



ID: 356818
Sample Name: TdX45jQWjj.exe
Cookbook: default.jbs
Time: 17:16:26
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report TdX45jQWjj.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 6
System Summary: 6
Signature Overview 6
AV Detection: 7
Compliance: 7
Networking: 7
E-Banking Fraud: 7
Operating System Destruction: 7
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 8
Malware Analysis System Evasion: 8
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 12
Contacted Domains 12
URLs from Memory and Binaries 12
Contacted IPs 15
Public 15
General Information 15
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 17
Domains 17
ASN 17
JA3 Fingerprints 17
Dropped Files 18
Created / dropped Files 18
Static File Info 21
General 21
File Icon 22

Static PE Info 22
General 22
Entrypoint Preview 22
Data Directories 24
Sections 24
Resources 24
Imports 24
Version Infos 25
Network Behavior 25
Network Port Distribution 25
TCP Packets 25
UDP Packets 27
DNS Queries 28
DNS Answers 29
Code Manipulations 29
Statistics 29
Behavior 29
System Behavior 30
Analysis Process: TdX45jQWjj.exe PID: 6960 Parent PID: 5928 30
General 30
File Activities 30
File Created 30
File Deleted 30
File Written 31
File Read 32
Analysis Process: schtasks.exe PID: 6004 Parent PID: 6960 32
General 32
File Activities 32
File Read 32
Analysis Process: conhost.exe PID: 6224 Parent PID: 6004 33
General 33
Analysis Process: RegSvcs.exe PID: 3012 Parent PID: 6960 33
General 33
File Activities 34
File Created 34
File Deleted 35
File Written 35
File Read 37
Registry Activities 37
Key Value Created 37
Analysis Process: schtasks.exe PID: 6936 Parent PID: 3012 37
General 38
File Activities 38
File Read 38
Analysis Process: conhost.exe PID: 6920 Parent PID: 6936 38
General 38
Analysis Process: schtasks.exe PID: 6668 Parent PID: 3012 38
General 38
File Activities 39
File Read 39
Analysis Process: conhost.exe PID: 6688 Parent PID: 6668 39
General 39
Analysis Process: RegSvcs.exe PID: 6716 Parent PID: 936 39
General 39
File Activities 39
File Created 39
File Written 40
File Read 40
Analysis Process: conhost.exe PID: 6800 Parent PID: 6716 41
General 41
Analysis Process: dhcpmon.exe PID: 6808 Parent PID: 936 41
General 41
File Activities 41
File Created 41
File Written 41
File Read 42
Analysis Process: conhost.exe PID: 6812 Parent PID: 6808 42
General 42
Analysis Process: dhcpmon.exe PID: 3028 Parent PID: 3440 43
General 43
File Activities 43
File Created 43

File Written 43
File Read 44
Analysis Process: conhost.exe PID: 1868 Parent PID: 3028 44
General 44
Disassembly 45
Code Analysis 45

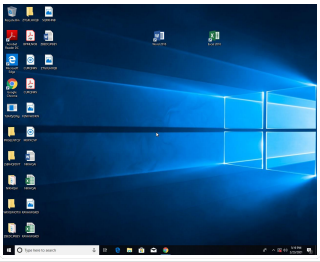
Analysis Report TdX45jQWjj.exe

Overview

General Information

Sample Name:	TdX45jQWjj.exe
Analysis ID:	356818
MD5:	f261164b55c3be5.
SHA1:	634a546e3841af2.
SHA256:	b40e22d33523ae..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

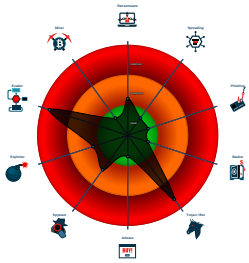
Nanocore

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

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- Connects to many ports of the same…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- TdX45jQWjj.exe (PID: 6960 cmdline: 'C:\Users\user\Desktop\TdX45jQWjj.exe' MD5: F261164B55C3BE5C3C86150FF2A7CC27)
  - schtasks.exe (PID: 6004 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RTOqzQABo' /XML 'C:\Users\user\AppData\Local\Temp\tmp84A9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6224 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 3012 cmdline: {path} MD5: 71369277D09DA0830C8C59F9E22BB23A)
    - schtasks.exe (PID: 6936 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpDEF3.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6668 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpE1E2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6688 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 6716 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6808 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 3028 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 1868 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
00000000.00000002.395064094.00000000046E5000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xc136d:$x1: NanoCore.ClientPluginHost • 0xc13aa:$x2: IClientNetworkHost • 0xc4edd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.395064094.00000000046E5000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.395064094.00000000046E5000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xc10d5:$a: NanoCore • 0xc10e5:$a: NanoCore • 0xc1319:$a: NanoCore • 0xc132d:$a: NanoCore • 0xc136d:$a: NanoCore • 0xc1134:$b: ClientPlugin • 0xc1336:$b: ClientPlugin • 0xc1376:$b: ClientPlugin • 0xc125b:$c: ProjectData • 0xc1c62:$d: DESCrypto • 0xc962e:$e: KeepAlive • 0xc761c:$g: LogClientMessage • 0xc3817:$i: get_Connected • 0xc1f98:$j: #=q • 0xc1fc8:$j: #=q • 0xc1fe4:$j: #=q • 0xc2014:$j: #=q • 0xc2030:$j: #=q • 0xc204c:$j: #=q • 0xc207c:$j: #=q • 0xc2098:$j: #=q
00000000.00000002.394099052.0000000004251000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x251a25:$x1: NanoCore.ClientPluginHost • 0x251a62:$x2: IClientNetworkHost • 0x255595:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.394099052.0000000004251000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.RegSvcs.exe.2ef16fc.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x40c2:$x1: NanoCore.ClientPluginHost
8.2.RegSvcs.exe.2ef16fc.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x40c2:$x2: NanoCore.ClientPluginHost • 0x41a0:$s4: PipeCreated • 0x40dc:$s5: IClientLoggingHost
8.2.RegSvcs.exe.3f2ec9e.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x4083:$x1: NanoCore.ClientPluginHost
8.2.RegSvcs.exe.3f2ec9e.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x4083:$x2: NanoCore.ClientPluginHost • 0x4161:$s4: PipeCreated • 0x409d:$s5: IClientLoggingHost
8.2.RegSvcs.exe.5b90000.9.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1646:$x1: NanoCore.ClientPluginHost
Click to see the 47 entries				

Sigma Overview

System Summary:



