA-512:	D4A89A81B39D43A15F461978D59558C3D8367C9A518A312D0FE26417152F077B9CF3E53273968BDC97224EF2C518CD2CD8A9B6D235D29545149CC70BD186B84
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmpFC43.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\tmpFC43.tmp	
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135021273392143
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mn4xtn:cbk4oL600QydbQxIYODOLedq3Z4j
MD5:	40B11EF601FB28F9B2E69D36857BF2EC
SHA1:	B6454020AD2CEED193F4792B77001D0BD741B370
SHA-256:	C51E12D18CC664425F6711D8AE2507068884C7057092CFA11884100E1E9D49E1
SHA-512:	E3C5BCC714CBFCA4B8058DDCDDF231DCEFA69C15881CE3F8123E59ED45CFB5DA052B56E1945DCF8DC7F800D62F9A4EECB82BCA69A66A1530787AEFFEB15E 2BD5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpFF61.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
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
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:PajVP:ijVP
MD5:	65075989286889C893451A913787CFA5
SHA1:	8FDFC75DD6A78C5D386915B78D732610065955FB
SHA-256:	59F0476D7901FADD5876D37ACFB8D8FA33FDB8279CA4F9B0FA44827C9FDE5B88
SHA-512:	C69DA3E0C0B01DF26EE2622B0683585FF4C3D318C718576351586571708AD5203D4825C8C84DB6137C3ACD5B94EA76F802B83A0B1956B88D9D14EA254A46AE0
Malicious:	**true**
Preview:	...!..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.795707286467131
Encrypted:	false
SSDEEP:	3:oMty8WbSX/MNn:oMLWus
MD5:	D685103573539B7E9FDBF5F1D7DD96CE
SHA1:	4B2FE6B5C0B37954B314FCAEE1F12237A9B02D07
SHA-256:	D78BC23B0CA3EDDF52D56AB85CDC30A71B3756569CB32AA2F6C28DBC23C76E8E

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
SHA-512:	17769A5944E8929323A34269ABEEF0861D5C6799B0A27F5545FBFADC80E5AB684A471AD6F6A7FC623002385154EA89DE94013051E09120AB94362E542AB0F1DD
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe

C:\Users\user\AppData\Roaming\eVEWVTvFLGVU.exe	
Process:	C:\Users\user\Desktop\cp573oYDUX.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	793600
Entropy (8bit):	7.943634916057093
Encrypted:	false
SSDEEP:	12288:ZEA3LLUEMjhvUbJG16KfU32GOK2F5WRPVba0G/JZgC498Fj31Q2QuUmz:bL0iG16KfYrOK26RPZaA2dFFT
MD5:	33CF3AF09D2A1789A2BBAD009A43EDD5
SHA1:	FFE606ADDD5694451511DD347BBC85A404328C9D
SHA-256:	8DA32EA516FEB3BC471BA01ED18CB0ACA1A9F39966C86CA4624DD2CEA2E226CD
SHA-512:	9534E6EC15F7D1C237E254A3DAC79C7E44CC4C7989F3DBB8A4F0B682A3F3CFBBD46E6DDDFFA0E2A7E6BBD3E2B74389492559A8AD89FED85309CB848D5A1F60CB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?.5`.....0.....0... ...@....@.. ..... ..@.....0..O....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....0.....H.....Ho...2.....4...(...X.....&.(.....*...0..9.....~.....,".r...p.....(....o....s.....~.....+..*....0.....~.....+..*" .....*.0..!.....(....r!..p~....o.....t.....+..*....0..!.....(....r1..p~....o.....t.....+..*....0.....r5..p.+..*..0.....rA..p.+..*"'.(.....*^..}.....(.....(%....**...(.....*..0..;.....rO..pr...p.(.....,.. (.....+..s.....o.....(.....*..0..I.....r...pr...p.(.....

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1145
Entropy (8bit):	4.462201512373672
Encrypted:	false
SSDEEP:	24:zKLXkzPDObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0zPDQntKKH1MqJC
MD5:	46EBEB88876A00A52CC37B1F8E0D0438
SHA1:	5E5DB352F964E5F398301662FF558BD905798A65
SHA-256:	D65BD5A6CC112838AFE8FA70BF61FD13C1313BCE3EE3E76C50E454D7B581238B
SHA-512:	E713E6F304A469FB71235C598BC7E2C6F8458ABC61DAF3D1F364F66579CAFA4A7F3023E585BDA552FB400009E7805A8CA0311A50D5EDC9C2AD2D067772A071BE
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo Suppress logo output... /quiet Suppress logo output and success output...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.943634916057093
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	cp573oYDUX.exe
File size:	793600
MD5:	33cf3af09d2a1789a2bbad009a43edd5
SHA1:	ffe606addd5694451511dd347bbc85a404328c9d

General

SHA256:	8da32ea516feb3bc471ba01ed18cb0aca1a9f39966c86ca4624dd2cea2e226cd
SHA512:	9534e6ec15f7d1c237e254a3dac79c7e44cc4c7989f3dbb8a4f0b682a3f3cfbbd46e6dddffa0e2a7e6bbd3e2b74389492559a8ad89fed85309cb848d5a1f60cb
SSDEEP:	12288:ZEA3LLUEMjhvUbJG16KfU32GOK2F5WRPVba0G/JZgC498Fj31Q2QuUmz:bL0iG16KfYrOK26RPZaA2dFFT
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L...?.5`.............0.............0... ...@....@.. ....….@................................

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c30d2
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:	0x6035BA3F [Wed Feb 24 02:30:23 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc3080	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc4000	0x5b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc6000	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	0xc10d8	0xc1200	False	0.935377477751	data	7.94883955827	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x5b4	0x600	False	0.430989583333	data	4.18690260245	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc6000	0xc	0x200	False	0.044921875	data	0.0940979256627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc4090	0x324	data		
RT_MANIFEST	0xc43c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

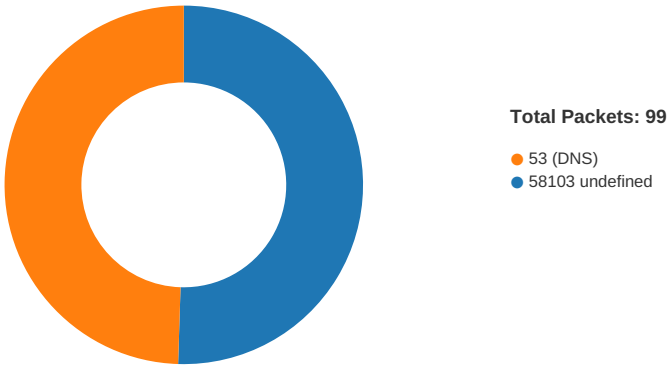
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	4.0.0.0
InternalName	Ck2rVn.exe
FileVersion	4.0.0.0
CompanyName	
LegalTrademarks	
Comments	

Description	Data
ProductName	ITP_RMSS
ProductVersion	4.0.0.0
FileDescription	ITP_RMSS
OriginalFilename	Ck2rVn.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 16:10:38.953803062 CET	49724	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:10:38.982628107 CET	58103	49724	87.237.165.78	192.168.2.6
Feb 24, 2021 16:10:39.493839025 CET	49724	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:10:39.523427963 CET	58103	49724	87.237.165.78	192.168.2.6
Feb 24, 2021 16:10:40.026274920 CET	49724	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:10:40.055999041 CET	58103	49724	87.237.165.78	192.168.2.6
Feb 24, 2021 16:10:44.133502007 CET	49727	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:10:44.162616014 CET	58103	49727	87.237.165.78	192.168.2.6
Feb 24, 2021 16:10:44.665113926 CET	49727	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:10:44.692055941 CET	58103	49727	87.237.165.78	192.168.2.6
Feb 24, 2021 16:10:45.196480036 CET	49727	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:10:45.223663092 CET	58103	49727	87.237.165.78	192.168.2.6
Feb 24, 2021 16:10:49.426067114 CET	49728	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:10:49.453262091 CET	58103	49728	87.237.165.78	192.168.2.6
Feb 24, 2021 16:10:49.962439060 CET	49728	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:10:49.989728928 CET	58103	49728	87.237.165.78	192.168.2.6
Feb 24, 2021 16:10:50.493711948 CET	49728	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:10:50.523130894 CET	58103	49728	87.237.165.78	192.168.2.6
Feb 24, 2021 16:10:54.526827097 CET	49729	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:10:54.562397957 CET	58103	49729	79.134.225.43	192.168.2.6
Feb 24, 2021 16:10:55.072269917 CET	49729	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:10:55.104984045 CET	58103	49729	79.134.225.43	192.168.2.6
Feb 24, 2021 16:10:55.619213104 CET	49729	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:10:55.651684046 CET	58103	49729	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:00.457012892 CET	49730	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:00.491065025 CET	58103	49730	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:00.994596004 CET	49730	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:01.029591084 CET	58103	49730	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:01.619633913 CET	49730	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:01.652059078 CET	58103	49730	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:05.996933937 CET	49741	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:06.029486895 CET	58103	49741	79.134.225.43	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 16:11:06.542004108 CET	49741	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:06.574748039 CET	58103	49741	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:07.276410103 CET	49741	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:07.309014082 CET	58103	49741	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:11.628916025 CET	49745	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:11.656161070 CET	58103	49745	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:12.261209011 CET	49745	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:12.288264990 CET	58103	49745	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:12.870593071 CET	49745	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:12.898427010 CET	58103	49745	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:16.972337008 CET	49751	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:17.000792980 CET	58103	49751	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:17.574356079 CET	49751	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:17.601228952 CET	58103	49751	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:18.261704922 CET	49751	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:18.291177988 CET	58103	49751	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:22.386017084 CET	49752	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:22.413485050 CET	58103	49752	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:22.918452978 CET	49752	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:22.946038961 CET	58103	49752	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:23.449760914 CET	49752	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:23.476892948 CET	58103	49752	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:27.628334999 CET	49753	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:27.662491083 CET	58103	49753	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:28.168908119 CET	49753	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:28.202835083 CET	58103	49753	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:28.715854883 CET	49753	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:28.750176907 CET	58103	49753	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:32.796241999 CET	49754	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:32.829065084 CET	58103	49754	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:33.341175079 CET	49754	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:33.373945951 CET	58103	49754	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:33.890563011 CET	49754	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:33.924868107 CET	58103	49754	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:37.953883886 CET	49755	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:37.986879110 CET	58103	49755	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:38.497858047 CET	49755	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:38.531111002 CET	58103	49755	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:39.044795990 CET	49755	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:11:39.077517033 CET	58103	49755	79.134.225.43	192.168.2.6
Feb 24, 2021 16:11:43.156795979 CET	49756	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:43.186810017 CET	58103	49756	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:43.701292992 CET	49756	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:43.728566885 CET	58103	49756	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:44.232594013 CET	49756	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:44.260241985 CET	58103	49756	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:48.317481041 CET	49762	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:48.344979048 CET	58103	49762	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:48.858040094 CET	49762	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:48.885418892 CET	58103	49762	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:49.389276981 CET	49762	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:49.416731119 CET	58103	49762	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:53.590868950 CET	49763	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:53.618211031 CET	58103	49763	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:54.124125957 CET	49763	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:54.152458906 CET	58103	49763	87.237.165.78	192.168.2.6
Feb 24, 2021 16:11:54.655369043 CET	49763	58103	192.168.2.6	87.237.165.78
Feb 24, 2021 16:11:56.654846907 CET	58103	49763	87.237.165.78	192.168.2.6
Feb 24, 2021 16:12:00.811273098 CET	49764	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:12:00.844180107 CET	58103	49764	79.134.225.43	192.168.2.6
Feb 24, 2021 16:12:01.349611998 CET	49764	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:12:01.386795998 CET	58103	49764	79.134.225.43	192.168.2.6
Feb 24, 2021 16:12:01.913440943 CET	49764	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:12:01.947032928 CET	58103	49764	79.134.225.43	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 16:12:05.961186886 CET	49766	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:12:05.993784904 CET	58103	49766	79.134.225.43	192.168.2.6
Feb 24, 2021 16:12:06.506625891 CET	49766	58103	192.168.2.6	79.134.225.43
Feb 24, 2021 16:12:06.539789915 CET	58103	49766	79.134.225.43	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 16:10:07.518027067 CET	63791	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:07.529794931 CET	53	63791	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:08.229974031 CET	64267	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:08.242146015 CET	53	64267	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:08.897500038 CET	49448	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:08.910022974 CET	53	49448	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:09.922713995 CET	60342	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:09.934758902 CET	53	60342	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:09.958610058 CET	61346	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:09.976557016 CET	53	61346	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:10.592065096 CET	51774	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:10.604959965 CET	53	51774	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:11.916075945 CET	56023	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:11.928503036 CET	53	56023	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:12.923096895 CET	58384	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:12.934818029 CET	53	58384	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:13.814424992 CET	60261	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:13.828752995 CET	53	60261	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:14.830136061 CET	56061	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:14.843961000 CET	53	56061	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:15.931255102 CET	58336	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:15.942899942 CET	53	58336	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:16.926970005 CET	53781	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:16.939821959 CET	53	53781	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:18.007355928 CET	54064	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:18.019748926 CET	53	54064	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:19.094878912 CET	52811	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:19.107601881 CET	53	52811	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:20.110537052 CET	55299	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:20.125304937 CET	53	55299	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:20.831885099 CET	63745	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:20.844845057 CET	53	63745	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:21.523874044 CET	50055	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:21.535721064 CET	53	50055	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:22.613850117 CET	61374	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:22.626470089 CET	53	61374	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:38.918437958 CET	50339	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:38.940557003 CET	53	50339	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:43.555535078 CET	63307	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:43.569211006 CET	53	63307	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:44.119376898 CET	49694	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:44.131638050 CET	53	49694	8.8.8.8	192.168.2.6
Feb 24, 2021 16:10:49.411509037 CET	54982	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:10:49.424482107 CET	53	54982	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:01.354537010 CET	50010	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:01.367275000 CET	53	50010	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:01.961107969 CET	63718	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:01.973623037 CET	53	63718	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:02.452449083 CET	62116	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:02.465662003 CET	53	62116	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:02.775964975 CET	63816	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:02.793160915 CET	55014	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:02.794636011 CET	53	63816	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:02.807427883 CET	53	55014	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:03.064794064 CET	62208	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:03.078361034 CET	53	62208	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 16:11:03.339365005 CET	57574	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:03.354017019 CET	53	57574	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:03.961036921 CET	51818	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:03.974280119 CET	53	51818	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:04.277424097 CET	56628	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:04.291400909 CET	53	56628	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:05.023027897 CET	60778	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:05.034997940 CET	53	60778	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:06.226900101 CET	53799	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:06.240196943 CET	53	53799	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:08.062889099 CET	54683	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:08.075159073 CET	53	54683	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:08.394944906 CET	59329	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:08.408041000 CET	53	59329	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:11.606597900 CET	64021	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:11.627228975 CET	53	64021	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:12.298700094 CET	56129	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:12.314606905 CET	53	56129	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:16.955619097 CET	58177	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:16.970276117 CET	53	58177	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:22.370347023 CET	50700	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:22.384215117 CET	53	50700	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:43.134542942 CET	54069	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:43.154480934 CET	53	54069	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:43.965912104 CET	61178	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:43.979415894 CET	53	61178	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:44.294032097 CET	57017	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:44.306591988 CET	53	57017	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:46.697841883 CET	56327	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:46.715770006 CET	53	56327	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:48.302930117 CET	50243	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:48.315598965 CET	53	50243	8.8.8.8	192.168.2.6
Feb 24, 2021 16:11:53.576647997 CET	62055	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:11:53.589582920 CET	53	62055	8.8.8.8	192.168.2.6
Feb 24, 2021 16:12:05.182383060 CET	61249	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:12:05.194192886 CET	53	61249	8.8.8.8	192.168.2.6
Feb 24, 2021 16:12:16.545772076 CET	65252	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:12:16.559621096 CET	53	65252	8.8.8.8	192.168.2.6
Feb 24, 2021 16:12:21.669437885 CET	64367	53	192.168.2.6	8.8.8.8
Feb 24, 2021 16:12:21.681693077 CET	53	64367	8.8.8.8	192.168.2.6
Feb 24, 2021 16:12:26.796633959 CET	55066	53	192.168.2.6	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 16:10:38.918437958 CET	192.168.2.6	8.8.8.8	0xd1ea	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:44.119376898 CET	192.168.2.6	8.8.8.8	0x448d	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:49.411509037 CET	192.168.2.6	8.8.8.8	0x4f17	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:11.606597900 CET	192.168.2.6	8.8.8.8	0xac0b	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:16.955619097 CET	192.168.2.6	8.8.8.8	0xe707	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:22.370347023 CET	192.168.2.6	8.8.8.8	0x9ae5	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:43.134542942 CET	192.168.2.6	8.8.8.8	0xb17	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:48.302930117 CET	192.168.2.6	8.8.8.8	0x6eec	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:53.576647997 CET	192.168.2.6	8.8.8.8	0x2f73	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:12:16.545772076 CET	192.168.2.6	8.8.8.8	0xadff	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:12:21.669437885 CET	192.168.2.6	8.8.8.8	0x448	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 16:12:26.796633959 CET	192.168.2.6	8.8.8.8	0xa791	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

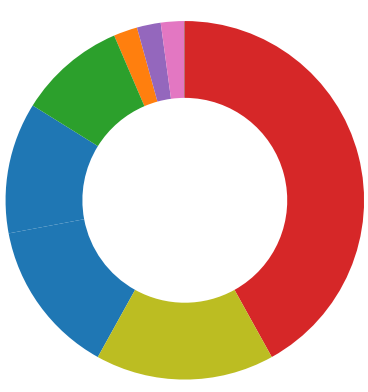
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 16:10:38.940557003 CET	8.8.8.8	192.168.2.6	0xd1ea	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:44.131638050 CET	8.8.8.8	192.168.2.6	0x448d	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:49.424482107 CET	8.8.8.8	192.168.2.6	0x4f17	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:11.627228975 CET	8.8.8.8	192.168.2.6	0xac0b	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:16.970276117 CET	8.8.8.8	192.168.2.6	0xe707	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:22.384215117 CET	8.8.8.8	192.168.2.6	0x9ae5	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:43.154480934 CET	8.8.8.8	192.168.2.6	0xb17	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:48.315598965 CET	8.8.8.8	192.168.2.6	0x6eec	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:53.589582920 CET	8.8.8.8	192.168.2.6	0x2f73	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:12:16.559621096 CET	8.8.8.8	192.168.2.6	0xadff	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:12:21.681693077 CET	8.8.8.8	192.168.2.6	0x448	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: cp573oYDUX.exe PID: 7012 Parent PID: 5888

