ID: 341895
Cookbook: browseurl.jbs
Time: 03:53:20
Date: 20/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

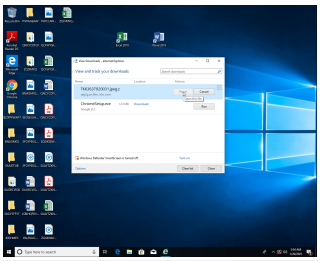
Analysis Report https://onedrive.live.com/download?cid…

Overview

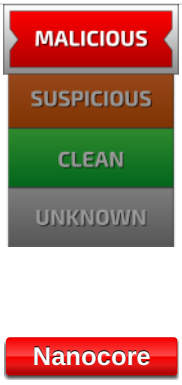
General Information

Sample URL:	http://https://onedrive.live.com/download?cid=F9306F27ACC5AABA&resid=F9306F27ACC5AABA!278&authkey=AEXuJUX0kEgNwa0
Analysis ID:	341895

Most interesting Screenshot:



Detection

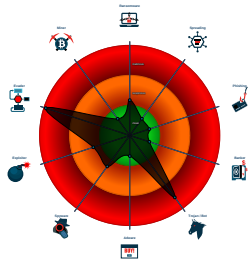


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e….
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- Connects to many ports of the same…
- Contains functionality to check if a d…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5152 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5168 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5152 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - unarchiver.exe (PID: 3440 cmdline: 'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z' MD5: 8B435F8731563566F3F49203BA277865)
    - 7za.exe (PID: 4848 cmdline: 'C:\Windows\System32\7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z' MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
      - conhost.exe (PID: 2024 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 5876 cmdline: 'cmd.exe' /C 'C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5776 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - FNYVlhLumPogrzL.exe (PID: 2208 cmdline: C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.exe MD5: E2369B4A4D2E2C7F1F8AF4F7743532E9)
        - schtasks.exe (PID: 1536 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\FxuoZREPj' /XML 'C:\Users\user\AppData\Local\Temp\tmpE9ED.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
          - conhost.exe (PID: 5744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - RegSvcs.exe (PID: 4912 cmdline: {path} MD5: 71369277D09DA0830C8C59F9E22BB23A)
          - schtasks.exe (PID: 4156 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp7D78.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
            - conhost.exe (PID: 4168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - schtasks.exe (PID: 5564 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp81FD.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
            - conhost.exe (PID: 4840 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 4868 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 1180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 4120 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 3880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.473292400.000000000578 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
0000000E.00000002.473292400.000000000578 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
0000000E.00000002.473649492.000000000605 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0000000E.00000002.473649492.000000000605 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
0000000E.00000002.473649492.000000000605 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.RegSvcs.exe.5780000.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
14.2.RegSvcs.exe.5780000.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
14.2.RegSvcs.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8J YUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
14.2.RegSvcs.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
14.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 9 entries				

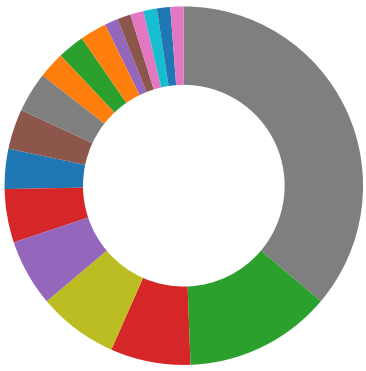
Sigma Overview

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:

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Compliance:

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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)

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected 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)

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

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:

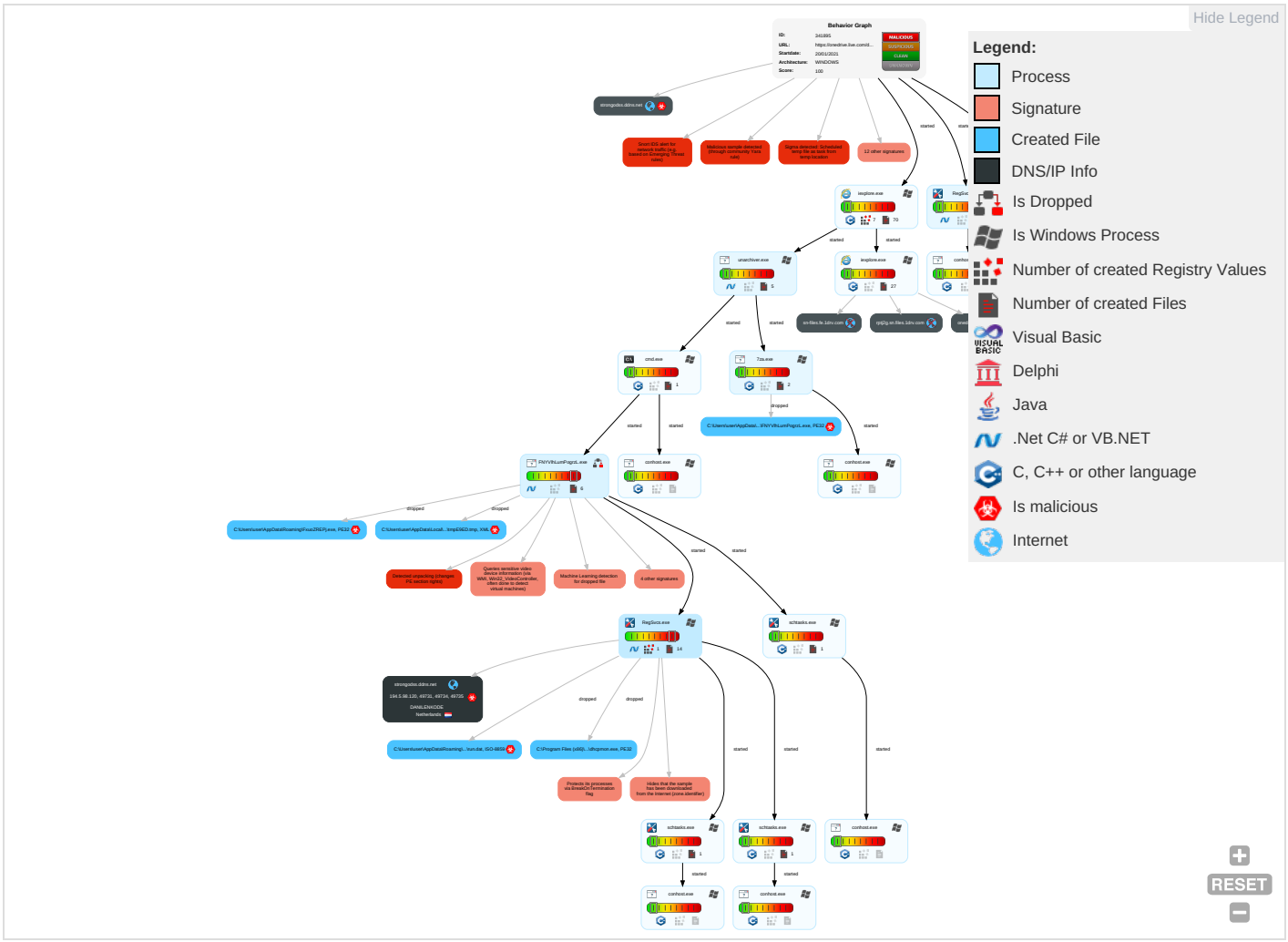
Detected Nanocore Rat

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 1 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Exploitation for Client Execution 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 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Scheduled Task/Job 1	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 2 3	NTDS	Security Software Discovery 3 2 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 4	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4	Cached Domain Credentials	Process Discovery 2	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

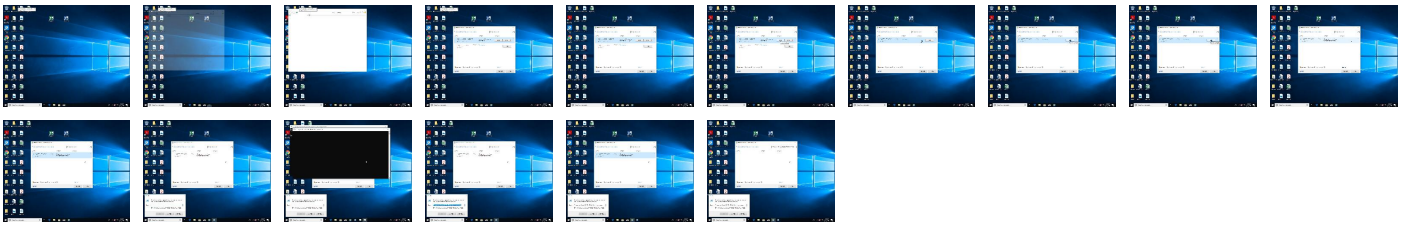
Behavior Graph

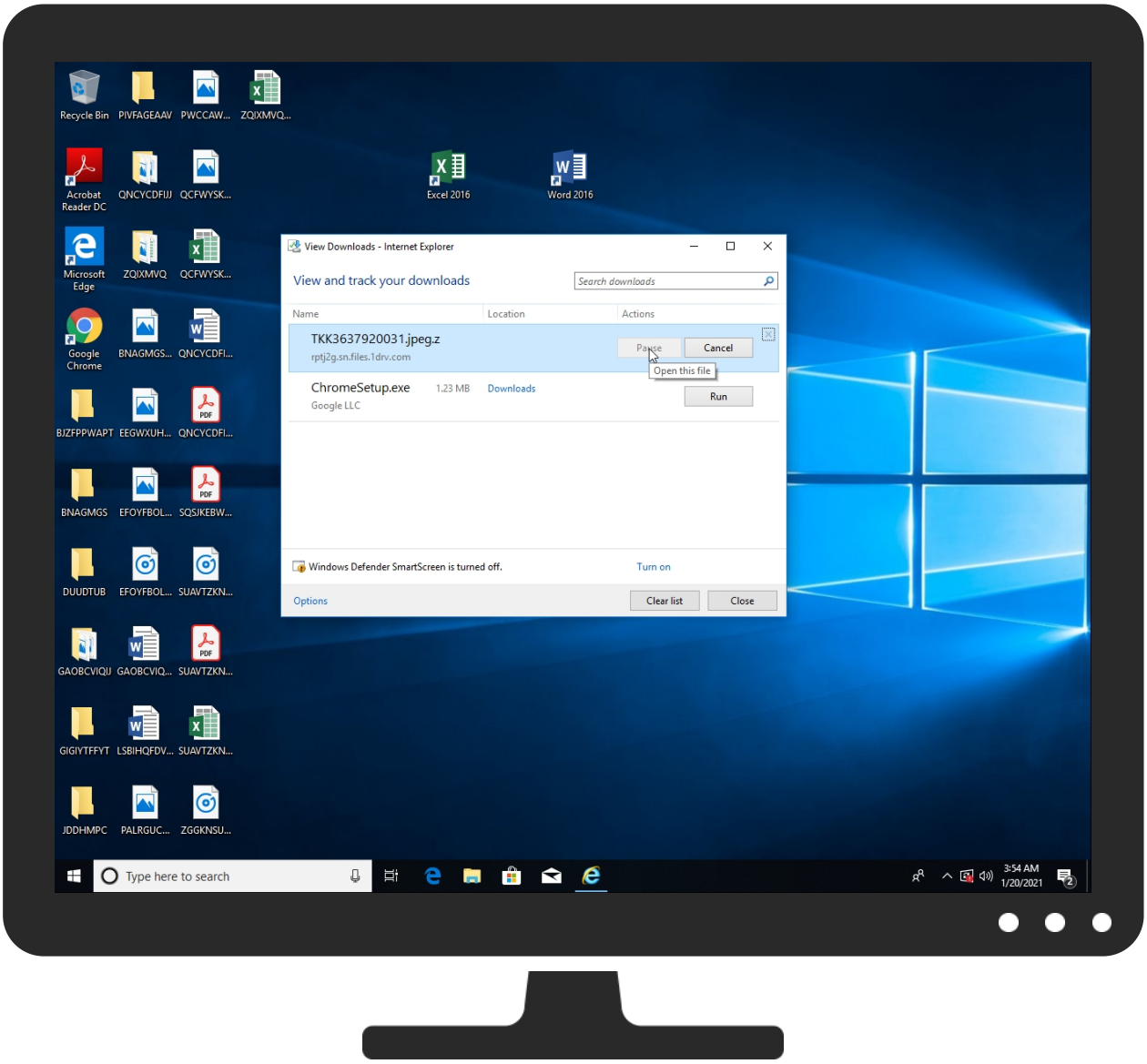


Screenshots

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
http://https://onedrive.live.com/download?cid=F9306F27ACC5AABA&resid=F9306F27ACC5AABA%21278&authkey=AEXuJUX0kEgNwa0	1%	Virustotal		Browse
http://https://onedrive.live.com/download?cid=F9306F27ACC5AABA&resid=F9306F27ACC5AABA%21278&authkey=AEXuJUX0kEgNwa0	0%	Avira URL Cloud	safe	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\FxuoZREPj.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.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		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.RegSvcs.exe.6050000.5.unpack	100%	Avira	TR/NanoCore.fadte		Download File
14.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.2.FNYVlhLumPogrzL.exe.8c0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
strongodss.ddns.net	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnW	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmG	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.tiro.com	0%	URL Reputation	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.goodfont.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnG	0%	Avira URL Cloud	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.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.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.founder.com.cn/cn/cThe	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.sakkal.comp	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.sakkal.comr	0%	Avira URL Cloud	safe	
http://www.fontbureau.comam	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnv	0%	Avira URL Cloud	safe	
http://www.urwpp.de2	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.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.tiro.com(	0%	Avira URL Cloud	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.fontbureau.como8	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.urwpp.deO	0%	Avira URL Cloud	safe	
http://www.fontbureau.comion	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.urwpp.dey	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn7	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
strongodss.ddns.net	194.5.98.120	true	true	• 4%, Virustotal, Browse	unknown
onedrive.live.com	unknown	unknown	false		high
rptj2g.sn.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
0	true		low

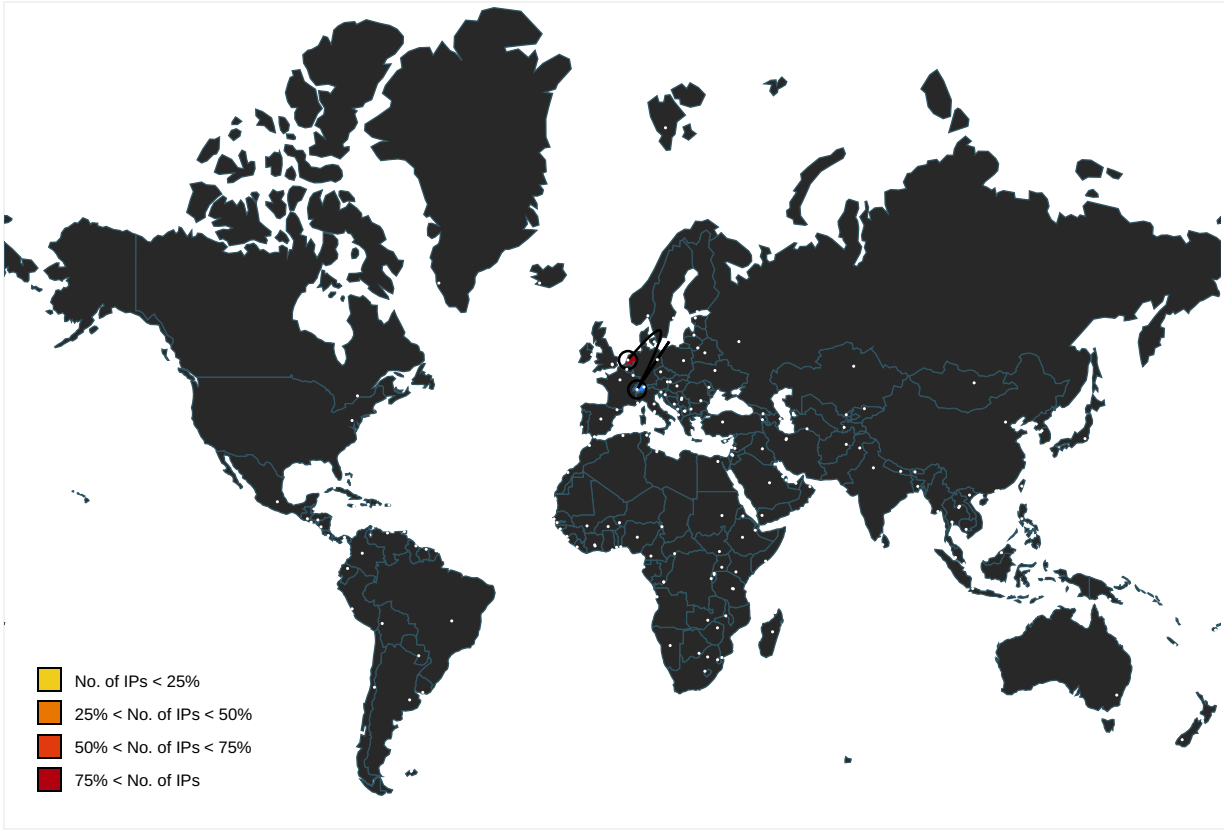
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.000000000581200.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/frere-jones.html(	FNYVlhLumPogrzL.exe, 0000000A.00000003.259925336.000000000559C000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.000000000581200.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.000000000581200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnW	FNYVlhLumPogrzL.exe, 0000000A.00000003.257114831.000000000558000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.000000000581200.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htmG	FNYVlhLumPogrzL.exe, 0000000A.00000003.261981799.000000000559C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.000000000581200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.000000000581200.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.kr	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.00000000058120000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnG	FNYVlhLumPogrzL.exe, 0000000A.00000003.257114831.00000000055800000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.00000000058120000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.00000000058120000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.00000000058120000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.00000000058120000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.comp	FNYVlhLumPogrzL.exe, 0000000A.00000003.258338420.00000000559C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.00000000058120000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersm	FNYVlhLumPogrzL.exe, 0000000A.00000003.259925336.00000000559C000.00000004.00000001.sdmp	false		high
http://www.sakkal.comr	FNYVlhLumPogrzL.exe, 0000000A.00000003.258338420.00000000559C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comam	FNYVlhLumPogrzL.exe, 0000000A.00000002.281721786.00000000055570000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnv	FNYVlhLumPogrzL.exe, 0000000A.00000003.256845249.00000000559C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de2	FNYVlhLumPogrzL.exe, 0000000A.00000003.259111467.00000000559C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.00000000058120000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	FNYVlhLumPogrzL.exe, 0000000A.00000003.258338420.00000000559C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.00000000058120000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.00000000058120000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.00000000058120000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersz	FNYVlhLumPogrzL.exe, 0000000A.00000003.259679205.00000000559C000.00000004.00000001.sdmp	false		high
http://www.tiro.com(	FNYVlhLumPogrzL.exe, 0000000A.00000003.257491913.00000000559F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.de	FNYVlhLumPogrzL.exe, 0000000A.00000003.261253439.00000000559C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.00000000058120000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como8	FNYVlhLumPogrzL.exe, 0000000A.00000002.281721786.00000000055570000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	FNYVlhLumPogrzL.exe, 0000000A.00000003.258413038.00000000559C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designerst	FNYVlhLumPogrzL.exe, 0000000A.00000003.259679205.000000000559C000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.0000000005812000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.0000000005812000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/	FNYVlhLumPogrzL.exe, 0000000A.00000003.261814632.000000000559C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deO	FNYVlhLumPogrzL.exe, 0000000A.00000003.261207771.000000000559C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/v	FNYVlhLumPogrzL.exe, 0000000A.00000003.259181693.000000000559C000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comion	FNYVlhLumPogrzL.exe, 0000000A.00000002.281721786.0000000005570000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.0000000005812000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.0000000005812000.00000004.00000001.sdmp	false		high
http://www.urwpp.dey	FNYVlhLumPogrzL.exe, 0000000A.00000003.259111467.000000000559C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	FNYVlhLumPogrzL.exe, 0000000A.00000003.257114831.0000000005580000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.0000000005812000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn7	FNYVlhLumPogrzL.exe, 0000000A.00000003.257114831.0000000005580000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.0000000005812000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	FNYVlhLumPogrzL.exe, 0000000A.00000002.282117897.0000000005812000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/	FNYVlhLumPogrzL.exe, 0000000A.00000003.259181693.000000000559C000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.120	unknown	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	341895
Start date:	20.01.2021
Start time:	03:53:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://onedrive.live.com/download?cid=F9306F27ACC5AABA&resid=F9306F27ACC5AABA!278&authkey=AEXuJUX0kEgNwa0
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:	40
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.win@28/24@16/1
EGA Information:	• Successful, ratio: 80%

HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
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): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 52.255.188.83, 88.221.62.148, 13.107.42.13, 104.43.139.144, 13.107.42.12, 152.199.19.161, 2.20.84.85, 51.11.168.160, 92.122.213.247, 92.122.213.194, 67.26.73.254, 67.27.157.254, 8.253.207.121, 8.248.135.254, 8.248.141.254, 20.54.26.129 • Excluded domains from analysis (whitelisted): odc-web-brs.onedrive.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, l-0004.l-msedge.net, iecvlist.microsoft.com, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, go.microsoft.com, l-0003.l-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, sn-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, fs.microsoft.com, odc-web-geo.onedrive.akadns.net, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, odc-sn-files-geo.onedrive.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, odc-sn-files-brs.onedrive.akadns.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • Execution Graph export aborted for target unarchiver.exe, PID 3440 because it is empty • 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
03:54:36	API Interceptor	1x Sleep call for process: FNYVlhLumPogrzL.exe modified
03:54:44	API Interceptor	743x Sleep call for process: RegSvcs.exe modified
03:54:44	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
03:54:45	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe" s>$(Arg0)
03:54:45	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

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:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
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\FNYVlhLumPogrzL.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.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:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\FNYVlhLumPogrzL.exe.log	
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\4de99804c29261edb63c93616550f034\System.Management.ni.dll",0..

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
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Reputation:	low
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\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
Reputation:	low
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{322791B1-5B16-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32344
Entropy (8bit):	1.7988366230192592
Encrypted:	false
SSDEEP:	48:Iw5GcprEGwpLGhG/ap8brGIpcxHWGvnZpvxn/Gojqp9xnaOGo4tpmxuaZBGWFb9s:rfZ8Zk2b9WxTtxufxotMxlxl6Ev2
MD5:	A7487A67F1CB3462A5E7EA02EB4F883C
SHA1:	E0D53960F1724B3002F51DF542F04338E1640213
SHA-256:	DA997F577F74485F00B532187927744363FA512DB89829135ADE1DF865EB85D6
SHA-512:	A6E3A820033D9E51BD04BD3E4C035954303FDE22D50609C885F6F6151A5ECD3363831419D5C3D0B280DD5BCDD4A763A81B7CD23BF568BA8A9D2DC41897D3FA3
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{322791B3-5B16-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5986040283144574

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{322791B3-5B16-11EB-90E4-ECF4BB862DED}.dat	
Encrypted:	false
SSDEEP:	48:IwLGcpryGwpaeG4pQChGrapbS/rGQpBoLbGHHpcohPsTGUpQoKpVGcpm:rRZ6Qe60BS/Fjp2Ik6Ng
MD5:	B11D6E0F8AC61F0BB9D78A02AE101162
SHA1:	C8539092773AF6C520BB68D5D3758EE101071655
SHA-256:	73B18FC940E4AD252295C53FFBFE7F34C89C50289DEB6992423492E3125FD440
SHA-512:	27213E8F6F7F4ADEBA86B31DEC319D7C986203A257E5E742B4E725A07B46A430305EEE6EA3869105095A4067A3476ECA441377E9FCF3CD6567977214A14EC111
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z.h1ixtx1.partial	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RAR archive data, v5
Category:	dropped
Size (bytes):	1135642
Entropy (8bit):	**7.999815833560986**
Encrypted:	**true**
SSDEEP:	24576:UExCZp6dTHfYmoNvEo9c+P7lO93tsmMnSTnt/B83qZUJQ96u/KV7tb:/CZp6QmGD9caOrsbnSTnt/BWq0QHQ7V
MD5:	EE856182C24F0FC4FA822F4882E5A2C2
SHA1:	846DA7258045528D385C7197960807558402A235
SHA-256:	86256445950E138455F808B4BF6A086227CC254E5A42AB929626A3DB67218D08
SHA-512:	D8C8B406CB08200490D846605628B4D0E7661F96EEA7F41ED83382CB785E0337E59895E250E9BD4689C9A6012D4B0E53604EC0CAF553326DAAAD7943B9A300D
Malicious:	false
Reputation:	low
Preview:	Rar!....0.9 .....s!X5.....]/...#..FNYVlhLumPogrzL.exe...jP.....@0c30U.EPeT.T....t.q....o:.Uot.9.....E. ....m..A&..$....l...'.....^.....@.C.... .(.....U..... ..d....@. .....b.p.....'.....P..c...a.....w)..9.7..38.6.106..9.0..8.6.4.p...@....\...l.`..?.K....g._.... .....8.....~/.u....._..`_.u.....|_...y...!...../.....HT.....D...0.....#.....?.^\|OS.(gz=.\..... ..7K.....K{?.6.....'./..H....k.....e25.....M.....~.....u.....P.8z..g.....d.....Y..QY.<...Y.t.?..U.<.(9..i..Lh.!.J.....<.o.....j.....(..+..&/.x.;.....%U..g+[..`.I....l5.].r....s.."..... .O..@....'..V.M.{...q<O..]...iV..)f...b.....N.....f....fPW...?G.....J..c.?.e..DTY.....\ybr.Y`&V.@.....*...E....}r..J.ahLh..8...6..w..._.z...K...#..L.>I.e....A..f.7g.....^X*..sQ'F0....Qq.....*._. ^..`.T../K...1%..O...H.L.Y.4....$u.^..W.s.Z...=2...M.#...w|.....lc4i<e..;..T...a.....y.....k.7h.....x..P....l..s...PO;b.....f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z.h1ixtx1.partial:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E 8
Malicious:	false
Reputation:	low
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	modified
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:W:W
MD5:	ECCBC87E4B5CE2FE28308FD9F2A7BAF3
SHA1:	77DE68DAECD823BABBB58EDB1C8E14D7106E83BB
SHA-256:	4E07408562BEDB8B60CE05C1DECFE3AD16B72230967DE01F640B7E4729B49FCE
SHA-512:	3BAFBF08882A2D10133093A1B8433F50563B93C14ACD05B79028EB1D12799027241450980651994501423A66C276AE26C43B739BC65C4E16B10C3AF6C202AEBB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z:Zone.Identifier	
Preview:	3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\TKK3637920031.jpeg[1].z	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RAR archive data, v5
Category:	dropped
Size (bytes):	1135642
Entropy (8bit):	**7.999815833560986**
Encrypted:	**true**
SSDEEP:	24576:UExCZp6dTHfYmoNvEo9c+P7lO93tsmMnSTnt/B83qZUJQ96u/KV7tb:/CZp6QmGD9caOrsbnSTnt/BWq0QHQ7V
MD5:	EE856182C24F0FC4FA822F4882E5A2C2
SHA1:	846DA7258045528D385C7197960807558402A235
SHA-256:	86256445950E138455F808B4BF6A086227CC254E5A42AB929626A3DB67218D08
SHA-512:	D8C8B406CB08200490D846605628B4D0E7661F96EEA7F41ED83382CB785E0337E59895E250E9BD4689C9A6012D4B0E53604EC0CAF553326DAAAD7943B9A300D
Malicious:	false
Reputation:	low
Preview:	Rar!....0.9 .....s!X5.....]/...#..FNYVlhLumPogrzL.exe...jP.....@0c30U.EPeT.T....t.q....o:.Uot.9.....E. ....m..A&..$....l...'.....^.....@.C.... .(.....U..... ..d....@. .....b.p.....'.....P..c...a.....w)..9.7..38.6.106..9.0..8.6.4.p...@....\...I.`..?.K....g._.... .....8.....~/.u....._..`_.u.....\|_...y...!...../.....HT.....D...0.....#.....?.^\|OS.(gz=.\..... ..7K.....K{?.6.....'./..H....k.....e25.....M.....~.....u.....P.8z..g.....d....Y..QY.<...Y.t.?..U.<.(9..i..Lh.!.J.....<.o.....j.....(..+..&/.x.;....%U..g+[..`.I....l5.].r....s..".... .O..@....'..V.M.{...q<O..]...iV..)f...b.....N.....f....fPW...?G.....J..c.?.e..DTY.....\ybr.Y`&V.@.....*...E....}r..J.ahLh..8...6..w..._.z...K...#..L.>I.e....A..f.7g.....^X*..sQ'F0....Qq.....*._. ^..`.T../K...1%..O...H.L.Y.4....$u.^..W.s.Z...=2...M.#...w|.....lc4i<e..;..T...a.....y.....k.7h.....x..P....I..s...PO;b.....f

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	89
Entropy (8bit):	4.406442624860051
Encrypted:	false
SSDEEP:	3:oVXUoV9nT498JOGXnEoV9q4u7n:o9UoV90qEoV9q4m
MD5:	D3502D5124CC72EEADBC026B602DF179
SHA1:	B9B87B7A44940CD0F026A6859C0B83D3BEEE00E6
SHA-256:	DA9E6042C62714DF48DFB11A669BB50650CDD75CCB481FEF2D5BC88781945562
SHA-512:	4EC85300B08B436C63B0CA2B746D147C7A9DCF6D8574AC305077BD97E08E603E4FB46F4D816A2702B53B0647FCF4800B3CBE663E8ABBFE3E331656280E00F7C
Malicious:	false
Reputation:	low
Preview:	[2021/01/20 03:54:07.301] Latest deploy version: ..[2021/01/20 03:54:07.316] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\bpkrjtup.j3x\unarchiver.log	
Process:	C:\Windows\SysWOW64\unarchiver.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2503
Entropy (8bit):	5.230675390203555
Encrypted:	false
SSDEEP:	48:kcdDyjcbWcyGncyGbncyGncyGphcyGbncyGncyGpCDyjcyGHxcyGPDyjcyGGicyN:lQde9eUdw0
MD5:	EA43926E4B4D250F520897C7F577A097
SHA1:	9E1545DB57DBE43B041D4DCC1669A91032B165DE
SHA-256:	821DCF685A76A7EC2E87165109A46A790A18089201E7FA3E32B761B5E0BAD1FC
SHA-512:	4CD9F65C789DA016911BED4E82ADF65133C3DA9D3AC0C2B447E1C00CBDECDCEADC02FFBF1C3B03CD606134D988F839221B30090CDD8D33301EC4250965A3 AB
Malicious:	false
Reputation:	low
Preview:	01/20/2021 3:54 AM: Unpack: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z..01/20/2021 3:54 AM: Tmp dir: C:\ Users\user\AppData\Local\Temp\vjk3yugy.hgt..01/20/2021 3:54 AM: Received from standard out: ..01/20/2021 3:54 AM: Received from standard out: 7-Zip 18.05 (x86) : Copyright (c) 1999-2018 Igor Pavlov : 2018-04-30..01/20/2021 3:54 AM: Received from standard out: ..01/20/2021 3:54 AM: Received from standard out: Scanning the drive for archives:..01/20/2021 3:54 AM: Received from standard out: 1 file, 1135642 bytes (1110 KiB)..01/20/2021 3:54 AM: Received from standard out: ..01/20/2021 3:5 4 AM: Received from standard out: Extracting archive: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z..01/20/2021 3:54 AM: Received from standard out: WARNING:..01/20/2021 3:54 AM: Received from standard out: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\M EEXW4H4\TKK3637920031.jpeg.z..01/20/2021 3:54

C:\Users\user\AppData\Local\Temp\tmp7D78.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

C:\Users\user\AppData\Local\Temp\tmp7D78.tmp	
Size (bytes):	1320
Entropy (8bit):	5.135021273392143
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mn4xtn:cbk4oL600QydbQxIYODOLedq3Z4j
MD5:	40B11EF601FB28F9B2E69D36857BF2EC
SHA1:	B6454020AD2CEED193F4792B77001D0BD741B370
SHA-256:	C51E12D18CC664425F6711D8AE2507068884C7057092CFA11884100E1E9D49E1
SHA-512:	E3C5BCC714CBFCA4B8058DDCDDF231DCEFA69C15881CE3F8123E59ED45CFB5DA052B56E1945DCF8DC7F800D62F9A4EECB82BCA69A66A1530787AEFFEB15E2BD5
Malicious:	false
Reputation:	low
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\tmp81FD.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
Reputation:	low
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\tmpE9ED.tmp	
Process:	C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.194281179975877
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBetn:cbh47TlNQ//rydbz9l3YODOLNdq3q
MD5:	4AFEB34191C071F283C4F2BC626AF07E
SHA1:	EAB2F0CF9C862D7F97E9E9921E19266069658424
SHA-256:	CA9238A1CC8E52FAA083A8865A0623EAACCD12F3F95AA96D89CB53E3DFA11737
SHA-512:	2B8E7F57A6F7B64B8C77B8960B445047865BB36B54BCC2A16811ECA1335A65BF3C7685711444EA7974C57EE7F712BBB625A68F49F6EE3F2559C51733AB46F38D
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.exe	
Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1505792

C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.exe	
Entropy (8bit):	7.429842059066444
Encrypted:	false
SSDEEP:	24576:8+6JbyWvhKxiSA7Xv7z4JNWDxvSNSNb5jNb:dchKiS+vvVYM5D
MD5:	E2369B4A4D2E2C7F1F8AF4F7743532E9
SHA1:	FF73F21E4CA57111DCB38051A92CE59AC48E7498
SHA-256:	CE82DC0464405C155279812B9506998991C7FB74CE59DFCABEE337DA9CDB757A
SHA-512:	26AB837582235DB7300873CEE599FEF96503FB1B80EE9B81AB54B12BDF5C7D4E4FAB660FB7F931AC4F00CC684EC4BC35EF40539A3671907729F0E517CF52FEB6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....h.`.....0.....@..... ....@.. .....`..... ..@.....K....`..... .....@.....H.....}PT.(h{>.].. ...^.....@....text...`.....b..... ..`.rsr c.....`.....>.....@..@.reloc..... .....@..B.....@..... ..`..... ....

C:\Users\user\AppData\Local\Temp\~DFC5EFD22772502ADF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12981
Entropy (8bit):	0.44390090907631574
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loUF9lo09lWvpbWpdL:kBqoIPZvpSpdL
MD5:	F4EC83EB47B455BD5E2BC09BAA0CBC72
SHA1:	05FEF35A8F33B35B3B8A6F22B912BADADB237C77
SHA-256:	95DDC1E3B611A39DE76BA208B601354349D4B332945E53D408A5BC3C40AB2B9D
SHA-512:	B8E253CBAA3F710FF9FD0AB7E7EDCFE020F3F636B3FBCA0B3997E652305812E780D8009B9B926E098CEFA1C0D2B6AC0F0C5F3647FD0184BE2AC60817B961038
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE94FC4F1589F59FF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29989
Entropy (8bit):	0.3301349720454092
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwtyqv9lwtyqv9l2tyqs:kBqoxKAuvScS+oLoFou+oboKy
MD5:	67E50969A57D1702F83443D98F965B36
SHA1:	4F417FCA16108ADDBE783277DC520E0B15783042
SHA-256:	244970D1466095F000EACF6003A8964EB318311E2D7415B70A3517C9D9361CCF
SHA-512:	C366FD66431A41A3378859B9B7C14E1BEE38BB171B02197C087EE577538CE6DCC0F74E67337BF7EEE51D55D7E85687E01AF966CFE215D1FC20404CD4EFD6C84
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	1488
Entropy (8bit):	7.094528505897445
Encrypted:	false
SSDEEP:	24:IQnybgCUtvd7RFBFSBvv8UQnybgCUtvd7RFBFSBvv8UQnybgCUtvd7RFBFSBvv8R:Ik/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/tP
MD5:	FA1E30035440350B350A67A97D629526

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
SHA1:	F28C5C85A69BDC11296921DD4840F57EA624C5E8
SHA-256:	A1B53D5F3983483EA34CC768A38248F849160EEE6C8477C451CF5CE2985D5DE9
SHA-512:	359FF4147C7C5A0C6331A05E9129C08DCF678285F4DACFBAA86AD33B9D50EE8F028B9836AB6D9E1DAC54E11144EC34020153E2E73158DA0311B278BF446E406
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL....f.Z#.|...@HkG....G..O*V.....pz...."....r...w&&|..c..3}~.....~...os..f.....4..1 .gJ.'.d".L...A.t...F.{....C.|&.wGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL....f.Z#.|...@HkG....G..O*V.....pz...."... .r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L...A.t...F.{....C.|&.wGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL....f.Z#.|...@H kG....G..O*V.....pz...."....r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L...A.t...F.{....C.|&.wGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B... ....].P...W.4C}uL....f.Z#.|...@HkG....G..O*V.....pz...."....r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L...A.t...F.{....C.|&.wGj.h\.3.

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:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:6f4:04
MD5:	6262F7C072E709CB42A451761371F212
SHA1:	70CBCCEA7042E0E927B8C3939EB82F73815C6072
SHA-256:	AAC01F2674B55898586C9D2527C7E2835201CDEDBAC46DD3164BC6487111C2D1
SHA-512:	0BA0EB1B54EA34EBD46AE817088AAC38ACA02AF831EDBFB934C60AD8BCFE1BA9C6D0DD9CA82445BE1516BDBFAFDDC81DA42AE2FC9D2AA8AEC7E5CECBC 5E0297E
Malicious:	**true**
Reputation:	low
Preview:	.gb,:..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
SHA-512:	17769A5944E8929323A34269ABEEF0861D5C6799B0A27F5545FBFADC80E5AB684A471AD6F6A7FC623002385154EA89DE94013051E09120AB94362E542AB0F1DD
Malicious:	false
Reputation:	low
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe

C:\Users\user\AppData\Roaming\FxuoZREPj.exe	
Process:	C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1505792
Entropy (8bit):	7.429842059066444
Encrypted:	false
SSDEEP:	24576:8+6JbyWvhKxiSA7Xv7z4JNWDxvSNSNb5jNb:dchKiS+vvYM5D
MD5:	E2369B4A4D2E2C7F1F8AF4F7743532E9
SHA1:	FF73F21E4CA57111DCB38051A92CE59AC48E7498
SHA-256:	CE82DC0464405C155279812B9506998991C7FB74CE59DFCABEE337DA9CDB757A
SHA-512:	26AB837582235DB7300873CEE599FEF96503FB1B80EE9B81AB54B12BDF5C7D4E4FAB660FB7F931AC4F00CC684EC4BC35EF40539A3671907729F0E517CF52FEB 6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

C:\Users\user\AppData\Roaming\FxuoZREPj.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....h.`.....0.....@..... ....@.. .....`..... ..@.....K....`..... .....@.....H.....}PT.(h{>.]... ...^.....@....text...`.....b..... ..`.rsr c.....`.....>.....@..@.reloc..... .....@..B.....@..... ..`..... ....

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	219
Entropy (8bit):	4.93892350100959
Encrypted:	false
SSDEEP:	6:zx3M7/LDkRLELQbSBYBXVNYUqKRLipilFWepYF:zKLLDkOcPBFNYUXQpmWeSF
MD5:	B806DB526EF386AF03CC861D9EDAC7F0
SHA1:	752F5CFD27F955733B3C0AA2BD2C93B5F6E04E95
SHA-256:	B6428BBB155A23F61A036BFCFD37556FC1B324CEC458BB9C663501B223EA270E
SHA-512:	C17DB7F8CCB1FB6F6C1AEBDAA8005E63F969BCB5BBF5BE2E39325ED9567E7665A305928948961270C0109EE7BF2808DB630DF9F840C21D1B650BB9C9026A15 1
Malicious:	false
Reputation:	low
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....The following installation error occurred:..1: Assembly not found: '0'...

Static File Info

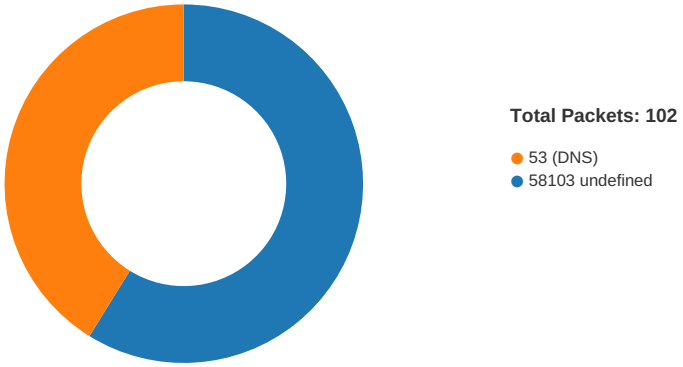
No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/20/21-03:54:48.008225	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	58103	192.168.2.3	194.5.98.120
01/20/21-03:54:56.820534	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	58103	192.168.2.3	194.5.98.120
01/20/21-03:55:03.342741	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	58103	192.168.2.3	194.5.98.120
01/20/21-03:55:09.582405	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	58103	192.168.2.3	194.5.98.120
01/20/21-03:55:15.909410	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	58103	192.168.2.3	194.5.98.120
01/20/21-03:55:22.587171	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	58103	192.168.2.3	194.5.98.120
01/20/21-03:55:29.017083	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	58103	192.168.2.3	194.5.98.120
01/20/21-03:55:35.413547	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	58103	192.168.2.3	194.5.98.120
01/20/21-03:55:41.772538	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	58103	192.168.2.3	194.5.98.120
01/20/21-03:55:48.143018	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	58103	192.168.2.3	194.5.98.120
01/20/21-03:55:54.481130	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	58103	192.168.2.3	194.5.98.120
01/20/21-03:56:00.951320	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	58103	192.168.2.3	194.5.98.120
01/20/21-03:56:07.393192	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	58103	192.168.2.3	194.5.98.120
01/20/21-03:56:13.758406	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	58103	192.168.2.3	194.5.98.120

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 03:54:47.529011011 CET	49731	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:47.830319881 CET	58103	49731	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:47.831140041 CET	49731	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:48.008224964 CET	49731	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:48.440855980 CET	58103	49731	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:48.442153931 CET	49731	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:48.956835032 CET	58103	49731	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:48.957067966 CET	49731	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:49.266015053 CET	58103	49731	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:49.266845942 CET	49731	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:49.766807079 CET	58103	49731	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:49.767000914 CET	49731	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:49.937417984 CET	49731	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:50.168019056 CET	58103	49731	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:50.168078899 CET	58103	49731	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:50.168143988 CET	49731	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:50.168407917 CET	49731	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:54.082894087 CET	49734	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:56.816750050 CET	58103	49734	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:56.820005894 CET	49734	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:56.820533991 CET	49734	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:57.237874985 CET	58103	49734	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:57.240032911 CET	49734	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:57.780216932 CET	58103	49734	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:57.780397892 CET	49734	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:58.098011017 CET	58103	49734	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:58.098129988 CET	49734	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:58.597875118 CET	58103	49734	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:58.597979069 CET	49734	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:58.827852964 CET	49734	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:58.964821100 CET	58103	49734	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:58.964873075 CET	58103	49734	194.5.98.120	192.168.2.3
Jan 20, 2021 03:54:58.964911938 CET	49734	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:54:58.964951992 CET	49734	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:03.030318975 CET	49735	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:03.337780952 CET	58103	49735	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:03.337918997 CET	49735	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:03.342741013 CET	49735	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:03.749732018 CET	58103	49735	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:03.749826908 CET	49735	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:04.264760971 CET	58103	49735	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:04.264966011 CET	49735	58103	192.168.2.3	194.5.98.120

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 03:55:04.602734089 CET	58103	49735	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:04.604691029 CET	49735	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:05.101712942 CET	58103	49735	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:05.101844072 CET	49735	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:05.140908957 CET	49735	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:09.275145054 CET	49737	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:09.580842018 CET	58103	49737	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:09.581091881 CET	49737	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:09.582405090 CET	49737	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:09.997281075 CET	58103	49737	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:09.997512102 CET	49737	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:10.496800900 CET	58103	49737	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:10.497140884 CET	49737	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:10.803798914 CET	58103	49737	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:10.803916931 CET	49737	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:11.310498953 CET	58103	49737	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:11.310585976 CET	49737	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:11.453814030 CET	49737	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:11.687410116 CET	58103	49737	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:11.687463999 CET	58103	49737	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:11.687587023 CET	49737	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:15.585464001 CET	49741	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:15.887204885 CET	58103	49741	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:15.887425900 CET	49741	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:15.909410000 CET	49741	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:16.408720970 CET	58103	49741	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:16.408848047 CET	49741	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:16.442087889 CET	58103	49741	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:16.485321045 CET	49741	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:16.900816917 CET	58103	49741	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:16.900907040 CET	49741	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:17.610424042 CET	49741	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:17.782635927 CET	49741	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:18.011898041 CET	58103	49741	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:18.011975050 CET	49741	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:18.426985979 CET	58103	49741	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:18.427213907 CET	49741	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:22.268893957 CET	49747	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:22.572755098 CET	58103	49747	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:22.572989941 CET	49747	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:22.587171078 CET	49747	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:23.016845942 CET	58103	49747	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:23.017102957 CET	49747	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:23.521816015 CET	58103	49747	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:23.521918058 CET	49747	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:23.827804089 CET	58103	49747	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:23.828015089 CET	49747	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:24.336815119 CET	58103	49747	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:24.337004900 CET	49747	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:24.548867941 CET	49747	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:24.718024015 CET	58103	49747	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:24.718075991 CET	58103	49747	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:24.718169928 CET	49747	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:24.718225002 CET	49747	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:28.702466965 CET	49748	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:29.015722990 CET	58103	49748	194.5.98.120	192.168.2.3
Jan 20, 2021 03:55:29.015849113 CET	49748	58103	192.168.2.3	194.5.98.120
Jan 20, 2021 03:55:29.017082930 CET	49748	58103	192.168.2.3	194.5.98.120

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 03:54:02.729190111 CET	64185	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:02.777236938 CET	53	64185	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 03:54:03.676873922 CET	65110	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:03.725008011 CET	53	65110	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:05.009159088 CET	58361	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:05.065478086 CET	53	58361	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:05.975086927 CET	63492	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:06.036607981 CET	53	63492	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:06.782747984 CET	60831	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:06.833441019 CET	53	60831	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:07.205457926 CET	60100	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:07.266216040 CET	53	60100	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:07.570934057 CET	53195	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:07.618897915 CET	53	53195	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:08.362644911 CET	50141	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:08.413484097 CET	53	50141	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:08.452466965 CET	53023	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:08.508713007 CET	53	53023	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:08.942565918 CET	49563	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:09.068635941 CET	53	49563	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:09.562359095 CET	51352	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:09.610358000 CET	53	51352	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:11.150671005 CET	59349	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:11.207175970 CET	53	59349	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:12.354487896 CET	57084	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:12.402340889 CET	53	57084	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:13.234826088 CET	58823	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:13.291002989 CET	53	58823	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:37.231033087 CET	57568	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:37.279220104 CET	53	57568	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:37.368045092 CET	50540	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:37.441246986 CET	53	50540	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:38.233452082 CET	57568	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:38.289963961 CET	53	57568	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:38.800327063 CET	54366	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:38.848335028 CET	53	54366	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:39.268102884 CET	57568	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:39.315892935 CET	53	57568	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:41.279442072 CET	57568	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:41.335787058 CET	53	57568	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:45.296365976 CET	57568	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:45.352533102 CET	53	57568	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:47.450515985 CET	53034	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:47.508745909 CET	53	53034	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:51.053227901 CET	57762	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:51.110755920 CET	53	57762	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:51.975824118 CET	55435	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:52.023802042 CET	53	55435	8.8.8.8	192.168.2.3
Jan 20, 2021 03:54:54.022315025 CET	50713	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:54:54.081486940 CET	53	50713	8.8.8.8	192.168.2.3
Jan 20, 2021 03:55:02.969752073 CET	56132	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:03.028991938 CET	53	56132	8.8.8.8	192.168.2.3
Jan 20, 2021 03:55:05.512104988 CET	58987	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:05.583679914 CET	53	58987	8.8.8.8	192.168.2.3
Jan 20, 2021 03:55:09.214670897 CET	56579	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:09.271351099 CET	53	56579	8.8.8.8	192.168.2.3
Jan 20, 2021 03:55:15.236490011 CET	60633	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:15.284336090 CET	53	60633	8.8.8.8	192.168.2.3
Jan 20, 2021 03:55:15.525748968 CET	61292	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:15.584012985 CET	53	61292	8.8.8.8	192.168.2.3
Jan 20, 2021 03:55:19.599678040 CET	63619	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:19.657581091 CET	53	63619	8.8.8.8	192.168.2.3
Jan 20, 2021 03:55:22.181852102 CET	64938	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:22.238539934 CET	53	64938	8.8.8.8	192.168.2.3
Jan 20, 2021 03:55:28.639046907 CET	61946	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:28.699803114 CET	53	61946	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 03:55:35.047111034 CET	64910	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:35.103317022 CET	53	64910	8.8.8.8	192.168.2.3
Jan 20, 2021 03:55:41.396301031 CET	52123	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:41.455311060 CET	53	52123	8.8.8.8	192.168.2.3
Jan 20, 2021 03:55:47.752219915 CET	56130	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:47.812983990 CET	53	56130	8.8.8.8	192.168.2.3
Jan 20, 2021 03:55:49.185046911 CET	56338	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:49.232865095 CET	53	56338	8.8.8.8	192.168.2.3
Jan 20, 2021 03:55:49.798393965 CET	59420	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:49.869008064 CET	53	59420	8.8.8.8	192.168.2.3
Jan 20, 2021 03:55:54.105278969 CET	58784	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:55:54.153218031 CET	53	58784	8.8.8.8	192.168.2.3
Jan 20, 2021 03:56:00.576467037 CET	63978	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:56:00.633006096 CET	53	63978	8.8.8.8	192.168.2.3
Jan 20, 2021 03:56:07.011157990 CET	62938	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:56:07.070544004 CET	53	62938	8.8.8.8	192.168.2.3
Jan 20, 2021 03:56:13.384819031 CET	55708	53	192.168.2.3	8.8.8.8
Jan 20, 2021 03:56:13.441323996 CET	53	55708	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 20, 2021 03:54:08.362644911 CET	192.168.2.3	8.8.8.8	0x64e8	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Jan 20, 2021 03:54:08.942565918 CET	192.168.2.3	8.8.8.8	0xaff6	Standard query (0)	rptj2g.sn.files.1drv.com	A (IP address)	IN (0x0001)
Jan 20, 2021 03:54:47.450515985 CET	192.168.2.3	8.8.8.8	0x690a	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 03:54:54.022315025 CET	192.168.2.3	8.8.8.8	0xb3dd	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:02.969752073 CET	192.168.2.3	8.8.8.8	0x23e	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:09.214670897 CET	192.168.2.3	8.8.8.8	0x15f8	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:15.525748968 CET	192.168.2.3	8.8.8.8	0xd3bb	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:22.181852102 CET	192.168.2.3	8.8.8.8	0xa3e3	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:28.639046907 CET	192.168.2.3	8.8.8.8	0xe619	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:35.047111034 CET	192.168.2.3	8.8.8.8	0xa1f4	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:41.396301031 CET	192.168.2.3	8.8.8.8	0x7d01	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:47.752219915 CET	192.168.2.3	8.8.8.8	0x24af	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:54.105278969 CET	192.168.2.3	8.8.8.8	0x52c0	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 03:56:00.576467037 CET	192.168.2.3	8.8.8.8	0x5f55	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 03:56:07.011157990 CET	192.168.2.3	8.8.8.8	0x5f4e	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 03:56:13.384819031 CET	192.168.2.3	8.8.8.8	0xd468	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

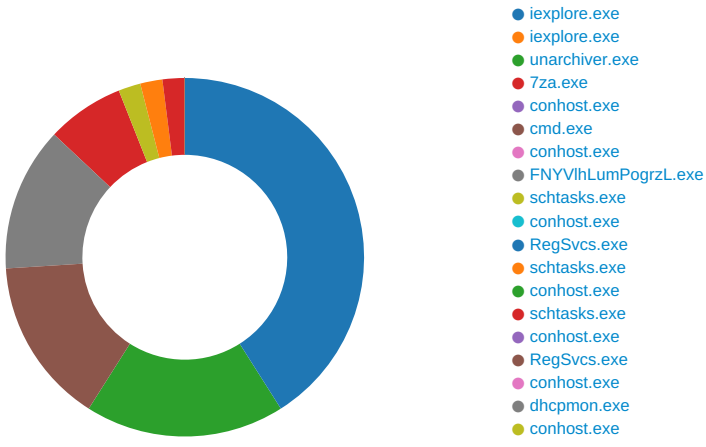
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 20, 2021 03:54:08.413484097 CET	8.8.8.8	192.168.2.3	0x64e8	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2021 03:54:09.068635941 CET	8.8.8.8	192.168.2.3	0xaff6	No error (0)	rptj2g.sn.files.1drv.com	sn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2021 03:54:09.068635941 CET	8.8.8.8	192.168.2.3	0xaff6	No error (0)	sn-files.fe.1drv.com	odc-sn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2021 03:54:47.508745909 CET	8.8.8.8	192.168.2.3	0x690a	No error (0)	strongodss.ddns.net		194.5.98.120	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 20, 2021 03:54:54.081486940 CET	8.8.8.8	192.168.2.3	0xb3dd	No error (0)	strongodss .ddns.net		194.5.98.120	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:03.028991938 CET	8.8.8.8	192.168.2.3	0x23e	No error (0)	strongodss .ddns.net		194.5.98.120	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:09.271351099 CET	8.8.8.8	192.168.2.3	0x15f8	No error (0)	strongodss .ddns.net		194.5.98.120	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:15.584012985 CET	8.8.8.8	192.168.2.3	0xd3bb	No error (0)	strongodss .ddns.net		194.5.98.120	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:22.238539934 CET	8.8.8.8	192.168.2.3	0xa3e3	No error (0)	strongodss .ddns.net		194.5.98.120	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:28.699803114 CET	8.8.8.8	192.168.2.3	0xe619	No error (0)	strongodss .ddns.net		194.5.98.120	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:35.103317022 CET	8.8.8.8	192.168.2.3	0xa1f4	No error (0)	strongodss .ddns.net		194.5.98.120	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:41.455311060 CET	8.8.8.8	192.168.2.3	0x7d01	No error (0)	strongodss .ddns.net		194.5.98.120	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:47.812983990 CET	8.8.8.8	192.168.2.3	0x24af	No error (0)	strongodss .ddns.net		194.5.98.120	A (IP address)	IN (0x0001)
Jan 20, 2021 03:55:54.153218031 CET	8.8.8.8	192.168.2.3	0x52c0	No error (0)	strongodss .ddns.net		194.5.98.120	A (IP address)	IN (0x0001)
Jan 20, 2021 03:56:00.633006096 CET	8.8.8.8	192.168.2.3	0x5f55	No error (0)	strongodss .ddns.net		194.5.98.120	A (IP address)	IN (0x0001)
Jan 20, 2021 03:56:07.070544004 CET	8.8.8.8	192.168.2.3	0x5f4e	No error (0)	strongodss .ddns.net		194.5.98.120	A (IP address)	IN (0x0001)
Jan 20, 2021 03:56:13.441323996 CET	8.8.8.8	192.168.2.3	0xd468	No error (0)	strongodss .ddns.net		194.5.98.120	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 5152 Parent PID: 792

General

Start time:	03:54:06
Start date:	20/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6ba4a0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5168 Parent PID: 5152

General

Start time:	03:54:06
Start date:	20/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5152 CREDAT:17410 /prefetch:2
Imagebase:	0xcd0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: unarchiver.exe PID: 3440 Parent PID: 5152

General

Start time:	03:54:23
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\unarchiver.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z'
Imagebase:	0xa30000
File size:	10240 bytes
MD5 hash:	8B435F8731563566F3F49203BA277865
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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\Local\Temp\bpkrjtup.j3x	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7263B02B	unknown
C:\Users\user\AppData\Local\Temp\bpkrjtup.j3x\unarchiver.log	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7266B31E	unknown
C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7263B02B	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bpkrjtup.j3x\unarchiver.log	unknown	119	30 31 2f 32 30 2f 32 30 32 31 20 33 3a 35 34 20 41 4d 3a 20 55 6e 70 61 63 6b 3a 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 49 4e 65 74 43 61 63 68 65 5c 49 45 5c 4d 45 45 58 57 34 48 34 5c 54 4b 4b 33 36 33 37 39 32 30 30 33 31 2e 6a 70 65 67 2e 7a 0d 0a	01/20/2021 3:54 AM: Unpack: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z..	success or wait	1	7266B157	unknown
C:\Users\user\AppData\Local\Temp\bpkrjtup.j3x\unarchiver.log	unknown	77	30 31 2f 32 30 2f 32 30 32 31 20 33 3a 35 34 20 41 4d 3a 20 54 6d 70 20 64 69 72 3a 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 76 6a 6b 33 79 75 67 79 2e 68 67 74 0d 0a	01/20/2021 3:54 AM: Tmp dir: C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt..	success or wait	1	7266B157	unknown
C:\Users\user\AppData\Local\Temp\bpkrjtup.j3x\unarchiver.log	unknown	50	30 31 2f 32 30 2f 32 30 32 31 20 33 3a 35 34 20 41 4d 3a 20 52 65 63 65 69 76 65 64 20 66 72 6f 6d 20 73 74 61 6e 64 61 72 64 20 6f 75 74 3a 20 0d 0a	01/20/2021 3:54 AM: Received from standard out: ..	success or wait	28	7266B157	unknown
C:\Users\user\AppData\Local\Temp\bpkrjtup.j3x\unarchiver.log	unknown	31	30 31 2f 32 30 2f 32 30 32 31 20 33 3a 35 34 20 41 4d 3a 20 47 65 74 20 66 69 6c 65 73 0d 0a	01/20/2021 3:54 AM: Get files..	success or wait	1	7266B157	unknown
C:\Users\user\AppData\Local\Temp\bpkrjtup.j3x\unarchiver.log	unknown	37	30 31 2f 32 30 2f 32 30 32 31 20 33 3a 35 34 20 41 4d 3a 20 4e 62 72 20 6f 66 20 66 69 6c 65 73 3a 20 31 0d 0a	01/20/2021 3:54 AM: Nbr of files: 1..	success or wait	1	7266B157	unknown
C:\Users\user\AppData\Local\Temp\bpkrjtup.j3x\unarchiver.log	unknown	112	30 31 2f 32 30 2f 32 30 32 31 20 33 3a 35 34 20 41 4d 3a 20 46 6f 75 6e 64 20 69 6e 74 65 72 65 73 74 69 6e 67 20 66 69 6c 65 3a 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 76 6a 6b 33 79 75 67 79 2e 68 67 74 5c 46 4e 59 56 6c 68 4c 75 6d 50 6f 67 72 7a 4c 2e 65 78 65 0d 0a	01/20/2021 3:54 AM: Found interesting file: C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.exe..	success or wait	1	7266B157	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
unknown	unknown	1024	success or wait	2	7266C1B7	unknown
unknown	unknown	1024	pipe broken	1	7266C1B7	unknown
unknown	unknown	1024	unknown	1	7266C1B7	unknown
unknown	unknown	1024	unknown	1	7266C1B7	unknown

Analysis Process: 7za.exe PID: 4848 Parent PID: 3440

General

Start time:	03:54:24
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z'
Imagebase:	0x1280000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	12863B0	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.exe	unknown	1023488	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 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 05 00 fa 68 07 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 de 05 00 00 18 11 00 00 00 00 00 0a 40 17 00 00 80 0f 00 00 20 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 17 00 00 04 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....h.`.......... ....0.............@....... ....@.. .......................` ....@.................	success or wait	17	1286987	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z	unknown	1024	success or wait	1	128686E	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z	unknown	64	success or wait	1	128686E	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z	unknown	512	success or wait	1	128686E	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z	unknown	8	success or wait	1	128686E	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TKK3637920031.jpeg.z	unknown	1048576	success or wait	2	128686E	ReadFile

Analysis Process: conhost.exe PID: 2024 Parent PID: 4848

General

Start time:	03:54:24
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: cmd.exe PID: 5876 Parent PID: 3440

General

Start time:	03:54:25
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /C 'C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.exe'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5776 Parent PID: 5876

General

Start time:	03:54:25
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: FNYVlhLumPogrzL.exe PID: 2208 Parent PID: 5876

General

Start time:	03:54:25
Start date:	20/01/2021
Path:	C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.exe
Imagebase:	0x8c0000
File size:	1505792 bytes
MD5 hash:	E2369B4A4D2E2C7F1F8AF4F7743532E9
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: 0000000A.00000002.281072105.00000000041F1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.281072105.00000000041F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.281072105.00000000041F1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.277584166.00000000030D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.280831636.0000000004071000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.280831636.0000000004071000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.280831636.0000000004071000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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\FxuoZREPj.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	54418AF	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE9ED.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	121BC88	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\FNYVlhLumPogrzL.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\tmpE9ED.tmp	success or wait	1	5442526	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\FxuoZREPj.exe	unknown	1505792	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 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 05 00 fa 68 07 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 de 05 00 00 18 11 00 00 00 00 00 0a 40 17 00 00 80 0f 00 00 20 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 17 00 00 04 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....h.`.......... ....0..............@....... ....@.. .......................` ....@.................	success or wait	1	5441B37	WriteFile
C:\Users\user\AppData\Local\Temp\tmpE9ED.tmp	unknown	1642	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 68 61 72 64 7a 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 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10- 25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	5441B37	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\FNYVlhLumPogrzL.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\AppData\Local\Temp\vjk3yugy.hgt\FNYVlhLumPogrzL.exe	unknown	1505792	success or wait	1	5441B37	ReadFile

Analysis Process: schtasks.exe PID: 1536 Parent PID: 2208

General

Start time:	03:54:39
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\FxuoZREPj' /XML 'C:\Users\user\AppData\Local\Temp\tmpE9ED.tmp'
Imagebase:	0x1030000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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\tmpE9ED.tmp	unknown	2	success or wait	1	103AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE9ED.tmp	unknown	1643	success or wait	1	103ABD9	ReadFile

Analysis Process: conhost.exe PID: 5744 Parent PID: 1536

General

Start time:	03:54:40
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RegSvcs.exe PID: 4912 Parent PID: 2208

General

Start time:	03:54:40
Start date:	20/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd80000
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: 0000000E.00000002.473292400.0000000005780000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.473292400.0000000005780000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.473649492.0000000006050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.473649492.0000000006050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.473649492.0000000006050000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.473627286.0000000006040000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.473627286.0000000006040000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.472189305.00000000043C2000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.466149209.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.466149209.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.466149209.0000000000402000.00000040.00000001.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\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	56707A1	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	567089B	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	56707A1	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	5670B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7D78.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5670D1C	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	567089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp81FD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5670D1C	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	56707A1	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	56707A1	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
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	11	567089B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7D78.tmp	success or wait	1	2E3BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp81FD.tmp	success or wait	1	2E3BF0E	DeleteFileW

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	e8 67 62 2c 3a bd d8 48	.gb,:..H	success or wait	1	5670A53	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 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	5670B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7D78.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	5670A53	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	5670A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp81FD.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	5670A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	248	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 de e3 a5 9f 66 d7 5a 23 80 7c 9b cc 91 a7 40 48 6b 47 10 1f c3 d0 b1 47 d7 d6 4f 2a 56 2e 15 0e d3 ab 8a d8 9f 99 c3 dc e8 70 7a ba ae a5 8f 22 84 0a 07 be 72 b5 c3 10 77 26 26 7c ed ce 63 bb d0 33 7d 7e 84 eb d7 1d 9d 7e b6 cb b6 ff 6f 73 f4 b2 66 d6 05 e9 12 d4 e2 ca 34 12 de 31 9f 67 4a de 27 d7 64 22 d1 4c ba 0b cc 41 90 74 b3 c3 87 d5 46 f9 7b ca c8 ab 14 80 43 0c 7c 26 aa 77	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ....f.Z#.|....@HkG.....G..O* V.....pz....".....r...w&&| ..c..3}~.....~....os..f..... 4..1.gJ.'.d".L...A.t....F.{... ..C.|&.w	success or wait	6	5670A53	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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	5670A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	5670A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	5670A53	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	5670C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 4156 Parent PID: 4912

General

Start time:	03:54:42
Start date:	20/01/2021
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\tmp7D78.tmp'
Imagebase:	0x1030000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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\tmp7D78.tmp	unknown	2	success or wait	1	103AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7D78.tmp	unknown	1321	success or wait	1	103ABD9	ReadFile

Analysis Process: conhost.exe PID: 4168 Parent PID: 4156

General

Start time:	03:54:43
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: schtasks.exe PID: 5564 Parent PID: 4912

General

Start time:	03:54:43
Start date:	20/01/2021
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\tmp81FD.tmp'
Imagebase:	0x1030000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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\tmp81FD.tmp	unknown	2	success or wait	1	103AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp81FD.tmp	unknown	1311	success or wait	1	103ABD9	ReadFile

Analysis Process: conhost.exe PID: 4840 Parent PID: 5564

General

Start time:	03:54:44
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RegSvcs.exe PID: 4868 Parent PID: 528

General

Start time:	03:54:45
Start date:	20/01/2021
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:	0x690000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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\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	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
\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	7266DFAB	unknown
\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	7266DFAB	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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: 1180 Parent PID: 4868

General

Start time:	03:54:46
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: 4120 Parent PID: 528

General

Start time:	03:54:45
Start date:	20/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xea0000
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:	low

Analysis Process: conhost.exe PID: 3880 Parent PID: 4120

General

Start time:	03:54:46
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis