ID: 384233
Sample Name: zunUbtZ2Y3.exe
Cookbook: default.jbs
Time: 19:05:11
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

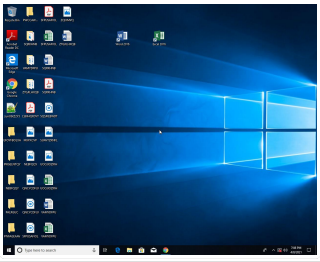
Analysis Report zunUbtZ2Y3.exe

Overview

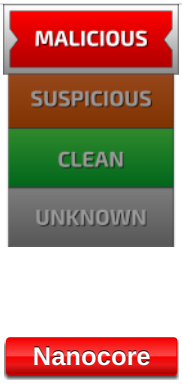
General Information

Sample Name:	zunUbtZ2Y3.exe
Analysis ID:	384233
MD5:	5ea59097fb7eed4.
SHA1:	919a1f62dc03584.
SHA256:	b4457b3e745bbe..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



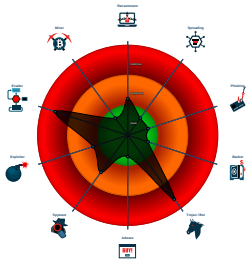
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM autoit script
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Drops PE files with a suspicious file…

Classification



Startup

- **System is w10x64**
- zunUbtZ2Y3.exe (PID: 4728 cmdline: 'C:\Users\user\Desktop\zunUbtZ2Y3.exe' MD5: 5EA59097FB7EED4AC42B666AC548D39C)
  - nfiuc.pif (PID: 984 cmdline: 'C:\Users\user\AppData\Roaming\22032878\nfiuc.pif' xaso.fhr MD5: 51663CBA5E7E841A0443112BF5E57049)
    - RegSvcs.exe (PID: 5660 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
      - schtasks.exe (PID: 5844 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp3E2B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 5896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 5556 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp4272.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 2864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 5036 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 4936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 1472 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 1440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nfiuc.pif (PID: 1380 cmdline: 'C:\Users\user\AppData\Roaming\22032878\nfiuc.pif' C:\Users\user\AppData\Roaming\22032878\xaso.fhr MD5: 51663CBA5E7E841A0443112BF5E57049)
  - RegSvcs.exe (PID: 4876 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- wscript.exe (PID: 4612 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\22032878\Update.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- dhcpmon.exe (PID: 2044 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 4808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "8080abe9-dca0-4fda-b289-40c56bb7",
  "Group": "FREE",
  "Domain1": "strongodss.ddns.net",
  "Domain2": "79.134.225.40",
  "Port": 48154,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8009,
  "BufferSize": "02000100",
  "MaxPacketSize": "",
  "GCThreshold": "",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000003.708352984.000000000474B000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10c2d:$x1: NanoCore.ClientPluginHost • 0x10c6a:$x2: IClientNetworkHost • 0x1479d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000B.00000003.708352984.000000000474B000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000B.00000003.708352984.000000000474B000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x10995:$a: NanoCore • 0x109a5:$a: NanoCore • 0x10bd9:$a: NanoCore • 0x10bed:$a: NanoCore • 0x10c2d:$a: NanoCore • 0x109f4:$b: ClientPlugin • 0x10bf6:$b: ClientPlugin • 0x10c36:$b: ClientPlugin • 0x10b1b:$c: ProjectData • 0x11522:$d: DESCrypto • 0x18eee:$e: KeepAlive • 0x16edc:$g: LogClientMessage • 0x130d7:$i: get_Connected • 0x11858:$j: #=q • 0x11888:$j: #=q • 0x118a4:$j: #=q • 0x118d4:$j: #=q • 0x118f0:$j: #=q • 0x1190c:$j: #=q • 0x1193c:$j: #=q • 0x11958:$j: #=q
0000000C.00000002.729421320.0000000000D02000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000002.729421320.0000000000D02000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 125 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.3.nfiuc.pif.4272830.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
1.3.nfiuc.pif.4272830.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
1.3.nfiuc.pif.4272830.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
1.3.nfiuc.pif.4272830.2.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
2.2.RegSvcs.exe.391560b.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1646:$x1: NanoCore.ClientPluginHost • 0x151e3:$x1: NanoCore.ClientPluginHost • 0x2e182:$x1: NanoCore.ClientPluginHost • 0x15210:$x2: IClientNetworkHost • 0x2e1af:$x2: IClientNetworkHost
Click to see the 126 entries				

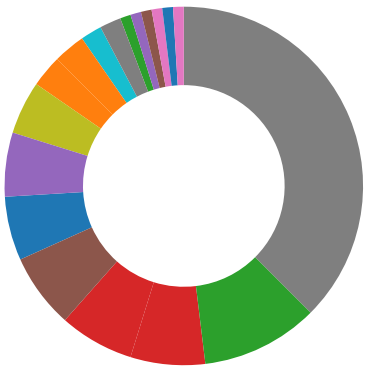
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

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

Networking:

- C2 URLs / IPs found in malware configuration
- 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

Persistence and Installation Behavior:

- Drops PE files with a suspicious file extension

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Yara detected AntiVM autoit script

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:

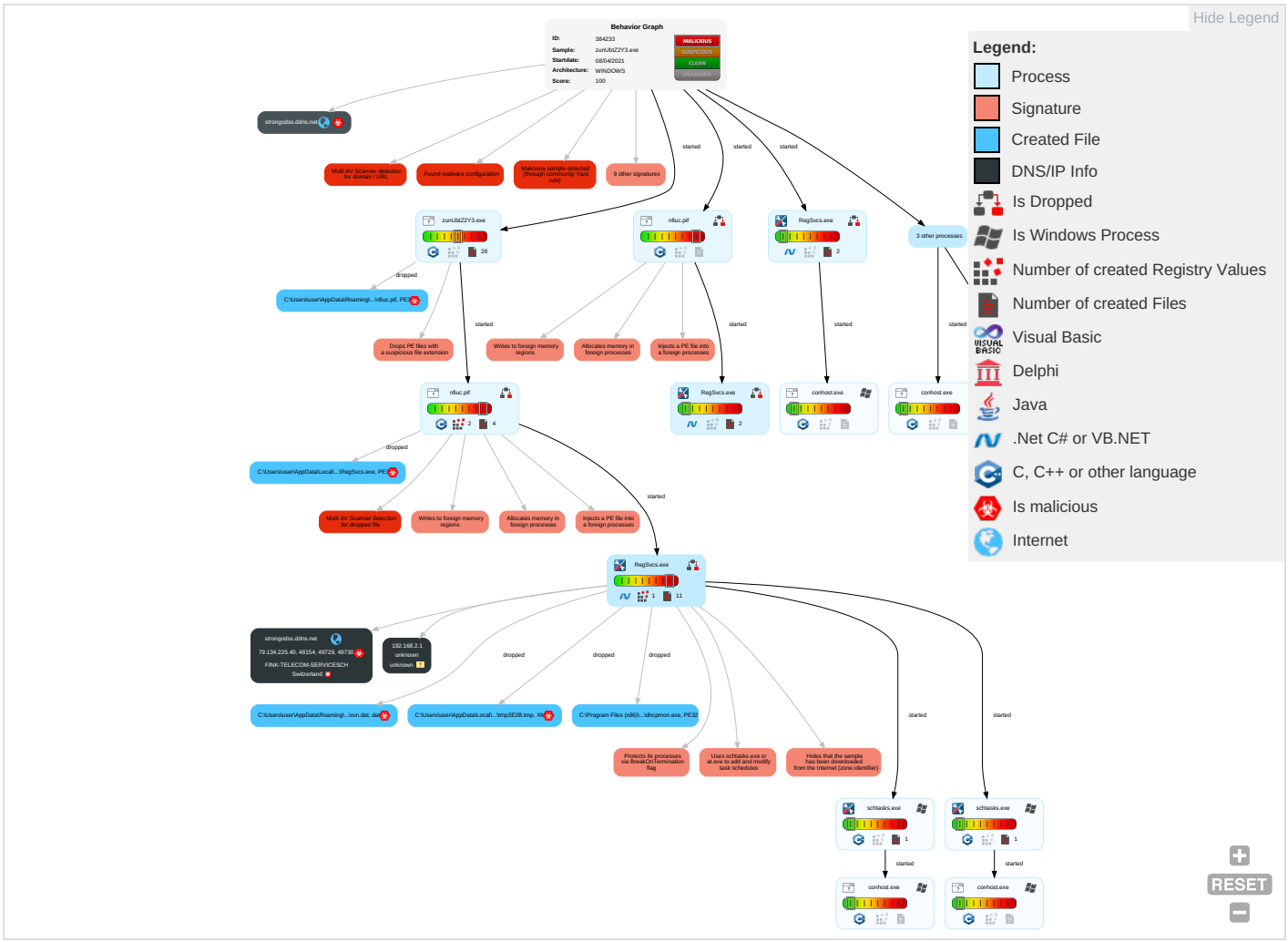
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts	Scripting 1 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1	Input Capture 1 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encryp Chann
Default Accounts	Native API 1	Scheduled Task/Job 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non-St Port 1
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Process Injection 3 1 2	Scripting 1 1	Security Account Manager	System Information Discovery 3 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remot Softwa
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Scheduled Task/Job 1	Obfuscated Files or Information 2	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 2	LSA Secrets	Security Software Discovery 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Applica Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

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
zunUbtZ2Y3.exe	43%	Virustotal		Browse
zunUbtZ2Y3.exe	54%	ReversingLabs	Win32.Backdoor.NanoCore	

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\Local\Temp\RegSvcs.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\22032878\nfiuc.pif	19%	Metadefender		Browse
C:\Users\user\AppData\Roaming\22032878\nfiuc.pif	45%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.RegSvcs.exe.60b0000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File
2.2.RegSvcs.exe.500000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.RegSvcs.exe.d00000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://secure.globalsign.net/cacert/PrimObject.crt0	0%	Virustotal		Browse
http://secure.globalsign.net/cacert/PrimObject.crt0	0%	Avira URL Cloud	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://www.globalsign.net/repository09	0%	Virustotal		Browse
http://www.globalsign.net/repository09	0%	Avira URL Cloud	safe	
79.134.225.40	0%	Avira URL Cloud	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
strongodss.ddns.net	0%	Avira URL Cloud	safe	
http://www.globalsign.net/repository/03	0%	URL Reputation	safe	
http://www.globalsign.net/repository/03	0%	URL Reputation	safe	
http://www.globalsign.net/repository/03	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
strongodss.ddns.net	79.134.225.40	true	true	• 8%, Virustotal, Browse	unknown

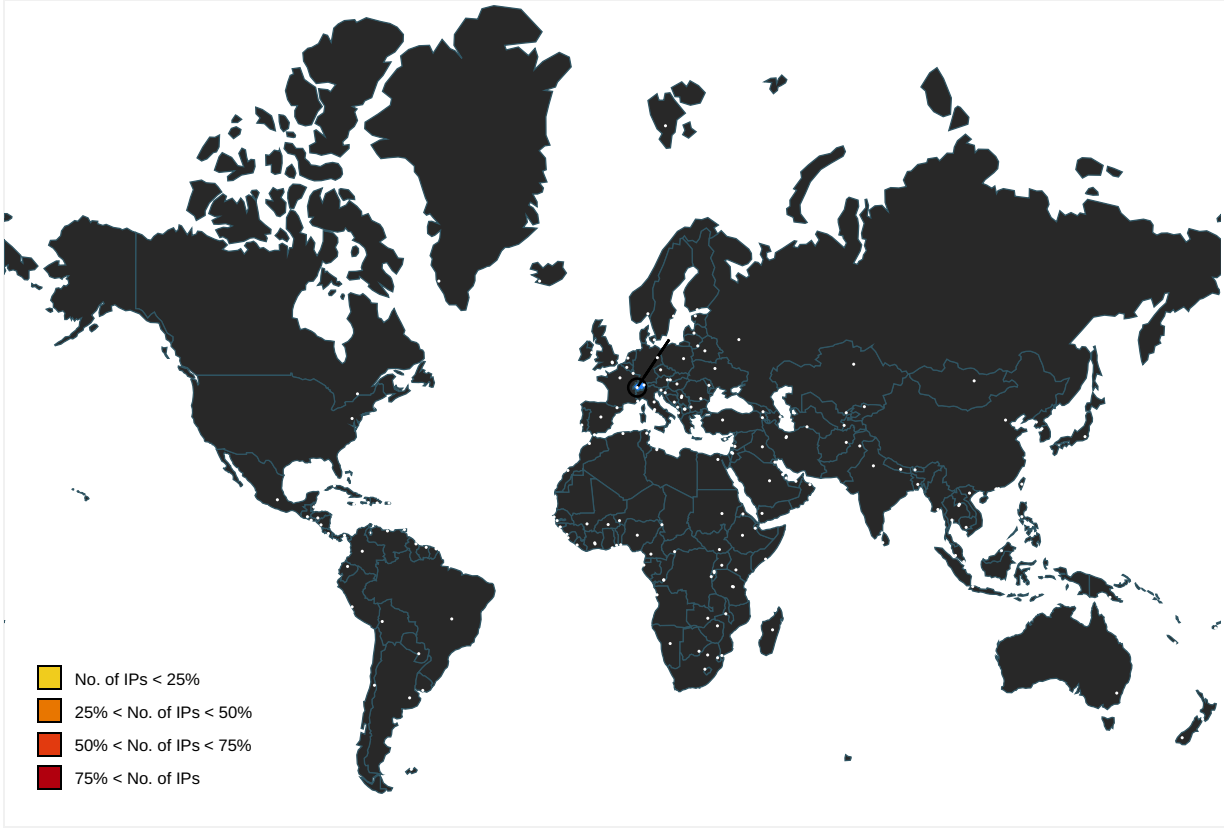
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
79.134.225.40	true	• Avira URL Cloud: safe	unknown
strongodss.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://secure.globalsign.net/cacert/PrimObject.crt0	nfiuc.pif.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://secure.globalsign.net/cacert/ObjectSign.crt09	nfiuc.pif.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.globalsign.net/repository09	nfiuc.pif.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.autoitscript.com/autoit3/0	nfiuc.pif.0.dr	false		high
http://www.globalsign.net/repository/0	nfiuc.pif.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.globalsign.net/repository/03	nfiuc.pif.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.40	strongodss.ddns.net	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384233
Start date:	08.04.2021
Start time:	19:05:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zunUbtZ2Y3.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:	16
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@21/35@11/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 35.9% (good quality ratio 33.6%) • Quality average: 78.7% • Quality standard deviation: 29%
HCA Information:	• Successful, ratio: 52% • 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 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.43.193.48, 104.43.139.144, 52.147.198.201, 52.255.188.83, 8.238.28.126, 8.238.35.126, 8.238.29.126, 8.241.83.126, 8.238.36.254 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net, skypedataprdcolcus15.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • 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. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:06:13	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user\AppData\Roaming\22032878\nfiuc.pif C:\Users\user\AppData\Roaming\22032878\xaso.fhr
19:06:19	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\RegSvcs.exe" s>$(Arg0)
19:06:19	API Interceptor	922x Sleep call for process: RegSvcs.exe modified
19:06:21	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
19:06:22	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user\AppData\Roaming\22032878\Update.vbs
19:06:30	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.40	cJtVGjtNGZ.exe	Get hash	malicious	Browse	
	3aDHivUqWtumbXb.exe	Get hash	malicious	Browse	
	fMy120EQiT6NaRd.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.394792.29952.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.578.18498.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.DownLoader36.32796.17922.exe	Get hash	malicious	Browse	
	HOqJcenF6O.exe	Get hash	malicious	Browse	
	0I2ddZZKv7.exe	Get hash	malicious	Browse	
	Q2BZ01fmwK.exe	Get hash	malicious	Browse	
	eO769dBnEg.exe	Get hash	malicious	Browse	
	compiled_report_2020_xls.exe	Get hash	malicious	Browse	
	all_reports_compiled_xls_2020_contact_details.exe	Get hash	malicious	Browse	
	9dAVqCPNyn.exe	Get hash	malicious	Browse	
	M5NwREJ2Yc.exe	Get hash	malicious	Browse	
	lyrvDJCi1i.exe	Get hash	malicious	Browse	
	FUyv1AeebX.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.6124.10543.exe	Get hash	malicious	Browse	
	U0GqWnTbUO.exe	Get hash	malicious	Browse	
	Clqf4jiA3N.exe	Get hash	malicious	Browse	
	dUWLmGj0PC.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
strongodss.ddns.net	cJtVGjtNGZ.exe	Get hash	malicious	Browse	• 79.134.225.40
	3aDHivUqWtumbXb.exe	Get hash	malicious	Browse	• 105.112.99.199
	fMy120EQiT6NaRd.exe	Get hash	malicious	Browse	• 79.134.225.40
	SecuriteInfo.com.Variant.Bulz.394792.29952.exe	Get hash	malicious	Browse	• 105.112.98.171
	SecuriteInfo.com.Trojan.PackedNET.578.18498.exe	Get hash	malicious	Browse	• 105.112.98.171
	nq0aCrCXyE.exe	Get hash	malicious	Browse	• 87.237.165.78
	73SriHObnQ.exe	Get hash	malicious	Browse	• 87.237.165.78
	rb86llCYzA.exe	Get hash	malicious	Browse	• 87.237.165.78
	uB8OTxUd3O.exe	Get hash	malicious	Browse	• 87.237.165.78
	NNb2NBgsob.exe	Get hash	malicious	Browse	• 87.237.165.78
	cp573oYDUX.exe	Get hash	malicious	Browse	• 87.237.165.78
	Y5XyMnx8Ng.exe	Get hash	malicious	Browse	• 87.237.165.78
	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	• 87.237.165.78
	M5QDAaK9yM.exe	Get hash	malicious	Browse	• 87.237.165.78
	TdX45jQWjj.exe	Get hash	malicious	Browse	• 87.237.165.78

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	EASTERS.exe	Get hash	malicious	Browse	• 79.134.225.118
	LIST OF POEA DELISTED AGENCIES.pdf.exe	Get hash	malicious	Browse	• 79.134.225.9
	AWB.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	AIC7VMxudf.exe	Get hash	malicious	Browse	• 79.134.225.30
	9mm case for ROYAL METAL INDUSTRIES 3milmonth Specification drawings.exe	Get hash	malicious	Browse	• 79.134.225.21
	PO50164.exe	Get hash	malicious	Browse	• 79.134.225.79
	Fast color scan to a PDFfile_1_20210331084231346.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	n7dIHuG3v6.exe	Get hash	malicious	Browse	• 79.134.225.92
	F6JT4fXIAQ.exe	Get hash	malicious	Browse	• 79.134.225.92
	order_inquiry2094.xls.exe	Get hash	malicious	Browse	• 79.134.225.102
	5H957qLghX.exe	Get hash	malicious	Browse	• 79.134.225.25
	yBio5dWAOl.exe	Get hash	malicious	Browse	• 79.134.225.7
	wDlaJji4Vv.exe	Get hash	malicious	Browse	• 79.134.225.7
	DkZY1k3y9F.exe	Get hash	malicious	Browse	• 79.134.225.23
	hbvo9thTAX.exe	Get hash	malicious	Browse	• 79.134.225.7
	SCAN ORDER DOC 040202021.exe	Get hash	malicious	Browse	• 79.134.225.71
	Waybill Doc_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	gfcYixSdyD.exe	Get hash	malicious	Browse	• 79.134.225.71

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	cJtVGjtNGZ.exe	Get hash	malicious	Browse	• 79.134.225.40
	Transferwise beneficiary detailspdf.exe	Get hash	malicious	Browse	• 79.134.225.22

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	bank transfer.exe	Get hash	malicious	Browse	
	nunu.exe	Get hash	malicious	Browse	
	quotation.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	UPDATED SOA.exe	Get hash	malicious	Browse	
	comprobante de pago bancario.exe	Get hash	malicious	Browse	
	ANS_309487487_#049844874.exe	Get hash	malicious	Browse	
	Dekont_12VK2102526 VAKIF KATILIM.exe	Get hash	malicious	Browse	
	taiwan.exe	Get hash	malicious	Browse	
	SWIFT COPY.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	purchase order.exe	Get hash	malicious	Browse	
	Payment Advice.exe	Get hash	malicious	Browse	
	Quotation.pdf...exe	Get hash	malicious	Browse	
	PURCHASE ORDER.exe	Get hash	malicious	Browse	
	money.exe	Get hash	malicious	Browse	
	TT COPY.exe	Get hash	malicious	Browse	
	$$$.exe	Get hash	malicious	Browse	
	ORDER.exe	Get hash	malicious	Browse	
	PO-0561.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D(B42
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Joe Sandbox View:	• Filename: bank transfer.exe, Detection: malicious, Browse • Filename: nunu.exe, Detection: malicious, Browse • Filename: quotation.exe, Detection: malicious, Browse • Filename: GS_ PO NO.1862021.exe, Detection: malicious, Browse • Filename: UPDATED SOA.exe, Detection: malicious, Browse • Filename: comprobante de pago bancario.exe, Detection: malicious, Browse • Filename: ANS_309487487_#049844874.exe, Detection: malicious, Browse • Filename: Dekont_12VK2102526 VAKIF KATILIM.exe, Detection: malicious, Browse • Filename: taiwan.exe, Detection: malicious, Browse • Filename: SWIFT COPY.exe, Detection: malicious, Browse • Filename: GS_ PO NO.1862021.exe, Detection: malicious, Browse • Filename: purchase order.exe, Detection: malicious, Browse • Filename: Payment Advice.exe, Detection: malicious, Browse • Filename: Quotation.pdf...exe, Detection: malicious, Browse • Filename: PURCHASE ORDER.exe, Detection: malicious, Browse • Filename: money.exe, Detection: malicious, Browse • Filename: TT COPY.exe, Detection: malicious, Browse • Filename: $$$.exe, Detection: malicious, Browse • Filename: ORDER.exe, Detection: malicious, Browse • Filename: PO-0561.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(...~....,(....~....o....9]...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\RegSvcs.exe	
Process:	C:\Users\user\AppData\Roaming\22032878\nfiuc.pif
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D0B42

C:\Users\user\AppData\Local\Temp\RegSvcs.exe	
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....\|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]...

C:\Users\user\AppData\Local\Temp\tmp3E2B.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.103583470672722
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Yfkxtn:cbk4oL600QydbQxIYODOLedq3jkj
MD5:	990B7A403BC76992021F9FA8008904F2
SHA1:	42911051D889BC22633FB4EC99794202975260A8
SHA-256:	2C4DC85A9C8127D7F864AB718245EBC0C5B625C04837AC84E012429E956936EE
SHA-512:	C5FF697E356C84B83D18952A5EDA27E225E649B89F8E43BEE565C6DFC87B12D15D8AD0698C03D6915786120042DABFBCB11493E233B8B3B2742EE8C0C5E4A0 C
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <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\tmp4272.tmp	
Process:	C:\Users\user\AppData\Local\Temp\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\22032878\Update.vbs	
Process:	C:\Users\user\AppData\Roaming\22032878\nfiuc.pif
File Type:	ASCII text, with no line terminators
Category:	modified
Size (bytes):	134
Entropy (8bit):	4.980914870423424
Encrypted:	false
SSDEEP:	3:FER/n0eFH5Ot+kiEaKC5pPex1t+kiEaKC5pZEZxHn:FER/lFHIwknaZ5hevwknaZ53EPHn
MD5:	C81CE4477142FA6E216A1742FF5D153D
SHA1:	95F3BE4488F26D0BED40A1447847C6BBFDB4EA63
SHA-256:	CBB4B78FA8848000511B01CCDD1EC3AEF39F9552856B859ABC94AFA384302A8E
SHA-512:	65C567656834FC42F0D3BEC85B062C5E46E56AB1108EBED54486D0E9C90E3EA6F88D178C923C2EBEB25ED97DB6DAD07010C79001CF10B8275E9E41D5C65D8E 5
Malicious:	false
Preview:	CreateObject("WScript.Shell").Run "C:\Users\user\AppData\Roaming\22032878\nfiuc.pif C:\Users\user\AppData\Roaming\22032878\xaso.fhr"

C:\Users\user\AppData\Roaming\22032878\btdbvndt.bmp	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	559
Entropy (8bit):	5.590049640287996
Encrypted:	false
SSDEEP:	12:M6UJPoPptZaSIVFJXXX3jlwlC30ADU+Tv/TSbgJPD:M6UJPSptwSwnXyrB+zTT5
MD5:	BAEC341B881A94D65AC13E41DD97957F
SHA1:	BD5DB45977FA111B4E1631081FDD091F9B06D30B
SHA-256:	31EC8CE62360246F905DB095A8BF7529DC149133B6F67CE1CEC6CD70BFCAB8D5
SHA-512:	425ED5648F5DA202C6C3646F4359165EFA5151150AA87D3BC6E276B19CE18F7EBF5A9296E4A8341DFFF5A055A9E50E19A24ABB422B5B23C8EE044FD7B148590I
Malicious:	false
Preview:	BFI31154Y8Exd190438M3BD7g0r2R70eM2D60LmtIxt3PhG48591..Ui2zv4r6Fsee9d8uqZpQlqT8DF4IFw38n2OAybT5qF35254g55TjE6..xd26f1qZJPJf7Ie2I3w2 55WqNbhHWY4HUqX775k94zl719Je04UfwN..ugo2804m8RU953Vz6Ji9Q6fu3VPxkx494SbBx3H1Au857OSsx4avd11ngE6N890eOdO6iWwO337lF2z0c0sxCFcB92tvCO 382ZTBR393tJEDb9fb6C51qA087M78z6QY9qk..0XRr9VL7x9huc602dab0w2u4vr3KjlDRP0QK237B3H3ph87i27DL83O9537lmj9s..d939hl0fQnVPOP9U743323i2Q Y27B8u1c340p8v2UWRiKHb49c213aze951b90gpR3678pyeSr6v9P5X36766O..vMNi519gS381U5032zoY16b1472b3y11U0G32nM34Gjxy4zV474d3VyNQ66Bc464Ki6 AU39R36683221998093SfgmPp7608793t187V..

C:\Users\user\AppData\Roaming\22032878\dnxuddwt.ppt	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.405974627564001
Encrypted:	false
SSDEEP:	12:LLTIGOWK2eKGIHAb4pN/QfCT1G49RMqpcDiO0:EjWKvKfHAgNY6T1nFpcGO0
MD5:	AD0538F8F9BEB5F33E161A05B15C877D
SHA1:	1881300024085A1930A6B2B5D824A2C19E6414B2
SHA-256:	3FC4C9B80B7A6FE0D976EC37A05494803E2BA8F031C6D519B01560E664D366A3
SHA-512:	FCF4C424073D1CC80AE26784D4B6133ADE3A294504B00B9A595D7672EF4C4628128F9A884F2FE1C36705370ED00DDC93F0D2A9253CE669551816AC572008F0F7
Malicious:	false
Preview:	6xAJOA6D4434LDiE2R0BR3C87227265ZdKsRoWg2Df01m492c2jAO68Yk19407C03F79mb3X1M24eVZI84J18K0PO648C99b06X5xU461T484b1v6JD0260fH35f2lACOy QECV3..2T6p60i3r1oW01rDb351C5c39N2lB769Z8g03VW0..PEXTY5911wer4fl2s4550tX101Y7r36G7h8Ou6D6002n5F83B11g477Wi8rl5jwB03138C6v2c6Ig2006 N1I2mxfk1Q2B79wsi0bR9l7W8L8S074XOde8xdhi0743M8na93c11F8924..Fi9Js73U49aw17H11080O5v1xR1Oa01ch79404l93K48314..15Qq3Cm362933653Lyq65 3A514D05bsb936E3G3h865kZxpqp727B4M896106ozhKwkb5gDl8LB47SOTA0l8875b2RZ43WK773Yk3161B2d828ut73WCRv1b12p6466326ikCJ6u8i1X8y58HKfkfKS..

C:\Users\user\AppData\Roaming\22032878\eseh.pdf	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	572
Entropy (8bit):	5.456380250671965
Encrypted:	false
SSDEEP:	12:e2/NvUgY4/WBDY8CIc++k3pxOQKq6dsXmBhuVsb:e2/NHYE2FCvFk+PfdZ
MD5:	33E70D61804B626A7EDDCEE87A50DA87
SHA1:	198945C6DB88B833EED534835F6BC025E6A71DA7
SHA-256:	5DBF289E2085BE6771F0F280E2BCACF93854DDE58D19CA96C3718211EE6E8448
SHA-512:	0F87F2A271BDD1916C302E4F37C11AF7E5916B203F825D1896097C4B63547C2D01A42CA7B762FFD219CAA979F312CF74B71C22BC2ED0AADDEEB1BF163991E4F
Malicious:	false
Preview:	7d63I6Kx6MWfF2R6363p5n12Qw17W7292j44c8Q780uaFPoH8755GKJ7B778146Q6q617c7VIZ87YSE43f1NJ2M4FDkF6086430QYyZk433530EdYQ6s3Na1 v4R09U90VK99j8774Z758..o51VdSPs112l17t33a1R87WgM6fvhZC80Q2FtAKZXJx891290I7..n37q5Ttm1R5xiQGRUNfF67052E8DX7z696049p77Q05pPY0sVZiR93 ycPb639X5n1oS4..Kzw757vR99ipV392yUhCe8ax6T5UaS05xSq3bd3572C1H077g35hLq45xB0s4IL5RFs71y3iG9w1rL3..567q201p6P7sRd35821mQ782z670T6p5x dbzd3bM02d42F3mC54R2928117MLe74kd1ohZxJg87x969uup8e6499m10..2TJ315B5hh7f5Pe8j0x3mINy92j6566UF9142Ae0ML5h6M782ZGVj88Y9C3a9gT2wh57g3 k3U25461b3T995ySIvuG04200AS7af71sX1965SS7U6bT4Az049hm9L4ZD75..

C:\Users\user\AppData\Roaming\22032878\fbekvf.mp3	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	532
Entropy (8bit):	5.50565576271383
Encrypted:	false
SSDEEP:	12:b9hcDkVJKY8kVT8lYSIDnwYghb1ViaEADd51M5KeXJ:HcQzKnOFIxgp1VWAhHs
MD5:	2950A51EBF5FD41C3B90A189699A5DED
SHA1:	1E19E946CC40011B7151C211436315D3701BC971

C:\Users\user\AppData\Roaming\22032878\fbekvf.mp3	
SHA-256:	E1550F370DC76E180F02AA73DCF1D908E14CC10B4ABA8AB584BBCB123D4DF7A7
SHA-512:	AF304E6670515BC3CF737A28778361452DF8993E39EF59B10E13C8AD67BD3A704B38F1FFBE327D20F20DAA23F5AEE08B91BA46D8B5168DF5E68AC73450A2079I
Malicious:	false
Preview:	3Z3l845782I..h0Pf96401dEPDd083891vz350l8881Y2X0Ol88SG7ZSTu360459x1Vshf4K324bJf3Qpj3aoVp15M49lnhy0LA5..R664qeXfw44t86N36m550nY53OLM YQ7Q6R336a4tr8I54VCq5..c8275yo6863a5I22dtzK26ZOhu8i4974m7C8S62D..96iKm99677CG8I9909EO975YtvzLR592l5b714J9e0Mr41Vb599KMRrU5J58cEIVQ 0W40zFw2d105dqaUI0D6E253dEZ4bB6W3A1j6Jn227JN7T4E77wF2D19U7ees26A8h54409nTadg68u..8m7n43Qg3Tg0gvb2L7G8vM075wz8V2an4Bj2bS2..OG7Wr8fM 79F8w4s2Y0IseXqQ01g4534445O86CLA62A671uWfG7uq3q08NDC7S25D1n8t39t55A1oWzAjZl46hGt70p4c2RIUE9224e5dfUBVg877WiV6cs5G38Z40c8mqs6lu0394 i815201y31..

C:\Users\user\AppData\Roaming\22032878\kuodio.log	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	583
Entropy (8bit):	5.52430412603607
Encrypted:	false
SSDEEP:	12:UFz4xSMqGXlcJ9znBM5GS8DVmT4k1tHSZUiJBFvgWAzNfiMiUIzRNAI:a4xB8pBM5GvJmT4OQf5AxqMiUIzROI
MD5:	604A9356E128FD0B739F8F9A195BFA14
SHA1:	B670B7377CEFE687441689BBF18390AC011BB3B3
SHA-256:	524E4FE024A8E1F68FA315625B6CDCDCB4E243F431F328BD48D67977276F0904
SHA-512:	0D0F5191CCF4691F1D3FF558D551796695B13D3F6AF8CA72108F131F8FC96FD1E01F3A73595F824C6B5FCA605B3B304434D045BCE6872EDF633D840A5668E12C
Malicious:	false
Preview:	36JlgAv6Rq72ii5..2Qd31t1432K660t1qe3304KVe0M5xwd695u3cq1I9hb5p71TlfQtH0aY370q03025VeTs48OD6T4vG4QOIuT5q74bzTY4Q00l7..B0LZ251852l2M 289vQEz0BvH7EFqOX03C26BoAV0l9nk9VRHXz37796A2uiNO8SpS2XBE..57582U4e71GNuDI8w7119C193V8U2..6lf4510Y0V71sw7H4kEs2Ey220f8gV7xcG19n3237 EH309lkg99KpmfLh3Lnn19Wv3Rt52Z5U6583p3gPCvR82WGST..Rcl5U574qJn50Z5F7xqPx5b7T921ZC090983QEV2RMz1ud086bZ6E13T4DH3wfOtM3U4324s4J37OrW efsY4841gd80Cy4660hV2U0o790L1biQ2fv..RH65M27DMT1pw508876U5122GAR269NE4463n8823D7P2413yU868vkYhgspc34ZNs39p4I135C5Ts8809u6G8a5y4sVW 5tPmL0mT39wZ1325p50114pg5HzB265T2441Vca8E33F1fl7L824LE98jjIA6..

C:\Users\user\AppData\Roaming\22032878\lojmm.bin	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	547
Entropy (8bit):	5.499043982252092
Encrypted:	false
SSDEEP:	12:azDCtiP4Wo1NSbTSXzA0XEgds26u5HLBSWfROnQov:gC9WNbsAsETRu5HLBSVQy
MD5:	8FF06F5C040CF50CCD9B8F1121B0384C
SHA1:	82A63F1862169346F605467A45CFEFA8E9E0125A
SHA-256:	C372657ABEEE57A4524E9DC9BC4F464B08D697E313E18C00D18524FF5103F74C
SHA-512:	627644BD0C2AF74F50EFABC4ACDF0E44DEBC6A09E1BFE9644842A70C29BD687BB6DC073A63086E15BC529F7346D62B499FF77D7A348B4E16A1AD13D422A44D 62
Malicious:	false
Preview:	48H9326y1g99359d51a933G2kmIq0l935327Hu21tw7YT374e05yIb4384B3834041D5842..49sRS711O5thlv9DN2At2apZ6Rz2q6r2R027W2rGsnm086577x2Sd5UOo G7mSagr08g2fNyC5v1DB7lpAxawq9Mi59RU16M15L0707VkL3E614GE8M4o5P17MzN24TW..Bn2Yp408p7yN..9Uc8IVtl7a2ob88p7T609y4016k227k569A70o3X62Re Z94Gb7lN72or49wC0r8c2ueQP67L4aIi7j4uIw5yrUlvb6j0BDQP092g6Gr9Ggac07J8w419LUNLH4X924cp96y7i833c3r8P1v247..4KDe10m4mw8F2h79Ek701gw9Of b356X941MHR4b6X..36WwJ3on0655Mx5Ohj97b90c90u8r1V53UD1m..53s1zs4502U3840aT76eo8da8..45j0eII113QW079T84NTDc144n1g01AqGkDpWZD4g9Eo52f 78BK4184cV594Hta769mzf75K..

C:\Users\user\AppData\Roaming\22032878\lqjmggks.ico	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	485356
Entropy (8bit):	4.382161397132145
Encrypted:	false
SSDEEP:	6144:a0AXl49W0rfr9tfam7kPcC9jdzKGb0KjcrKUIMgZIKmenPRyiwmF:a0AiA0brfaRz9NwZrKUIMgZIKfPRBws
MD5:	C5C34E7F2131E3E95F01D8A2F56DB3B5
SHA1:	2643784461E9B597FAA0981F13D80EC80F121A7B
SHA-256:	A499D02518697CE0191BFDD7D5C9F82936ABDD6252DE0860D4236B1A09BA0EA8
SHA-512:	0CF82DAB5F26B5C66BB79436BA89F8F5F8CABD1F451B8E4205322D250CD2188A7C8F50EA83E12933A0F44DCEFA95C313AB4E05CA1CE5908FA91CFB1B7C7A2F 2F
Malicious:	false

C:\Users\user\AppData\Roaming\22032878\lqjmggks.ico	
Preview:	F96c7V93z3E9xlB6an0f0Jk6dnd2zNdGY9B..x6h13A2N15f7tVlJ4zqwi43g6jqw8O8l35u97jxaK8tw63Sp..U735c8O18zhlx0aj96Yq1K426j3Sv46494QM78Nvo0A6r05Fz5uaE1930..iZ2DD5u2s8j1455t62l9L47t3C7G1s2Fj4b3Pa6f0pIDBLgApwY5FV9WWhJx9uS..t60Na04xd50322077gLdfHK..0dk578OkYOU68EL6Eh51R17l6SI2P40H67kG68i6Q7B0pX3lTM490EYEkq446NXW5kS682..c1bP7Rh9xn56773F93cI9tHD89SQex17S92LZU2vO3w445alG35cX700246H84o5a2924..853cVJzJ9r4e699UC61216RVaZ1gJ19E16L1f17D0460y28CcE6TRT25dvHp4oL933e56Nl4F7U10LVxd37KEysUjA6..S87o05Pk33C921H7S3549sP34583YC..9uWx8pVewI975F714JXQ5t492z6m9cAN4f57a4j5qZ8..7C58T097RzwZnD262ot1JlK0DH1254Z3WjKosk1ycUikw75i744i137NX4N6LT1063NIaVhSrGrH1U65d0J9N47P..5EO7J79J5NiS8C6Pr355l712yM77BjNh176K6067tn7HA5NG23PF..p185Bzr36A3HIRQk81UJchw0fJ54z7qoOWy..h6VJh35O3Gw60s7FlizB955Sk2S83HBoak5r3N29Ne2V78zAO400lo5204Z1..3Pbp00f4S3M8V8421l4PGcS0005AsOz2996dvPY1Xc0o0Kut4SPkH41PboWu1U41Bo04hY3633LVy5dMGS9..K02b76A4BpcFbq6ZSxx6erfv7CDig877e9RpeiYaE5RgpW4k7O8wl6db87O3V2O6Kb11L2i6G2y49mVw5d2e8j6A230..SI4A1Yt67g3zlj2IG3nc7Q1003nQ5Q

C:\Users\user\AppData\Roaming\22032878\nfiuc.pif	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	664816
Entropy (8bit):	6.570907651581873
Encrypted:	false
SSDEEP:	12288:eBzZm7d9AZAYJVB7ii/XAvKxRJBnwvogSJ4M4G4ajl5DGDt2:wcneJVBvXAvwRJdwvZ5ajl5DGR2
MD5:	51663CBA5E7E841A0443112BF5E57049
SHA1:	724815819609CE9AA6674D16C91B2A4202583F4D
SHA-256:	B5B9D67F36E0B504692B8DD25EFA62400F7A50D623DEBC849F42233C0F5319EB
SHA-512:	58EA9D766112650ED84E8243E464FECF378C5BB2F249093965AE65395ADA1CC1152F5DDFDE442B8511D2B943C46A9EE9117718E1AFB4A30DE32DDC7AB7AE1C8
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 45%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1b.....P.)....Q.....y.....i.....}...N.....d.....`.....m.....g....Rich.....PE..L....%O.....".....d..... ....@.....p.....@...@.....@.....T.....p<.....c..... ..D.....text..... ..`.rdata..... .....@..@.data...X.....h.....@....rsrc...p<.....>...R.....@..@.reloc...u.....v.....@..B.....

C:\Users\user\AppData\Roaming\22032878\plee.xl	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	573
Entropy (8bit):	5.499991624458592
Encrypted:	false
SSDEEP:	12:RaHZ6e0gr4O9I7yssHpgd9YTUlIeoFz5z04SM34arY8/T2mkMX6:RaLXW77sJgIYSeM7pjYYRK
MD5:	48FE7BDA227A704E88CE662329BE36E6
SHA1:	EC4BD966BBADA72FFE5E21002DCB5107FCBAB1CE
SHA-256:	692BF4E2325382E6BC40418806CC450FCC3163D861C37C7AE9528A412555BB73
SHA-512:	C0B84C62A25FC3F692A0D79AFE55811EF95657A9476003911C3CA9646DF315371CF11920DA9A8D70CEC6EB34D2D7D919D02211C9634873F6F88161ECC999DB5
Malicious:	false
Preview:	gQ09Nuz15L7138b..YJ2Zan82YA37Grdz78Of3Oz10x005jT2022l5Ua5gG2QrJ2ra14w203JQ1158531053x6v4Vs29uq7121709f3P89k812l1p3D430TNC543..0Hk4Jm1344Uy623wU1bV94rm27q8ZU2w478AE27GMlCF8a044W9m04GcPM70kQ2Y70wD2r553v..7f608wS80LPx6o8coA1ieRg5eF04u7u6BX08Kla1d36CCo2hO5f28Akc3078ys47o18M..bD3o9988..M10kSF8TK23br20qno5q0AI57R97x4Y4..Y2DP7E9H80h05fS4e3B025E4X76tT0Tb2L475VQz5..4yn83hEZDtbk6Apq7t3937107dI4f6Y8qdw1dC34410F2l125v64U7EXjtG3845GB8gU96k62MRLK..Cml272NiH87k71Q53405Vh9Ue3i08986zx43tvm0k4x4L71RrX9nlzk98fKhSnnx7419pN17H500Zy22Deejp31vxFrl4934XY7kQn5V5aZzY3523OBrzEv525507747wuj87..

C:\Users\user\AppData\Roaming\22032878\poqhjae.xml	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.430182663949951
Encrypted:	false
SSDEEP:	12:C20k3o0JVlwOZTiiT8pGF6Z/Ofup7Uf06ahK4SI/UHWTg45qz3VbmbwWESbWKmWA:C2ZjlTJ8pGF+/OmCXas4B/a45qz3VbmK
MD5:	4D6C493CBB6EE4AA30D1D3CACBFAB719
SHA1:	0F3AA84F48D3034831B41DB70B97B543AEF09671
SHA-256:	A9B846EB017D3625686790EFD741EC3E1EE9C9B7F0E589C7DDE8FCD2C60028E7
SHA-512:	0272556F9B46C928A69F94FFE1C2BF99BCEEED5E6901088602413D8D83B1C3BC1A3E7C3472463BCA0E27F308D22B491680A6ED8F5CD8E4AF71A38B997FC6FA9
Malicious:	false

C:\Users\user\AppData\Roaming\22032878\poqhjae.xml	
Preview:	16aOQ7S05hG107W95U98662Y942vJ89E9i87601mCQ85j2eP3F01h0317l5dqh91baH..N8eu6O20569zj7BvtAn3DGMp7IfVvy177741YJ2x3Ul368Trl813f58AV8..LV613Y78a5i31H7zLG3537M05w7dr7157tD680J44X0212061J..2J2070mH1838009vSIDVIed..50Sjbz6638WI499jXiVI281pbcMnFv70f65l9y66c3f79x7H8QAtAW5814783q76Uc7o..k6d7fAGBbJxKJ0I33578R4392d843424S32827pkNn1X3RO21uEx89V1AcNN1EaovR..8XQWFCCbf550Qu38Vfu6a48703Hzv008d34W58K06qiT43XUgSD72Ud763S96382C16x91yb38hN28iFC5405550b638..47C4W66G5fJb11805sXE5ek00O3I821..345i7a0d5WAu7f78a90n..228ii14Y40il2dZX3AL0R0F2X631s67LnX4621RV61ats6L34F1RL69n1970VX046X54210ZuUbY63v6pGDK1FpJGU9BN8S4C7X08QdXAT6300ZZI74O541tl3D3b9rPZ7485kb77K67omMl73Xm7w8n710nUSSwF76KqU318..

C:\Users\user\AppData\Roaming\22032878\rkevqw.txt	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	559
Entropy (8bit):	5.522582367791629
Encrypted:	false
SSDEEP:	12:TpFIKVNQKFMX8Ex1fP68zDARMrOtMdrtL+uy+ahky:TpOK79F4hDfLzKMr8kp+gby
MD5:	A183CDFA1098B2EC3E6B8E310FCD0BF5
SHA1:	679C458CACFA7E8B54ED146CC73402CA64D79FD3
SHA-256:	A3D37F1F39C36630F742778251270704AD1B5C5F7F688778920F29E82A51C631
SHA-512:	AF9AA237367FCAA8ECD571D533292C74D6F05C2ABA741DB89BAF7F0AE72286A186D7D6D37BE7B6F1EA0D060974492CF05FFAD37F0DEE0C0A39EC883CD67910C
Malicious:	false
Preview:	57Zpt22j03pkV4rC11kjZ90R71Iy856B0ZR1iiEbTXH8bSudM305RGB8W0BRrA578VI47313k118uFLj4440jSF9z395L816543A25K4s6JM78r9MXf298RaGY0TIWN56..80347VB8y3zIwm45F36..85QK3Id100C..r9407721835c9M044P817GrN3j59h5221Xv..PFn398K4t7l8s47f591W72q7uSiz0J7MeLh505v00J5tAPY988jlL..5Q77R1r6xSkl75093cJhjrq3Ne3473o8mcaSuVR97363D8euan5Ud010NDZ3ifor3j63Y0064Nh47GJA2y2tHm94Hz4d5E..37Q8ipe037Z52u58MPu84056i0Z99yg0W679r2ar9V54HY0nQ9759WYWlD5uZ56715pTbLLb0H5O4r1Rx99ahigA2..4Ku3i2zEXBZ8K6Q3Gy7YZ5MeyK1g64Z9QE2FUf96Lkr87QgTg03UA9U5F6Y3w82N7o8a6wMJ15xUum615837zN99R7d5o267gFjrk3E0f0218ZMlQ..

C:\Users\user\AppData\Roaming\22032878\rnpxxre.icm	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	550
Entropy (8bit):	5.478420245483416
Encrypted:	false
SSDEEP:	12:jydRJFLqz6Bs+nww++yOqAdBC8+BBuFGU9u904k1Rz3i+m:wRJi2s9FBkBC3et4k3Pm
MD5:	4889DDFC0C45FAB0B2E44FB4A306E9A6
SHA1:	1183C9BFDC5422E4EBCE88C19B6087808A4B312B
SHA-256:	CBFD442D9A41B4746AC363EF4F26DB832E928E76353834BC0C5FFCB77832EBFF
SHA-512:	F61537698859E19576FA01BA0C2C13F12BE93C4A942BBC5737C2DE2BD176428A98B6375FACDB76BEA29CDC5A2BDA02350A6571EBD7D8E0C4F45EE1FE33218AD7
Malicious:	false
Preview:	29o29u2HX8CpS37Cv65aFR5QU15F93256XY1z0pCC4Lh03Zk9H85dm1z2Qu..17e2s5wIa3O9TPN23YxH21cYuWpRwB3Nd4T5l6311x035k29EYc8r28O7q5q38Sh0J5b..F7vnT2K9OlGxw..L138QD0Q52pV1851PUB1280KL4Z913738Q48o4B70898mKe29Vw0pK89uI7537vC9771r534iH93tb7NY8Q5k6hm88Uxy7G05e1P224yw7BgitOyRkaV263J3z3sNP4..Mx36gL0g1p3VC8Zk760t87Iy4kHO08644jag95v4v3583c35948u128W39T067796E..24HeXjTr171ULl8D7ct4015zX1e6548h9X8t4410N0SU9uNc51R13bgR4P57WAzE260Is112T060549140023lx74wHr6rX5r8t8pYS30yr3972B88A02186oi959R5122..75Cs97YR70Lz0495G6524Uq979s1as7pp8lYE6dGlyx9Mn3tz1A5j6q9F6qNA7okZqY0jW7rm..

C:\Users\user\AppData\Roaming\22032878\tejpjdone.dat	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	520
Entropy (8bit):	5.456583021020405
Encrypted:	false
SSDEEP:	12:mbAILbQBRciICyX7Zsc0XyvH80SnKuzExcRkRaS1ax3eQgDGwxLJ15:ILbHidyXWc0XA8pnXzQcuR9U3e7dJ15
MD5:	53EAE0D6898062E81046FDD92DD7912A
SHA1:	D4CAA9D47FA27F439D22A45A6B75E53274430DEE
SHA-256:	323B98DCB2B894092EC267B5616A5D05CAB4F2795BCB8333E2A7163252BA13EB
SHA-512:	F47AB84732E7482EA10FFF850C4578348F21A98F624A8594E15F8DFE3BB7579ADE91BB20674D4DC490E78A373E870A7A0A468A47E6CA2FD71BEA254AA5DA51D4
Malicious:	false
Preview:	13028J9C2G09RW3H50qg4QL110U26fMTvVfM6886P5A11..m1749Hp9oagD7805M9619BU..7h974G842ZNo18aV9ic1W21ZB0NY8yX2M024A4E4qLJy5BJ04Em6yx164f12LG5A1j1vv328fQ5r5Jb4g5j9750E7R9XYaeWU247OS6plc1679VG..xy1e44eTS43u52T14587mI4MRpB4o00f7uWF957sqOCeXad237460u26xkT9Z25RS0IFLGA01CX8q8TVQa638y1khcM32RQ97375F1X4Z8sH9..cHE4S90v20qD84Z6rO340Nvr4R43CTuw6wA633u52781rbo447yPC7AOh1M496Z930Drp9NJEn24T1303D553LL43Svk64826Dos94gzDr387063iB84269gZ91qkFlyF881U38w5Mzj09..Eb0g371FK3M7019N886q7637e7D60X468YY9067mXDt3x223p9wY78Y3C6167s8Owr675w4NUt199..

C:\Users\user\AppData\Roaming\22032878\txum.exe	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	575
Entropy (8bit):	5.526129708681296
Encrypted:	false
SSDEEP:	12:nGXtVjd0Wk1KObRrHnf82p8Skg8iniHqeJsLKsnTkYO+H32GRUZ9cEuBUfh:nGXtVjdsbFf85g8iniKeyL5O+TRUZylo
MD5:	F4405478D69CB8C97303399BA69354C4
SHA1:	67555AE21178B5233AC5A3582AF6AE163F4CB531
SHA-256:	E2173B7F096A160EB049F7D31B939CCA386CE7F6C1A3BCE6BFAF3BE44F026DFE
SHA-512:	357B87044E733F99736463444B79E055D06E8C407B1E7C2E74C49CDB9593AFF98B7E2A193896D62975C1FF7D9860792AA74D4A49FFE2019120DF8B758A6BEFCC
Malicious:	false
Preview:	JUZa1580659YZ7M5FQ7P6a7x527M4924e6J6811h442V92Df37h8g02wNo69o3..5636yDLuc..660Qg25n1e53z5C442tTAEbg6s5E4NRW807UT181QSYf56jUi4R7tcD eLa627NH7324i8A83KIdz4o3eP..8t7388Urs28F8xer3m8o72144ehxzzEI3lmXw794BypO02811w8J63FDA49wSL1570P31360cy3x89K10D6fa6w86g0y21n8PX0CzJ p1o13Jreu2PapIn0217ndKY1Z2ig8P35ub6Uj7It94MdQX83K..fE512f4sqhdkf7rIJ1a20G1C4Ln16R5oQ02mP15195609EC0Qh24M0Z75s7uw431658P9EY58Q6UK95 P1Kg31gtT8946CntdaT..61vp62wX66oW2F82BNW8Dp7u7r9f1lS236i1TYTr57K112Q45Wz5cnqM0j09m6txK8407c4E7..34B28NLfbMWO7p299cs45t41Drc65Exw8s A0JGO0F936c24Oc323JV04WLh249nsZl71azwj4W537xnnlm8AZm3..

C:\Users\user\AppData\Roaming\22032878\ucjondx.exe	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	503
Entropy (8bit):	5.411685378015985
Encrypted:	false
SSDEEP:	12:CvzQprZl1VRsjCbqfR7G8WJyku1aV5nqfXKbYFrdNXYIX7Y:BcQjCb6c8aEaVpqyIBlLY
MD5:	C75A9014ED721FB41E33021171F17395
SHA1:	BEDAC4FCB9E9C70764A4E977597A2CE026C72778
SHA-256:	7725496DA1E6CD5A0EC7B39748D1B4559D2DB1D100813B920E8790BE47985088
SHA-512:	4A07C4C7D497BB5E33B743D3776AF0B7732A01455320741E83E97928D4ED383D984DBD782DC94B703B43DFF8BFDFBFEF01EACAF2B515F66912F65B28DA48A3E E
Malicious:	false
Preview:	OjF0669rS6fen4M39F94e9iw67g7mEWRAk9Tb5P26f9S3e3mBy5lsq68dT7mwn5ma3417b3662U41231wA44bu7877Uin1949z17s5D..0T306t43e2r8OTzMYV3574iB0 981O4uq86Vg8f3mbA..tX41o4j3DcDQ1F9hn1A0l7711Pd79kJ9U1H0E3C8A37hu1Qy33iu2S3tE56..5J5R2bM9Re6dJ0d6F87o43n6346fW..N4E7x8336ZVg..q4bV1 ..v5QF1wTW6c058898vGUG60836Y7594701m9xA424DA6g9w3e4Nv1508z85VM0o9XA34XQHe514m..0ohe6u8qnBWb0p3b9524775281feeV592o0612HB6265mX5q..D 0B7I..7w6BO10sQpfj7b58X647n648Xvo15i4Jd4018QY31Gqbs172B906y168EE48I81018Je8jK6YQ94gUu35B71g38..6cRwm0s7r6Bg8D4G..

C:\Users\user\AppData\Roaming\22032878\vhcpj.log	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	566
Entropy (8bit):	5.516316428481893
Encrypted:	false
SSDEEP:	12:8uYNnG1JvdT5nhK7hkzwm9nSWI8xrW6vQCM6YHGD1i:Jq0vdT5hK7h0JBxrW+Qf6YHs1i
MD5:	158639DFE28B8CDD93F5F1A78B87EA56
SHA1:	09119918EBE955BEC813B17C2FB74ECCB5B3FB0F
SHA-256:	9BB7FFEDC07EF18132CB3EDB065DCAE945A4A139BE62479F19895368521211C2
SHA-512:	C195EAEC103492B36A01777FD49FBC0A4E8AB0571D64F423E5F96A96705158059D1523349092B2F3A09305F680876E3216DA52341CEB25028EC9E88333132803
Malicious:	false
Preview:	4ES4z22SfQiv5u64jL4a8dg6kh81851xEAFU5w173K58nAW03ZV9O19..5cbES03Mr07RZ5977Fa19LSk220m359wz99a7m4pU84743h2554mx9U8Xa4BLlzVKF1h5442u 9u3W4Jc1Otm88R125DtBJ5WT9..338Sf4..M9Ndr1k7ZMeZ8uGm2o8Dgp39C6q3Fl2xLx4qj1Yy0r1R7tREy486729639560A6Z3CWI4fC73x54..H8d0241aK4xKtV4J0 0VOz1am5W69ysy5423Cu3r1ahD9Zo79h10si5lQbM26vv6dF9Fa157W63l..x9aC2FDmG..5YZls4600290SM56yDN5SSv1QO02L3Ac678N2c3DF2ht49146t6LO3j4uX4 065f2..gN4GApe0vuF51Mv4Z4N14144M16y4c775pw10n3n61..NG8L3l692i44cG762966ck09zfkhm28c82B3a02wSQwb8zZN3RoNd68tO2A8740090O2F2E59Rf23W1 4njTmA529o2X2T14cILbBkv30g7wX0ai2Cb87j37p26t..

C:\Users\user\AppData\Roaming\22032878\vmwkpdfbe.xls	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	565
Entropy (8bit):	5.5416700480025565
Encrypted:	false
SSDEEP:	12:PyF+p25R4Xfas62k++wQjd0twFkWTU/jljaOcLNGydO3hLxdI6S27DxR01+:Ku2AH62k+5Qh0tmkWQwLNGOO3uo7DxRZ
MD5:	45ADEFB7B7309472FAE812C9004915E3
SHA1:	78BA0C1D1BC8C15B4E8175DC4719C32F4C5E3E5A

C:\Users\user\AppData\Roaming\22032878\vmwkpdfbe.xls	
SHA-256:	83440C3453A12458150A99C915DD1D7DCF5F256B44FEC3D8625C5D836B9BBF3A
SHA-512:	AEC3D4C8C9909AD4F5692B24B1A6D6FE50310CE53B25CF7F9EFF8CC316CCFB948B90E78B4AD542A4F1FD7F81E5996AF7B144F48843C747B95F779897C38ABB 2
Malicious:	false
Preview:	565P0p5J86fU934u0T9u8My8c5rxe47qH7L53N4296gy26W5180i12226S9qw18eaI8825y57f5U53..E3r3xhnTN2bMH8hdb35DLaRSq3f0Ni07q5XV2HTq872dHKU114 X8W35el8LT78w30aM41P0KeORV6cvRm6..E3Xw9YWDflrUBDwbTI4vv1s3f25r8PwM66rJPV1UX56469zNQ7012..8LmM575R708SKi1nuH8uz408rFq92f8ubc8M7Ao2G Wo173vy1r937XSi74619Y2hYm37yX551P3PaR06Sn36GIzbrJ8bJuaXwr484T8pUlf6qD55e50G1T31548Uy7KxS065OIhn6GItwPQ3x12q9EUYmy8L3k2951hA9h04v23 868..637QC48z17TV1X..7lRcT3mQ584Ts5z64TA5w6n6d4N4..cy0N5X6p752D9RRrm78731O0L7E5y3B..V49iQ9240i1I9E31q9g4VKcA2NX1P112xJ9488yWKcISM5 Xe37z0Rau33r56k159jK07QrMtos0Z7Y0r24QK3g0aM..

C:\Users\user\AppData\Roaming\22032878\vxhqol.jpg	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	504
Entropy (8bit):	5.436588232072642
Encrypted:	false
SSDEEP:	12:i9Dkb1roXOYZ0dVKXkjQH0ygqHi9K0QOqzl:2kNYZkVKU0H0ygqC9K0bWl
MD5:	854039E8892A6AF3BB237C8C5FDBEDA2
SHA1:	EEC1068497F4C8C178BB4E273433646FF0AB4DD4
SHA-256:	7A69FB54E9B5F631D1C7878ABD4A1EDA15AAAC43F32828DEE31F35F89298143B
SHA-512:	71A415DEA79742A177AF1DF0D856F017639216373862510F1089FA8A049056D528FDF2942C79089396B0AE28A3E48B24523BBCDC4A0AEB188C4DAC85655028AA
Malicious:	false
Preview:	JB48R3Foul8PdP243s669600ssmcx39a2O2D78..15T664P0C9W7ML7127J9g1kgTz26iD89LTrDQ7sdD353Z1O45T58l5o75O6cfiunZlc92jd05UBYIvFDS2mhOMI388 S448ap5Q9v6y837K0EU68C5U0145M8wtD20s61Qa..9156F8N8j0Gh9208692JP673U92m9F..P2AX1ZA5s505D47N55v0Yw4Di50kMB808930b2y57fN1s1J1ta4cMyp2 993pe4JoX10fDwib18cTyC0V4x9Z9mq1..360Up10hQMX8N082TO80s0X4e3Hno3oi427857Oq3s9D2267C995IzekVRcoC432yUfo82vH1p1bc5cs5t2aSv12s48jI683 szs203Y34IGd..F81837q9u694Lu191oa5kZ875U0156435HO5g1..461854Jd45946BHq1X74271682VO0k02mKY6Y5b4U59FgV40H8204h90KS..

C:\Users\user\AppData\Roaming\22032878\wawopnh.xml	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	542
Entropy (8bit):	5.435844680914607
Encrypted:	false
SSDEEP:	12:f0NCiBAoKCMuCJME3Khwu2Tf5N10v7sTbvDflrhv/I/LjWNkRn:2lotMEF5XTbjdtIPWNs
MD5:	CA3375B40AE610E80B80F479BCD7CA79
SHA1:	188BBEE5E1F86DA84AC17AF971CAC635C6447BB8
SHA-256:	65C7147B661E9B75ECFFF54706E894AA25E6399E7EF1C8DFE9E56B53643C425F
SHA-512:	1725511DD6135BC890D4FDC33D585254D884A2242C9EA314A512DDD42AF3321326EE25A00BBC2D72637ECDC85D512B4A808D8A38C920408A9A438D55254755A
Malicious:	false
Preview:	69w10kQ29VC35732..0ix02sq0wJ1O557f..H54QGEb2Nnn241862N9I06CLV70J7010gB61120R543o80Ox03mEe..w323043CXjsYF89sl0..2N65z7i40827Ymt3GC7 b5002X26tvV43l9x2925r3Dvv7eVR51kzmC6..84Xi8C8w2I917q11yz80U41096UXP340O3bQ1E5odFLPUQN13Oi973Z4IGkcG2..765F48DjtHtpq463e7Klef6t42c2 f13W96..5zbr85X25Pj8wd124mY89nxU244m2CAJs6QzO6823xr7J1pi99Mt137682UG6JX2b1988Y02N39220S..9Y5pUwQ06V57zE8H9jx63g13u2lE1CPNK6kpp8..3 be4V63pT0R23U287A95251g8H6P86786hV2Q47sU8W2K8J18TQbYKX671O0j0I81..o2hz730w4Wcu664u2J973v1yrRq15961C403213ZS4ttzonOnW58CvwvI880QKUM rye32x448yCQSCxE68J0..

C:\Users\user\AppData\Roaming\22032878\xaso.fhr	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	data
Category:	dropped
Size (bytes):	89158036
Entropy (8bit):	7.047537320550963
Encrypted:	false
SSDEEP:	393216:wL/HcmIzTYbzRoYe0wveaBt8KVp+ziboJL/nUuELfLu/W8tVGNoJy9Uh12y/Oasn:N
MD5:	849C1F5F156BC2BA9528E0F6B7BCE4A6
SHA1:	CAC5BBA70ABD7B8F72382DDE6D25010A702D88E4
SHA-256:	D7782A1453D34566C6B8B6D71DA32BA153DB1A90CB2F3483C6C759D8C8E66D62
SHA-512:	F7C68FF539EB5A8E83BE5D88723BF1436DF0EE01EBF4A1C1122AC92EFA151D67184D29BBEAF873B066F41B4DD2F7751EECD7ABD1DEEC5F3BE9C3818331244 3B
Malicious:	false
Preview:	..;...$.^^.)....L..].c!.}...5..J{..1.(cW.>.>E..]...A.P.K.{..[..v...P...C.%d...&..x>..?..6g.....S;.....m.a.r.....#.c.s..M..9..O5uA...<.o.....=t.'.O...[..0gV...x ..dhD.jx.#U;...z...C...3X...y./.s ....o8....L$.p.#.`DA..m.}.A.....5...eV:`.>...).!p.>.....E.q..5.....\..fI.F.3e..Q.2.5p:O.#hy6...nb.P.'..F@....3.7.s.6.7.4.m.N.9.N.N.T.6.9.O.6.1.d.h.s.9.4.3.A.v.8.j.C.q.I.P.4.O.t.A. W.S.W.N.0.y.0.A.R.D.l.....[..wm...[....V.].^./.T.....+IU.....p]..p."...(x.n(..rU}s.....c..#|.~.....n.JN.q.{MZ.+m..1u...Z2q..E...N.|k?..]..._*&1H.:Ad.....6.7.1.P.0.6.u.o.2.2.....8.K .U.Q.b.9.n.3.0.8.4.I.Z.6.1.7.G.s.8.M.W.L.9.A.9.Y.4.6.2.1.A.3.7.4.Z.2.Z.0.4.j.f.T.D.g.S.Z.w.....b.7.8.p.9.K.8.3.5.8.9.q.8.8.y.r.2.M.E.0.7.6.H.r.4.5.6.8.B.G.6.8.P.....V.....u..|..`) ..g.J..k..z=...;.R.@.-v8.....n.Q..@ ..uH..}..jDyW;U+w.I.Ry....._...y....L.v.".@.I?b..D.o..G?)G._.u*.Y.<6].y1.....q.`_.)K.C.....]a9..Bz.....PA.S.....AE.].D.,...._....h.....nEK..... G.Jh...).....

C:\Users\user\AppData\Roaming\22032878\xltllfaf.dat	
Process:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	516
Entropy (8bit):	5.508661863014793
Encrypted:	false
SSDEEP:	12:JOFKaWmJJVJBVWQYHyWQGG5DnnZd0pjY/BaZ2JkAbR:UeEJVJCQYSW34nZdz/BaZ2JkAbR
MD5:	5126D494BCFE29FCCEB72C7D472EB601
SHA1:	D0C8FF41C88B85FC0862A05B974A71B4BEFCA006
SHA-256:	B1AB630B7C84E02AD585F4762E029D780040F1329788894174124574A2168B2B
SHA-512:	A534A08CEF6C4A683E1D5B8240A30A79727B079327AC1E21A4D6B5B91751B009E37D43582CB5252247239E4A18FD34B9EB1A10651484917E6572EFBAED89BE5C
Malicious:	false
Preview:	g160X..Jd160vB35824sr10B47su7T37k0RMg0Fb..0XBJ814321Vs22c6Y3P8Iuf3866Z0b16X4MT5f497Vu8Ts0EX342Q9SK041IJS4uVR6ERkFz8pFC5L2GH2by20i5 224NcK3E0N2W2Z3fd05Dg1P029j6Jd8IW4Ye9vp9..iQ7q23wBoh9Z7u2hP834Q7z903tsm1l9ruq8yj01i30eS8Go7KU6571Z9cx2948wbTa3i54KK371N183079571V. .0g28V48L6A7eSwf1u0454ZwQ7..5656Ugt0Y097L007Q48Xo61HU50..mi7mql942thjQTT66dIZL3G735L3321SKfqebt65U37lsyh6994377qt25m1uvp6jb662B397 q983..322Jx02hf3JJT5ByBg1nX2a3D5b3P2N1oak38f..F3VkGK65ky4MuHXwh79cJrl09F99kllu1Q17oD3814GA7Q2P6N1iih8eU19439JXpr83C387qX4ec9..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:cgPn:cgPn
MD5:	68C37A35BAB3DEEE0C4AD3AE407363F6
SHA1:	8EABC744E14B3D9C79FB928183A6B0E472363298
SHA-256:	02AAF7E7E62DEB355B4F7E0E9F1C78965957D8EE3F7E319590C4B30D5DE6D2A3
SHA-512:	97A588C6F7BDB36DDB7200FDF27FC0B01CA7B0FA131E354F98294D9B2E68AE6B972FF6B6A3A86F450BB8683FED29CA85266AB02D2E2C728EA74AD2E5D5541B36
Malicious:	**true**
Preview:	z.G....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	45
Entropy (8bit):	4.324534762707879
Encrypted:	false
SSDEEP:	3:oNt+kiE2J5xAIwGMNn:oNwkn23fA
MD5:	47370DB2229FE5D11F48C7C4DCF1D3DA
SHA1:	02F189B1593B564FAF6B30C1573A6C4156EEA2B8
SHA-256:	8DA13D1ABADD97A50839C4237102C680E32B80F56B8B594ACC289D603779F743
SHA-512:	0FAE24E7BA758031C3850E96BFB9F93B71E9CDF886A83F83F8B0BB57C76403DA0563E3B9117360968AA279927EB7FB8F77BA48B446635E60D159AFFB96979550
Malicious:	false
Preview:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe

C:\Users\user\temp\lqjmggks.ico	
Process:	C:\Users\user\AppData\Roaming\22032878\nfiuc.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	77
Entropy (8bit):	4.951742632043194
Encrypted:	false
SSDEEP:	3:YRRvut8EENvuAp8XRGdYHJUgm17n:Avx9Hwm17
MD5:	D12EFF1149B52E35D77B216A783E46A0
SHA1:	16D6CB1900FF3AADDC4B1DF98ACE37F064923701
SHA-256:	0DDC47409A7323ACD044E09756C93E78635D1A32DAA4FBDC3483FDE8B4E754FE
SHA-512:	8A965C18E4DA732A9D130D8486449ED6D9BDA8FE0312BE952B89FE07F87B5364DE99983A8DFB42D0E7FD48101B871885EDF0E0DEB3DE4C39E35D12646B341CA
Malicious:	false
Preview:	[S3tt!ng]..stpth=%appdata%..Key=Chrome..Dir3ctory=22032878..ExE_c=nfiuc.pif..

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.8085078655708235
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	zunUbtZ2Y3.exe
File size:	986265
MD5:	5ea59097fb7eed4ac42b666ac548d39c
SHA1:	919a1f62dc0358405d1d8a07dd9c1c7f1a6c1d87
SHA256:	b4457b3e745bbed3ab4d61442ae846c3a06d42280c2937e406e48fea05fed6e0
SHA512:	84f9e8568fe4d17885cdd66faee17ede2a6b2ab1c8ec3817c12576e5f88ad274f3e26e6b5b46734ea4d426b2ca5b0ce1e5fa5b9e2b6617eac5977422a33335d6
SSDEEP:	24576:BAOcZpJXVxqwjJqe6qRNoIc1Jek/LKFT361Y5a+nyn:biqwn6qRvcCk/LcT3G2/nyn
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$...._..0...._..5...._...../y..../y..#...&...,...._....._.'...._f.'...._..'..

File Icon

Icon Hash:	1ab8e6e663d6c77a

Static PE Info

General

Entrypoint:	0x41e1f9
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5E7C7DC7 [Thu Mar 26 10:02:47 2020 UTC]
TLS Callbacks:	

General

CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	fcf1390e9ce472c7270447fc5c61a0c1

Entrypoint Preview

Instruction
call 00007FBA084690DFh
jmp 00007FBA08468AD3h
cmp ecx, dword ptr [0043D668h]
jne 00007FBA08468C45h
ret
jmp 00007FBA08469255h
ret
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 00433068h
mov dword ptr [ecx], 00434284h
ret
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007FBA0845C051h
mov dword ptr [esi], 00434290h
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 00434298h
mov dword ptr [ecx], 00434290h
ret
lea eax, dword ptr [ecx+04h]
mov dword ptr [ecx], 00434278h
push eax
call 00007FBA0846BDEDh
pop ecx
ret
push ebp
mov ebp, esp
push esi
mov esi, ecx
lea eax, dword ptr [esi+04h]
mov dword ptr [esi], 00434278h
push eax
call 00007FBA0846BDD6h
test byte ptr [ebp+08h], 00000001h
pop ecx
je 00007FBA08468C4Ch
push 0000000Ch
push esi
call 00007FBA0846820Fh
pop ecx
pop ecx

Instruction
mov eax, esi
pop esi
pop ebp
retn 0004h
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007FBA08468BAEh
push 0043A410h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FBA0846B4D5h
int3
push ebp
mov ebp, esp
sub esp, 0Ch

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [EXP] VS2015 UPD3.1 build 24215 • [LNK] VS2015 UPD3.1 build 24215 • [IMP] VS2008 SP1 build 30729 • [C++] VS2015 UPD3.1 build 24215 • [RES] VS2015 UPD3 build 24213

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3b540	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3b574	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x62000	0x57e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x68000	0x210c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x397d0	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x34218	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x32000	0x260	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x3aaec	0x120	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x30581	0x30600	False	0.589268410853	data	6.70021125825	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x32000	0xa332	0xa400	False	0.455030487805	data	5.23888424127	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3d000	0x238b0	0x1200	False	0.368272569444	data	3.83993526939	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x61000	0xe8	0x200	False	0.333984375	data	2.12166381533	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x57e8	0x5800	False	0.618430397727	data	6.34217881671	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x68000	0x210c	0x2200	False	0.786534926471	data	6.61038519378	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PNG	0x62524	0xb45	PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced	English	United States
PNG	0x6306c	0x15a9	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced	English	United States
RT_ICON	0x64618	0xea8	data		
RT_DIALOG	0x654c0	0x286	data	English	United States
RT_DIALOG	0x65748	0x13a	data	English	United States
RT_DIALOG	0x65884	0xec	data	English	United States
RT_DIALOG	0x65970	0x12e	data	English	United States
RT_DIALOG	0x65aa0	0x338	data	English	United States
RT_DIALOG	0x65dd8	0x252	data	English	United States
RT_STRING	0x6602c	0x1e2	data	English	United States
RT_STRING	0x66210	0x1cc	data	English	United States
RT_STRING	0x663dc	0x1b8	data	English	United States
RT_STRING	0x66594	0x146	Hitachi SH big-endian COFF object file, not stripped, 17152 sections, symbol offset=0x73006500	English	United States
RT_STRING	0x666dc	0x446	data	English	United States
RT_STRING	0x66b24	0x166	data	English	United States
RT_STRING	0x66c8c	0x152	data	English	United States
RT_STRING	0x66de0	0x10a	data	English	United States
RT_STRING	0x66eec	0xbc	data	English	United States
RT_STRING	0x66fa8	0xd6	data	English	United States
RT_GROUP_ICON	0x67080	0x14	data		
RT_MANIFEST	0x67094	0x753	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

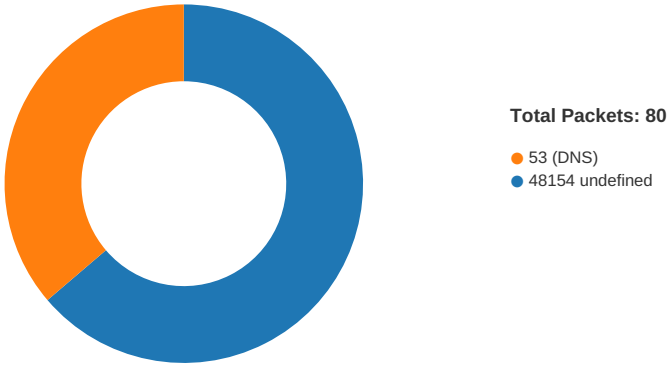
DLL	Import
KERNEL32.dll	GetLastError, SetLastError, FormatMessageW, GetCurrentProcess, DeviceIoControl, SetFileTime, CloseHandle, CreateDirectoryW, RemoveDirectoryW, CreateFileW, DeleteFileW, CreateHardLinkW, GetShortPathNameW, GetLongPathNameW, MoveFileW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, SetFileAttributesW, GetFileAttributesW, FindClose, FindFirstFileW, FindNextFileW, GetVersionExW, GetCurrentDirectoryW, GetFullPathNameW, FoldStringW, GetModuleFileNameW, GetModuleHandleW, FindResourceW, FreeLibrary, GetProcAddress, GetCurrentProcessId, ExitProcess, SetThreadExecutionState, Sleep, LoadLibraryW, GetSystemDirectoryW, CompareStringW, AllocConsole, FreeConsole, AttachConsole, WriteConsoleW, GetProcessAffinityMask, CreateThread, SetThreadPriority, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetEvent, ResetEvent, ReleaseSemaphore, WaitForSingleObject, CreateEventW, CreateSemaphoreW, GetSystemTime, SystemTimeToTzSpecificLocalTime, TzSpecificLocalTimeToSystemTime, SystemTimeToFileTime, FileTimeToLocalFileTime, LocalFileTimeToFileTime, FileTimeToSystemTime, GetCPInfo, IsDBCSLeadByte, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, LockResource, GlobalLock, GlobalUnlock, GlobalFree, LoadResource, SizeofResource, SetCurrentDirectoryW, GetExitCodeProcess, GetLocalTime, GetTickCount, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, OpenFileMappingW, GetCommandLineW, SetEnvironmentVariableW, ExpandEnvironmentStringsW, GetTempPathW, MoveFileExW, GetLocaleInfoW, GetTimeFormatW, GetDateFormatW, GetNumberFormatW, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapSize, SetStdHandle, GetProcessHeap, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, TerminateProcess, RtlUnwind, EncodePointer, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, HeapReAlloc, GetStringTypeW, LCMapStringW, FindFirstFileExA, FindNextFileA, IsValidCodePage, GetOEMCP, GetCommandLineA, GetEnvironmentStringsW, FreeEnvironmentStringsW, DecodePointer
gdiplus.dll	GdiplusShutdown, GdiplusStartup, GdipCreateHBITMAPFromBitmap, GdipCreateBitmapFromStreamICM, GdipCreateBitmapFromStream, GdipDisposeImage, GdipCloneImage, GdipFree, GdipAlloc

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 19:06:22.620886087 CEST	49729	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:22.652494907 CEST	48154	49729	79.134.225.40	192.168.2.4
Apr 8, 2021 19:06:23.191631079 CEST	49729	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:23.220431089 CEST	48154	49729	79.134.225.40	192.168.2.4
Apr 8, 2021 19:06:23.793153048 CEST	49729	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:23.820961952 CEST	48154	49729	79.134.225.40	192.168.2.4
Apr 8, 2021 19:06:28.064795971 CEST	49730	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:28.128407955 CEST	48154	49730	79.134.225.40	192.168.2.4
Apr 8, 2021 19:06:28.629535913 CEST	49730	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:28.658983946 CEST	48154	49730	79.134.225.40	192.168.2.4
Apr 8, 2021 19:06:29.161240101 CEST	49730	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:45.241498947 CEST	49731	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:45.283296108 CEST	48154	49731	79.134.225.40	192.168.2.4
Apr 8, 2021 19:06:45.792494059 CEST	49731	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:45.821454048 CEST	48154	49731	79.134.225.40	192.168.2.4
Apr 8, 2021 19:06:46.323725939 CEST	49731	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:46.351846933 CEST	48154	49731	79.134.225.40	192.168.2.4
Apr 8, 2021 19:06:50.357165098 CEST	49732	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:50.383476973 CEST	48154	49732	79.134.225.40	192.168.2.4
Apr 8, 2021 19:06:50.886672020 CEST	49732	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:50.941688061 CEST	48154	49732	79.134.225.40	192.168.2.4
Apr 8, 2021 19:06:51.449187994 CEST	49732	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:51.475914955 CEST	48154	49732	79.134.225.40	192.168.2.4
Apr 8, 2021 19:06:55.487030029 CEST	49734	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:55.516375065 CEST	48154	49734	79.134.225.40	192.168.2.4
Apr 8, 2021 19:06:56.027918100 CEST	49734	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:56.060997963 CEST	48154	49734	79.134.225.40	192.168.2.4
Apr 8, 2021 19:06:56.574592113 CEST	49734	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:06:56.614638090 CEST	48154	49734	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:00.623497963 CEST	49735	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:00.649844885 CEST	48154	49735	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:01.153237104 CEST	49735	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:01.181440115 CEST	48154	49735	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:01.684487104 CEST	49735	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:01.712518930 CEST	48154	49735	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:05.763751984 CEST	49736	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:05.791877031 CEST	48154	49736	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:06.294255018 CEST	49736	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:06.333509922 CEST	48154	49736	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:06.841219902 CEST	49736	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:06.880198956 CEST	48154	49736	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:10.942399979 CEST	49737	48154	192.168.2.4	79.134.225.40

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 19:07:10.968601942 CEST	48154	49737	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:11.482073069 CEST	49737	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:11.510613918 CEST	48154	49737	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:12.013405085 CEST	49737	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:12.041044950 CEST	48154	49737	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:16.087563992 CEST	49738	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:16.131514072 CEST	48154	49738	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:16.638901949 CEST	49738	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:16.678667068 CEST	48154	49738	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:17.185780048 CEST	49738	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:17.213973999 CEST	48154	49738	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:21.234503984 CEST	49739	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:21.268208981 CEST	48154	49739	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:21.779815912 CEST	49739	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:21.806183100 CEST	48154	49739	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:22.311167955 CEST	49739	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:22.338645935 CEST	48154	49739	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:26.344662905 CEST	49740	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:26.380091906 CEST	48154	49740	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:26.889715910 CEST	49740	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:26.916086912 CEST	48154	49740	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:27.420909882 CEST	49740	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:27.448138952 CEST	48154	49740	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:31.454761982 CEST	49741	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:31.496349096 CEST	48154	49741	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:31.999481916 CEST	49741	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:32.025599957 CEST	48154	49741	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:32.530734062 CEST	49741	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:32.559684038 CEST	48154	49741	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:36.622771025 CEST	49742	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:36.651227951 CEST	48154	49742	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:37.156196117 CEST	49742	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:37.188601017 CEST	48154	49742	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:37.702990055 CEST	49742	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:37.730161905 CEST	48154	49742	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:41.789257050 CEST	49743	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:41.820215940 CEST	48154	49743	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:42.328563929 CEST	49743	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:42.358417034 CEST	48154	49743	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:42.859678984 CEST	49743	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:42.887836933 CEST	48154	49743	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:46.940459967 CEST	49744	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:46.969897985 CEST	48154	49744	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:47.485060930 CEST	49744	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:47.517096043 CEST	48154	49744	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:48.031974077 CEST	49744	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:48.072392941 CEST	48154	49744	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:52.081202030 CEST	49745	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:52.137236118 CEST	48154	49745	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:52.641819954 CEST	49745	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:52.691555023 CEST	48154	49745	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:53.204392910 CEST	49745	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:53.232636929 CEST	48154	49745	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:57.237580061 CEST	49746	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:57.265291929 CEST	48154	49746	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:57.767136097 CEST	49746	48154	192.168.2.4	79.134.225.40
Apr 8, 2021 19:07:57.796385050 CEST	48154	49746	79.134.225.40	192.168.2.4
Apr 8, 2021 19:07:58.298547029 CEST	49746	48154	192.168.2.4	79.134.225.40

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 19:05:57.661624908 CEST	56483	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:05:57.674237967 CEST	53	56483	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 19:06:00.447801113 CEST	51025	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:00.460355997 CEST	53	51025	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:01.313884974 CEST	61516	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:01.326870918 CEST	53	61516	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:02.940396070 CEST	49182	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:02.953514099 CEST	53	49182	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:04.592571974 CEST	59920	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:04.605730057 CEST	53	59920	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:06.054282904 CEST	57458	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:06.069225073 CEST	53	57458	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:06.800720930 CEST	50579	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:06.816744089 CEST	53	50579	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:07.656873941 CEST	51703	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:07.669852972 CEST	53	51703	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:08.537900925 CEST	65248	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:08.552381992 CEST	53	65248	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:09.308515072 CEST	53723	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:09.321402073 CEST	53	53723	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:10.267388105 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:10.280556917 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:11.103508949 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:11.116632938 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:11.992616892 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:12.005228043 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:12.846138000 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:12.862572908 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:13.601794004 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:13.614360094 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:14.382998943 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:14.395639896 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:15.955348969 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:15.968251944 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:22.594480991 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:22.607168913 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:28.039309025 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:28.061603069 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:45.224353075 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:45.239716053 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 8, 2021 19:06:52.416388988 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:06:52.428383112 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 8, 2021 19:07:05.747019053 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:07:05.761940956 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 8, 2021 19:07:10.927253962 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:07:10.940756083 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 8, 2021 19:07:16.072588921 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:07:16.085952997 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 8, 2021 19:07:36.600106001 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:07:36.621063948 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 8, 2021 19:07:41.767921925 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:07:41.787542105 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 8, 2021 19:07:46.925127029 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:07:46.938282013 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 19:08:07.500602007 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:08:07.513406038 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 19:08:12.678395033 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 8, 2021 19:08:12.698591948 CEST	53	56627	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 19:06:22.594480991 CEST	192.168.2.4	8.8.8.8	0x727e	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 19:06:28.039309025 CEST	192.168.2.4	8.8.8.8	0x1207	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 19:06:45.224353075 CEST	192.168.2.4	8.8.8.8	0xc34c	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 19:07:05.747019053 CEST	192.168.2.4	8.8.8.8	0x83e8	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 19:07:10.927253962 CEST	192.168.2.4	8.8.8.8	0x4728	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 19:07:16.072588921 CEST	192.168.2.4	8.8.8.8	0x41fb	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 19:07:36.600106001 CEST	192.168.2.4	8.8.8.8	0x309e	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 19:07:41.767921925 CEST	192.168.2.4	8.8.8.8	0xbdd9	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 19:07:46.925127029 CEST	192.168.2.4	8.8.8.8	0x44e	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 19:08:07.500602007 CEST	192.168.2.4	8.8.8.8	0x1c40	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Apr 8, 2021 19:08:12.678395033 CEST	192.168.2.4	8.8.8.8	0xa8d7	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

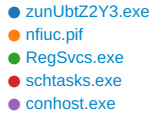
DNS Answers

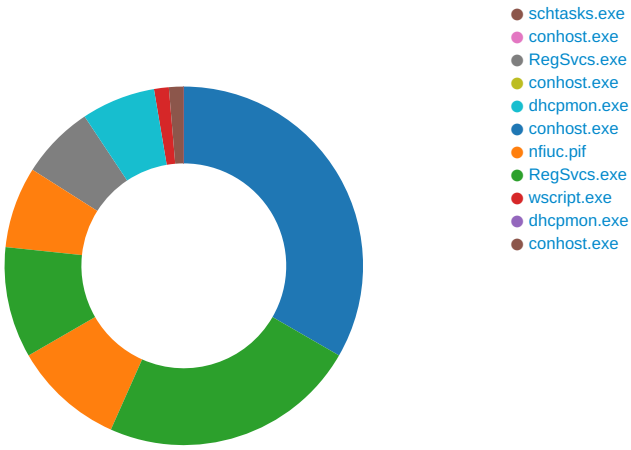
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 19:06:22.607168913 CEST	8.8.8.8	192.168.2.4	0x727e	No error (0)	strongodss .ddns.net		79.134.225.40	A (IP address)	IN (0x0001)
Apr 8, 2021 19:06:28.061603069 CEST	8.8.8.8	192.168.2.4	0x1207	No error (0)	strongodss .ddns.net		79.134.225.40	A (IP address)	IN (0x0001)
Apr 8, 2021 19:06:45.239716053 CEST	8.8.8.8	192.168.2.4	0xc34c	No error (0)	strongodss .ddns.net		79.134.225.40	A (IP address)	IN (0x0001)
Apr 8, 2021 19:07:05.761940956 CEST	8.8.8.8	192.168.2.4	0x83e8	No error (0)	strongodss .ddns.net		79.134.225.40	A (IP address)	IN (0x0001)
Apr 8, 2021 19:07:10.940756083 CEST	8.8.8.8	192.168.2.4	0x4728	No error (0)	strongodss .ddns.net		79.134.225.40	A (IP address)	IN (0x0001)
Apr 8, 2021 19:07:16.085952997 CEST	8.8.8.8	192.168.2.4	0x41fb	No error (0)	strongodss .ddns.net		79.134.225.40	A (IP address)	IN (0x0001)
Apr 8, 2021 19:07:36.621063948 CEST	8.8.8.8	192.168.2.4	0x309e	No error (0)	strongodss .ddns.net		79.134.225.40	A (IP address)	IN (0x0001)
Apr 8, 2021 19:07:41.787542105 CEST	8.8.8.8	192.168.2.4	0xbdd9	No error (0)	strongodss .ddns.net		79.134.225.40	A (IP address)	IN (0x0001)
Apr 8, 2021 19:07:46.938282013 CEST	8.8.8.8	192.168.2.4	0x44e	No error (0)	strongodss .ddns.net		79.134.225.40	A (IP address)	IN (0x0001)
Apr 8, 2021 19:08:07.513406038 CEST	8.8.8.8	192.168.2.4	0x1c40	No error (0)	strongodss .ddns.net		79.134.225.40	A (IP address)	IN (0x0001)
Apr 8, 2021 19:08:12.698591948 CEST	8.8.8.8	192.168.2.4	0xa8d7	No error (0)	strongodss .ddns.net		79.134.225.40	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: zunUbtZ2Y3.exe PID: 4728 Parent PID: 5932

General

Start time:	19:06:03
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\zunUbtZ2Y3.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\zunUbtZ2Y3.exe'
Imagebase:	0x1350000
File size:	986265 bytes
MD5 hash:	5EA59097FB7EED4AC42B666AC548D39C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1359F1F	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	1359F1F	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1359F1F	CreateDirectoryW
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	1359F1F	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1359F1F	CreateDirectoryW
C:\Users\user\AppData\Roaming\22032878__tmp_rar_sfx_access_check_5048640	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\lqjmggks.ico	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\xaso.fhr	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\nfiuc.pif	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\fbekvf.mp3	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\vxhqol.jpg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\kuodio.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\plee.xl	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\rkevqw.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\tejpjdone.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\wawopnh.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\xltllfaf.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\btdbvndt.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\vmwkpdfbe.xls	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\eseh.pdf	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\vhcpj.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\ucjondx.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\poqhjae.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\lojmm.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\txum.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\dnxuddwt.ppt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW
C:\Users\user\AppData\Roaming\22032878\rnpxxre.icm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13595B6	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878__tmp_rar_sfx_access_check_5048640	success or wait	1	1359E2F	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\lqjmggks.ico	unknown	485356	46 39 36 63 37 56 39 33 7a 33 45 39 78 6c 42 36 61 6e 30 66 30 4a 6b 36 64 6e 64 32 7a 4e 64 47 59 39 42 0d 0a 78 36 68 31 33 41 32 4e 31 35 66 37 74 56 49 4a 34 7a 71 77 69 34 33 67 36 6a 71 77 38 4f 38 49 33 35 75 39 37 6a 78 61 4b 38 74 77 36 33 53 70 0d 0a 55 37 33 35 63 38 4f 31 38 7a 68 6c 78 30 61 6a 39 36 59 71 31 4b 34 32 36 6a 33 53 76 34 36 34 39 34 51 4d 37 38 4e 76 6f 30 41 36 72 30 35 46 7a 35 75 61 45 31 39 33 30 0d 0a 69 5a 32 44 44 35 75 32 73 38 6a 31 34 35 35 74 36 32 6c 39 4c 34 37 74 33 43 37 47 31 73 32 46 6a 34 62 33 50 61 36 66 30 70 49 44 42 4c 67 41 70 77 59 35 46 56 39 57 57 68 4a 78 39 75 53 0d 0a 74 36 30 4e 61 30 34 78 64 35 30 33 32 32 30 37 37 67 4c 64 66 48 4b 0d 0a 30 64 6b 35 37 38 4f 6b 59 4f 55 36 38 45 4c 36 45 68 35	F96c7V93z3E9xlB6an0f0J k6dnd2zN dGY9B..x6h13A2N15f7tVI J4zqwi43 g6jqw8O8l35u97jxaK8tw63 Sp..U73 5c8O18zhlx0aj96Yq1K426j 3Sv4649 4QM78Nvo0A6r05Fz5uaE 1930..iZ2D D5u2s8j1455t62l9L47t3C7 G1s2Fj4 b3Pa6f0pIDBLgApwY5FV9 WWhJx9uS. .t60Na04xd50322077gLdfH K..0dk5 78OkYOU68EL6Eh5	success or wait	1	1359CC2	WriteFile
C:\Users\user\AppData\Roaming\22032878\xaso.fhr	unknown	4193069	ff fe 3b 00 aa aa 24 a6 5e 5e b4 29 94 ba d8 8e 1f 4c a9 00 5d c8 63 21 d0 7d e6 f3 af d3 a8 35 d6 13 4a 7b ef fd 31 ff 28 63 57 9e 3e e5 8d 3e 45 1f e5 5d 0f 90 a2 41 11 50 84 4b ed 7b f0 a9 05 5b db e3 76 a0 06 14 50 8b fc 84 43 13 25 64 c0 10 06 26 eb 1e 78 3e 8b e2 3f af a9 36 67 e5 01 15 f5 89 8b 53 3b a2 03 af 15 e9 85 6d 1d 61 08 72 1d e0 e9 b9 d1 00 0d 00 0a 00 23 00 63 00 73 00 c8 4d 7f e1 a5 39 05 d5 4f 35 75 41 c6 83 9b f4 3c f1 6f 0d 0a 96 08 07 83 96 3d 74 e2 27 c4 4f 06 fd 9f 5b cc ea 30 67 56 02 fc b3 78 20 9d d0 b3 64 68 44 9e 6a 78 15 23 55 3b 10 d4 1d 7a f0 f2 a2 f8 43 80 15 b4 33 58 8d d4 17 79 c0 2f e4 73 f5 cd b3 be 98 6f 38 8e c7 cd d7 4c 24 ba 70 83 23 d1 60 44 41 91 e8 6d 0e 7d 05 41 fb a0 8d 0c be ad a3 ed 35 1d b3 de 65 56 3a 60	..;...$.^^.).....L..].c!.}.... .5..J{..1. (cW.>..>E..]...A.P.K.{... [..v...P...C.%d...&..x>.. ?..6g.....S;.....m.a.r..... ....#.c.s..M...9..O5uA....<.o. .....=t.'.O...[..0gV...x ...d hD.jx.#U;...z....C...3X...y./. s.....o8....L$.p.#.`DA..m.}.A .....5...eV:`	success or wait	24	1359CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\nfiuc.pif	unknown	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c2 1e 94 bf 86 7f fa ec 86 7f fa ec 86 7f fa ec 15 31 62 ec 84 7f fa ec 9d e2 50 ec 29 7f fa ec 9d e2 51 ec b3 7f fa ec 8f 07 79 ec 8f 7f fa ec 8f 07 69 ec a7 7f fa ec 86 7f fb ec 96 7d fa ec 9d e2 4e ec ce 7f fa ec 9d e2 64 ec 9a 7f fa ec 9d e2 60 ec 87 7f fa ec 86 7f 6d ec 87 7f fa ec 9d e2 67 ec 87 7f fa ec 52 69 63 68 86 7f fa ec 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $........................1b... ....P.).....Q.......y.......i. ....}....N.......d....... `.......m.......g.....Rich.... ........PE..L..	success or wait	21	1359CC2	WriteFile
C:\Users\user\AppData\Roaming\22032878\fbekvf.mp3	unknown	532	33 5a 33 6c 38 34 35 37 38 32 49 0d 0a 68 30 50 66 39 36 34 30 31 64 45 50 44 64 30 38 33 38 39 31 76 7a 33 35 30 6c 38 38 38 31 59 32 58 30 4f 6c 38 38 53 47 37 5a 53 54 75 33 36 30 34 35 39 78 31 56 73 68 66 34 4b 33 32 34 62 4a 66 33 51 70 6a 33 61 6f 56 70 31 35 4d 34 39 6c 6e 68 79 30 4c 41 35 0d 0a 52 36 36 34 71 65 58 66 77 34 34 74 38 36 4e 33 36 6d 35 35 30 6e 59 35 33 4f 4c 4d 59 51 37 51 36 52 33 33 36 61 34 74 72 38 49 35 34 56 43 71 35 0d 0a 63 38 32 37 35 79 6f 36 38 36 33 61 35 49 32 32 64 74 7a 4b 32 36 5a 4f 68 75 38 69 34 39 37 34 6d 37 43 38 53 36 32 44 0d 0a 39 36 69 4b 6d 39 39 36 37 37 43 47 38 49 39 39 30 39 45 4f 39 37 35 59 74 76 7a 4c 52 35 39 32 6c 35 62 37 31 34 4a 39 65 30 4d 72 34 31 56 62 35 39 39 4b 4d 52 72 55 35 4a 35 38	3Z3l845782I..h0Pf96401d EPDd083 891vz350l8881Y2X0Ol88S G7ZSTu36 0459x1Vshf4K324bJf3Qpj 3aoVp15M 49lnhy0LA5..R664qeXfw44 t86N36m 550nY53OLMYQ7Q6R336 a4tr8I54VCq 5..c8275yo6863a5I22dtzK 26ZOhu8 i4974m7C8S62D..96iKm99 677CG8I9 909EO975YtvzLR592l5b71 4J9e0Mr4 1Vb599KMRrU5J58	success or wait	1	1359CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\vxhqol.jpg	unknown	504	4a 42 34 38 52 33 46 6f 75 49 38 50 64 50 32 34 33 73 36 36 39 36 30 30 73 73 6d 63 78 33 39 61 32 4f 32 44 37 38 0d 0a 31 35 54 36 36 34 50 30 43 39 57 37 4d 4c 37 31 32 37 4a 39 67 31 6b 67 54 7a 32 36 69 44 38 39 4c 54 72 44 51 37 73 64 44 33 35 33 5a 31 4f 34 35 54 35 38 6c 35 6f 37 35 4f 36 63 66 69 75 6e 5a 6c 63 39 32 6a 64 30 35 55 42 59 49 76 46 44 53 32 6d 68 4f 4d 49 33 38 38 53 34 34 38 61 70 35 51 39 76 36 79 38 33 37 4b 30 45 55 36 38 43 35 55 30 31 34 35 4d 38 77 74 44 32 30 73 36 31 51 61 0d 0a 39 31 35 36 46 38 4e 38 6a 30 47 68 39 32 30 38 36 39 32 4a 50 36 37 33 55 39 32 6d 39 46 0d 0a 50 32 41 58 31 5a 41 35 73 35 30 35 44 34 37 4e 35 35 76 30 59 77 34 44 69 35 30 6b 4d 42 38 30 38 39 33 30 62 32 79 35 37 66 4e 31 73 31 4a 31 74 61 34	JB48R3FouI8PdP243s669 600ssmcx3 9a2O2D78..15T664P0C9W 7ML7127J9 g1kgTz26iD89LTrDQ7sdD 353Z1O45T 58l5o75O6cfiunZlc92jd05U BYIvFD S2mhOMI388S448ap5Q9v 6y837K0EU6 8C5U0145M8wtD20s61Qa. .9156F8N8 j0Gh9208692JP673U92m9 F..P2AX1Z A5s505D47N55v0Yw4Di50 kMB808930 b2y57fN1s1J1ta4	success or wait	1	1359CC2	WriteFile
C:\Users\user\AppData\Roaming\22032878\kuodio.log	unknown	583	33 36 4a 6c 67 41 76 36 52 71 37 32 69 69 35 0d 0a 32 51 64 33 31 74 31 34 33 32 4b 36 36 30 74 31 71 65 33 33 30 34 4b 56 65 30 4d 35 78 77 64 36 39 35 75 33 63 71 31 49 39 68 62 35 70 37 31 54 49 66 51 74 48 30 61 59 33 37 30 71 30 33 30 32 35 56 65 54 73 34 38 4f 44 36 54 34 76 47 34 51 4f 49 75 54 35 71 37 34 62 7a 54 59 34 51 30 30 6c 37 0d 0a 42 30 4c 5a 32 35 31 38 35 32 6c 32 4d 32 38 39 76 51 45 7a 30 42 76 48 37 45 46 71 4f 58 30 33 43 32 36 42 6f 41 56 30 6c 39 6e 6b 39 56 52 48 58 7a 33 37 37 39 36 41 32 75 69 4e 4f 38 53 70 53 32 58 42 45 0d 0a 35 37 35 38 32 55 34 65 37 31 47 4e 75 44 49 38 77 37 31 31 39 43 31 39 33 56 38 55 32 0d 0a 36 6c 66 34 35 31 30 59 30 56 37 31 73 77 37 48 34 6b 45 73 32 45 79 32 32 30 66 38 67 56 37 78 63 47 31 39	36JlgAv6Rq72ii5..2Qd31t1 432K66 0t1qe3304KVe0M5xwd695 u3cq1l9hb 5p71TIfQtH0aY370q03025 VeTs48OD 6T4vG4QOIuT5q74bzTY4 Q00l7..B0L Z251852l2M289vQEz0Bv H7EFqOX03C 26BoAV0l9nk9VRHXz377 96A2uiNO8S pS2XBE..57582U4e71GNu DI8w7119C 193V8U2..6lf4510Y0V71s w7H4kEs2 Ey220f8gV7xcG19	success or wait	1	1359CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\plee.xl	unknown	573	67 51 30 39 4e 75 7a 31 35 4c 37 31 33 38 62 0d 0a 59 4a 32 5a 61 6e 38 32 59 41 33 37 47 72 64 7a 37 38 4f 66 33 4f 7a 31 30 78 30 30 35 6a 54 32 30 32 32 6c 35 55 61 35 67 47 32 51 72 4a 32 72 61 31 34 77 32 30 33 4a 51 31 31 35 38 35 33 31 30 35 33 78 36 76 34 56 73 32 39 75 71 37 31 32 31 37 30 39 66 33 50 38 39 6b 38 31 32 6c 31 70 33 44 34 33 30 54 4e 43 35 34 33 0d 0a 30 48 6b 34 4a 6d 31 33 34 34 55 79 36 32 33 77 55 31 62 56 39 34 72 6d 32 37 71 38 5a 55 32 77 34 37 38 41 45 32 37 47 4d 6c 43 46 38 61 30 34 34 57 39 6d 30 34 47 63 50 4d 37 30 6b 51 32 59 37 30 77 44 32 72 35 35 33 76 0d 0a 37 66 36 30 38 77 53 38 30 4c 50 78 36 6f 38 63 6f 41 31 69 65 52 67 35 65 46 30 34 75 37 75 36 42 58 30 38 4b 6c 61 31 64 33 36 43 43 6f 32 68 4f 35 66 32 38	gQ09Nuz15L7138b..YJ2Za n82YA37G rdz78Of3Oz10x005jT2022l 5Ua5gG2 QrJ2ra14w203JQ11585310 53x6v4Vs 29uq7121709f3P89k812l1p 3D430TN C543..0Hk4Jm1344Uy623 wU1bV94rm 27q8ZU2w478AE27GMlCF 8a044W9m04 GcPM70kQ2Y70wD2r553v ..7f608wS8 0LPx6o8coA1ieRg5eF04u 7u6BX08Kl a1d36CCo2hO5f28	success or wait	1	1359CC2	WriteFile
C:\Users\user\AppData\Roaming\22032878\rkevqw.txt	unknown	559	35 37 5a 70 74 32 32 6a 30 33 70 6b 56 34 72 43 31 31 6b 6a 5a 39 30 52 37 31 49 79 38 35 36 42 30 5a 52 31 69 69 45 62 54 58 48 38 62 53 75 64 4d 33 30 35 52 47 42 38 57 30 42 52 72 41 35 37 38 56 49 34 37 33 31 33 6b 31 31 38 75 46 4c 6a 34 34 34 30 6a 53 46 39 7a 33 39 35 4c 38 31 36 35 34 33 41 32 35 4b 34 73 36 4a 4d 37 38 72 39 4d 58 66 32 39 38 52 61 47 59 30 54 49 57 4e 35 36 0d 0a 38 30 33 34 37 56 42 38 79 33 7a 49 77 6d 34 35 46 33 36 0d 0a 38 35 51 4b 33 49 64 31 30 30 43 0d 0a 72 39 34 30 37 37 32 31 38 33 35 63 39 4d 30 34 34 50 38 31 37 47 72 4e 33 6a 35 39 68 35 32 32 31 58 76 0d 0a 50 46 6e 33 39 38 4b 34 74 37 6c 38 73 34 37 66 35 39 31 57 37 32 71 37 75 53 69 7a 30 4a 37 4d 65 4c 68 35 30 35 76 30 30 4a 35 74 41 50 59 39 38 38 6a 6c 4c	57Zpt22j03pkV4rC11kjZ90 R71Iy85 6B0ZR1iiEbTXH8bSudM3 05RGB8W0BR rA578VI47313k118uFLj444 0jSF9z3 95L816543A25K4s6JM78r 9MXf298Ra GY0TIWN56..80347VB8y3 zIwm45F36 ..85QK3Id100C..r9407721 835c9M0 44P817GrN3j59h5221Xv.. PFn398K4 t7l8s47f591W72q7uSiz0J7 MeLh505v00J5tAPY988jlL	success or wait	1	1359CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\tejpjdone.dat	unknown	520	31 33 30 32 38 4a 39 43 32 47 30 39 52 57 33 48 35 30 71 67 34 51 4c 31 31 30 55 32 36 66 4d 54 76 56 66 4d 36 38 38 36 50 35 41 31 31 0d 0a 6d 31 37 34 39 48 70 39 6f 61 67 44 37 38 30 35 4d 39 36 31 39 42 55 0d 0a 37 68 39 37 34 47 38 34 32 5a 4e 6f 31 38 61 56 39 69 63 31 57 32 31 5a 42 30 4e 59 38 79 58 32 4d 30 32 34 41 34 45 34 71 4c 4a 79 35 42 4a 30 34 45 6d 36 79 78 31 36 34 66 31 32 4c 47 35 41 31 6a 31 76 76 33 32 38 66 51 35 72 35 4a 62 34 67 35 6a 39 37 35 30 45 37 52 39 58 59 61 65 57 55 32 34 37 4f 53 36 70 6c 63 31 36 37 39 56 47 0d 0a 78 79 31 65 34 34 65 54 53 34 33 75 35 32 54 31 34 35 38 37 6d 49 34 4d 52 70 42 34 6f 30 30 66 37 75 57 46 39 35 37 73 71 4f 43 65 58 61 64 32 33 37 34 36 30 75 32 36 78 6b 54 39 5a 32 35 52 53 30 49 46 4c	13028J9C2G09RW3H50qg4QL110U26f MTvVfM6886P5A11..m1749Hp9oagD7 805M9619BU..7h974G842ZNo18aV9i c1W21ZB0NY8yX2M024A4E4qLJy5BJ0 4Em6yx164f12LG5A1j1vv328fQ5r5J b4g5j9750E7R9XYaeWU247OS6plc16 79VG..xy1e44eTS43u52T14587mI4M RpB4o00f7uWF957sqOCeXad237460u 26xkT9Z25RS0IFL	success or wait	1	1359CC2	WriteFile
C:\Users\user\AppData\Roaming\22032878\wawopnh.xml	unknown	542	36 39 77 31 30 6b 51 32 39 56 43 33 35 37 33 32 0d 0a 30 69 78 30 32 73 71 30 77 4a 31 4f 35 35 37 66 0d 0a 48 35 34 51 47 45 62 32 4e 6e 6e 32 34 31 38 36 32 4e 39 49 30 36 43 4c 56 37 30 4a 37 30 31 30 67 42 36 31 31 32 30 52 35 34 33 6f 38 30 4f 78 30 33 6d 45 65 0d 0a 77 33 32 33 30 34 33 43 58 6a 73 59 46 38 39 73 6c 30 0d 0a 32 4e 36 35 7a 37 69 34 30 38 32 37 59 6d 74 33 47 43 37 62 35 30 30 32 58 32 36 74 76 56 34 33 6c 39 78 32 39 32 35 72 33 44 76 76 37 65 56 52 35 31 6b 7a 6d 43 36 0d 0a 38 34 58 69 38 43 38 77 32 49 39 31 37 71 31 31 79 7a 38 30 55 34 31 30 39 36 55 58 50 33 34 30 4f 33 62 51 31 45 35 6f 64 46 4c 50 55 51 4e 31 33 4f 69 39 37 33 5a 34 49 47 6b 63 47 32 0d 0a 37 36 35 46 34 38 44 6a 74 48 74 70 71 34 36 33 65 37 4b 6c 65 66 36	69w10kQ29VC35732..0ix02sq0wJ1O 557f..H54QGEb2Nnn241862N9I06CL V70J7010gB61120R543o80Ox03mEe. .w323043CXjsYF89sl0..2N65z7i40 827Ymt3GC7b5002X26tvV43l9x2925 r3Dvv7eVR51kzmC6..84Xi8C8w2I91 7q11yz80U41096UXP340O3bQ1E5odF LPUQN13Oi973Z4IGkcG2. .765F48Dj tHtpq463e7Klef6	success or wait	1	1359CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\xltllfaf.dat	unknown	516	67 31 36 30 58 0d 0a 4a 64 31 36 30 76 42 33 35 38 32 34 73 72 31 30 42 34 37 73 75 37 54 33 37 6b 30 52 4d 67 30 46 62 0d 0a 30 58 42 4a 38 31 34 33 32 31 56 73 32 32 63 36 59 33 50 38 49 75 66 33 38 36 36 5a 30 62 31 36 58 34 4d 54 35 66 34 39 37 56 75 38 54 73 30 45 58 33 34 32 51 39 53 4b 30 34 31 49 4a 53 34 75 56 52 36 45 52 6b 46 7a 38 70 46 43 35 4c 32 47 48 32 62 79 32 30 69 35 32 32 34 4e 63 4b 33 45 30 4e 32 57 32 5a 33 66 64 30 35 44 67 31 50 30 32 39 6a 36 4a 64 38 49 57 34 59 65 39 76 70 39 0d 0a 69 51 37 71 32 33 77 42 6f 68 39 5a 37 75 32 68 50 38 33 34 51 37 7a 39 30 33 74 73 6d 31 49 39 72 75 71 38 79 6a 30 31 69 33 30 65 53 38 47 6f 37 4b 55 36 35 37 31 5a 39 63 78 32 39 34 38 77 62 54 61 33 69 35 34 4b 4b 33 37 31 4e 31 38 33 30 37 39	g160X..Jd160vB35824sr10 B47su7T 37k0RMg0Fb..0XBJ81432 1Vs22c6Y3 P8luf3866Z0b16X4MT5f49 7Vu8Ts0E X342Q9SK041IJS4uVR6E RkFz8pFC5L 2GH2by20i5224NcK3E0N2 W2Z3fd05D g1P029j6Jd8lW4Ye9vp9..i Q7q23wB oh9Z7u2hP834Q7z903tsm 1l9ruq8yj 01i30eS8Go7KU6571Z9cx 2948wbTa3 i54KK371N183079	success or wait	1	1359CC2	WriteFile
C:\Users\user\AppData\Roaming\22032878\btdbvndt.bmp	unknown	559	42 46 49 33 31 31 35 34 59 38 45 78 64 31 39 30 34 33 38 4d 33 42 44 37 67 30 72 32 52 37 30 65 4d 32 44 36 30 4c 6d 74 49 78 74 33 50 68 47 34 38 35 39 31 0d 0a 55 69 32 7a 76 34 72 36 46 73 65 65 39 64 38 75 71 5a 70 51 6c 71 54 38 44 46 34 6c 46 77 33 38 6e 32 4f 41 79 62 54 35 71 46 33 35 32 35 34 67 35 35 54 6a 45 36 0d 0a 78 64 32 36 66 31 71 5a 4a 50 4a 66 37 49 65 32 49 33 77 32 35 35 57 71 4e 62 68 48 57 59 34 48 55 71 58 37 37 35 6b 39 34 7a 6c 37 31 39 4a 65 30 34 55 66 77 4e 0d 0a 75 67 6f 32 38 30 34 6d 38 52 55 39 35 33 56 7a 36 4a 69 39 51 36 66 75 33 56 50 78 6b 78 34 39 34 53 62 42 78 33 48 31 41 75 38 35 37 4f 53 73 78 34 61 76 64 31 31 6e 67 45 36 4e 38 39 30 65 4f 64 4f 36 69 57 77 4f 33 33 37 6c 46 32 7a 30 63 30 73 78 43 46 63 42 39	BFl31154Y8Exd190438M3 BD7g0r2R7 0eM2D60LmtIxt3PhG4859 1..Ui2zv4 r6Fsee9d8uqZpQlqT8DF4l Fw38n2OA ybT5qF35254g55TjE6..xd2 6f1qZJP Jf7Ie2l3w255WqNbhHWY4 HUqX775k9 4zl719Je04UfwN..ugo2804 m8RU953 Vz6Ji9Q6fu3VPxkx494Sb Bx3H1Au85 7OSsx4avd11ngE6N890e OdO6iWwO33 7lF2z0c0sxCFcB9	success or wait	1	1359CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\vmwkpdfbe.xls	unknown	565	35 36 35 50 30 70 35 4a 38 36 66 55 39 33 34 75 30 54 39 75 38 4d 79 38 63 35 72 78 65 34 37 71 48 37 4c 35 33 4e 34 32 39 36 67 79 32 36 57 35 31 38 30 69 31 32 32 32 36 53 39 71 77 31 38 65 61 49 38 38 32 35 79 35 37 66 35 55 35 33 0d 0a 45 33 72 33 78 68 6e 54 4e 32 62 4d 48 38 68 64 62 33 35 44 4c 61 52 53 71 33 66 30 4e 69 30 37 71 35 58 56 32 48 54 71 38 37 32 64 48 4b 55 31 31 34 58 38 57 33 35 65 6c 38 4c 54 37 38 77 33 30 61 4d 34 31 50 30 4b 65 4f 52 56 36 63 76 52 6d 36 0d 0a 45 33 58 77 39 59 57 44 66 6c 72 55 42 44 77 62 54 49 34 76 76 31 73 33 66 32 35 72 38 50 77 4d 36 36 72 4a 50 56 31 55 58 35 36 34 36 39 7a 4e 51 37 30 31 32 0d 0a 38 4c 6d 4d 35 37 35 52 37 30 38 53 4b 69 31 6e 75 48 38 75 7a 34 30 38 72 46 71 39 32 66 38 75 62 63 38 4d	565P0p5J86fU934u0T9u8 My8c5rxe4 7qH7L53N4296gy26W5180 i12226S9q w18eaI8825y57f5U53..E3r 3xhnTN2 bMH8hdb35DLaRSq3f0Ni0 7q5XV2HTq 872dHKU114X8W35el8LT 78w30aM41P 0KeORV6cvRm6..E3Xw9Y WDflrUBDwb TI4vv1s3f25r8PwM66rJPV 1UX56469 zNQ7012..8LmM575R708 SKi1nuH8uz 408rFq92f8ubc8M	success or wait	1	1359CC2	WriteFile
C:\Users\user\AppData\Roaming\22032878\eseh.pdf	unknown	572	37 64 36 33 49 36 4b 78 36 4d 57 66 46 32 52 36 33 36 33 70 35 6e 31 32 51 77 31 37 57 37 32 39 32 6a 34 34 63 38 51 37 38 30 75 61 46 50 6f 48 38 37 35 35 47 4b 4a 37 42 37 37 38 31 34 36 51 36 71 36 31 37 63 37 56 49 5a 38 37 59 53 45 34 33 66 31 4e 4a 32 4d 34 46 44 6b 46 36 30 38 36 34 33 30 51 59 79 5a 6b 34 33 33 35 33 30 45 64 59 51 36 73 33 4e 61 31 76 34 52 30 39 55 39 30 56 4b 39 39 6a 38 37 37 34 5a 37 35 38 0d 0a 6f 35 31 56 64 53 50 73 31 31 32 6c 31 37 74 33 33 61 31 52 38 37 57 67 4d 36 66 76 68 5a 43 38 30 51 32 46 74 41 4b 5a 58 4a 78 38 39 31 32 39 30 49 37 0d 0a 6e 33 37 71 35 54 74 6d 31 52 35 78 69 51 47 52 55 4e 66 46 36 37 30 35 32 45 38 44 58 37 7a 36 39 36 30 34 39 70 37 37 51 30 35 70 50 59 30 73 56 5a 69 52 39 33 79 63 50 62 36	7d63I6Kx6MWfF2R6363p5 n12Qw17W7 292j44c8Q780uaFPoH875 5GKJ7B778 146Q6q617c7VIZ87YSE43 f1NJ2M4FD kF6086430QYyZk433530E dYQ6s3Na1 v4R09U90VK99j8774Z758. .o51VdSP s112l17t33a1R87WgM6fvh ZC80Q2Ft AKZXJx891290I7..n37q5Tt m1R5xiQ GRUNfF67052E8DX7z696 049p77Q05p PY0sVZiR93ycPb6	success or wait	1	1359CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\vhcpj.log	unknown	566	34 45 53 34 7a 32 32 53 66 51 69 76 35 75 36 34 6a 4c 34 61 38 64 67 36 6b 68 38 31 38 35 31 78 45 41 46 55 35 77 31 37 33 4b 35 38 6e 41 57 30 33 5a 56 39 4f 31 39 0d 0a 35 63 62 45 53 30 33 4d 72 30 37 52 5a 35 39 37 37 46 61 31 39 4c 53 6b 32 32 30 6d 33 35 39 77 7a 39 39 61 37 6d 34 70 55 38 34 37 34 33 68 32 35 35 34 6d 78 39 55 38 58 61 34 42 4c 6c 7a 56 4b 46 31 68 35 34 34 32 75 39 75 33 57 34 4a 63 31 4f 74 6d 38 38 52 31 32 35 44 74 42 4a 35 57 54 39 0d 0a 33 33 38 53 66 34 0d 0a 4d 39 4e 64 72 31 6b 37 5a 4d 65 5a 38 75 47 6d 32 6f 38 44 67 70 33 39 43 36 71 33 46 6c 32 78 4c 78 34 71 6a 31 59 79 30 72 31 52 37 74 52 45 79 34 38 36 37 32 39 36 33 39 35 36 30 41 36 5a 33 43 57 49 34 66 43 37 33 78 35 34 0d 0a 48 38 64 30 32 34 31 61 4b 34 78 4b	4ES4z22SfQiv5u64jL4a8d g6kh8185 1xEAFU5w173K58nAW03 ZV9O19..5cb ES03Mr07RZ5977Fa19LS k220m359wz 99a7m4pU84743h2554mx 9U8Xa4BLlz VKF1h5442u9u3W4Jc1Ot m88R125DtB J5WT9..338Sf4..M9Ndr1k 7ZMeZ8uG m2o8Dgp39C6q3Fl2xLx4qj 1Yy0r1R7 tREy486729639560A6Z3C WI4fC73x5 4..H8d0241aK4xK	success or wait	1	1359CC2	WriteFile
C:\Users\user\AppData\Roaming\22032878\ucjondx.exe	unknown	503	4f 6a 46 30 36 36 39 72 53 36 66 65 6e 34 4d 33 39 46 39 34 65 39 69 77 36 37 67 37 6d 45 57 52 41 6b 39 54 62 35 50 32 36 66 39 53 33 65 33 6d 42 79 35 6c 73 71 36 38 64 54 37 6d 77 6e 35 6d 61 33 34 31 37 62 33 36 36 32 55 34 31 32 33 31 77 41 34 34 62 75 37 38 37 37 55 69 6e 31 39 34 39 7a 31 37 73 35 44 0d 0a 30 54 33 30 36 74 34 33 65 32 72 38 4f 54 7a 4d 59 56 33 35 37 34 69 42 30 39 38 31 4f 34 75 71 38 36 56 67 38 66 33 6d 62 41 0d 0a 74 58 34 31 6f 34 6a 33 44 63 44 51 31 46 39 68 6e 31 41 30 6c 37 37 31 31 50 64 37 39 6b 4a 39 55 31 48 30 45 33 43 38 41 33 37 68 75 31 51 79 33 33 69 75 32 53 33 74 45 35 36 0d 0a 35 4a 35 52 32 62 4d 39 52 65 36 64 4a 30 64 36 46 38 37 6f 34 33 6e 36 33 34 36 66 57 0d 0a 4e 34 45 37 78 38 33 33 36 5a 56 67 0d 0a	OjF0669rS6fen4M39F94e9 iw67g7mE WRAk9Tb5P26f9S3e3mB y5lsq68dT7m wn5ma3417b3662U41231 wA44bu7877 Uin1949z17s5D..0T306t43 e2r8OTz MYV3574iB0981O4uq86V g8f3mbA..t X41o4j3DcDQ1F9hn1A0l7 711Pd79kJ 9U1H0E3C8A37hu1Qy33iu 2S3tE56.. 5J5R2bM9Re6dJ0d6F87o4 3n6346fW. .N4E7x8336ZVg..	success or wait	1	1359CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\poqhjae.xml	unknown	664	31 36 61 4f 51 37 53 30 35 68 47 31 30 37 57 39 35 55 39 38 36 36 32 59 39 34 32 76 4a 38 39 45 39 69 38 37 36 30 31 6d 43 51 38 35 6a 32 65 50 33 46 30 31 68 30 33 31 37 49 35 64 71 68 39 31 62 61 48 0d 0a 4e 38 65 75 36 4f 32 30 35 36 39 7a 6a 37 42 76 74 41 6e 33 44 47 4d 70 37 49 66 56 76 79 31 37 37 37 34 31 59 4a 32 78 33 55 6c 33 36 38 54 72 6c 38 31 33 66 35 38 41 56 38 0d 0a 4c 56 36 31 33 59 37 38 61 35 69 33 31 48 37 7a 4c 47 33 35 33 37 4d 30 35 77 37 64 72 37 31 35 37 74 44 36 38 30 4a 34 34 58 30 32 31 32 30 36 31 4a 0d 0a 32 4a 32 30 37 30 6d 48 31 38 33 38 30 30 39 76 53 49 44 56 49 65 64 0d 0a 35 30 53 6a 62 7a 36 36 33 38 57 49 34 39 39 6a 58 69 56 49 32 38 31 70 62 63 4d 6e 46 76 37 30 66 36 35 6c 39 79 36 36 63 33 66 37 39 78 37 48 38	16aOQ7S05hG107W95U9 8662Y942vJ8 9E9i87601mCQ85j2eP3F0 1h0317I5d qh91baH..N8eu6O20569zj 7BvtAn3D GMp7IfVvy177741YJ2x3Ul 368Trl81 3f58AV8..LV613Y78a5i31 H7zLG353 7M05w7dr7157tD680J44X 0212061J. .2J2070mH1838009vSIDV led..50Sj bz6638WI499jXiVI281pbc MnFv70f6 5l9y66c3f79x7H8	success or wait	1	1359CC2	WriteFile
C:\Users\user\AppData\Roaming\22032878\lojmm.bin	unknown	547	34 38 48 39 33 32 36 79 31 67 39 39 33 35 39 64 35 31 61 39 33 33 47 32 6b 6d 49 71 30 6c 39 33 35 33 32 37 48 75 32 31 74 77 37 59 54 33 37 34 65 30 35 79 49 62 34 33 38 34 42 33 38 33 34 30 34 31 44 35 38 34 32 0d 0a 34 39 73 52 53 37 31 31 4f 35 74 68 49 76 39 44 4e 32 41 74 32 61 70 5a 36 52 7a 32 71 36 72 32 52 30 32 37 57 32 72 47 73 6e 6d 30 38 36 35 37 37 78 32 53 64 35 55 4f 6f 47 37 6d 53 61 67 72 30 38 67 32 66 4e 79 43 35 76 31 44 42 37 6c 70 41 78 61 77 71 39 4d 69 35 39 52 55 31 36 4d 31 35 4c 30 37 30 37 56 6b 4c 33 45 36 31 34 47 45 38 4d 34 6f 35 50 31 37 4d 7a 4e 32 34 54 57 0d 0a 42 6e 32 59 70 34 30 38 70 37 79 4e 0d 0a 39 55 63 38 49 56 74 6c 37 61 32 6f 62 38 38 70 37 54 36 30 39 79 34 30 31 36 6b 32 32 37 6b 35 36 39 41 37 30 6f 33	48H9326y1g99359d51a933 G2kmlq0l 935327Hu21tw7YT374e05 ylb4384B3 834041D5842..49sRS711 O5thIv9DN 2At2apZ6Rz2q6r2R027W2 rGsnm0865 77x2Sd5UOoG7mSagr08g 2fNyC5v1DB 7lpAxawq9Mi59RU16M15L 0707VkL3E 614GE8M4o5P17MzN24T W..Bn2Yp408 p7yN..9Uc8IVtl7a2ob88p7 T609y40 16k227k569A70o3	success or wait	1	1359CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\txum.exe	unknown	575	4a 55 5a 61 31 35 38 30 36 35 39 59 5a 37 4d 35 46 51 37 50 36 61 37 78 35 32 37 4d 34 39 32 34 65 36 4a 36 38 31 31 68 34 34 32 56 39 32 44 66 33 37 68 38 67 30 32 77 4e 6f 36 39 6f 33 0d 0a 35 36 33 36 79 44 4c 75 63 0d 0a 36 36 30 51 67 32 35 6e 31 65 35 33 7a 35 43 34 34 32 74 54 41 45 62 67 36 73 35 45 34 4e 52 57 38 30 37 55 54 31 38 31 51 53 59 66 35 36 6a 55 69 34 52 37 74 63 44 65 4c 61 36 32 37 4e 48 37 33 32 34 69 38 41 38 33 4b 49 64 7a 34 6f 33 65 50 0d 0a 38 74 37 33 38 38 55 72 73 32 38 46 38 78 65 72 33 6d 38 6f 37 32 31 34 34 65 68 78 7a 7a 45 49 33 6c 6d 58 77 37 39 34 42 79 70 4f 30 32 38 31 31 77 38 4a 36 33 46 44 41 34 39 77 53 4c 31 35 37 30 50 33 31 33 36 30 63 79 33 78 38 39 4b 31 30 44 36 66 61 36 77 38 36 67 30 79 32 31 6e 38 50	JUZa1580659YZ7M5FQ7P 6a7x527M49 24e6J6811h442V92Df37h8 g02wNo69 o3..5636yDLuc..660Qg25n 1e53z5C 442tTAEbg6s5E4NRW807 UT181QSYf5 6jUi4R7tcDeLa627NH7324i 8A83KId z4o3eP..8t7388Urs28F8xe r3m8o72 144ehxzzEI3lmXw794Byp O02811w8J 63FDA49wSL1570P31360 cy3x89K10D 6fa6w86g0y21n8P	success or wait	1	1359CC2	WriteFile
C:\Users\user\AppData\Roaming\22032878\dnxuddwt.ppt	unknown	522	36 78 41 4a 4f 41 36 44 34 34 33 34 4c 44 69 45 32 52 30 42 52 33 43 38 37 32 32 37 32 36 35 5a 64 4b 73 52 6f 57 67 32 44 66 30 31 6d 34 39 32 63 32 6a 41 4f 36 38 59 6b 31 39 34 30 37 43 30 33 46 37 39 6d 62 33 58 31 4d 32 34 65 56 5a 49 38 34 4a 31 38 4b 30 50 4f 36 34 38 43 39 39 62 30 36 58 35 78 55 34 36 31 54 34 38 34 62 31 76 36 4a 44 30 32 36 30 66 48 33 35 66 32 6c 41 43 4f 79 51 45 43 56 33 0d 0a 32 54 36 70 36 30 69 33 72 31 6f 57 30 31 72 44 62 33 35 31 43 35 63 33 39 4e 32 6c 42 37 36 39 5a 38 67 30 33 56 57 30 0d 0a 50 45 58 54 59 35 39 31 31 77 65 72 34 66 6c 32 73 34 35 35 30 74 58 31 30 31 59 37 72 33 36 47 37 68 38 4f 75 36 44 36 30 30 32 6e 35 46 38 33 42 31 31 67 34 37 37 57 69 38 72 49 35 6a 77 42 30 33 31 33 38 43 36 76 32 63 36 49	6xAJOA6D4434LDiE2R0B R3C8722726 5ZdKsRoWg2Df01m492c2j AO68Yk194 07C03F79mb3X1M24eVZI 84J18K0PO6 48C99b06X5xU461T484b1 v6JD0260f H35f2lACOyQECV3..2T6p 60i3r1oW0 1rDb351C5c39N2lB769Z8g 03VW0..P EXTY5911wer4fl2s4550tX 101Y7r36 G7h8Ou6D6002n5F83B11 g477Wi8rI5 jwB03138C6v2c6I	success or wait	1	1359CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\rnpxxre.icm	unknown	550	32 39 6f 32 39 75 32 48 58 38 43 70 53 33 37 43 76 36 35 61 46 52 35 51 55 31 35 46 39 33 32 35 36 58 59 31 7a 30 70 43 43 34 4c 68 30 33 5a 6b 39 48 38 35 64 6d 31 7a 32 51 75 0d 0a 31 37 65 32 73 35 77 49 61 33 4f 39 54 50 4e 32 33 59 78 48 32 31 63 59 75 57 70 52 77 42 33 4e 64 34 54 35 6c 36 33 31 31 78 30 33 35 6b 32 39 45 59 63 38 72 32 38 4f 37 71 35 71 33 38 53 68 30 4a 35 62 0d 0a 46 37 76 6e 54 32 4b 39 4f 6c 47 78 77 0d 0a 4c 31 33 38 51 44 30 51 35 32 70 56 31 38 35 31 50 55 42 31 32 38 30 4b 4c 34 5a 39 31 33 37 33 38 51 34 38 6f 34 42 37 30 38 39 38 6d 4b 65 32 39 56 77 30 70 4b 38 39 75 49 37 35 33 37 76 43 39 37 37 31 72 35 33 34 69 48 39 33 74 62 37 4e 59 38 51 35 6b 36 68 6d 38 38 55 78 79 37 47 30 35 65 31 50 32 32 34 79 77 37 42 67 69	29o29u2HX8CpS37Cv65a FR5QU15F93 256XY1z0pCC4Lh03Zk9H 85dm1z2Qu. .17e2s5wIa3O9TPN23YxH 21cYuWpRw B3Nd4T5l6311x035k29EY c8r28O7q5 q38Sh0J5b..F7vnT2K9OlG xw..L138 QD0Q52pV1851PUB1280 KL4Z913738Q 48o4B70898mKe29Vw0pK 89uI7537vC 9771r534iH93tb7NY8Q5k6 hm88Uxy7 G05e1P224yw7Bgi	success or wait	1	1359CC2	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\zunUbtZ2Y3.exe	unknown	8192	success or wait	129	1359678	ReadFile

Analysis Process: nfiuc.pif PID: 984 Parent PID: 4728

General

Start time:	19:06:08
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\22032878\nfiuc.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\22032878\nfiuc.pif' xaso.fhr
Imagebase:	0xee0000
File size:	664816 bytes
MD5 hash:	51663CBA5E7E841A0443112BF5E57049
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.677255613.000000000423F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.677255613.000000000423F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.677255613.000000000423F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.677318458.0000000004272000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.677318458.0000000004272000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.677318458.0000000004272000.00000004.00000001.sdmp, Author:

Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.679566684.00000000041A1000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.679566684.00000000041A1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.679566684.00000000041A1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.679501436.00000000041D5000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.679501436.00000000041D5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.679501436.00000000041D5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.679383356.000000000420A000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.679383356.000000000420A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.679383356.000000000420A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.678729204.0000000004155000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.678729204.0000000004155000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.678729204.0000000004155000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.676679410.00000000041D5000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.676679410.00000000041D5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.676679410.00000000041D5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.677221211.000000000420A000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.677221211.000000000420A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.677221211.000000000420A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.677158257.000000000420A000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.677158257.000000000420A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.677158257.000000000420A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.676738123.0000000004155000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.676738123.0000000004155000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.676738123.0000000004155000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.676806998.00000000041A1000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.676806998.00000000041A1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.676806998.00000000041A1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.676882345.0000000004121000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.676882345.0000000004121000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.676882345.0000000004121000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.679249376.0000000004121000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.679249376.0000000004121000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.679249376.0000000004121000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.677081542.0000000004155000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.677081542.0000000004155000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.677081542.0000000004155000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 19%, Metadefender, Browse • Detection: 45%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F1362A	CreateDirectoryW
C:\Users\user\AppData\Roaming\22032878\Update.vbs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	F0629C	CreateFileW
C:\Users\user\AppData\Local\Temp\RegSvcs.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	F2BEBA	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\Update.vbs	unknown	134	43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 2e 52 75 6e 20 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 32 32 30 33 32 38 37 38 5c 6e 66 69 75 63 2e 70 69 66 20 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 32 32 30 33 32 38 37 38 5c 78 61 73 6f 2e 66 68 72 22	CreateObject("Wscript.Shell").Run "C:\Users\user\AppData\Roaming\22032878\nfiuc.pif C:\Users\user\AppData\Roaming\22032878\xaso.fhr"	success or wait	1	F23D5E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0	45152	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7a 58 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 83 00 00 00 20 00 00 00 a0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 e0 00 00 00 02 00 00 a9 22 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...zX.Z.......... ....0..d..........V.... ....@.. ...."....`................	success or wait	1	F2BEBA	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\xaso.fhr	unknown	65536	success or wait	1362	EFDB2F	ReadFile
C:\Users\user\AppData\Roaming\22032878\xaso.fhr	unknown	8192	end of file	2	EFDB2F	ReadFile
C:\Users\user\AppData\Roaming\22032878\xaso.fhr	unknown	65536	success or wait	1	EE3B98	ReadFile
C:\Users\user\AppData\Roaming\22032878\xaso.fhr	unknown	65536	success or wait	1314	EE3B98	ReadFile
C:\Users\user\AppData\Roaming\22032878\xaso.fhr	unknown	65536	end of file	1	EE3B98	ReadFile
C:\Users\user\AppData\Roaming\22032878\Update.vbs	unknown	65536	end of file	1	EE3B98	ReadFile
C:\Users\user\AppData\Roaming\22032878\lqjmggks.ico	unknown	65536	success or wait	1	EE3B98	ReadFile
C:\Users\user\AppData\Roaming\22032878\lqjmggks.ico	unknown	65536	success or wait	8	EE3B98	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	Chrome	unicode	C:\Users\user\AppData\Roaming\22032878\nfiuc.pif C:\Users\user\AppData\Roaming\22032878\xaso.fhr	success or wait	1	F4ADDA	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	AutoUpdate	unicode	C:\Users\user\AppData\Roaming\22032878\Update.vbs	success or wait	1	F4ADDA	RegSetValueExW

Analysis Process: RegSvcs.exe PID: 5660 Parent PID: 984

General

Start time:	19:06:13
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe

Imagebase:	0x70000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.923227276.00000000028C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.927044565.00000000060B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.927044565.00000000060B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.927044565.00000000060B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.927012461.00000000060A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.927012461.00000000060A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.926952371.0000000006010000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.926952371.0000000006010000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.922381074.0000000000502000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.922381074.0000000000502000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.922381074.0000000000502000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.924061373.0000000003909000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.924061373.0000000003909000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	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	6D3DCF06	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	6C22BEFF	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	6C221E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C22BEFF	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	6C22DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp3E2B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C227038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp4272.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C227038	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	6C22BEFF	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	6C22BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3E2B.tmp	success or wait	1	6C226A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp4272.tmp	success or wait	1	6C226A95	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	7a 14 47 9f b0 fa d8 48	z.G....H	success or wait	1	6C221B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	45152	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7a 58 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 83 00 00 00 20 00 00 00 a0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 e0 00 00 00 02 00 00 a9 22 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...zX.Z.......... ....0..d..........V.... ....@.. ...."....`................	success or wait	1	6C22DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp3E2B.tmp	unknown	1308	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	6C221B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	45	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 52 65 67 53 76 63 73 2e 65 78 65	C:\Users\user\AppData\Local\Temp\RegSvcs.exe	success or wait	1	6C221B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4272.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	6C221B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D39D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D39D72F	unknown
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	unknown	4096	success or wait	1	6D39D72F	unknown
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	unknown	512	success or wait	1	6D39D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6C22646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 5844 Parent PID: 5660

General

Start time:	19:06:17
Start date:	08/04/2021
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\tmp3E2B.tmp'
Imagebase:	0x1270000
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\tmp3E2B.tmp	unknown	2	success or wait	1	127AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3E2B.tmp	unknown	1309	success or wait	1	127ABD9	ReadFile

Analysis Process: conhost.exe PID: 5896 Parent PID: 5844

General

Start time:	19:06:17
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 5556 Parent PID: 5660

General

Start time:	19:06:18
Start date:	08/04/2021
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\tmp4272.tmp'
Imagebase:	0x1270000
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\tmp4272.tmp	unknown	2	success or wait	1	127AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4272.tmp	unknown	1311	success or wait	1	127ABD9	ReadFile

Analysis Process: conhost.exe PID: 2864 Parent PID: 5556

General

Start time:	19:06:18
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 5036 Parent PID: 968

General

Start time:	19:06:19
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0
Imagebase:	0xff0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6C221B4F	WriteFile
\Device\ConDrv	unknown	141	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 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 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 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6C221B4F	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	6C221B4F	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	6C221B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	unknown	142	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 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 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	6D6EC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile

Analysis Process: conhost.exe PID: 4936 Parent PID: 5036

General

Start time:	19:06:20
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 1472 Parent PID: 968

General

Start time:	19:06:21
Start date:	08/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x60000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6C221B4F	WriteFile
\Device\ConDrv	unknown	141	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 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 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 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6C221B4F	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	6C221B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\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	6C221B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	142	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 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 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	6D6EC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile

Analysis Process: conhost.exe PID: 1440 Parent PID: 1472

General

Start time:	19:06:22
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: nfiuc.pif PID: 1380 Parent PID: 3424

General

Start time:	19:06:22
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\22032878\nfiuc.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\22032878\nfiuc.pif' C:\Users\user\AppData\Roaming\22032878\xaso.fhr
Imagebase:	0xee0000
File size:	664816 bytes

MD5 hash:	51663CBA5E7E841A0443112BF5E57049
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.708352984.000000000474B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.708352984.000000000474B000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.708352984.000000000474B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.708271591.0000000004718000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.708271591.0000000004718000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.708271591.0000000004718000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.710662958.0000000004646000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.710662958.0000000004646000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.710662958.0000000004646000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.710938676.0000000004611000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.710938676.0000000004611000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.710938676.0000000004611000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.707826555.00000000046AF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.707826555.00000000046AF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.707826555.00000000046AF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.710381105.000000000467A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.710381105.000000000467A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.710381105.000000000467A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.707511293.000000000467A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.707511293.000000000467A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.707511293.000000000467A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.709101376.00000000039C8000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.709101376.00000000039C8000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.709101376.00000000039C8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.707372891.00000000046AF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.707372891.00000000046AF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.707372891.00000000046AF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.710427838.00000000046E2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source:

	0000000B.00000003.710427838.00000000046E2000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.710427838.00000000046E2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.707926521.00000000046E3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.707926521.00000000046E3000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.707926521.00000000046E3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.710514323.00000000046E2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.710514323.00000000046E2000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.710514323.00000000046E2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.707412308.0000000004611000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.707412308.0000000004611000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.707412308.0000000004611000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.709214730.00000000039A5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.709214730.00000000039A5000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.709214730.00000000039A5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.707670444.0000000004646000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.707670444.0000000004646000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.707670444.0000000004646000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.707301176.0000000004646000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.707301176.0000000004646000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.707301176.0000000004646000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.710256620.00000000046AF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.710256620.00000000046AF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.710256620.00000000046AF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000003.708173598.00000000046E3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000003.708173598.00000000046E3000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.708173598.00000000046E3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	cannot delete	1	F2BE65	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\Update.vbs	unknown	134	43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 2e 52 75 6e 20 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 32 32 30 33 32 38 37 38 5c 6e 66 69 75 63 2e 70 69 66 20 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 32 32 30 33 32 38 37 38 5c 78 61 73 6f 2e 66 68 72 22	CreateObject("Wscript.Shell").Run "C:\Users\user\AppData\Roaming\22032878\nfiuc.pif C:\Users\user\AppData\Roaming\22032878\xaso.fhr"	success or wait	1	F23D5E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22032878\xaso.fhr	unknown	65536	success or wait	1362	EFDB2F	ReadFile
C:\Users\user\AppData\Roaming\22032878\xaso.fhr	unknown	8192	end of file	2	EFDB2F	ReadFile
C:\Users\user\AppData\Roaming\22032878\xaso.fhr	unknown	65536	success or wait	1	EE3B98	ReadFile
C:\Users\user\AppData\Roaming\22032878\xaso.fhr	unknown	65536	success or wait	1314	EE3B98	ReadFile
C:\Users\user\AppData\Roaming\22032878\xaso.fhr	unknown	65536	end of file	1	EE3B98	ReadFile
C:\Users\user\AppData\Roaming\22032878\Update.vbs	unknown	65536	success or wait	1	EE3B98	ReadFile
C:\Users\user\AppData\Roaming\22032878\Update.vbs	unknown	65536	end of file	1	EE3B98	ReadFile
C:\Users\user\AppData\Roaming\22032878\lqjmggks.ico	unknown	65536	success or wait	1	EE3B98	ReadFile
C:\Users\user\AppData\Roaming\22032878\lqjmggks.ico	unknown	65536	success or wait	8	EE3B98	ReadFile

Analysis Process: RegSvcs.exe PID: 4876 Parent PID: 1380

General

Start time:	19:06:28
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x8e0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.729421320.0000000000D02000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.729421320.0000000000D02000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.729421320.0000000000D02000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.732406620.0000000004439000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.732406620.0000000004439000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.732316965.0000000003431000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.732316965.0000000003431000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	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	6D3DCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: wscript.exe PID: 4612 Parent PID: 3424

General

Start time:	19:06:30
Start date:	08/04/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false

Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\22032878\Update.vbs'
Imagebase:	0x7ff7764a0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: dhcpmon.exe PID: 2044 Parent PID: 3424

General

Start time:	19:06:38
Start date:	08/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x940000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 4808 Parent PID: 2044

General

Start time:	19:06:39
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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