General

Start time:	16:10:14
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\cp573oYDUX.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\cp573oYDUX.exe'
Imagebase:	0x7a0000
File size:	793600 bytes
MD5 hash:	33CF3AF09D2A1789A2BBAD009A43EDD5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.373693780.00000000042F3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.373693780.00000000042F3000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.373693780.00000000042F3000.00000004.00000001.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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Roaming\eVEWVTvFLGVU.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	722131B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp53F8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	291B2B8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\cp573oYDUX.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp53F8.tmp	success or wait	1	7221F92	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\eVEWVTvFLGVU.exe	unknown	793600	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 3f ba 35 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 12 0c 00 00 08 00 00 00 00 00 00 d2 30 0c 00 00 20 00 00 00 40 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...?.5`.......... ....0.............0... ...@....@.. ....@................	success or wait	1	72215A3	WriteFile
C:\Users\user\AppData\Local\Temp\tmp53F8.tmp	unknown	1657	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 3e 0d 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 0d 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 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </Registratio	success or wait	1	72215A3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\cp573oYDUX.exe.log	unknown	655	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Users\user\Desktop\cp573oYDUX.exe	unknown	793600	success or wait	1	72215A3	ReadFile

Analysis Process: schtasks.exe PID: 3800 Parent PID: 7012

General

Start time:	16:10:33
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eVEWVTvFLGVU' /XML 'C:\Users\user\AppData\Local\Temp\tmp53F8.tmp'
Imagebase:	0x120000
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\tmp53F8.tmp	unknown	2	success or wait	1	12AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp53F8.tmp	unknown	1658	success or wait	1	12ABD9	ReadFile

Analysis Process: conhost.exe PID: 4112 Parent PID: 3800

General

Start time:	16:10:34
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 2264 Parent PID: 7012

General

Start time:	16:10:34
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x6c0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
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: 00000007.00000002.600652707.0000000005030000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.600652707.0000000005030000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.594405865.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.594405865.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.594405865.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.599620352.0000000003DA7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.599620352.0000000003DA7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.601347713.0000000005990000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.601347713.0000000005990000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.601373463.00000000059A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.601373463.00000000059A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.601373463.00000000059A0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

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	72FB60AC	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	72FB60AC	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	4FB07A1	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	4FB089B	CreateFileW
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	4FB07A1	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	4FB0B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpFC43.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4FB0D1C	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	4FB089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpFF61.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4FB0D1C	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	4FB07A1	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	4FB07A1	CreateDirectoryW
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	72FB60AC	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	72FB60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFC43.tmp	success or wait	1	72637D95	unknown
C:\Users\user\AppData\Local\Temp\tmpFF61.tmp	success or wait	1	72637D95	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	unknown	8	f4 8c 7f c6 21 d9 d8 48	....!..H	success or wait	1	4FB0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 cf ce 7b 5a 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 50 00 00 00 20 00 00 00 00 00 00 de 6b 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 00 00 00 10 00 00 b1 5b 01 00 03 00 40 05 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......PE..L..... {Z.................P... ....k... ....@.. ....[....@.................	success or wait	1	4FB0B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpFC43.tmp	unknown	1320	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.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	4FB0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	57	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 32 2e 30 2e 35 30 37 32 37 5c 52 65 67 53 76 63 73 2e 65 78 65	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	success or wait	1	4FB0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFF61.tmp	unknown	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	4FB0A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4FB0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	4FB0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	4FB0A53	ReadFile

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	4FB0C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 6632 Parent PID: 2264

General

Start time:	16:10:36
Start date:	24/02/2021
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\tmpFC43.tmp'
Imagebase:	0x120000
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\tmpFC43.tmp	unknown	2	success or wait	1	12AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFC43.tmp	unknown	1321	success or wait	1	12ABD9	ReadFile

Analysis Process: conhost.exe PID: 6620 Parent PID: 6632

General

Start time:	16:10:36
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 5996 Parent PID: 2264

General

Start time:	16:10:36
Start date:	24/02/2021
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\tmpFF61.tmp'
Imagebase:	0x120000
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\tmpFF61.tmp	unknown	2	success or wait	1	12AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFF61.tmp	unknown	1311	success or wait	1	12ABD9	ReadFile

Analysis Process: conhost.exe PID: 5144 Parent PID: 5996

General

Start time:	16:10:37
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 5692 Parent PID: 936

General

Start time:	16:10:38
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0
Imagebase:	0xbe0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

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	72FB60AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	13BA53F	WriteFile
\Device\ConDrv	unknown	145	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....	success or wait	1	13BA53F	WriteFile
\Device\ConDrv	unknown	45	0a 54 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 3a 0d 0a	.The following installation error occurred:..	success or wait	1	13BA53F	WriteFile
\Device\ConDrv	unknown	29	31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	1: Assembly not found: '0'...	success or wait	1	13BA53F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	unknown	120	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 32 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: conhost.exe PID: 5684 Parent PID: 5692

General

Start time:	16:10:38
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 5680 Parent PID: 936

General

Start time:	16:10:38
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xe00000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	13FA53F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	145	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....	success or wait	1	13FA53F	WriteFile
\Device\ConDrv	unknown	45	0a 54 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 3a 0d 0a	.The following installation error occurred:..	success or wait	1	13FA53F	WriteFile
\Device\ConDrv	unknown	29	31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	1: Assembly not found: '0'...	success or wait	1	13FA53F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	120	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 32 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: conhost.exe PID: 6916 Parent PID: 5680

General

Start time:	16:10:39
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 7144 Parent PID: 3440

General

Start time:	16:10:48
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xc20000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

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	72FB60AC	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	72FB60AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7266DCB3	unknown
\Device\ConDrv	unknown	145	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....	success or wait	1	7266DFAB	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	256	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 0d 0a 20 20 20 20 20 2f 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 65 72 72 6f 72 20 69 66 20 69 74 20 61 6c 72 65 61 64 79 20 65 78 69 73 74 73 2e 0d 0a 20 20 20 20 20 2f 65 78 61 70 70 20	USAGE: regsvcs.exe [options] A ssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp	success or wait	3	7266DFAB	unknown
\Device\ConDrv	unknown	232	53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 71 75 69 65 74 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or inte rfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	7266DFAB	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: conhost.exe PID: 7116 Parent PID: 7144

General

Start time:	16:10:49
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis