ID: 385025
Sample Name:
OjAJYVQ7iK.exe
Cookbook: default.jbs
Time: 09:01:13
Date: 11/04/2021
Version: 31.0.0 Emerald

Table of Contents

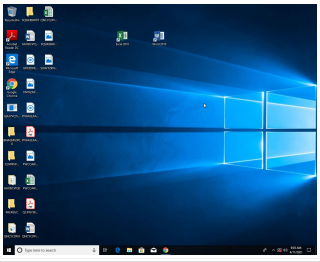
Analysis Report OjAJYVQ7iK.exe

Overview

General Information

Sample Name:	OjAJYVQ7iK.exe
Analysis ID:	385025
MD5:	d7d3373ffbd938d..
SHA1:	44a01528433887..
SHA256:	9829c2298ab328..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

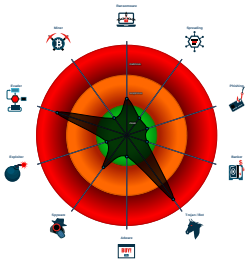
Nanocore

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates many large memory junks
- C2 URLs / IPs found in malware con…

Classification



Startup

- **System is w10x64**
- OjAJYVQ7iK.exe (PID: 4856 cmdline: 'C:\Users\user\Desktop\OjAJYVQ7iK.exe' MD5: D7D3373FFBD938DA6C7C8AA3DC57FA49)
  - OjAJYVQ7iK.exe (PID: 6772 cmdline: C:\Users\user\Desktop\OjAJYVQ7iK.exe MD5: D7D3373FFBD938DA6C7C8AA3DC57FA49)
    - schtasks.exe (PID: 6956 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp691F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 7084 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp6C3D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 7096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- OjAJYVQ7iK.exe (PID: 7164 cmdline: C:\Users\user\Desktop\OjAJYVQ7iK.exe 0 MD5: D7D3373FFBD938DA6C7C8AA3DC57FA49)
- dhcpmon.exe (PID: 5572 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: D7D3373FFBD938DA6C7C8AA3DC57FA49)
  - dhcpmon.exe (PID: 5884 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: D7D3373FFBD938DA6C7C8AA3DC57FA49)
- dhcpmon.exe (PID: 5624 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: D7D3373FFBD938DA6C7C8AA3DC57FA49)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "89ddcccb-9ca7-4a7e-8f49-ad5044b8",
  "Group": "CRYPTED",
  "Domain1": "ludwigh.duckdns.org",
  "Domain2": "ghfsquad.duckdns.org",
  "Port": 8192,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Enable",
  "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": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "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
00000019.00000002.423134588.000000000462 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000019.00000002.423134588.000000000462 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x49a9d:$a: NanoCore • 0x49af6:$a: NanoCore • 0x49b33:$a: NanoCore • 0x49bac:$a: NanoCore • 0x5d257:$a: NanoCore • 0x5d26c:$a: NanoCore • 0x5d2a1:$a: NanoCore • 0x7624b:$a: NanoCore • 0x76260:$a: NanoCore • 0x76295:$a: NanoCore • 0x49aff:$b: ClientPlugin • 0x49b3c:$b: ClientPlugin • 0x4a43a:$b: ClientPlugin • 0x4a447:$b: ClientPlugin • 0x5d013:$b: ClientPlugin • 0x5d02e:$b: ClientPlugin • 0x5d05e:$b: ClientPlugin • 0x5d275:$b: ClientPlugin • 0x5d2aa:$b: ClientPlugin • 0x76007:$b: ClientPlugin • 0x76022:$b: ClientPlugin
00000019.00000002.421572574.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000019.00000002.421572574.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000019.00000002.421572574.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
25.2.dhcpmon.exe.3643ac8.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
25.2.dhcpmon.exe.3643ac8.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
25.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
25.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
25.2.dhcpmon.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 14 entries				

Sigma Overview

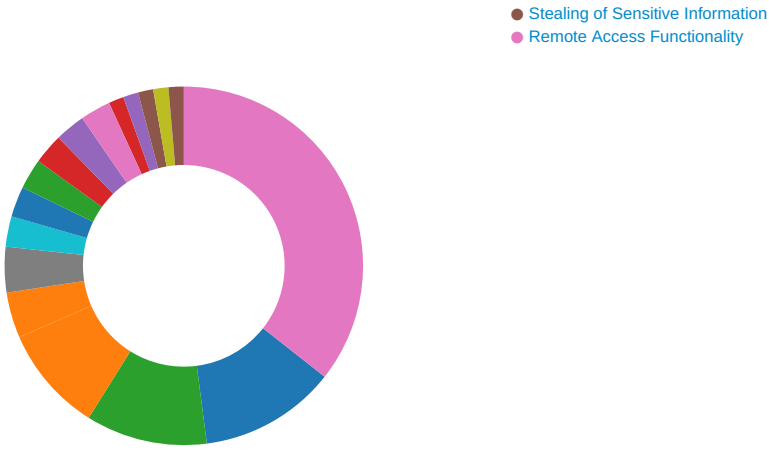
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

- AV Detection
- Compliance
- 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



Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking:

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

Boot Survival:

- Creates an undocumented autostart registry key
- 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:

Allocates many large memory junks

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

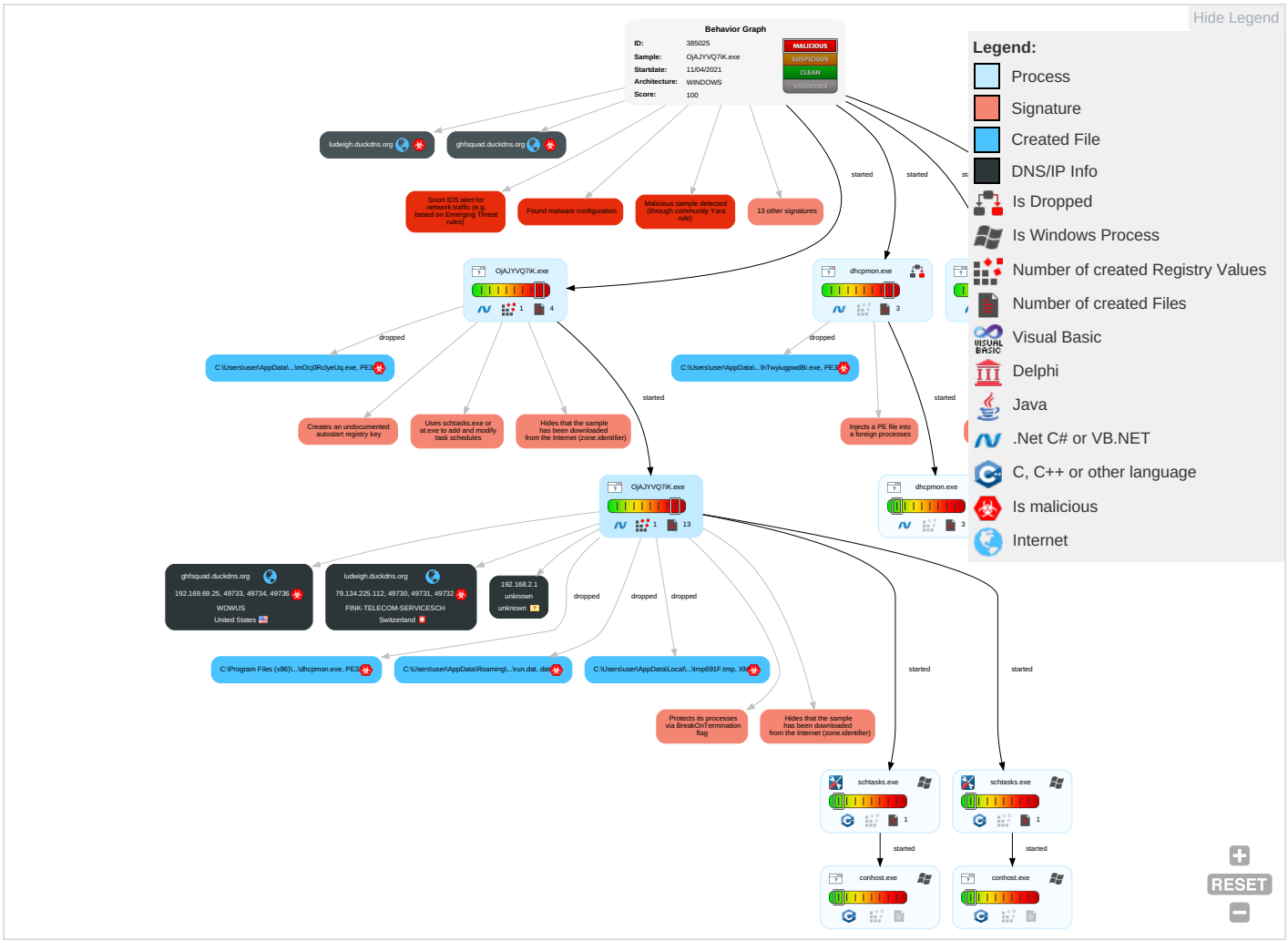
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 1	Masquerading 2	Input Capture 1 1	Security Software Discovery 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	System Information Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu 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
OjAJYVQ7iK.exe	81%	Virustotal		Browse
OjAJYVQ7iK.exe	51%	Metadefender		Browse
OjAJYVQ7iK.exe	89%	ReversingLabs	ByteCode-MSIL.Trojan.Persistence	
OjAJYVQ7iK.exe	100%	Avira	HEUR/AGEN.1137075	
OjAJYVQ7iK.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	HEUR/AGEN.1137075	
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\hTwyiugpwdBi.exe	100%	Avira	HEUR/AGEN.1137075	
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\mOcj0RclyeUq.exe	100%	Avira	HEUR/AGEN.1137075	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\hTwyiugpwdBi.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\mOcj0RclyeUq.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	51%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	89%	ReversingLabs	ByteCode-MSIL.Trojan.Persistence	
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\hTwyiugpwdBi.exe	51%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\hTwyiugpwdBi.exe	89%	ReversingLabs	ByteCode-MSIL.Trojan.Persistence	
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\mOcj0RclyeUq.exe	51%	Metadefender		Browse
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\mOcj0RclyeUq.exe	89%	ReversingLabs	ByteCode-MSIL.Trojan.Persistence	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
25.0.dhcpmon.exe.e50000.0.unpack	100%	Avira	HEUR/AGEN.1118533		Download File
16.0.OjAJYVQ7iK.exe.e60000.0.unpack	100%	Avira	HEUR/AGEN.1118533		Download File
21.0.OjAJYVQ7iK.exe.980000.0.unpack	100%	Avira	HEUR/AGEN.1118533		Download File
25.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
22.0.dhcpmon.exe.fa0000.0.unpack	100%	Avira	HEUR/AGEN.1118533		Download File
24.0.dhcpmon.exe.b50000.0.unpack	100%	Avira	HEUR/AGEN.1118533		Download File
25.2.dhcpmon.exe.e50000.1.unpack	100%	Avira	HEUR/AGEN.1118533		Download File
1.0.OjAJYVQ7iK.exe.570000.0.unpack	100%	Avira	HEUR/AGEN.1118533		Download File

Domains

Source	Detection	Scanner	Label	Link
ghfsquad.duckdns.org	5%	Virustotal		Browse
ludwigh.duckdns.org	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cners	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.coma-d#	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr/	0%	Avira URL Cloud	safe	
ghfsquad.duckdns.org	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krj	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/t	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Verd	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://en.wg	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn.	0%	Avira URL Cloud	safe	
http://www.fonts.comcc	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/7	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/7	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/7	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
ludwigh.duckdns.org	0%	Avira URL Cloud	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.founder.com.cn/cns-cTt	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ana	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/nX	0%	Avira URL Cloud	safe	
http://www.tiro.comm	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.fonts.comt	0%	Avira URL Cloud	safe	
http://www.tiro.comc	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Micri	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ghfsquad.duckdns.org	192.169.69.25	true	true	• 5%, Virustotal, Browse	unknown
ludwigh.duckdns.org	79.134.225.112	true	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

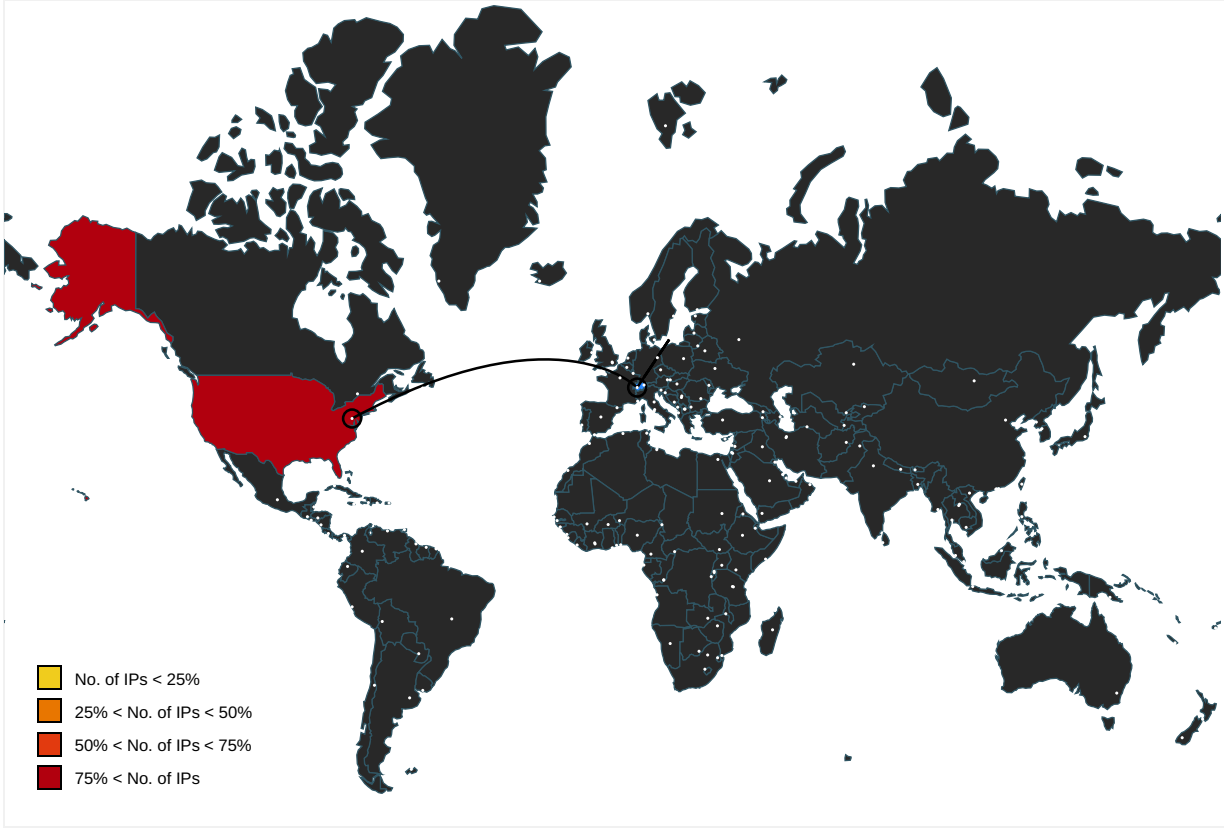
Name	Malicious	Antivirus Detection	Reputation
ghfsquad.duckdns.org	true	• Avira URL Cloud: safe	unknown
ludwigh.duckdns.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cners	OjAJYVQ7iK.exe, 00000001.00000003.195587180.0000000004FF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersP?	OjAJYVQ7iK.exe, 00000001.00000003.198068340.0000000004FF9000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.coma-d#	OjAJYVQ7iK.exe, 00000001.00000003.194547907.000000000500B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr/	OjAJYVQ7iK.exe, 00000001.00000003.195250311.0000000004FF9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krj	OjAJYVQ7iK.exe, 00000001.00000003.195250311.0000000004FF9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	OjAJYVQ7iK.exe, 00000001.00000003.194725696.000000000500B000.00000004.00000001.sdmp, OjAJYVQ7iK.exe, 00000001.00000003.194739543.000000000500B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	OjAJYVQ7iK.exe, 00000001.00000003.198423875.0000000004FFD000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/t	OjAJYVQ7iK.exe, 00000001.00000003.196509907.0000000004FF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	OjAJYVQ7iK.exe, 00000001.00000003.196509907.0000000004FF4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comX	OjAJYVQ7iK.exe, 00000001.00000003.194562488.000000000500B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Verd	OjAJYVQ7iK.exe, 00000001.00000003.196509907.0000000004FF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	OjAJYVQ7iK.exe, 00000001.00000003.194547907.000000000500B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	OjAJYVQ7iK.exe, 00000001.00000003.195713949.0000000004FF4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.wg	OjAJYVQ7iK.exe, 00000001.00000003.194304933.000000000106D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn.	OjAJYVQ7iK.exe, 00000001.00000003.195587180.0000000004FF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comcc	OjAJYVQ7iK.exe, 00000001.00000003.194586100.000000000500B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/7	OjAJYVQ7iK.exe, 00000001.00000003.196509907.0000000004FF4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	OjAJYVQ7iK.exe, 00000001.00000003.195576488.000000000502D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comic	OjAJYVQ7iK.exe, 00000001.00000003.194586100.000000000500B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cns-cTt	OjAJYVQ7iK.exe, 00000001.00000003.195576488.000000000502D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	OjAJYVQ7iK.exe, 00000001.00000003.196509907.0000000004FF4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ana	OjAJYVQ7iK.exe, 00000001.00000003.196509907.0000000004FF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	OjAJYVQ7iK.exe, 00000001.00000003.196509907.0000000004FF4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/nX	OjAJYVQ7iK.exe, 00000001.00000003.195713949.0000000004FF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comm	OjAJYVQ7iK.exe, 00000001.00000003.194711594.000000000500B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/(	OjAJYVQ7iK.exe, 00000001.00000003.196509907.0000000004FF4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	OjAJYVQ7iK.exe, 00000001.00000003.194547907.000000000500B000.00000004.00000001.sdmp	false		high
http://www.fonts.comt	OjAJYVQ7iK.exe, 00000001.00000003.194562488.000000000500B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers:	OjAJYVQ7iK.exe, 00000001.00000003.198068340.0000000004FF9000.00000004.00000001.sdmp	false		high
http://www.tiro.comc	OjAJYVQ7iK.exe, 00000001.00000003.194711594.000000000500B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Micri	OjAJYVQ7iK.exe, 00000001.00000003.196509907.0000000004FF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.112	ludwigh.duckdns.org	Switzerland		6775	FINK-TELECOM-SERVICESCH	true
192.169.69.25	ghfsquad.duckdns.org	United States		23033	WOWUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385025
Start date:	11.04.2021
Start time:	09:01:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OjAJYVQ7iK.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@14/8@28/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 52.147.198.201, 168.61.161.212, 104.43.193.48, 52.255.188.83, 20.50.102.62, 23.54.113.104, 23.0.174.185, 23.0.174.200, 23.10.249.26, 23.10.249.43, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:03:10	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
09:03:11	API Interceptor	351x Sleep call for process: OjAJYVQ7iK.exe modified
09:03:12	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\OjAJYVQ7iK.exe" s>$(Arg0)
09:03:13	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.112	Purchase Order Confirmation.exe	Get hash	malicious	Browse	
	JOIN DOO ORDER.exe	Get hash	malicious	Browse	
192.169.69.25	ttmPnejtED.js	Get hash	malicious	Browse	• pluginsrv.duckdns.org:7744/is-ready
	New Order.xlsx	Get hash	malicious	Browse	• systemserverrootmapforfiletrn.duckdns.org/explorer/black.exe
	Your Transport Plan has Changed - Maersk.xlsx	Get hash	malicious	Browse	• covidinternationalspreadsoomuchtrueheaded.duckdns.org/covid/blk.exe
	XQqVczq7eQ.exe	Get hash	malicious	Browse	• wetransferfax.duckdns.org/sftp.exe
	http://office365update.duckdns.org	Get hash	malicious	Browse	• office365update.duckdns.org/
	TUdme7rF2G.rtf	Get hash	malicious	Browse	• wsdykungcommunicationtarisupliermg55gms.duckdns.org/kungdoc/winlog.exe
	http://communicationideadedicatedserversystem.duckdns.org/bns/vbc.exe	Get hash	malicious	Browse	• communicationideadedicatedserversystem.duckdns.org/bns/vbc.exe
	doc04483720200602121810.xlsx	Get hash	malicious	Browse	• honeyspossecurityfileexchangeservice.duckdns.org/org/vbc.exe
	doc04483720200602121810.xlsx	Get hash	malicious	Browse	• honeyspossecurityfileexchangeservice.duckdns.org/org/vbc.exe
	BBVA-Confirming Facturas Pagadas al Vencimiento.xlsx	Get hash	malicious	Browse	• mkpksb2overhypetheykillppelforlifehelgg.duckdns.org/mkpk2doc/regasm.exe
	VqtnFLslNj_Purchase Order.vbs	Get hash	malicious	Browse	• onyeeze.duckdns.org:5000/is-ready
	1.bin.js	Get hash	malicious	Browse	• unknownsoft.duckdns.org:7755/is-ready
	Doc1.mht	Get hash	malicious	Browse	• pluginsrv2.duckdns.org:8899/is-ready
	http://https://cdn.discordapp.com/attachments/692273473430749187/695380419897458718/RFQ.tar.gz	Get hash	malicious	Browse	• pluginsrv2.duckdns.org:8000/is-ready

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://systemserverrootmapforfiletrn.duckdns.org/explorer/black.exe	Get hash	malicious	Browse	• systemserverrootmapforfiletrn.duckdns.org/explorer/black.exe
	help.wsf	Get hash	malicious	Browse	• postventa-vodafone.duckdns.org/is-ready
	order.xlsx	Get hash	malicious	Browse	• windowsfirewallsecurityauthorise.duckdns.org/big/svch.html
	order.xlsx	Get hash	malicious	Browse	• windowsfirewallsecurityauthorise.duckdns.org/big/svch.html
	54RFQ EU (190926) CRYPTED.js	Get hash	malicious	Browse	• pluginsrv1.duckdns.org:7757/is-ready
	5Hb61XJTf8.jar	Get hash	malicious	Browse	• pluginsrv1.duckdns.org:7757/is-ready

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WOWUS	1FC9626D978197A611B62BF796D472A6F8AB372E70DDF.exe	Get hash	malicious	Browse	• 192.169.69.26
	A4816D4FECD6D2806D5B105C3AAB55F4A1EB5DEB3B126.exe	Get hash	malicious	Browse	• 192.169.69.26
	qnJXJsqt1M.exe	Get hash	malicious	Browse	• 192.169.69.26
	1RkccAiQMy.exe	Get hash	malicious	Browse	• 192.169.69.25
	NaHU7wO2Wf.exe	Get hash	malicious	Browse	• 192.169.69.25
	hQtNCi8128.exe	Get hash	malicious	Browse	• 192.169.69.25
	FB11.exe	Get hash	malicious	Browse	• 216.244.74.42
	CDFCB9455FC457AC23BE82004BDCF4120E3C8D6FD2918.exe	Get hash	malicious	Browse	• 192.169.69.25
	EUjk8F87b8.exe	Get hash	malicious	Browse	• 192.169.69.25
	MglhrJiLUL.exe	Get hash	malicious	Browse	• 192.169.69.26
	On35KJkYT4.exe	Get hash	malicious	Browse	• 192.169.69.26
	ORDER-0319.pdf.exe	Get hash	malicious	Browse	• 192.169.69.25
	ORDER-21031566AF.exe	Get hash	malicious	Browse	• 192.169.69.25
	ttmPnejtED.js	Get hash	malicious	Browse	• 192.169.69.25
	3Ad4ZKWT0L.exe	Get hash	malicious	Browse	• 192.169.69.25
	EbJIveZLAv.exe	Get hash	malicious	Browse	• 192.169.69.26
	Order_List.xlsx	Get hash	malicious	Browse	• 192.169.69.26
	payload3.exe	Get hash	malicious	Browse	• 192.169.69.25
	ORDER-02108 xls.exe	Get hash	malicious	Browse	• 192.169.69.25
	ORDER #0206.exe	Get hash	malicious	Browse	• 192.169.69.25
FINK-TELECOM-SERVICESCH	TSskTqG9V9.exe	Get hash	malicious	Browse	• 79.134.225.30
	Files Specification.xlsx	Get hash	malicious	Browse	• 79.134.225.30
	J62DQ7fO0b.exe	Get hash	malicious	Browse	• 79.134.225.30
	oE6O5K1emC.exe	Get hash	malicious	Browse	• 79.134.225.30
	zunUbtZ2Y3.exe	Get hash	malicious	Browse	• 79.134.225.40
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	yBio5dWAOI.exe	Get hash	malicious	Browse	• 79.134.225.7
	wDIaJji4Vv.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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\OjAJYVQ7iK.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	418304
Entropy (8bit):	7.933921685316817
Encrypted:	false
SSDEEP:	6144:akoMdtpU20db9m2HuW5G2u0NvHmVX0khUf8WbtXxB5Ojxqe6+j0m5Y:akzlWu0N+Af8OXpO17A
MD5:	D7D3373FFBD938DA6C7C8AA3DC57FA49
SHA1:	44A01528433887323F7CD6495387AD189252D72D
SHA-256:	9829C2298AB32875E7379274C578FCBFFCDDAA36A262C74F69D113217913E5CA
SHA-512:	15D51363CC6A2E448DAE680A64707F8E9732992E916F966C8583B719CE9454E8D9BB364356907F666673A2EC2872F4253751E327BAD72FBE69DFDEFEAFFD573F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 51%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....]..... .....0..X.....v... .....@.. ..... .@.....Pv..K..... ....H.....text....V... ...X..... ..`.rsrc.....Z.....@..@.relo c.....`.....@..B.....v.....H.....K...*.....I.....0.....*....0.....(....*..0.....(.....(....*....0.....(....*..0.....%.~....%- .&~.....s....%.....%.~....%-.&~.....s....%.....%.~....%-.&~.....s....%.....%.~....%-.&~.....s....%.....*..0.....s".....8.... .R..... .y1X ....a ...d ..B.YX .[S. .... .,.XZY Q..\Z I..1f b..q .s..aeeXa @..= ....af .=.. ....eZYfeaa S..J .a. e .~.. .*..Ya 1.|.Xafa .=

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	high, very likely benign file

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

C:\Users\user\AppData\Local\Temp\tmp691F.tmp	
Process:	C:\Users\user\Desktop\OjAJYVQ7iK.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	5.132166972547854
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Hxtn:cbk4oL600QydbQxIYODOLedq3wj
MD5:	D93A57D549AA03755BEF9B5AB70F8765
SHA1:	7D9E6AA25A97F334349173FF9C32CA635F6E6CD1
SHA-256:	52D72D1AF0AB2D125603529108AACE2FEED0E8D26286E1F1989C97A0629F88A7
SHA-512:	2666D70F97801BC9D07B96528DACC4962263896E9F6E22B46572EEAFAAA409096FC4BA89C4F3DEAF8D4C94BCAF415E0E6695ACCEA97A960303139CD1F31ABF0
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <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\tmp6C3D.tmp	
Process:	C:\Users\user\Desktop\OjAJYVQ7iK.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\OjAJYVQ7iK.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Tdm4n:9
MD5:	4D6613AC2CE40C13C7EBEA2D8595F1B9
SHA1:	3A948AAA215B9952A8B9E276F6DA3D70F05794B9
SHA-256:	3232EDB50BFEB4EB38E7A6776D4C8BADF53B3F35E815898EEB235589F43B21A0
SHA-512:	F3C577A4883C6C848DCA3144757E163F3B7D421222B6EFAAFE008B29AE3089D3CF797E20EE45B5491571D2BD5859A33B4FB9E128803F4DE8764E2F5ED0BA5B9
Malicious:	**true**
Reputation:	low
Preview:	\.M...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\OjAJYVQ7iK.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.59445640611102
Encrypted:	false
SSDEEP:	3:oNWXp5vqP3AdAn:oNWXpFqPwdA
MD5:	0EC34671363D574D0987FCB496CE9834
SHA1:	8C11DE2D2A58721605F56AE0A51AABAEAA236713
SHA-256:	2F573ADB61920142AAECBD7765C2759CC79E1C06F6CA3C912749B3415340D4CB
SHA-512:	206863D05A766EA050D2B14BE32557457C32E0F926AEE7F479F60967BB0EA903A79DA3534A110B85B9C7F6D6F2279067776C80FD91FC130416051328C396CA99
Malicious:	false
Reputation:	low
Preview:	C:\Users\user\Desktop\OjAJYVQ7iK.exe

C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\hTwyiugpwdBi.exe	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	418304
Entropy (8bit):	7.933921685316817
Encrypted:	false
SSDEEP:	6144:akoMdtpU20db9m2HuW5G2u0NvHmVX0khUf8WbtXxB5Ojxqe6+j0m5Y:akzlWu0N+Af8OXpO17A
MD5:	D7D3373FFBD938DA6C7C8AA3DC57FA49
SHA1:	44A01528433887323F7CD6495387AD189252D72D
SHA-256:	9829C2298AB32875E7379274C578FCBFFCDDAA36A262C74F69D113217913E5CA
SHA-512:	15D51363CC6A2E448DAE680A64707F8E9732992E916F966C8583B719CE9454E8D9BB364356907F666673A2EC2872F4253751E327BAD72FBE69DFDEFEAFFD573F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 51%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....]..... .....0..X.....v... .....@.. ..... .@.....Pv..K..... ....H.....text....V... ...X..... ..`.rsrc.....Z.....@..@.relo c.....`.....@..B.....v.....H.....K...*.....I.....0.....*....0.....(....*..0.....(....(....*....0.....(....*..0.....%.~....%- .&~.....s....%.....%.~....%-.&~.....s....%.....%.~....%-.&~.....s....%.....%.~....%-.&~.....s....%.....*..0.....s".....8.... .R..... .y1X ....a ...d ..B.YX .[S. .... .,.XZY Q..\Z I..1f b..q .s..aeeXa @..= ....af .=.. ....eZYfeaa S..J .a. e .~.. .*..Ya 1.|.Xafa .=

C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\mOcj0RclyeUq.exe	
Process:	C:\Users\user\Desktop\OjAJYVQ7iK.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	418304
Entropy (8bit):	7.933921685316817
Encrypted:	false
SSDEEP:	6144:akoMdtpU20db9m2HuW5G2u0NvHmVX0khUf8WbtXxB5Ojxqe6+j0m5Y:akzlWu0N+Af8OXpO17A
MD5:	D7D3373FFBD938DA6C7C8AA3DC57FA49
SHA1:	44A01528433887323F7CD6495387AD189252D72D
SHA-256:	9829C2298AB32875E7379274C578FCBFFCDDAA36A262C74F69D113217913E5CA
SHA-512:	15D51363CC6A2E448DAE680A64707F8E9732992E916F966C8583B719CE9454E8D9BB364356907F666673A2EC2872F4253751E327BAD72FBE69DFDEFEAFFD573F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 51%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....]..... .....0..X.....v... .....@.. ..... .@.....Pv..K..... ....H.....text....V... ...X..... ..`.rsrc.....Z.....@..@.relo c.....`.....@..B.....v.....H.....K...*.....I.....0.....*....0.....(....*..0.....(....(....*....0.....(....*..0.....%.~....%- .&~.....s....%.....%.~....%-.&~.....s....%.....%.~....%-.&~.....s....%.....%.~....%-.&~.....s....%.....*..0.....s".....8.... .R..... .y1X ....a ...d ..B.YX .[S. .... .,.XZY Q..\Z I..1f b..q .s..aeeXa @..= ....af .=.. ....eZYfeaa S..J .a. e .~.. .*..Ya 1.|.Xafa .=

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.933921685316817
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	OjAJYVQ7iK.exe
File size:	418304
MD5:	d7d3373ffbd938da6c7c8aa3dc57fa49
SHA1:	44a01528433887323f7cd6495387ad189252d72d
SHA256:	9829c2298ab32875e7379274c578fcbffcddaa36a262c74f69d113217913e5ca
SHA512:	15d51363cc6a2e448dae680a64707f8e9732992e916f966c8583b719ce9454e8d9bb364356907f666673a2ec2872f4253751e327bad72fbe69dfdefeaffd573f
SSDEEP:	6144:akoMdtpU20db9m2HuW5G2u0NvHmVX0khUf8WbtXxB5Ojxqe6+j0m5Y:akzlWu0N+Af8OXpO17A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....]..... .....0..X.....v... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46769e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5D8693DB [Sat Sep 21 21:19:23 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x67650	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x68000	0x5c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x656a4	0x65800	False	0.953658982451	data	7.94150093697	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x68000	0x5c8	0x600	False	0.420572916667	data	4.15341986668	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x680a0	0x32c	data		
RT_MANIFEST	0x683cc	0x1f5	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright XZ2Studio 2019
Assembly Version	1.0.0.0
InternalName	XZ2Studio.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	XZ2Studio
ProductVersion	1.0.0.0
FileDescription	XZ2Studio
OriginalFilename	XZ2Studio.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/11/21-09:03:32.697333	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	8192	192.168.2.3	192.169.69.25
04/11/21-09:03:38.116050	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	8192	192.168.2.3	192.169.69.25
04/11/21-09:03:42.824744	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	8192	192.168.2.3	192.169.69.25
04/11/21-09:04:14.335443	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	8192	192.168.2.3	192.169.69.25
04/11/21-09:04:20.360727	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	8192	192.168.2.3	192.169.69.25
04/11/21-09:04:29.937443	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	8192	192.168.2.3	192.169.69.25
04/11/21-09:04:56.151996	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	8192	192.168.2.3	192.169.69.25
04/11/21-09:05:01.123504	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	8192	192.168.2.3	192.169.69.25
04/11/21-09:05:05.501084	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	8192	192.168.2.3	192.169.69.25
04/11/21-09:05:26.396553	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	8192	192.168.2.3	192.169.69.25
04/11/21-09:05:31.020458	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	8192	192.168.2.3	192.169.69.25
04/11/21-09:05:35.440855	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	8192	192.168.2.3	192.169.69.25

Network Port Distribution

Total Packets: 86

- 53 (DNS)
- 8192 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 11, 2021 09:03:13.525330067 CEST	49730	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:13.556582928 CEST	8192	49730	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:14.137969017 CEST	49730	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:14.171170950 CEST	8192	49730	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:14.747070074 CEST	49730	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:14.778476000 CEST	8192	49730	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:19.319617987 CEST	49731	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:19.351015091 CEST	8192	49731	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:19.950701952 CEST	49731	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:19.982353926 CEST	8192	49731	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:20.638194084 CEST	49731	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:20.669919968 CEST	8192	49731	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:25.213694096 CEST	49732	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:25.244803905 CEST	8192	49732	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:25.747998953 CEST	49732	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:25.779243946 CEST	8192	49732	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:26.453629971 CEST	49732	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:26.486504078 CEST	8192	49732	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:32.098365068 CEST	49733	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:03:32.305557013 CEST	8192	49733	192.169.69.25	192.168.2.3
Apr 11, 2021 09:03:32.308167934 CEST	49733	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:03:32.697333097 CEST	49733	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:03:32.903028011 CEST	8192	49733	192.169.69.25	192.168.2.3
Apr 11, 2021 09:03:37.880736113 CEST	49734	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:03:38.115262985 CEST	8192	49734	192.169.69.25	192.168.2.3
Apr 11, 2021 09:03:38.115360975 CEST	49734	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:03:38.116050005 CEST	49734	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:03:38.329561949 CEST	8192	49734	192.169.69.25	192.168.2.3
Apr 11, 2021 09:03:42.579906940 CEST	49736	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:03:42.824110985 CEST	8192	49736	192.169.69.25	192.168.2.3
Apr 11, 2021 09:03:42.824229002 CEST	49736	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:03:42.824743986 CEST	49736	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:03:43.014324903 CEST	8192	49736	192.169.69.25	192.168.2.3
Apr 11, 2021 09:03:47.243073940 CEST	49737	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:47.277245045 CEST	8192	49737	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:47.952879906 CEST	49737	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:47.985168934 CEST	8192	49737	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:48.640487909 CEST	49737	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:48.672172070 CEST	8192	49737	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:52.742803097 CEST	49738	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:52.774352074 CEST	8192	49738	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:53.453830004 CEST	49738	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:53.486609936 CEST	8192	49738	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:54.141046047 CEST	49738	8192	192.168.2.3	79.134.225.112

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 11, 2021 09:03:54.172543049 CEST	8192	49738	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:58.531819105 CEST	49741	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:58.563457012 CEST	8192	49741	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:59.141422033 CEST	49741	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:59.172787905 CEST	8192	49741	79.134.225.112	192.168.2.3
Apr 11, 2021 09:03:59.750776052 CEST	49741	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:03:59.781976938 CEST	8192	49741	79.134.225.112	192.168.2.3
Apr 11, 2021 09:04:14.143338919 CEST	49748	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:04:14.334758043 CEST	8192	49748	192.169.69.25	192.168.2.3
Apr 11, 2021 09:04:14.335143089 CEST	49748	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:04:14.335443020 CEST	49748	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:04:14.550884008 CEST	8192	49748	192.169.69.25	192.168.2.3
Apr 11, 2021 09:04:20.143529892 CEST	49749	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:04:20.360270023 CEST	8192	49749	192.169.69.25	192.168.2.3
Apr 11, 2021 09:04:20.360425949 CEST	49749	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:04:20.360727072 CEST	49749	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:04:20.556380033 CEST	8192	49749	192.169.69.25	192.168.2.3
Apr 11, 2021 09:04:29.706922054 CEST	49750	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:04:29.936815023 CEST	8192	49750	192.169.69.25	192.168.2.3
Apr 11, 2021 09:04:29.937164068 CEST	49750	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:04:29.937443018 CEST	49750	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:04:30.134644985 CEST	8192	49750	192.169.69.25	192.168.2.3
Apr 11, 2021 09:04:39.381154060 CEST	49751	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:04:39.412664890 CEST	8192	49751	79.134.225.112	192.168.2.3
Apr 11, 2021 09:04:39.957245111 CEST	49751	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:04:39.989371061 CEST	8192	49751	79.134.225.112	192.168.2.3
Apr 11, 2021 09:04:40.644850969 CEST	49751	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:04:40.676879883 CEST	8192	49751	79.134.225.112	192.168.2.3
Apr 11, 2021 09:04:44.876153946 CEST	49752	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:04:44.907202005 CEST	8192	49752	79.134.225.112	192.168.2.3
Apr 11, 2021 09:04:45.457695961 CEST	49752	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:04:45.488878012 CEST	8192	49752	79.134.225.112	192.168.2.3
Apr 11, 2021 09:04:46.145287991 CEST	49752	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:04:46.179236889 CEST	8192	49752	79.134.225.112	192.168.2.3
Apr 11, 2021 09:04:50.373560905 CEST	49753	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:04:50.406244993 CEST	8192	49753	79.134.225.112	192.168.2.3
Apr 11, 2021 09:04:50.958172083 CEST	49753	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:04:50.991410017 CEST	8192	49753	79.134.225.112	192.168.2.3
Apr 11, 2021 09:04:51.645911932 CEST	49753	8192	192.168.2.3	79.134.225.112
Apr 11, 2021 09:04:51.677409887 CEST	8192	49753	79.134.225.112	192.168.2.3
Apr 11, 2021 09:04:55.906994104 CEST	49754	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:04:56.151336908 CEST	8192	49754	192.169.69.25	192.168.2.3
Apr 11, 2021 09:04:56.151650906 CEST	49754	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:04:56.151995897 CEST	49754	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:04:56.368913889 CEST	8192	49754	192.169.69.25	192.168.2.3
Apr 11, 2021 09:05:00.895567894 CEST	49755	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:05:01.122921944 CEST	8192	49755	192.169.69.25	192.168.2.3
Apr 11, 2021 09:05:01.123106956 CEST	49755	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:05:01.123503923 CEST	49755	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:05:01.317758083 CEST	8192	49755	192.169.69.25	192.168.2.3
Apr 11, 2021 09:05:05.333705902 CEST	49756	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:05:05.500477076 CEST	8192	49756	192.169.69.25	192.168.2.3
Apr 11, 2021 09:05:05.500689983 CEST	49756	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:05:05.501084089 CEST	49756	8192	192.168.2.3	192.169.69.25
Apr 11, 2021 09:05:05.723125935 CEST	8192	49756	192.169.69.25	192.168.2.3
Apr 11, 2021 09:05:09.740118980 CEST	49757	8192	192.168.2.3	79.134.225.112

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 11, 2021 09:01:51.001543999 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:01:51.016609907 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 11, 2021 09:01:51.985474110 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:01:51.998068094 CEST	53	60152	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 11, 2021 09:01:54.442686081 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:01:54.455429077 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 11, 2021 09:01:55.406850100 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:01:55.421691895 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 11, 2021 09:01:56.403810978 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:01:56.417076111 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 11, 2021 09:01:57.937777996 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:01:57.950561047 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 11, 2021 09:01:59.105138063 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:01:59.117631912 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 11, 2021 09:01:59.937426090 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:01:59.950126886 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 11, 2021 09:02:01.100388050 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:02:01.112405062 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 11, 2021 09:02:01.929836035 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:02:01.942621946 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 11, 2021 09:02:02.779949903 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:02:02.793458939 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 11, 2021 09:02:03.586522102 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:02:03.601074934 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 11, 2021 09:02:11.317183018 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:02:11.329839945 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 11, 2021 09:02:15.333024979 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:02:15.346276045 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 11, 2021 09:02:16.075911045 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:02:16.089235067 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 11, 2021 09:02:16.845942020 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:02:16.874038935 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 11, 2021 09:02:21.565097094 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:02:21.579391956 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 11, 2021 09:02:28.470307112 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:02:28.483464003 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 11, 2021 09:02:31.172571898 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:02:31.190458059 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 11, 2021 09:02:46.879281044 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:02:46.898739100 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 11, 2021 09:02:54.474730968 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:02:54.489046097 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:10.427225113 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:10.446085930 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:13.329710007 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:13.510900021 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:19.095187902 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:19.282011032 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:24.942365885 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:25.126991034 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:31.888231993 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:32.069762945 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:37.822982073 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:37.837412119 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:42.392299891 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:42.576694965 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:47.061103106 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:47.242060900 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:52.726169109 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:52.741607904 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:56.728641033 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:56.839498043 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:57.806426048 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:57.986140013 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:58.475516081 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:58.516133070 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:58.529424906 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:58.586220026 CEST	53	61946	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 11, 2021 09:03:58.957226038 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:58.973332882 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:59.451683998 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:59.466468096 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 11, 2021 09:03:59.927014112 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:03:59.939830065 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 11, 2021 09:04:00.297306061 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:04:00.310129881 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 11, 2021 09:04:01.261435032 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:04:01.403517008 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 11, 2021 09:04:09.049372911 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:04:09.229743958 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 11, 2021 09:04:18.565850973 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:04:18.579432964 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 11, 2021 09:04:24.565968990 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:04:24.579590082 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 11, 2021 09:04:34.144870043 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:04:34.328341961 CEST	53	56803	8.8.8.8	192.168.2.3
Apr 11, 2021 09:04:44.692733049 CEST	57145	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:04:44.875530958 CEST	53	57145	8.8.8.8	192.168.2.3
Apr 11, 2021 09:04:50.193170071 CEST	55359	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:04:50.372935057 CEST	53	55359	8.8.8.8	192.168.2.3
Apr 11, 2021 09:04:55.725264072 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:04:55.906214952 CEST	53	58306	8.8.8.8	192.168.2.3
Apr 11, 2021 09:05:00.381469965 CEST	64124	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:05:00.894798040 CEST	53	64124	8.8.8.8	192.168.2.3
Apr 11, 2021 09:05:05.319425106 CEST	49361	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:05:05.333096027 CEST	53	49361	8.8.8.8	192.168.2.3
Apr 11, 2021 09:05:09.726361036 CEST	63150	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:05:09.739528894 CEST	53	63150	8.8.8.8	192.168.2.3
Apr 11, 2021 09:05:15.226532936 CEST	53279	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:05:15.241305113 CEST	53	53279	8.8.8.8	192.168.2.3
Apr 11, 2021 09:05:20.727413893 CEST	56881	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:05:20.741077900 CEST	53	56881	8.8.8.8	192.168.2.3
Apr 11, 2021 09:05:26.196145058 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:05:26.211993933 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 11, 2021 09:05:30.602714062 CEST	55667	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:05:30.786562920 CEST	53	55667	8.8.8.8	192.168.2.3
Apr 11, 2021 09:05:35.228240967 CEST	54833	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:05:35.245070934 CEST	53	54833	8.8.8.8	192.168.2.3
Apr 11, 2021 09:05:39.650465012 CEST	62476	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:05:39.833180904 CEST	53	62476	8.8.8.8	192.168.2.3
Apr 11, 2021 09:05:45.291413069 CEST	49705	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:05:45.475127935 CEST	53	49705	8.8.8.8	192.168.2.3
Apr 11, 2021 09:05:50.779489040 CEST	61477	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:05:50.792150974 CEST	53	61477	8.8.8.8	192.168.2.3
Apr 11, 2021 09:05:56.277096987 CEST	61633	53	192.168.2.3	8.8.8.8
Apr 11, 2021 09:05:56.461711884 CEST	53	61633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 11, 2021 09:03:13.329710007 CEST	192.168.2.3	8.8.8.8	0xe04c	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:19.095187902 CEST	192.168.2.3	8.8.8.8	0xed0e	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:24.942365885 CEST	192.168.2.3	8.8.8.8	0x8990	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:31.888231993 CEST	192.168.2.3	8.8.8.8	0x8032	Standard query (0)	ghfsquad.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:37.822982073 CEST	192.168.2.3	8.8.8.8	0x6e72	Standard query (0)	ghfsquad.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:42.392299891 CEST	192.168.2.3	8.8.8.8	0x1dab	Standard query (0)	ghfsquad.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:47.061103106 CEST	192.168.2.3	8.8.8.8	0xe1f3	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 11, 2021 09:03:52.726169109 CEST	192.168.2.3	8.8.8.8	0x2c02	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:58.516133070 CEST	192.168.2.3	8.8.8.8	0x8b7	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:04:09.049372911 CEST	192.168.2.3	8.8.8.8	0xb04d	Standard query (0)	ghfsquad.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:04:18.565850973 CEST	192.168.2.3	8.8.8.8	0x5b4e	Standard query (0)	ghfsquad.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:04:24.565968990 CEST	192.168.2.3	8.8.8.8	0x28ae	Standard query (0)	ghfsquad.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:04:34.144870043 CEST	192.168.2.3	8.8.8.8	0x48f5	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:04:44.692733049 CEST	192.168.2.3	8.8.8.8	0xf89d	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:04:50.193170071 CEST	192.168.2.3	8.8.8.8	0x30f8	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:04:55.725264072 CEST	192.168.2.3	8.8.8.8	0x1d48	Standard query (0)	ghfsquad.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:00.381469965 CEST	192.168.2.3	8.8.8.8	0x76bc	Standard query (0)	ghfsquad.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:05.319425106 CEST	192.168.2.3	8.8.8.8	0xf720	Standard query (0)	ghfsquad.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:09.726361036 CEST	192.168.2.3	8.8.8.8	0x7833	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:15.226532936 CEST	192.168.2.3	8.8.8.8	0x2c65	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:20.727413893 CEST	192.168.2.3	8.8.8.8	0x2488	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:26.196145058 CEST	192.168.2.3	8.8.8.8	0x466c	Standard query (0)	ghfsquad.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:30.602714062 CEST	192.168.2.3	8.8.8.8	0x89f4	Standard query (0)	ghfsquad.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:35.228240967 CEST	192.168.2.3	8.8.8.8	0xf1f	Standard query (0)	ghfsquad.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:39.650465012 CEST	192.168.2.3	8.8.8.8	0x4bc6	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:45.291413069 CEST	192.168.2.3	8.8.8.8	0xfeb	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:50.779489040 CEST	192.168.2.3	8.8.8.8	0x590d	Standard query (0)	ludwigh.duckdns.org	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:56.277096987 CEST	192.168.2.3	8.8.8.8	0x63f5	Standard query (0)	ghfsquad.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

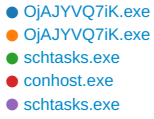
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 11, 2021 09:03:13.510900021 CEST	8.8.8.8	192.168.2.3	0xe04c	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:19.282011032 CEST	8.8.8.8	192.168.2.3	0xed0e	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:25.126991034 CEST	8.8.8.8	192.168.2.3	0x8990	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:32.069762945 CEST	8.8.8.8	192.168.2.3	0x8032	No error (0)	ghfsquad.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:37.837412119 CEST	8.8.8.8	192.168.2.3	0x6e72	No error (0)	ghfsquad.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:42.576694965 CEST	8.8.8.8	192.168.2.3	0x1dab	No error (0)	ghfsquad.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:47.242060900 CEST	8.8.8.8	192.168.2.3	0xe1f3	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:52.741607904 CEST	8.8.8.8	192.168.2.3	0x2c02	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:03:58.529424906 CEST	8.8.8.8	192.168.2.3	0x8b7	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:04:09.229743958 CEST	8.8.8.8	192.168.2.3	0xb04d	No error (0)	ghfsquad.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)

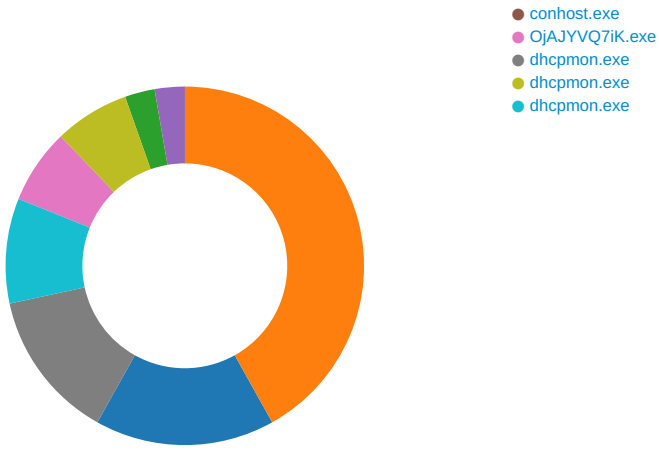
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 11, 2021 09:04:18.579432964 CEST	8.8.8.8	192.168.2.3	0x5b4e	No error (0)	ghfsquad.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
Apr 11, 2021 09:04:24.579590082 CEST	8.8.8.8	192.168.2.3	0x28ae	No error (0)	ghfsquad.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
Apr 11, 2021 09:04:34.328341961 CEST	8.8.8.8	192.168.2.3	0x48f5	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:04:44.875530958 CEST	8.8.8.8	192.168.2.3	0xf89d	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:04:50.372935057 CEST	8.8.8.8	192.168.2.3	0x30f8	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:04:55.906214952 CEST	8.8.8.8	192.168.2.3	0x1d48	No error (0)	ghfsquad.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:00.894798040 CEST	8.8.8.8	192.168.2.3	0x76bc	No error (0)	ghfsquad.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:05.333096027 CEST	8.8.8.8	192.168.2.3	0xf720	No error (0)	ghfsquad.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:09.739528894 CEST	8.8.8.8	192.168.2.3	0x7833	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:15.241305113 CEST	8.8.8.8	192.168.2.3	0x2c65	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:20.741077900 CEST	8.8.8.8	192.168.2.3	0x2488	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:26.211993933 CEST	8.8.8.8	192.168.2.3	0x466c	No error (0)	ghfsquad.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:30.786562920 CEST	8.8.8.8	192.168.2.3	0x89f4	No error (0)	ghfsquad.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:35.245070934 CEST	8.8.8.8	192.168.2.3	0xf1f	No error (0)	ghfsquad.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:39.833180904 CEST	8.8.8.8	192.168.2.3	0x4bc6	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:45.475127935 CEST	8.8.8.8	192.168.2.3	0xfeb	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:50.792150974 CEST	8.8.8.8	192.168.2.3	0x590d	No error (0)	ludwigh.duckdns.org		79.134.225.112	A (IP address)	IN (0x0001)
Apr 11, 2021 09:05:56.461711884 CEST	8.8.8.8	192.168.2.3	0x63f5	No error (0)	ghfsquad.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: OjAJYVQ7iK.exe PID: 4856 Parent PID: 5656

General

Start time:	09:01:57
Start date:	11/04/2021
Path:	C:\Users\user\Desktop\OjAJYVQ7iK.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\OjAJYVQ7iK.exe'
Imagebase:	0x570000
File size:	418304 bytes
MD5 hash:	D7D3373FFBD938DA6C7C8AA3DC57FA49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C91B75	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\mOcj0RclyeUq.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	6C91CF0	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\OjAJYVQ7iK.exe:Zone.Identifier	success or wait	1	6C919F5	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\mOcj0RclyeUq.exe	0	131072	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 db 93 86 5d 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 58 06 00 00 08 00 00 00 00 00 00 9e 76 06 00 00 20 00 00 00 80 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 c0 06 00 00 02 00 00 a8 f5 06 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......].......... ....0..X...........v... ....@.. ....@................	success or wait	4	6C91CF0	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\mOcj0RclyeUq.exe	unknown	418304	success or wait	1	6C92473	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	Shell	unicode	"C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\mOcj0RclyeUq.exe",explorer.exe	success or wait	1	6C91DE2	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	Shell	unicode	"C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\hTwyiugpwdBi.exe",explorer.exe	"C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\mOcj0RclyeUq.exe",explorer.exe	success or wait	16	6C91DE2	RegSetValueExW

Analysis Process: OjAJYVQ7iK.exe PID: 6772 Parent PID: 4856

General

Start time:	09:03:08
Start date:	11/04/2021
Path:	C:\Users\user\Desktop\OjAJYVQ7iK.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\OjAJYVQ7iK.exe
Imagebase:	0xe60000
File size:	418304 bytes
MD5 hash:	D7D3373FFBD938DA6C7C8AA3DC57FA49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\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	57B07A1	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	57B089B	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	57B07A1	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	57B0B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp691F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	57B0D1C	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	57B089B	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6C3D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	57B0D1C	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	57B07A1	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	57B07A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp691F.tmp	success or wait	1	72637D95	unknown
C:\Users\user\AppData\Local\Temp\tmp6C3D.tmp	success or wait	1	72637D95	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	5c e8 95 4d 03 fd d8 48	\..M...H	success or wait	1	57B0A53	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	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 db 93 86 5d 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 58 06 00 00 08 00 00 00 00 00 00 9e 76 06 00 00 20 00 00 00 80 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 06 00 00 02 00 00 a8 f5 06 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......]......... ....0..X...........v... ....@.. ....@.................	success or wait	4	57B0B20	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp691F.tmp	unknown	1300	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	57B0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	37	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 4f 6a 41 4a 59 56 51 37 69 4b 2e 65 78 65	C:\Users\user\Desktop\OjAJYVQ7iK.exe	success or wait	1	57B0A53	WriteFile
C:\Users\user\AppData\Local\Temp\tmp6C3D.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	57B0A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Users\user\Desktop\OjAJYVQ7iK.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Users\user\Desktop\OjAJYVQ7iK.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	57B0A53	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	57B0C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 6956 Parent PID: 6772

General

Start time:	09:03:10
Start date:	11/04/2021
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\tmp691F.tmp'
Imagebase:	0x230000
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\tmp691F.tmp	unknown	2	success or wait	1	23AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp691F.tmp	unknown	1301	success or wait	1	23ABD9	ReadFile

Analysis Process: conhost.exe PID: 6992 Parent PID: 6956

General

Start time:	09:03:10
Start date:	11/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 7084 Parent PID: 6772

General

Start time:	09:03:11
Start date:	11/04/2021
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\tmp6C3D.tmp'
Imagebase:	0x230000
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\tmp6C3D.tmp	unknown	2	success or wait	1	23AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6C3D.tmp	unknown	1311	success or wait	1	23ABD9	ReadFile

Analysis Process: conhost.exe PID: 7096 Parent PID: 7084

General

Start time:	09:03:11
Start date:	11/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: OjAJYVQ7iK.exe PID: 7164 Parent PID: 528

General

Start time:	09:03:12

Start date:	11/04/2021
Path:	C:\Users\user\Desktop\OjAJYVQ7iK.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\OjAJYVQ7iK.exe 0
Imagebase:	0x980000
File size:	418304 bytes
MD5 hash:	D7D3373FFBD938DA6C7C8AA3DC57FA49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

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

File Read

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

Analysis Process: dhcpmon.exe PID: 5572 Parent PID: 528

General

Start time:	09:03:13
Start date:	11/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xfa0000
File size:	418304 bytes
MD5 hash:	D7D3373FFBD938DA6C7C8AA3DC57FA49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 51%, Metadefender, Browse • Detection: 89%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\hTwyiugpwdBi.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	71E1C30	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\hTwyiugpwdBi.exe	0	131072	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 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 db 93 86 5d 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 58 06 00 00 08 00 00 00 00 00 00 9e 76 06 00 00 20 00 00 00 80 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 c0 06 00 00 02 00 00 a8 f5 06 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......]......... ....0..X...........v... ....@.. ....@.................	success or wait	4	71E1C30	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\hTwyiugpwdBi.exe	unknown	418304	success or wait	1	71E23B3	ReadFile

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	Shell	unicode	"C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\mOcj0RcleUq.exe",explorer.exe	"C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\hTwyiugpwdBi.exe",explorer.exe	success or wait	1	71E1D4A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	Shell	unicode	"C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\mOcj0RcleUq.exe",explorer.exe	"C:\Users\user\AppData\Roaming\UB0ea31R2rvgUZ7l\hTwyiugpwdBi.exe",explorer.exe	success or wait	16	71E1D4A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 5624 Parent PID: 3388

General

Start time:	09:03:19
Start date:	11/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xb50000
File size:	418304 bytes
MD5 hash:	D7D3373FFBD938DA6C7C8AA3DC57FA49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

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

File Read

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

Analysis Process: dhcpmon.exe PID: 5884 Parent PID: 5572

General

Start time:	09:03:33
Start date:	11/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xe50000

File size:	418304 bytes
MD5 hash:	D7D3373FFBD938DA6C7C8AA3DC57FA49
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: 00000019.00000002.423134588.0000000004621000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.423134588.0000000004621000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000002.421572574.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.421572574.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.421572574.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.423095541.0000000003621000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.423095541.0000000003621000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

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

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

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

Disassembly

Code Analysis