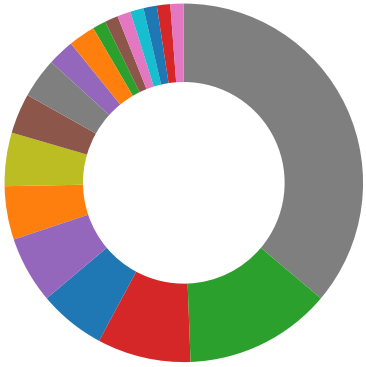
Sigma detected: NanoCore

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

Copyright null 2021



- 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:



- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT

Compliance:



- Uses 32bit PE files
- Uses new MSVCR Dlls
- Contains modern PE file flags such as dynamic base (ASLR) or NX
- Binary contains paths to debug symbols

Networking:



- Connects to many ports of the same IP (likely port scanning)
- Uses dynamic DNS services

E-Banking Fraud:



- Yara detected Nanocore RAT

Operating System Destruction:



- Protects its processes via BreakOnTermination flag

System Summary:



- Malicious sample detected (through community Yara rule)

Data Obfuscation:



- .NET source code contains potential unpacker

Boot Survival:



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

Copyright null 2021

Hooking and other Techniques for Hiding and Protection:



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

Malware Analysis System Evasion:



Yara detected AntiVM_3

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

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

HIPS / PFW / Operating System Protection Evasion:



Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:



Yara detected Nanocore RAT

Remote Access Functionality:



Detected Nanocore Rat

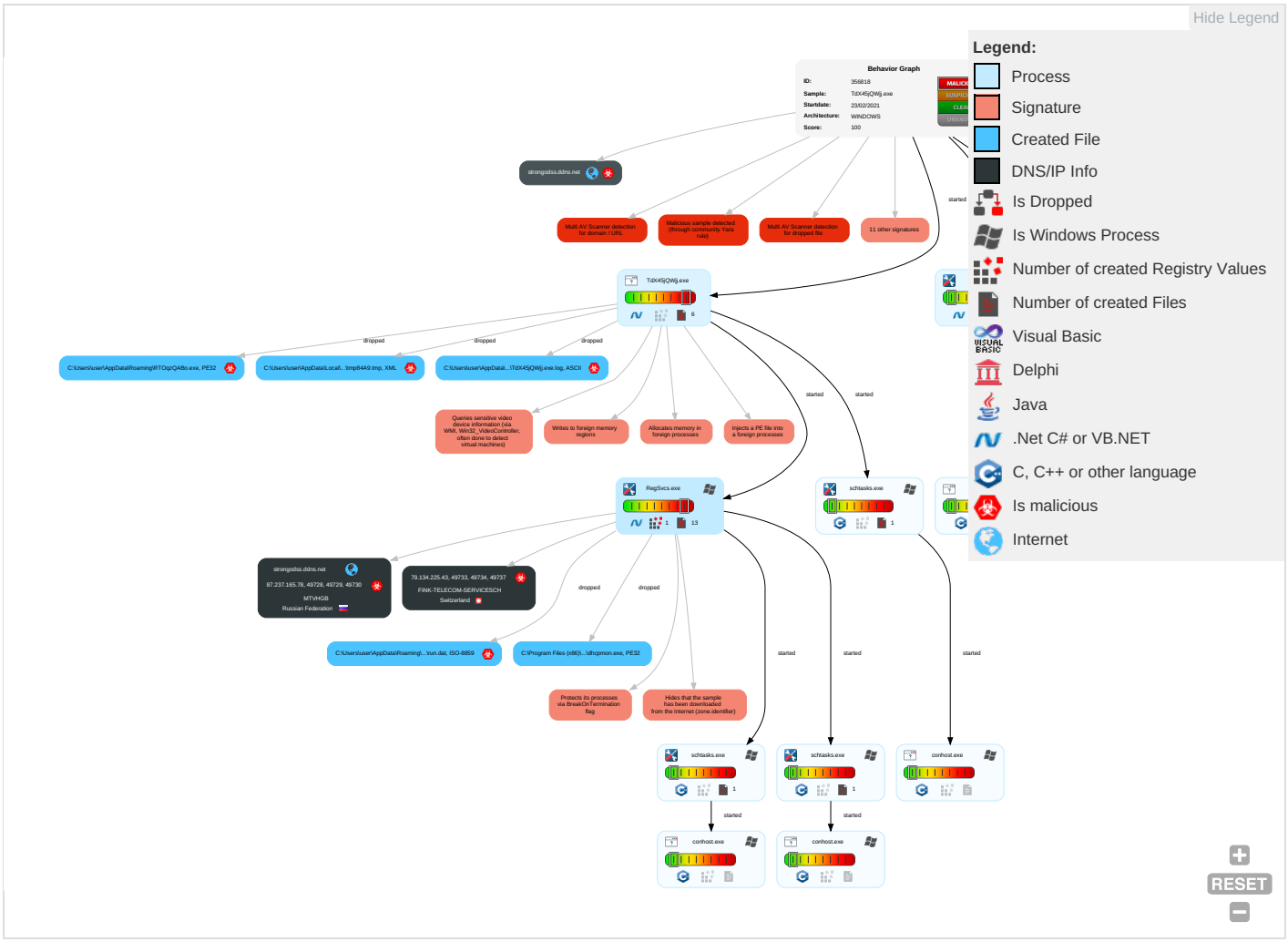
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 2 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 2	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Virtualization/Sandbox Evasion 1 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 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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

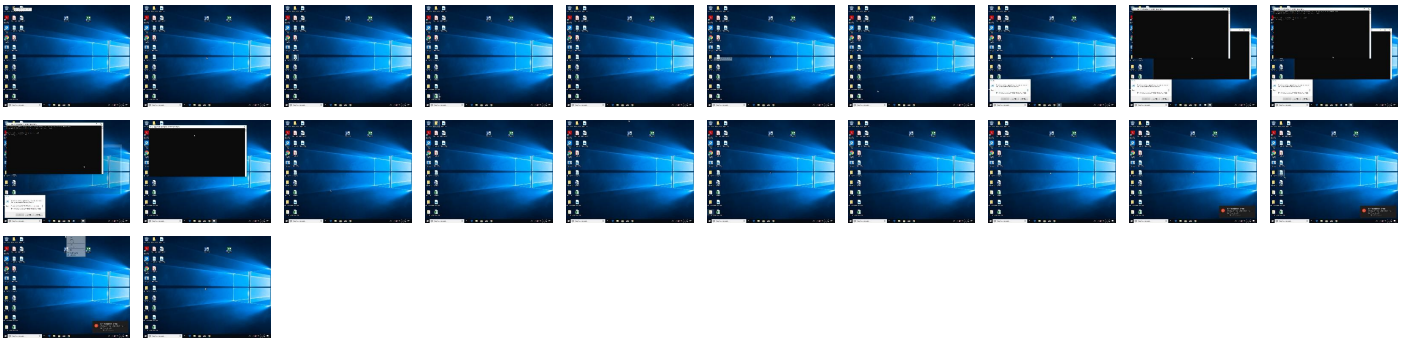
Behavior Graph



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
TdX45jQWjj.exe	19%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\RTOqzQABo.exe	19%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.RegSvcs.exe.5ba0000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.com.	0%	Virustotal		Browse
http://www.sajatypeworks.com.	0%	Avira URL Cloud	safe	
http://www.tiro.com6	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnW	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comn-u	0%	Avira URL Cloud	safe	
http://www.tiro.com0	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cna-d	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.esvstudybible.org/search?q=Whttp://www.blueletterbible.org/Bible.cfm?b=	0%	Avira URL Cloud	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.founder.c	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://topicalmemorysystem.googlecode.com/files/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.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://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnr-t	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.urwpp.de&	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnf	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comt-b	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.sakkal.comX	0%	Avira URL Cloud	safe	
http://www.fontbureau.comC	0%	Avira URL Cloud	safe	
http://www.tiro.comicx	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsiefd	0%	Avira URL Cloud	safe	
http://www.fontbureau.comH	0%	Avira URL Cloud	safe	
http://www.urwpp.deas	0%	Avira URL Cloud	safe	
http://www.esvstudybible.org/search?q=	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/C	0%	Avira URL Cloud	safe	
http://www.urwpp.deF0	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fonts.comW	0%	Avira URL Cloud	safe	
http://www.sakkal.com8	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.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.urwpp.deq	0%	Avira URL Cloud	safe	
http://www.fontbureau.comldco	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	
http://www.founder.com.cn/cn4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

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

URLs from Memory and Binaries

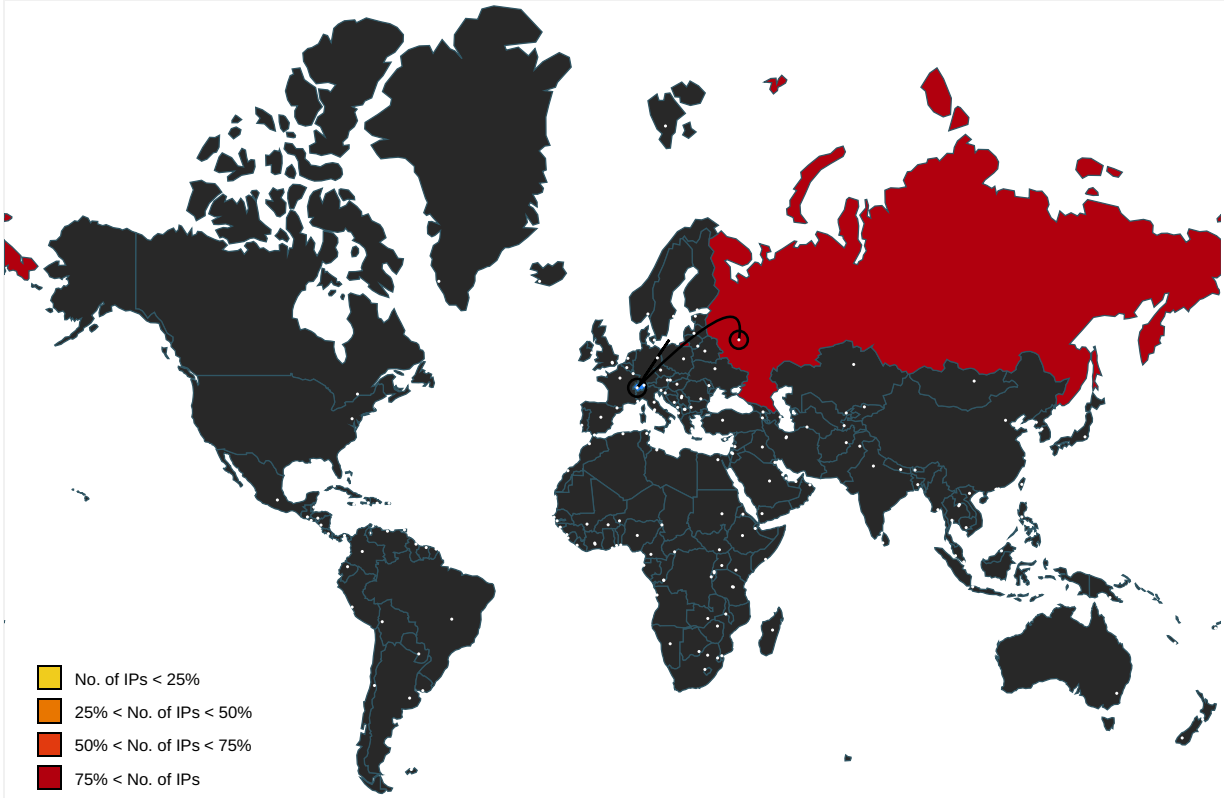
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com.	TdX45jQWjj.exe, 00000000.00000003.329212871.000000000166D000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false		high
http://www.tiro.com6	TdX45jQWjj.exe, 00000000.00000003.332995890.000000000556B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnW	TdX45jQWjj.exe, 00000000.00000003.332432427.0000000005571000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comn-u	TdX45jQWjj.exe, 00000000.00000003.329212871.000000000166D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com0	TdX45jQWjj.exe, 00000000.00000003.334600510.000000000557B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cna-d	TdX45jQWjj.exe, 00000000.00000003.332121914.0000000005563000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.esvstudybible.org/search?q=Whttp://www.blueletterbible.org/Bible.cfm?b=	TdX45jQWjj.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false		high
http://www.founder.c	TdX45jQWjj.exe, 00000000.00000003.333029459.0000000005566000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://topicalmemorysystem.googlecode.com/files/	TdX45jQWjj.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalsF	TdX45jQWjj.exe, 00000000.00000003.341606484.0000000005566000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp, TdX45jQWjj.exe, 00000000.00000003.329212871.000000000166D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	TdX45jQWjj.exe, 00000000.00000003.330218742.000000000559D000.00000004.00000001.sdmp, TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.blueletterbible.org/Bible.cfm?b=	TdX45jQWjj.exe	false		high
http://www.founder.com.cn/cnr-t	TdX45jQWjj.exe, 00000000.00000003.332121914.0000000005563000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de&	TdX45jQWjj.exe, 00000000.00000003.342118309.000000000557F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fonts.com	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	TdX45jQWjj.exe, 00000000.00000003.342496493.000000000557F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnf	TdX45jQWjj.exe, 00000000.00000003.332432427.0000000005571000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comt-b	TdX45jQWjj.exe, 00000000.00000003.329212871.000000000166D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com.TTF	TdX45jQWjj.exe, 00000000.00000003.341606484.0000000005566000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.comX	TdX45jQWjj.exe, 00000000.00000003.336154433.0000000005572000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comC	TdX45jQWjj.exe, 00000000.00000003.341606484.0000000005566000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comicx	TdX45jQWjj.exe, 00000000.00000003.334600510.000000000557B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comsiefd	TdX45jQWjj.exe, 00000000.00000003.341606484.0000000005566000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comH	TdX45jQWjj.exe, 00000000.00000003.341606484.0000000005566000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.biblegateway.com/passage/?search=	TdX45jQWjj.exe	false		high
http://www.urwpp.deas	TdX45jQWjj.exe, 00000000.00000003.337611054.000000000557F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.esvstudybible.org/search?q=	TdX45jQWjj.exe	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/C	TdX45jQWjj.exe, 00000000.00000003.335242026.0000000005566000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deF0	TdX45jQWjj.exe, 00000000.00000003.342496493.000000000557F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	TdX45jQWjj.exe, 00000000.00000003.335242026.0000000005566000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	TdX45jQWjj.exe, 00000000.00000002.395767153.0000000005560000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comW	TdX45jQWjj.exe, 00000000.00000003.329977481.000000000559D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.biblija.net/biblija.cgi?m=	TdX45jQWjj.exe	false		high
http://www.sakkal.com8	TdX45jQWjj.exe, 00000000.00000003.335896168.0000000005572000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false		high
http://www.urwpp.deq	TdX45jQWjj.exe, 00000000.00000003.337507075.000000000557F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comldco	TdX45jQWjj.exe, 00000000.00000002.395767153.0000000005560000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp, TdX45jQWjj.exe, 00000000.00000003.335447637.0000000005566000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn4	TdX45jQWjj.exe, 00000000.00000003.331982815.0000000005563000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	TdX45jQWjj.exe, 00000000.00000002.405149050.0000000006822000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/d	TdX45jQWjj.exe, 00000000.00000003.335242026.0000000005566000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/f	TdX45jQWjj.exe, 00000000.00000003.337840613.000000000557F000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356818
Start date:	23.02.2021
Start time:	17:16:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TdX45jQWjj.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34

Copyright null 2021

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@18/13@10/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.7% (good quality ratio 1.2%) • Quality average: 43% • Quality standard deviation: 34.1%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 23.211.6.115, 52.255.188.83, 104.43.139.144, 104.43.193.48, 168.61.161.212, 51.104.139.180, 8.248.131.254, 8.253.207.121, 8.253.204.121, 67.26.73.254, 8.248.137.254, 51.103.5.159, 52.155.217.156, 92.122.213.247, 92.122.213.194, 20.54.26.129, 184.30.24.56 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:17:26	API Interceptor	2x Sleep call for process: TdX45jQWjj.exe modified
17:17:47	API Interceptor	749x Sleep call for process: RegSvcs.exe modified
17:17:47	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
17:17:48	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe" s>$(Arg0)
17:17:48	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MTVHGB	QUOTATION 19 01 2021.exe	Get hash	malicious	Browse	• 87.237.165.162
FINK-TELECOM-SERVICESCH	e92b274943f4a3a557881ee0dd57772d.exe	Get hash	malicious	Browse	• 79.134.225.105
	WxTm2cWLHF.exe	Get hash	malicious	Browse	• 79.134.225.71
	Payment Confirmation.exe	Get hash	malicious	Browse	• 79.134.225.30
	rjHlt1zz28.exe	Get hash	malicious	Browse	• 79.134.225.49
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 79.134.225.49
	document.exe	Get hash	malicious	Browse	• 79.134.225.122
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 79.134.225.105
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 79.134.225.105
	256ec8f8f67b59c5e085b0bb63afcd13.exe	Get hash	malicious	Browse	• 79.134.225.105
	JOIN.exe	Get hash	malicious	Browse	• 79.134.225.30
	Delivery pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 79.134.225.105
	fnfqzfwC44.exe	Get hash	malicious	Browse	• 79.134.225.25
	Solicitud de oferta 6100003768.exe	Get hash	malicious	Browse	• 79.134.225.96
	Nrfgylra.exe	Get hash	malicious	Browse	• 79.134.225.96
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	Form pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	Quotation 3342688.exe	Get hash	malicious	Browse	• 79.134.225.120

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	a34b93ef-dea2-45f8-a5bf-4f6b0b5291c7.exe	Get hash	malicious	Browse	
	3fcd8c19-af88-4cd9-87e7-0bfea1de01a1.exe	Get hash	malicious	Browse	
	Vietnam Order.exe	Get hash	malicious	Browse	
	Dhl Shipping Document.exe	Get hash	malicious	Browse	
	PO-WJO-001, pdf.exe	Get hash	malicious	Browse	
	byWuWAR5FD.exe	Get hash	malicious	Browse	
	parcel_images.exe	Get hash	malicious	Browse	
	0712020.exe	Get hash	malicious	Browse	
	JfRbEbUkpV39K4L.exe	Get hash	malicious	Browse	
	DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe	Get hash	malicious	Browse	
	DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe	Get hash	malicious	Browse	
	zC3edqmNNt.exe	Get hash	malicious	Browse	
	Shipping Document.pdf..exe	Get hash	malicious	Browse	
	PPR & CPR_HEA_DECEMBER 4 2020.exe	Get hash	malicious	Browse	
	AdministratorDownloadsBL,.rar.exe	Get hash	malicious	Browse	
	signed_19272.zip(#U007e18 KB) (2).exe	Get hash	malicious	Browse	
	TT Swift Copy..,.exe	Get hash	malicious	Browse	
	Invoice-.exe	Get hash	malicious	Browse	
	Invoice..,.exe	Get hash	malicious	Browse	
	Bank Update Info.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7515815714465193
Encrypted:	false
SSDEEP:	384:BOj9Y8/gS7SDriLGKq1MHR5U4Ag6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgWSW72uw:B+gSAdN1MH3HAFRJngW2u
MD5:	71369277D09DA0830C8C59F9E22BB23A
SHA1:	37F9781314F0F6B7E9CB529A573F2B1C8DE9E93F
SHA-256:	D4527B7AD2FC4778CC5BE8709C95AEA44EAC0568B367EE14F7357D72898C3698
SHA-512:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: a34b93ef-dea2-45f8-a5bf-4f6b0b5291c7.exe, Detection: malicious, Browse • Filename: 3fcd8c19-af88-4cd9-87e7-0bfea1de01a1.exe, Detection: malicious, Browse • Filename: Vietnam Order.exe, Detection: malicious, Browse • Filename: Dhl Shipping Document.exe, Detection: malicious, Browse • Filename: PO-WJO-001, pdf.exe, Detection: malicious, Browse • Filename: byWuWAR5FD.exe, Detection: malicious, Browse • Filename: parcel_images.exe, Detection: malicious, Browse • Filename: 0712020.exe, Detection: malicious, Browse • Filename: JfRbEbUkpV39K4L.exe, Detection: malicious, Browse • Filename: DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe, Detection: malicious, Browse • Filename: DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe, Detection: malicious, Browse • Filename: zC3edqmNNt.exe, Detection: malicious, Browse • Filename: Shipping Document.pdf..exe, Detection: malicious, Browse • Filename: PPR & CPR_HEA_DECEMBER 4 2020.exe, Detection: malicious, Browse • Filename: AdministratorDownloadsBL,.rar.exe, Detection: malicious, Browse • Filename: signed_19272.zip(#U007e18 KB) (2).exe, Detection: malicious, Browse • Filename: TT Swift Copy..,.exe, Detection: malicious, Browse • Filename: Invoice-.exe, Detection: malicious, Browse • Filename: Invoice..,.exe, Detection: malicious, Browse • Filename: Bank Update Info.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....P... .....k... .....@.. .....[.. ..@.....k..K..... k..... ....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\TdX45jQWjj.exe.log	
Process:	C:\Users\user\Desktop\TdX45jQWjj.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:	BC05A2A1BE5B122FC6D3DEA66EF4258522F13351B9754378395AAD019631E312CFD3BC990F3E3D5C7BB0BDBA1EAD54A2B34A96DEE2FCCD703721E98F6192E[48]
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_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\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmp84A9.tmp	
Process:	C:\Users\user\Desktop\TdX45jQWjj.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1654
Entropy (8bit):	5.164840508589519
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3GNtn:cbha7JlNQV/rydbz9I3YODOLNdq3m
MD5:	96AE2E087DAE15CE7270C5FB8128CC1E
SHA1:	F3F852F3B0134DCB9B3E3F0DB1901E0462CE9930
SHA-256:	BB20A3526C68DB79050BC2325F6C3DD8AA632A70453916E5BA989EBC9CCC3201
SHA-512:	135FF3B63071F8B48191E42B6EA6500429CC3969D675120173EF1DDEBE64DC448F3F4FA6DFFBA45D4CDC1EBB07B909C8DEB5DD3899CEA9A746A862727E91F5F
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\tmp84A9.tmp	
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>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmpDEF3.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):	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
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\tmpE1E2.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:cg99t:cgF
MD5:	BC4D62E76C99B9DA2A2D11CAA27D85C5
SHA1:	FEBCC76A90A831BC18602642DA89F8A119A97791
SHA-256:	3F30A21FD0FBCF36E808D2B80AA932C54E57D6E82497C9219329DBE4F2018B41
SHA-512:	BBFD205513B3BF65D77F9ECF4C48A1F34324F9748C43005269F7E3D1934ECE2380CC7ACCBAAAA5BC398C6CD91B43A446072B30F91775D0C1101CC1321C0C524
Malicious:	**true**
Preview:	b.'.a..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
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe

C:\Users\user\AppData\Roaming\RTOqzQABo.exe	
Process:	C:\Users\user\Desktop\TdX45jQWjj.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	724480
Entropy (8bit):	6.873898218108219
Encrypted:	false
SSDEEP:	12288:4U1KZEwKE03lKYxU/3JHrcnfgqIxI9f105FnYGK53:4U1bE03lpS3JLcnf3e+y59S53
MD5:	F261164B55C3BE5C3C86150FF2A7CC27
SHA1:	634A546E3841AF29B068C7C6535206695EB704D0
SHA-256:	B40E22D33523AE869BA4A9A9159D37D61EC056FC14DC3DB7406D79620B801816
SHA-512:	2E082DF070977B7884D7E40E4811C1BE215872681A4E2120E3035805850DCE52D886EF923E0B8D9B96819AC5532E1209CB1B39E1CBD1E24C552B6DA593EF7AE
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 19%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...T.4`.....0.....".. ...@....@.. ..... ..@.....d"..O....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....".....H.....[.....C..H.....}.....(.....(.....{....r...p~/...(....o.....{....o....&*..0.....r...p(....&.....o....&...*... .....n..t.....o.....{....o....&*.....(.....*~..{....o.....{....o....(.....*.0..+.....{.....+...,..{....o.....(.....*..0.....s ...}.....(!...s".....s#...}.....s$...}.....s$...}.....s$...}.....{....s%...}.....s&... }.....s$...}.....s$...}.....s'...}.....{....o(.....{....o(..

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1145
Entropy (8bit):	4.462201512373672
Encrypted:	false
SSDEEP:	24:zKLXkzPDObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0zPDQntKKH1MqJC
MD5:	46EBEB88876A00A52CC37B1F8E0D0438
SHA1:	5E5DB352F964E5F398301662FF558BD905798A65
SHA-256:	D65BD5A6CC112838AFE8FA70BF61FD13C1313BCE3EE3E76C50E454D7B581238B
SHA-512:	E713E6F304A469FB71235C598BC7E2C6F8458ABC61DAF3D1F364F66579CAFA4A7F3023E585BDA552FB400009E7805A8CA0311A50D5EDC9C2AD2D067772A071B E
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [optio ns] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target app lication, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /rec onfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /no logo Suppress logo output... /quiet Suppress logo output and success output...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.873898218108219

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	TdX45jQWjj.exe
File size:	724480
MD5:	f261164b55c3be5c3c86150ff2a7cc27
SHA1:	634a546e3841af29b068c7c6535206695eb704d0
SHA256:	b40e22d33523ae869ba4a9a9159d37d61ec056fc14dc3db7406d79620b801816
SHA512:	2e082df070977b7884d7e40e4811c1be215872681a4e2120e3035805850dce52d886ef923e0b8d9b96819ac5532e1209cb1b39e1cbd1e24c552b6da593ef7aee
SSDEEP:	12288:4U1KZEwKE03lKYxU/3JHrcnfgqIxI9f105FnYGK53:4U1bE03lpS3JLcnf3e+y59S53
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...T.4`.....0....."... ...@....@.. .....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b22b6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6034B054 [Tue Feb 23 07:35:48 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb2264	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb4000	0x5bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb02bc	0xb0400	False	0.647197750443	data	6.88263810957	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb4000	0x5bc	0x600	False	0.429036458333	data	4.1755308999	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xb4090	0x32c	data		
RT_MANIFEST	0xb43cc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

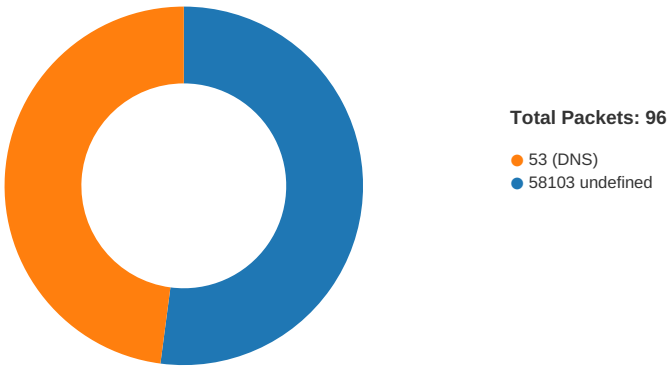
Copyright null 2021

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	yKpW14.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Core.Numero
ProductVersion	1.0.0.0
FileDescription	Core.Numero
OriginalFilename	yKpW14.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:17:49.816740036 CET	49728	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:17:49.866312027 CET	58103	49728	87.237.165.78	192.168.2.6
Feb 23, 2021 17:17:50.469731092 CET	49728	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:17:50.518347025 CET	58103	49728	87.237.165.78	192.168.2.6
Feb 23, 2021 17:17:51.167937994 CET	49728	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:17:51.216872931 CET	58103	49728	87.237.165.78	192.168.2.6
Feb 23, 2021 17:17:56.111509085 CET	49729	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:17:56.160279036 CET	58103	49729	87.237.165.78	192.168.2.6
Feb 23, 2021 17:17:56.668401003 CET	49729	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:17:56.719479084 CET	58103	49729	87.237.165.78	192.168.2.6
Feb 23, 2021 17:17:57.358163118 CET	49729	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:17:57.408514023 CET	58103	49729	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:01.533585072 CET	49730	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:01.582025051 CET	58103	49730	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:02.090732098 CET	49730	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:02.139506102 CET	58103	49730	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:02.653309107 CET	49730	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:02.701766014 CET	58103	49730	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:06.780617952 CET	49733	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:06.863351107 CET	58103	49733	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:07.372442961 CET	49733	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:07.452433109 CET	58103	49733	79.134.225.43	192.168.2.6

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:18:07.966236115 CET	49733	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:08.046123981 CET	58103	49733	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:12.063834906 CET	49734	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:12.143503904 CET	58103	49734	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:12.747900963 CET	49734	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:12.828243971 CET	58103	49734	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:13.435470104 CET	49734	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:13.512624979 CET	58103	49734	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:17.515353918 CET	49737	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:17.592787981 CET	58103	49737	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:18.138947964 CET	49737	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:18.218111992 CET	58103	49737	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:18.810132980 CET	49737	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:18.886920929 CET	58103	49737	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:23.099721909 CET	49750	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:23.148130894 CET	58103	49750	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:23.655040979 CET	49750	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:23.703653097 CET	58103	49750	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:24.217570066 CET	49750	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:24.266292095 CET	58103	49750	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:28.430910110 CET	49753	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:28.479902983 CET	58103	49753	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:29.030546904 CET	49753	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:29.081515074 CET	58103	49753	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:29.602902889 CET	49753	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:29.656091928 CET	58103	49753	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:33.783016920 CET	49754	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:33.831398964 CET	58103	49754	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:34.343411922 CET	49754	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:34.391799927 CET	58103	49754	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:34.906061888 CET	49754	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:34.957196951 CET	58103	49754	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:38.970818996 CET	49755	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:39.052138090 CET	58103	49755	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:39.562731028 CET	49755	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:39.642889977 CET	58103	49755	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:40.156390905 CET	49755	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:40.237574100 CET	58103	49755	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:44.253082037 CET	49756	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:44.330132961 CET	58103	49756	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:44.844403982 CET	49756	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:44.923239946 CET	58103	49756	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:45.438157082 CET	49756	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:45.515690088 CET	58103	49756	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:49.533921003 CET	49760	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:49.613707066 CET	58103	49760	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:50.126089096 CET	49760	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:50.203037977 CET	58103	49760	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:50.708053112 CET	49760	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:18:50.788264036 CET	58103	49760	79.134.225.43	192.168.2.6
Feb 23, 2021 17:18:54.901932001 CET	49761	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:54.953493118 CET	58103	49761	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:55.454627037 CET	49761	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:55.502931118 CET	58103	49761	87.237.165.78	192.168.2.6
Feb 23, 2021 17:18:56.017488003 CET	49761	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:18:56.066579103 CET	58103	49761	87.237.165.78	192.168.2.6
Feb 23, 2021 17:19:00.350300074 CET	49762	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:19:00.398675919 CET	58103	49762	87.237.165.78	192.168.2.6
Feb 23, 2021 17:19:00.970395088 CET	49762	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:19:01.021527052 CET	58103	49762	87.237.165.78	192.168.2.6
Feb 23, 2021 17:19:01.565815926 CET	49762	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:19:01.614341021 CET	58103	49762	87.237.165.78	192.168.2.6
Feb 23, 2021 17:19:05.837376118 CET	49765	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:19:05.886914968 CET	58103	49765	87.237.165.78	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:19:06.396033049 CET	49765	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:19:06.444776058 CET	58103	49765	87.237.165.78	192.168.2.6
Feb 23, 2021 17:19:06.960246086 CET	49765	58103	192.168.2.6	87.237.165.78
Feb 23, 2021 17:19:07.011647940 CET	58103	49765	87.237.165.78	192.168.2.6
Feb 23, 2021 17:19:11.158442974 CET	49766	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:19:11.239665031 CET	58103	49766	79.134.225.43	192.168.2.6
Feb 23, 2021 17:19:11.745487928 CET	49766	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:19:11.825278044 CET	58103	49766	79.134.225.43	192.168.2.6
Feb 23, 2021 17:19:12.339214087 CET	49766	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:19:12.419230938 CET	58103	49766	79.134.225.43	192.168.2.6
Feb 23, 2021 17:19:16.531472921 CET	49767	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:19:16.608556032 CET	58103	49767	79.134.225.43	192.168.2.6
Feb 23, 2021 17:19:17.120801926 CET	49767	58103	192.168.2.6	79.134.225.43
Feb 23, 2021 17:19:17.199274063 CET	58103	49767	79.134.225.43	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:17:09.184077024 CET	53	54513	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:10.261516094 CET	62044	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:10.318402052 CET	53	62044	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:10.698014975 CET	63791	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:10.764590025 CET	53	63791	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:11.418453932 CET	64267	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:11.477303028 CET	53	64267	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:12.567426920 CET	49448	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:12.618798971 CET	53	49448	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:13.725222111 CET	60342	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:13.776582956 CET	53	60342	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:15.202279091 CET	61346	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:15.250933886 CET	53	61346	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:16.409442902 CET	51774	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:16.458087921 CET	53	51774	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:17.203763962 CET	56023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:17.252573013 CET	53	56023	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:18.513149977 CET	58384	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:18.564690113 CET	53	58384	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:21.420331001 CET	60261	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:21.473280907 CET	53	60261	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:22.546210051 CET	56061	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:22.594912052 CET	53	56061	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:23.544114113 CET	58336	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:23.597176075 CET	53	58336	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:24.718357086 CET	53781	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:24.771702051 CET	53	53781	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:25.781019926 CET	54064	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:25.831368923 CET	53	54064	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:26.665043116 CET	52811	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:26.713695049 CET	53	52811	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:28.045661926 CET	55299	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:28.105572939 CET	53	55299	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:29.242130041 CET	63745	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:29.292561054 CET	53	63745	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:30.302110910 CET	50055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:30.353559971 CET	53	50055	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:45.749149084 CET	61374	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:45.803076982 CET	53	61374	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:49.724088907 CET	50339	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:49.785586119 CET	53	50339	8.8.8.8	192.168.2.6
Feb 23, 2021 17:17:56.046478987 CET	63307	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:17:56.108705044 CET	53	63307	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:01.465342045 CET	49694	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:01.531475067 CET	53	49694	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:04.277283907 CET	54982	53	192.168.2.6	8.8.8.8

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:18:04.327717066 CET	53	54982	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:05.928406000 CET	50010	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:06.000159979 CET	53	50010	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:16.739250898 CET	63718	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:16.822832108 CET	53	63718	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:17.364798069 CET	62116	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:17.422219038 CET	53	62116	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:18.057244062 CET	63816	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:18.072122097 CET	55014	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:18.116528034 CET	53	63816	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:18.131342888 CET	53	55014	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:18.182094097 CET	62208	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:18.250031948 CET	53	62208	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:18.626137972 CET	57574	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:18.686405897 CET	53	57574	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:19.258896112 CET	51818	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:19.342488050 CET	53	51818	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:19.996468067 CET	56628	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:20.056597948 CET	53	56628	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:20.854536057 CET	60778	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:20.913292885 CET	53	60778	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:22.093715906 CET	53799	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:22.142374039 CET	53	53799	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:23.032670975 CET	54683	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:23.097532034 CET	53	54683	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:23.788300991 CET	59329	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:23.845614910 CET	53	59329	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:24.421181917 CET	64021	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:24.478604078 CET	53	64021	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:28.319880962 CET	56129	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:28.378196001 CET	53	56129	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:33.718417883 CET	58177	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:33.780843973 CET	53	58177	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:48.620522022 CET	50700	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:48.695178986 CET	53	50700	8.8.8.8	192.168.2.6
Feb 23, 2021 17:18:54.838036060 CET	54069	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:18:54.900182009 CET	53	54069	8.8.8.8	192.168.2.6
Feb 23, 2021 17:19:00.232599974 CET	61178	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:19:00.292726040 CET	53	61178	8.8.8.8	192.168.2.6
Feb 23, 2021 17:19:01.121434927 CET	57017	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:19:01.172938108 CET	53	57017	8.8.8.8	192.168.2.6
Feb 23, 2021 17:19:02.884172916 CET	56327	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:19:02.941157103 CET	53	56327	8.8.8.8	192.168.2.6
Feb 23, 2021 17:19:05.774005890 CET	50243	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:19:05.835586071 CET	53	50243	8.8.8.8	192.168.2.6
Feb 23, 2021 17:19:27.155184031 CET	62055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:19:27.215336084 CET	53	62055	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:17:49.724088907 CET	192.168.2.6	8.8.8.8	0x8dda	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:17:56.046478987 CET	192.168.2.6	8.8.8.8	0x7f93	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:18:01.465342045 CET	192.168.2.6	8.8.8.8	0x5766	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:18:23.032670975 CET	192.168.2.6	8.8.8.8	0xcdaa	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:18:28.319880962 CET	192.168.2.6	8.8.8.8	0xf0	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:18:33.718417883 CET	192.168.2.6	8.8.8.8	0x8db7	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:18:54.838036060 CET	192.168.2.6	8.8.8.8	0xe570	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:19:00.232599974 CET	192.168.2.6	8.8.8.8	0xb91e	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:19:05.774005890 CET	192.168.2.6	8.8.8.8	0xd6c9	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:19:27.155184031 CET	192.168.2.6	8.8.8.8	0x9f73	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

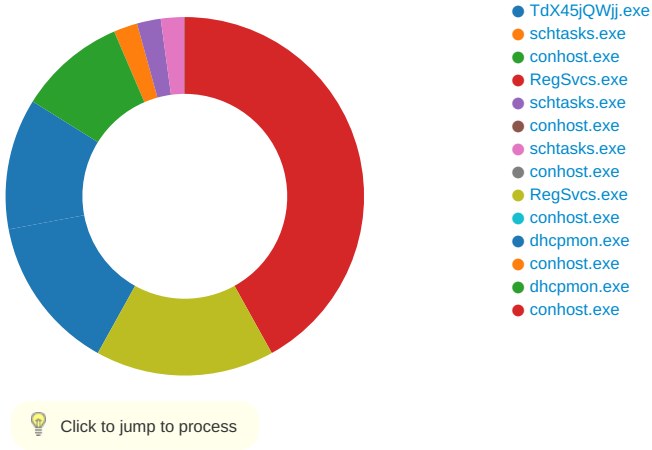
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:17:49.785586119 CET	8.8.8.8	192.168.2.6	0x8dda	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 23, 2021 17:17:56.108705044 CET	8.8.8.8	192.168.2.6	0x7f93	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 23, 2021 17:18:01.531475067 CET	8.8.8.8	192.168.2.6	0x5766	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 23, 2021 17:18:23.097532034 CET	8.8.8.8	192.168.2.6	0xcdaa	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 23, 2021 17:18:28.378196001 CET	8.8.8.8	192.168.2.6	0xf0	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 23, 2021 17:18:33.780843973 CET	8.8.8.8	192.168.2.6	0x8db7	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 23, 2021 17:18:54.900182009 CET	8.8.8.8	192.168.2.6	0xe570	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 23, 2021 17:19:00.292726040 CET	8.8.8.8	192.168.2.6	0xb91e	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 23, 2021 17:19:05.835586071 CET	8.8.8.8	192.168.2.6	0xd6c9	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 23, 2021 17:19:27.215336084 CET	8.8.8.8	192.168.2.6	0x9f73	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: TdX45jQWjj.exe PID: 6960 Parent PID: 5928

General

Start time:	17:17:16
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\TdX45jQWjj.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TdX45jQWjj.exe'
Imagebase:	0xa50000
File size:	724480 bytes
MD5 hash:	F261164B55C3BE5C3C86150FF2A7CC27
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.395064094.00000000046E5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.395064094.00000000046E5000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.395064094.00000000046E5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.394099052.0000000004251000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.394099052.0000000004251000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.394099052.0000000004251000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\RTOqzQABo.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6791C83	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp84A9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10FB5B8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\TdX45jQWjj.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\tmp84A9.tmp	success or wait	1	67928FA	DeleteFileW

Copyright null 2021

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RTOqzQABo.exe	unknown	724480	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\TdX45jQWjj.exe.log	unknown	655	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Users\user\Desktop\TdX45jQWjj.exe	unknown	724480	success or wait	1	6791F0B	ReadFile

Analysis Process: schtasks.exe PID: 6004 Parent PID: 6960

General

Start time:	17:17:43
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RTOqzQABo' /XML 'C:\Users\user\AppData\Local\Temp\tmp84A9.tmp'
Imagebase:	0x120000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp84A9.tmp	unknown	2	success or wait	1	12AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp84A9.tmp	unknown	1655	success or wait	1	12ABD9	ReadFile

Analysis Process: conhost.exe PID: 6224 Parent PID: 6004

General

Start time:	17:17:44
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 3012 Parent PID: 6960

General

Start time:	17:17:44
Start date:	23/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x8d0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright null 2021

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.602153062.0000000005900000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.602153062.0000000005900000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.595499721.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.595499721.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.595499721.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.602225959.0000000005B90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.602225959.0000000005B90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.602238562.0000000005BA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.602238562.0000000005BA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.602238562.0000000005BA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.600580275.0000000003F27000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.600580275.0000000003F27000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
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	51D07A1	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	51D089B	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	51D07A1	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	51D0B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpDEF3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	51D0D1C	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	51D089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE1E2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	51D0D1C	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	51D07A1	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	51D07A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDEF3.tmp	success or wait	1	11DBF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE1E2.tmp	success or wait	1	11DBF0E	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	62 bc 27 fe 61 d8 d8 48	b.'.a..H	success or wait	1	51D0A53	WriteFile

Copyright null 2021

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE1E2.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	51D0A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	51D0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	51D0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	51D0A53	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	51D0C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 6936 Parent PID: 3012

General

Start time:	17:17:46
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpDEF3.tmp'
Imagebase:	0x120000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDEF3.tmp	unknown	2	success or wait	1	12AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpDEF3.tmp	unknown	1321	success or wait	1	12ABD9	ReadFile

Analysis Process: conhost.exe PID: 6920 Parent PID: 6936

General

Start time:	17:17:46
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6668 Parent PID: 3012

General

Start time:	17:17:46
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpE1E2.tmp'
Imagebase:	0x120000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright null 2021

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\tmpE1E2.tmp	unknown	2	success or wait	1	12AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE1E2.tmp	unknown	1311	success or wait	1	12ABD9	ReadFile

Analysis Process: conhost.exe PID: 6688 Parent PID: 6668

General

Start time:	17:17:47
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6716 Parent PID: 936

General

Start time:	17:17:48
Start date:	23/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0
Imagebase:	0x90000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

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

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	86A53F	WriteFile
\Device\ConDrv	unknown	145	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....	success or wait	1	86A53F	WriteFile
\Device\ConDrv	unknown	45	0a 54 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 3a 0d 0a	.The following installation error occurred:..	success or wait	1	86A53F	WriteFile
\Device\ConDrv	unknown	29	31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	1: Assembly not found: '0'...	success or wait	1	86A53F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	unknown	120	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 32 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	7328A33A	WriteFile

File Read

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

Analysis Process: conhost.exe PID: 6800 Parent PID: 6716

General

Start time:	17:17:48
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 6808 Parent PID: 936

General

Start time:	17:17:48
Start date:	23/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x7a0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

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

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	284A53F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	145	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....	success or wait	1	284A53F	WriteFile
\Device\ConDrv	unknown	45	0a 54 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 3a 0d 0a	.The following installation error occurred:..	success or wait	1	284A53F	WriteFile
\Device\ConDrv	unknown	29	31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	1: Assembly not found: '0'...	success or wait	1	284A53F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	120	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 32 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	7328A33A	WriteFile

File Read

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

Analysis Process: conhost.exe PID: 6812 Parent PID: 6808

General

Start time:	17:17:48
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 3028 Parent PID: 3440

General

Start time:	17:17:55
Start date:	23/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x790000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	D5A53F	WriteFile
\Device\ConDrv	unknown	145	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....	success or wait	1	D5A53F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	256	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 2e 2e 0d 0a 20 20 20 20 2f 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 65 72 72 6f 72 20 69 66 20 69 74 20 61 6c 72 65 61 64 79 20 65 78 69 73 74 73 2e 2e 2e 20 20 20 20 2f 65 78 61 70 70 20	USAGE: regsvcs.exe [options] AssemblyName..Options:../? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp	success or wait	3	D5A53F	WriteFile
\Device\ConDrv	unknown	232	53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 71 75 69 65 74 20 20 20 20 20 20 20 20 20 20 20 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 2e 2e 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 2e 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 2e 2e 2e 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or interfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	D5A53F	WriteFile

File Read

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

Analysis Process: conhost.exe PID: 1868 Parent PID: 3028

General

Start time:	17:17:56
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis