ID: 623788
Sample Name:
5JbQqP8SDG.exe
Cookbook: default.jbs
Time: 20:23:39
Date: 10/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

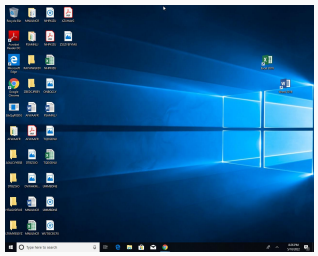
Windows Analysis Report

5JbQqP8SDG.exe

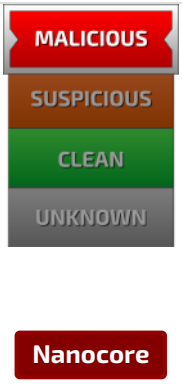
Overview

General Information

Sample Name:	5JbQqP8SDG.exe
Analysis ID:	623788
MD5:	250d122f4af32b5.
SHA1:	39346c41bcb751..
SHA256:	14f5c3ab5cbad5…
Tags:	exe NanoCore RAT
Infos:	



Detection



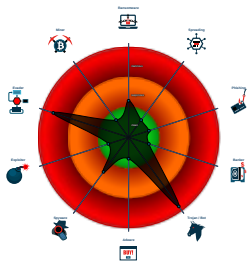
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Connects to many ports of the same…
- Protects its processes via BreakOn…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- 5JbQqP8SDG.exe (PID: 7036 cmdline: "C:\Users\user\Desktop\5JbQqP8SDG.exe" MD5: 250D122F4AF32B52435A02787689EBBD)
  - schtasks.exe (PID: 6368 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\GryVAO" /XML "C:\Users\user\AppData\Local\Temp\tmpBE25.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 5JbQqP8SDG.exe (PID: 4676 cmdline: {path} MD5: 250D122F4AF32B52435A02787689EBBD)
    - schtasks.exe (PID: 1408 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpFEC7.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6608 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5564 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmpBD8.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6652 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 5JbQqP8SDG.exe (PID: 5976 cmdline: C:\Users\user\Desktop\5JbQqP8SDG.exe 0 MD5: 250D122F4AF32B52435A02787689EBBD)
  - schtasks.exe (PID: 4536 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\GryVAO" /XML "C:\Users\user\AppData\Local\Temp\tmp3E23.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 5JbQqP8SDG.exe (PID: 7040 cmdline: {path} MD5: 250D122F4AF32B52435A02787689EBBD)
- dhcpmon.exe (PID: 6388 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 250D122F4AF32B52435A02787689EBBD)
  - schtasks.exe (PID: 4176 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\GryVAO" /XML "C:\Users\user\AppData\Local\Temp\tmp5777.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6360 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 4788 cmdline: {path} MD5: 250D122F4AF32B52435A02787689EBBD)
- dhcpmon.exe (PID: 6700 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 250D122F4AF32B52435A02787689EBBD)
  - schtasks.exe (PID: 7052 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\GryVAO" /XML "C:\Users\user\AppData\Local\Temp\tmp58BF.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 2260 cmdline: {path} MD5: 250D122F4AF32B52435A02787689EBBD)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000001D.00000002.617062843.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001D.00000002.617062843.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001D.00000002.617062843.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
0000001C.00000000.579285516.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001C.00000000.579285516.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 107 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.5JbQqP8SDG.exe.2c55fe0.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x40a6:$x1: NanoCore.ClientPluginHost
6.2.5JbQqP8SDG.exe.2c55fe0.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x40a6:$x2: NanoCore.ClientPluginHost • 0x4184:$s4: PipeCreated • 0x40c0:$s5: IClientLoggingHost
6.2.5JbQqP8SDG.exe.2c55fe0.3.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x40f0:$x2: NanoCore.ClientPlugin • 0x40a6:$x3: NanoCore.ClientPluginHost • 0x4106:$i3: IClientNetwork • 0x40c0:$i6: IClientLoggingHost • 0x3e3f:$s1: ClientPlugin • 0x40f9:$s1: ClientPlugin
11.2.5JbQqP8SDG.exe.37c1488.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
11.2.5JbQqP8SDG.exe.37c1488.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost

Click to see the 117 entries

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

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

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

Operating System Destruction

Protects its processes via BreakOnTermination flag

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

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

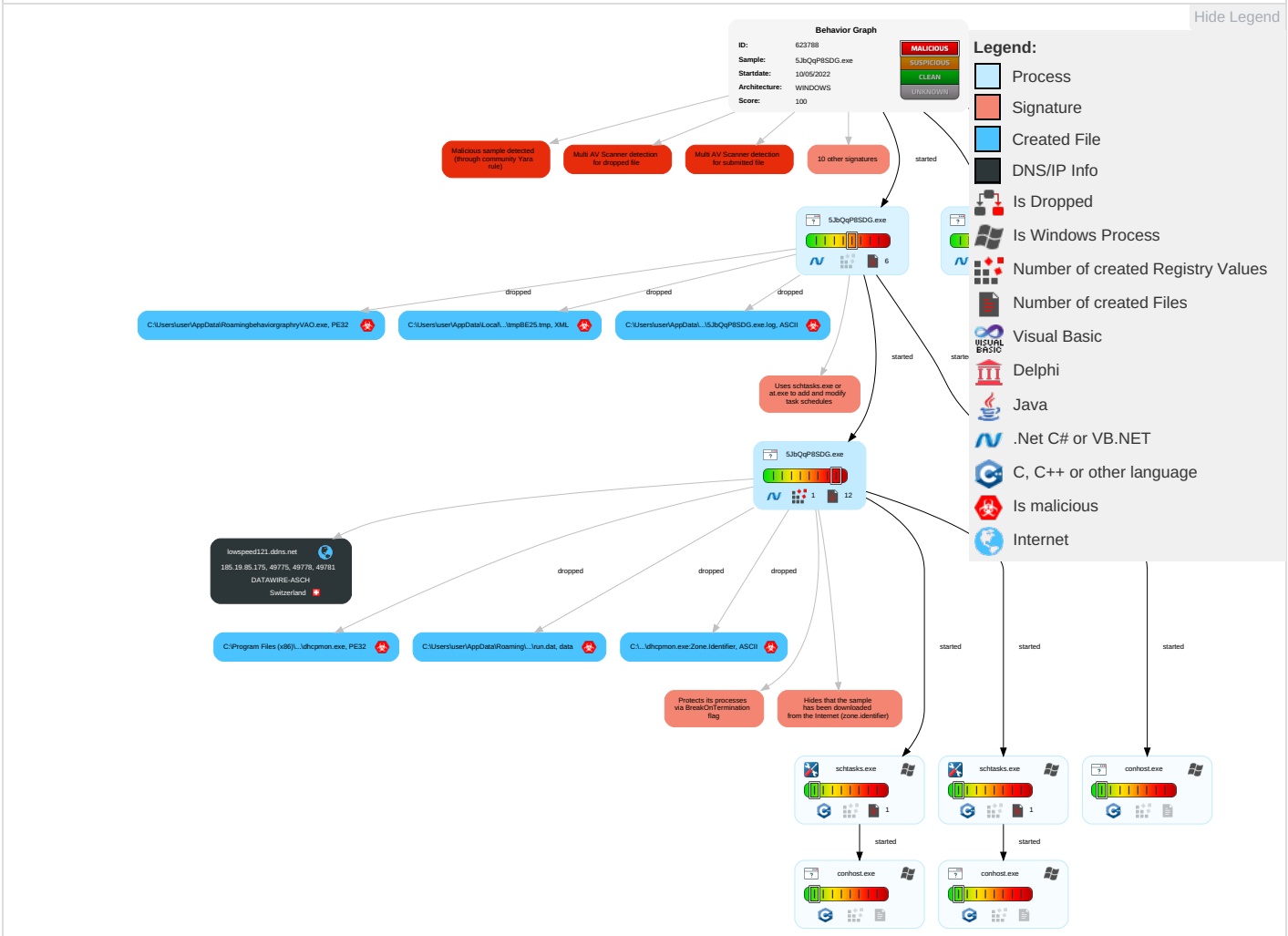
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 1 2 Process Injection	2 Masquerading	2 1 Input Capture	2 1 Security Software Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
5JbQqP8SDG.exe	58%	Virustotal		Browse
5JbQqP8SDG.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AveMariaRAT	
5JbQqP8SDG.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\GryVAO.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AveMariaRAT	
C:\Users\user\AppData\Roaming\GryVAO.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AveMariaRAT	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.5JbQqP8SDG.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.5JbQqP8SDG.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.5JbQqP8SDG.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.0.5JbQqP8SDG.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.5JbQqP8SDG.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.5JbQqP8SDG.exe.53e0000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
6.0.5JbQqP8SDG.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comepko8	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnU	0%	URL Reputation	safe	
http://www.sajatypeworks.com=	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn=	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr%	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnH	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.comK	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmc	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.agfamonotype.p	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.fonts.comu	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.urwpp.deX	0%	Avira URL Cloud	safe	
http://www.carterandcone.comexc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.fontbureau.co	0%	URL Reputation	safe	
http://www.fontbureau.comaU	0%	Avira URL Cloud	safe	
http://www.fontbureau.comicTF	0%	Avira URL Cloud	safe	
http://www.fontbureau.comaK	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comf	0%	URL Reputation	safe	
http://fontfabrik.com=	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl-nFp0	0%	Avira URL Cloud	safe	
http://www.fonts.comce	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnsof	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lowspeed121.ddns.net	185.19.85.175	true	false		high

URLs from Memory and Binaries

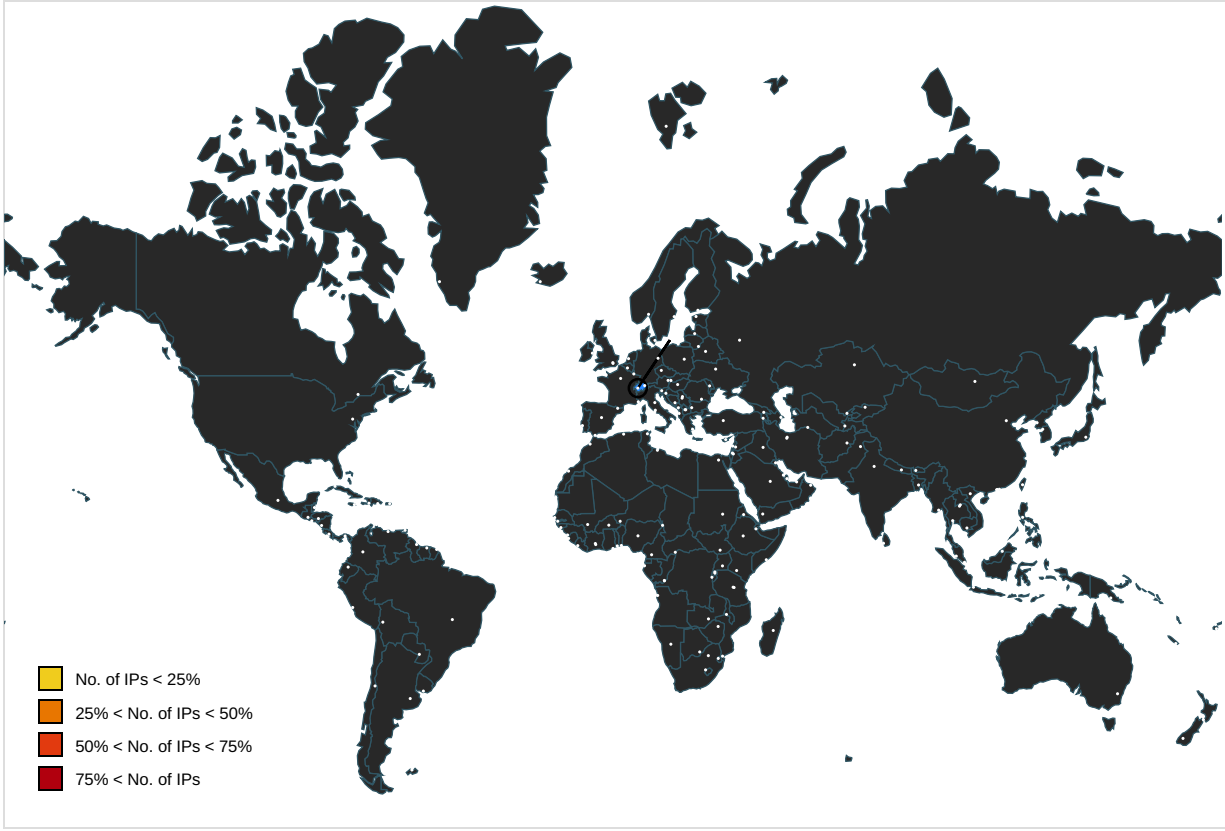
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comepko8	5JbQqP8SDG.exe, 00000000.00000003.450011274.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.450417445.0000000005ADA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnU	5JbQqP8SDG.exe, 00000000.00000003.442704852.0000000005AD4000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.442824583.0000000005ADB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.442475364.0000000005AD4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com=	5JbQqP8SDG.exe, 00000000.00000003.439246890.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.440416859.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.440348993.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.440205423.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn=	5JbQqP8SDG.exe, 00000000.00000003.442457599.0000000005B0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kr%	5JbQqP8SDG.exe, 00000000.00000003.441648603.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cnH	5JbQqP8SDG.exe, 00000000.00000003.442704852.0000000005AD4000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.442824583.0000000005ADB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.442475364.0000000005AD4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	5JbQqP8SDG.exe, 00000000.00000003.439756929.0000000005AF4000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439615586.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439331188.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439537582.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439692572.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439370513.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439404974.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439577851.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439246890.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comK	5JbQqP8SDG.exe, 00000000.00000003.439756929.0000000005AF4000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439615586.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439331188.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439537582.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439692572.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439370513.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439404974.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439577851.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439246890.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmc	5JbQqP8SDG.exe, 00000000.00000003.454422256.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com.	5JbQqP8SDG.exe, 00000000.00000003.451055165.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agfamonotype.p	5JbQqP8SDG.exe, 00000000.00000003.455928032.0000000005ADA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439615586.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439692572.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.441648603.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comu	5JbQqP8SDG.exe, 00000000.00000003.439615586.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de	5JbQqP8SDG.exe, 00000000.00000003.451055165.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	5JbQqP8SDG.exe, 00000000.00000002.487043671.0000000002C81000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 0000000B.00000002.585122976.0000000002631000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 0000000E.00000002.594285014.0000000003151000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deX	5JbQqP8SDG.exe, 00000000.00000003.451055165.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comexc	5JbQqP8SDG.exe, 00000000.00000003.444977276.0000000005ADD000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.445248230.0000000005ADD000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.445508362.0000000005ADD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com	5JbQqP8SDG.exe, 00000000.00000002.493627346.0000000005AD0000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.450011274.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.485024316.0000000005AD0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.comc	5JbQqP8SDG.exe, 00000000.00000003.439692572.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.c	5JbQqP8SDG.exe, 00000000.00000003.442704852.0000000005AD4000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.442475364.0000000005AD4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.co	5JbQqP8SDG.exe, 00000000.00000003.450011274.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comaU	5JbQqP8SDG.exe, 00000000.00000002.493627346.0000000005AD0000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.485024316.0000000005AD0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comicTF	5JbQqP8SDG.exe, 00000000.00000003.448954375.0000000005AD8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comaK	5JbQqP8SDG.exe, 00000000.00000003.451055165.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd	5JbQqP8SDG.exe, 00000000.00000003.450011274.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.450417445.0000000005ADA000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.451055165.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	5JbQqP8SDG.exe, 00000000.00000003.438967518.00000000013DD000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	5JbQqP8SDG.exe, 00000000.00000003.442457599.0000000005B0D000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.442475364.0000000005AD4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comf	5JbQqP8SDG.exe, 00000000.00000002.493627346.0000000005AD0000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.485024316.0000000005AD0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	5JbQqP8SDG.exe, 00000000.00000003.450491433.0000000005B0D000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.450590496.0000000005B0D000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.450679414.0000000005B0D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fontfabrik.com=	5JbQqP8SDG.exe, 00000000.00000003.440205423.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	5JbQqP8SDG.exe, 00000000.00000002.494046111.0000000006DC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comals	5JbQqP8SDG.exe, 00000000.00000003.451055165.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalic	5JbQqP8SDG.exe, 00000000.00000003.451055165.0000000005AD9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnl-nFp0	5JbQqP8SDG.exe, 00000000.00000003.442457599.0000000005B0D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comce	5JbQqP8SDG.exe, 00000000.00000003.439615586.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp, 5JbQqP8SDG.exe, 00000000.00000003.439692572.0000000005AEB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnsof	5JbQqP8SDG.exe, 00000000.00000003.442704852.0000000005AD4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.19.85.175	lowspeed121.ddns.net	Switzerland		48971	DATAWIRE-ASCH	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	623788
Start date and time: 10/05/202220:23:39	2022-05-10 20:23:39 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5JbQqP8SDG.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:	36
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@28/12@9/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 4.3% (good quality ratio 2.1%) • Quality average: 31.5% • Quality standard deviation: 39.4%

HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing behavior and disassembly information.
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:25:06	API Interceptor	711x Sleep call for process: 5JbQqP8SDG.exe modified
20:25:20	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
20:25:23	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\5JbQqP8SDG.exe" s>$(Arg0)
20:25:25	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
20:25:41	API Interceptor	4x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\5JbQqP8SDG.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	611328
Entropy (8bit):	7.644650096826273
Encrypted:	false
SSDEEP:	12288:LgjjSrFL2yMrcIqrxggKI3Ab2zBFW1iR011EaSvq/gK0ncptnxwTFMtRXZk6m:LgjjgAcIqrcIwb2zTb01m
MD5:	250D122F4AF32B52435A02787689EBBD
SHA1:	39346C41BCB75109DAC251320D4AFEA649538F85
SHA-256:	14F5C3AB5CBAD5D2F6E751E8B3D42204460B8B10A38285623734D631A2CEDA09
SHA-512:	36D7E91588D98689C76646AE237C84E1797D3371BB54640793E09C23E545CF5BC454779051853C196F7CA6F58FDA3DC080591BA1F86FF81B61928067C84E5488
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Umxb.....P..L.....>k... .....@.. ....@.....j..W..... ....H.....text...DK... ...L..... ..`.rsrc.....N..... ..@..@.reloc.....R.....@..B..... k.....H.....`.....Q...1.....*..(#...*..($...*.s%.....s&.....s'.....s(.....s).....*.~....o*...*.~.... o+...*.~....o,...*.~....o-...*.~....o....*R.....o1.....*..(2...*6..($...(%...*..(&...*.....(....*..('...*b..{....(...+}.....{....*b..{....(...+}.....{....*b..{....(...+}.....{....*b..{....(...+}.....{....*...{.....,rq..p((...z..|....(...+*...{.....,rq..p((...z..|....(...+*...{.....,rq..p((...z..|....(.

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

Process:	C:\Users\user\Desktop\5JbQqP8SDG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\5JbQqP8SDG.exe.log

Process:	C:\Users\user\Desktop\5JbQqP8SDG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7FF8
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log

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

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly \NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp3E23.tmp

Process:	C:\Users\user\Desktop\5JbQqP8SDG.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.168687909215862
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBbtn:cbhC7ZlNQF/rydbz9l3YODOLNdq3X
MD5:	C6382A296ACE45E0D6C9A4A14FF67E89
SHA1:	319FCC78DEC52BCB03209FC3A9FFB4007602874D
SHA-256:	13F650B6E05BB9EBA9D6AFAE4E792DF61FDF029DFBF87ABD0B9EE983FDB91286
SHA-512:	C500C66CBCDC85C485427DA11D54066BD092EE556A78075CA0F575EDAF1B5B98F6B75532252901766B46126D38D147B6742A80B640434F4DA140C20BC6849FC
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Local\Temp\tmp5777.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.168687909215862
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBbtn:cbhC7ZlNQF/rydbz9l3YODOLNdq3X
MD5:	C6382A296ACE45E0D6C9A4A14FF67E89
SHA1:	319FCC78DEC52BCB03209FC3A9FFB4007602874D
SHA-256:	13F650B6E05BB9EBA9D6AFAE4E792DF61FDF029DFBF87ABD0B9EE983FDB91286
SHA-512:	C500C66CBCDC85C485427DA11D54066BD092EE556A78075CA0F575EDAF1B5B98F6B75532252901766B46126D38D147B6742A80B640434F4DA140C20BC6849FC
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Local\Temp\tmpBD8.tmp

Process:	C:\Users\user\Desktop\5JbQqP8SDG.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Reputation:	unknown
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\tmpBE25.tmp

Process:	C:\Users\user\Desktop\5JbQqP8SDG.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.168687909215862
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBbtn:cbhC7ZlNQF/rydbz9l3YODOLNdq3X
MD5:	C6382A296ACE45E0D6C9A4A14FF67E89
SHA1:	319FCC78DEC52BCB03209FC3A9FFB4007602874D
SHA-256:	13F650B6E05BB9EBA9D6AFAE4E792DF61FDF029DFBF87ABD0B9EE983FDB91286
SHA-512:	C500C66CBCDC85C485427DA11D54066BD092EE556A78075CA0F575EDAF1B5B98F6B75532252901766B46126D38D147B6742A80B640434F4DA140C20BC6849FC
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Local\Temp\tmpFEC7.tmp

Process:	C:\Users\user\Desktop\5JbQqP8SDG.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.121610238297834
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0PdxXxtn:cbk4oL600QydbQxIYODOLedq3SXj
MD5:	397A97E4D9348E8C5A0A1AABCE2A141A
SHA1:	4165A2A21BB901CB63655774AD8E3B6F6B894FFF
SHA-256:	FC8358E632BD6B1AD28318263F46F30F57022D6692F503212DA2123ED60294DA
SHA-512:	BD41A5CC77A6ABB91838FE1DABB979B8790E5357ED9444877A047B9FAD06B0282FF646B4BCC2882DD8D2ACAA1FCA89313DD2DB54FC8829DD6E701D65C6594F0D
Malicious:	false
Reputation:	unknown
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\5JbQqP8SDG.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:y6ln:y6ln
MD5:	ED8BF78CAA6512D8C4DE221FC892B8E7
SHA1:	0C2CFB8F84BA2873E0195BE895E3BFFD9DAA5A5D
SHA-256:	D12CB0817649797E02AEBAC918FD4C3FDA757086CE726BBA9781FAF6D165AF0B
SHA-512:	6613AA1FE39368D7188788359E1D2C33862ACAFB19DB9E9ACA2AA902DC9A1D6BF91E8C5B3348AAF457128B96C48D0F5976E1F67A250659219641E5612C3F23C
Malicious:	**true**
Reputation:	unknown
Preview:	.....2.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat

Process:	C:\Users\user\Desktop\5JbQqP8SDG.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	38
Entropy (8bit):	4.511085408180429
Encrypted:	false
SSDEEP:	3:oNUWJRWQvH9BACn:oNNJAQvH92Cn
MD5:	E123BF011BFA42FE28C547BEB8B24E19
SHA1:	C481D8D3A7E0AFA805432B15C37545B946149727
SHA-256:	036BB6A73DF879739586F448D30FDC203B230C314FA7CFE57D9427B677CD19FA
SHA-512:	FFB39A79260DC8F91EF5EE98C145D888DA3EC5187014C9E28F60C1419FFBEED4F8F46F8C19DC283EB2ED810D7CA9F74E0F3E4B8FA4FB67EDFDD25A0DB111E3B2
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\5JbQqP8SDG.exe

C:\Users\user\AppData\Roaming\GryVAO.exe

Process:	C:\Users\user\Desktop\5JbQqP8SDG.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	611328
Entropy (8bit):	7.644650096826273
Encrypted:	false
SSDEEP:	12288:LgjjSrFL2yMrcIqrxggKI3Ab2zBFW1iR011EaSvq/gK0ncptnxwTFMtRXZk6m:LgjjgAcIqrcIwb2zTb01m
MD5:	250D122F4AF32B52435A02787689EBBD
SHA1:	39346C41BCB75109DAC251320D4AFEA649538F85
SHA-256:	14F5C3AB5CBAD5D2F6E751E8B3D42204460B8B10A38285623734D631A2CEDA09
SHA-512:	36D7E91588D98689C76646AE237C84E1797D3371BB54640793E09C23E545CF5BC454779051853C196F7CA6F58FDA3DC080591BA1F86FF81B61928067C84E5488
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Umxb.....P..L.....>k... .....@.. .....@.....j..W..... ....H.....text...DK... ...L..... ..`.rsrc.....N..... ..@..@.reloc.....R.....@..B..... k.....H.....`.....Q...1.....*..(#...*..($...*.s%.....s&.....s'.....s(.....s).....*.~....o*...*.~.... o+...*.~....o,...*.~....o-...*.~....o....*R.....o1.....*..(2...*6..($...(%...*..(&...*.....(....*..('...*b..{....(...+}.....{....*b..{....(...+}.....{....*b..{....(...+}.....{....*b..{....(...+}.....{....*...{.....,.rq..p((...z..|....(...+*...{.....,.rq..p((...z..|....(...+*...{.....,.rq..p((...z..|....(.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.644650096826273
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:	5JbQqP8SDG.exe
File size:	611328
MD5:	250d122f4af32b52435a02787689ebbd
SHA1:	39346c41bcb75109dac251320d4afea649538f85
SHA256:	14f5c3ab5cbad5d2f6e751e8b3d42204460b8b10a38285623734d631a2ceda09
SHA512:	36d7e91588d98689c76646ae237c84e1797d3371bb54640793e09c23e545cf5bc454779051853c196f7ca6f58fda3dc080591ba1f86ff81b61928067c84e5488
SSDEEP:	12288:LgjjSrFL2yMrcIqrxggKI3Ab2zBFW1iR011EaSvq/gK0ncptnxwTFMtRXZk6m:LgjjgAcIqrcIwb2zTb01m
TLSH:	D5D47B9CB110759EF45BD4B2CA686C64A691776B431F42039433E7AE9E2E5F3CE40CA3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Umxb.....P..L.....>k... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x496b3e
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:	0x62786D55 [Mon May 9 01:24:37 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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	0x96ae4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x98000	0x398	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9a000	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	0x94b44	0x94c00	False	0.799832589286	data	7.65135197379	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x98000	0x398	0x400	False	0.376953125	data	2.97811845606	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9a000	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	0x98058	0x33c	data		

Imports

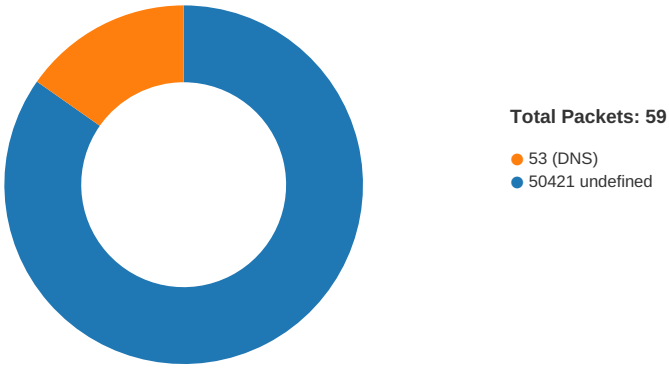
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright CPT185
Assembly Version	1.2.0.0
InternalName	eawGGIn.exe
FileVersion	1.2.0.0
CompanyName	CPT185
LegalTrademarks	
Comments	
ProductName	CPT185_Homework
ProductVersion	1.2.0.0
FileDescription	CPT185_Homework
OriginalFilename	eawGGIn.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 20:25:32.728507042 CEST	49775	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:32.746197939 CEST	50421	49775	185.19.85.175	192.168.2.5
May 10, 2022 20:25:33.344623089 CEST	49775	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:33.403633118 CEST	50421	49775	185.19.85.175	192.168.2.5
May 10, 2022 20:25:34.032136917 CEST	49775	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:34.062242985 CEST	50421	49775	185.19.85.175	192.168.2.5
May 10, 2022 20:25:38.412297964 CEST	49778	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:38.474441051 CEST	50421	49778	185.19.85.175	192.168.2.5
May 10, 2022 20:25:39.032617092 CEST	49778	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:39.072555065 CEST	50421	49778	185.19.85.175	192.168.2.5
May 10, 2022 20:25:39.641993046 CEST	49778	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:39.672367096 CEST	50421	49778	185.19.85.175	192.168.2.5
May 10, 2022 20:25:44.898557901 CEST	49781	50421	192.168.2.5	185.19.85.175

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 20:25:44.916450024 CEST	50421	49781	185.19.85.175	192.168.2.5
May 10, 2022 20:25:45.533144951 CEST	49781	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:45.552731991 CEST	50421	49781	185.19.85.175	192.168.2.5
May 10, 2022 20:25:46.110516071 CEST	49781	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:46.154194117 CEST	50421	49781	185.19.85.175	192.168.2.5
May 10, 2022 20:25:51.772958040 CEST	49784	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:51.814470053 CEST	50421	49784	185.19.85.175	192.168.2.5
May 10, 2022 20:25:52.346168041 CEST	49784	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:52.372033119 CEST	50421	49784	185.19.85.175	192.168.2.5
May 10, 2022 20:25:52.951143980 CEST	49784	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:52.990546942 CEST	50421	49784	185.19.85.175	192.168.2.5
May 10, 2022 20:25:57.005374908 CEST	49787	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:57.063580990 CEST	50421	49787	185.19.85.175	192.168.2.5
May 10, 2022 20:25:57.637762070 CEST	49787	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:57.657197952 CEST	50421	49787	185.19.85.175	192.168.2.5
May 10, 2022 20:25:58.239928007 CEST	49787	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:25:58.265409946 CEST	50421	49787	185.19.85.175	192.168.2.5
May 10, 2022 20:26:02.305550098 CEST	49789	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:02.337171078 CEST	50421	49789	185.19.85.175	192.168.2.5
May 10, 2022 20:26:03.002831936 CEST	49789	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:03.029366970 CEST	50421	49789	185.19.85.175	192.168.2.5
May 10, 2022 20:26:03.691318035 CEST	49789	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:03.709923983 CEST	50421	49789	185.19.85.175	192.168.2.5
May 10, 2022 20:26:10.671817064 CEST	49791	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:10.701931953 CEST	50421	49791	185.19.85.175	192.168.2.5
May 10, 2022 20:26:11.323120117 CEST	49791	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:11.343614101 CEST	50421	49791	185.19.85.175	192.168.2.5
May 10, 2022 20:26:12.019603968 CEST	49791	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:12.039122105 CEST	50421	49791	185.19.85.175	192.168.2.5
May 10, 2022 20:26:16.140109062 CEST	49797	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:16.159164906 CEST	50421	49797	185.19.85.175	192.168.2.5
May 10, 2022 20:26:16.738403082 CEST	49797	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:16.756925106 CEST	50421	49797	185.19.85.175	192.168.2.5
May 10, 2022 20:26:17.288614988 CEST	49797	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:17.306202888 CEST	50421	49797	185.19.85.175	192.168.2.5
May 10, 2022 20:26:21.410116911 CEST	49801	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:21.428174019 CEST	50421	49801	185.19.85.175	192.168.2.5
May 10, 2022 20:26:22.004448891 CEST	49801	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:22.033843994 CEST	50421	49801	185.19.85.175	192.168.2.5
May 10, 2022 20:26:22.694041014 CEST	49801	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:22.711700916 CEST	50421	49801	185.19.85.175	192.168.2.5
May 10, 2022 20:26:26.726931095 CEST	49803	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:26.754028082 CEST	50421	49803	185.19.85.175	192.168.2.5
May 10, 2022 20:26:27.348707914 CEST	49803	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:27.366638899 CEST	50421	49803	185.19.85.175	192.168.2.5
May 10, 2022 20:26:28.036252022 CEST	49803	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:28.063142061 CEST	50421	49803	185.19.85.175	192.168.2.5
May 10, 2022 20:26:32.088620901 CEST	49804	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:32.106316090 CEST	50421	49804	185.19.85.175	192.168.2.5
May 10, 2022 20:26:32.645987988 CEST	49804	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:32.663572073 CEST	50421	49804	185.19.85.175	192.168.2.5
May 10, 2022 20:26:33.349282980 CEST	49804	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:33.368165970 CEST	50421	49804	185.19.85.175	192.168.2.5
May 10, 2022 20:26:37.387248993 CEST	49805	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:37.404926062 CEST	50421	49805	185.19.85.175	192.168.2.5
May 10, 2022 20:26:38.005887032 CEST	49805	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:38.023646116 CEST	50421	49805	185.19.85.175	192.168.2.5
May 10, 2022 20:26:38.693451881 CEST	49805	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:38.711137056 CEST	50421	49805	185.19.85.175	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 20:26:42.812170029 CEST	49807	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:42.844466925 CEST	50421	49807	185.19.85.175	192.168.2.5
May 10, 2022 20:26:43.350069046 CEST	49807	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:43.368793964 CEST	50421	49807	185.19.85.175	192.168.2.5
May 10, 2022 20:26:44.026642084 CEST	49807	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:44.061487913 CEST	50421	49807	185.19.85.175	192.168.2.5
May 10, 2022 20:26:49.824131966 CEST	49809	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:49.848602057 CEST	50421	49809	185.19.85.175	192.168.2.5
May 10, 2022 20:26:50.350656986 CEST	49809	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:50.368242025 CEST	50421	49809	185.19.85.175	192.168.2.5
May 10, 2022 20:26:51.038208961 CEST	49809	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:51.055838108 CEST	50421	49809	185.19.85.175	192.168.2.5
May 10, 2022 20:26:55.132627964 CEST	49815	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:55.150667906 CEST	50421	49815	185.19.85.175	192.168.2.5
May 10, 2022 20:26:55.741739988 CEST	49815	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:55.759327888 CEST	50421	49815	185.19.85.175	192.168.2.5
May 10, 2022 20:26:56.351227999 CEST	49815	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:26:56.381736994 CEST	50421	49815	185.19.85.175	192.168.2.5
May 10, 2022 20:27:00.384252071 CEST	49841	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:27:00.401876926 CEST	50421	49841	185.19.85.175	192.168.2.5
May 10, 2022 20:27:00.945350885 CEST	49841	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:27:00.970081091 CEST	50421	49841	185.19.85.175	192.168.2.5
May 10, 2022 20:27:01.476583004 CEST	49841	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:27:01.496156931 CEST	50421	49841	185.19.85.175	192.168.2.5
May 10, 2022 20:27:05.512118101 CEST	49850	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:27:05.541635036 CEST	50421	49850	185.19.85.175	192.168.2.5
May 10, 2022 20:27:06.133254051 CEST	49850	50421	192.168.2.5	185.19.85.175
May 10, 2022 20:27:06.173866034 CEST	50421	49850	185.19.85.175	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 20:25:32.594398022 CEST	54322	53	192.168.2.5	8.8.8.8
May 10, 2022 20:25:32.613013983 CEST	53	54322	8.8.8.8	192.168.2.5
May 10, 2022 20:25:38.359194040 CEST	63712	53	192.168.2.5	8.8.8.8
May 10, 2022 20:25:38.380553007 CEST	53	63712	8.8.8.8	192.168.2.5
May 10, 2022 20:25:44.221904993 CEST	62466	53	192.168.2.5	8.8.8.8
May 10, 2022 20:25:44.240909100 CEST	53	62466	8.8.8.8	192.168.2.5
May 10, 2022 20:26:08.134268999 CEST	57352	53	192.168.2.5	8.8.8.8
May 10, 2022 20:26:08.155194998 CEST	53	57352	8.8.8.8	192.168.2.5
May 10, 2022 20:26:16.115792990 CEST	63241	53	192.168.2.5	8.8.8.8
May 10, 2022 20:26:16.137823105 CEST	53	63241	8.8.8.8	192.168.2.5
May 10, 2022 20:26:21.373483896 CEST	57809	53	192.168.2.5	8.8.8.8
May 10, 2022 20:26:21.391987085 CEST	53	57809	8.8.8.8	192.168.2.5
May 10, 2022 20:26:42.791327953 CEST	62680	53	192.168.2.5	8.8.8.8
May 10, 2022 20:26:42.808203936 CEST	53	62680	8.8.8.8	192.168.2.5
May 10, 2022 20:26:49.778464079 CEST	49407	53	192.168.2.5	8.8.8.8
May 10, 2022 20:26:49.799529076 CEST	53	49407	8.8.8.8	192.168.2.5
May 10, 2022 20:26:55.111569881 CEST	54463	53	192.168.2.5	8.8.8.8
May 10, 2022 20:26:55.130059958 CEST	53	54463	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 10, 2022 20:25:32.594398022 CEST	192.168.2.5	8.8.8.8	0x70e8	Standard query (0)	lowspeed121.ddns.net	A (IP address)	IN (0x0001)
May 10, 2022 20:25:38.359194040 CEST	192.168.2.5	8.8.8.8	0x9d84	Standard query (0)	lowspeed121.ddns.net	A (IP address)	IN (0x0001)
May 10, 2022 20:25:44.221904993 CEST	192.168.2.5	8.8.8.8	0xae7	Standard query (0)	lowspeed121.ddns.net	A (IP address)	IN (0x0001)

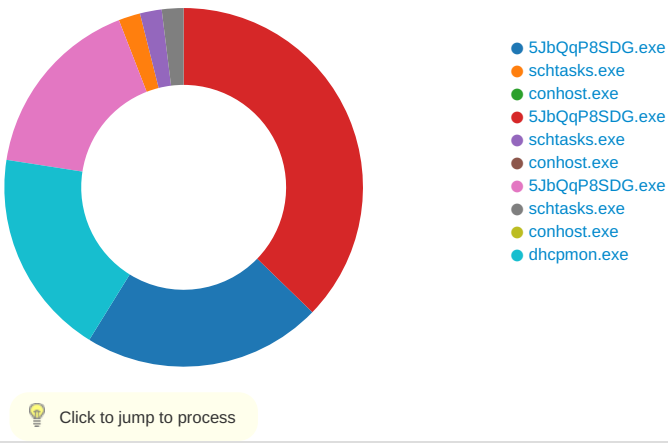
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 10, 2022 20:26:08.134268999 CEST	192.168.2.5	8.8.8.8	0xb5df	Standard query (0)	lowspeed12 1.ddns.net	A (IP address)	IN (0x0001)
May 10, 2022 20:26:16.115792990 CEST	192.168.2.5	8.8.8.8	0x41e3	Standard query (0)	lowspeed12 1.ddns.net	A (IP address)	IN (0x0001)
May 10, 2022 20:26:21.373483896 CEST	192.168.2.5	8.8.8.8	0x946	Standard query (0)	lowspeed12 1.ddns.net	A (IP address)	IN (0x0001)
May 10, 2022 20:26:42.791327953 CEST	192.168.2.5	8.8.8.8	0xb453	Standard query (0)	lowspeed12 1.ddns.net	A (IP address)	IN (0x0001)
May 10, 2022 20:26:49.778464079 CEST	192.168.2.5	8.8.8.8	0xa12	Standard query (0)	lowspeed12 1.ddns.net	A (IP address)	IN (0x0001)
May 10, 2022 20:26:55.111569881 CEST	192.168.2.5	8.8.8.8	0x20a2	Standard query (0)	lowspeed12 1.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2022 20:25:32.613013983 CEST	8.8.8.8	192.168.2.5	0x70e8	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 10, 2022 20:25:38.380553007 CEST	8.8.8.8	192.168.2.5	0x9d84	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 10, 2022 20:25:44.240909100 CEST	8.8.8.8	192.168.2.5	0xae7	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 10, 2022 20:26:08.155194998 CEST	8.8.8.8	192.168.2.5	0xb5df	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 10, 2022 20:26:16.137823105 CEST	8.8.8.8	192.168.2.5	0x41e3	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 10, 2022 20:26:21.391987085 CEST	8.8.8.8	192.168.2.5	0x946	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 10, 2022 20:26:42.808203936 CEST	8.8.8.8	192.168.2.5	0xb453	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 10, 2022 20:26:49.799529076 CEST	8.8.8.8	192.168.2.5	0xa12	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 10, 2022 20:26:55.130059958 CEST	8.8.8.8	192.168.2.5	0x20a2	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: 5JbQqP8SDG.exe PID: **7036**, Parent PID: **4932**

General

Target ID:	0
Start time:	20:24:53
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\5JbQqP8SDG.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\5JbQqP8SDG.exe"
Imagebase:	0x790000
File size:	611328 bytes
MD5 hash:	250D122F4AF32B52435A02787689EBBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.491093919.0000000003C89000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.491093919.0000000003C89000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.491093919.0000000003C89000.00000004.00000800.00020000.00000000.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	6E4ACF06	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	6E4ACF06	unknown
C:\Users\user\AppData\Roaming\GryVAO.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CA91E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpBE25.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CA97038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\5JbQqP8SDG.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E7BC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBE25.tmp	success or wait	1	6CA96A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\GryVAO.exe	0	611328	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 55 6d 78 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 4c 09 00 00 06 00 00 00 00 00 00 3e 6b 09 00 00 20 00 00 00 fd 09 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 fd 09 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PELUmxbPL>k @ @	success or wait	1	6CA91B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpBE25.tmp	0	1643	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationI	success or wait	1	6CA91B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\5JbQqP8SDG.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 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 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E7BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E485705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E48CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA91B4F	ReadFile
C:\Users\user\Desktop\5JbQqP8SDG.exe	unknown	611328	success or wait	1	6CA91B4F	ReadFile

Analysis Process: schtasks.exe PID: **6368**, Parent PID: **7036**

General

Target ID:	4
Start time:	20:25:13
Start date:	10/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\GryVAO" /XML "C:\Users\user\AppData\Local\Temp\tmpBE25.tmp
Imagebase:	0xd30000
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\tmpBE25.tmp	unknown	2	success or wait	1	D3AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBE25.tmp	unknown	1644	success or wait	1	D3ABD9	ReadFile

Analysis Process: conhost.exe PID: **6348**, Parent PID: **6368**

General

Target ID:	5
Start time:	20:25:13
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: 5JbQqP8SDG.exe PID: **4676**, Parent PID: **7036**

General

Target ID:	6
Start time:	20:25:14
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\5JbQqP8SDG.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7e0000
File size:	611328 bytes
MD5 hash:	250D122F4AF32B52435A02787689EBBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000000.483728850.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000000.483728850.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000000.483728850.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.720577614.0000000005400000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.720577614.0000000005400000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000006.00000002.720577614.0000000005400000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000000.482077079.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000000.482077079.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000000.482077079.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.720534425.00000000053E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.720534425.00000000053E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.720534425.00000000053E0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000006.00000002.720534425.00000000053E0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000000.482642247.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000000.482642247.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000000.482642247.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.706388161.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.706388161.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.706388161.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.720461431.0000000005230000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.720461431.0000000005230000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000006.00000002.720461431.0000000005230000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.712205262.0000000002C21000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.719803754.0000000003C69000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.719803754.0000000003C69000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000000.483222299.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000000.483222299.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000000.483222299.0000000000402000.00000040.00000400.00020000.00000000.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	6E4ACF06	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	6E4ACF06	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	6CA9BEFF	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	6CA91E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA9BEFF	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	6CA9DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CA9DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpFEC7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CA97038	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	6CA91E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpBD8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CA97038	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	6CA9BEFF	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	6CA9BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFEC7.tmp	success or wait	1	6CA96A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpBD8.tmp	success or wait	1	6CA96A95	DeleteFileW
C:\Users\user\Desktop\5JbQqP8SDG.exe:Zone.Identifier	success or wait	1	6CA12935	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	0	8	fd 10 fd fd fd 32 fd 48	2H	success or wait	1	6CA91B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 55 6d 78 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 4c 09 00 00 06 00 00 00 00 00 00 3e 6b 09 00 00 20 00 00 00 fd 09 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 fd 09 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PELUmxbPL>k @ @	success or wait	3	6CA9DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6CA9DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpFEC7.tmp	0	1301	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	6CA91B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	38	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 35 4a 62 51 71 50 38 53 44 47 2e 65 78 65	C:\Users\user\Desktop\5JbQqP8SDG.exe	success or wait	1	6CA91B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBD8.tmp	0	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	6CA91B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E485705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E48CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA91B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E46D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E46D72F	unknown
C:\Users\user\Desktop\5JbQqP8SDG.exe	unknown	4096	success or wait	1	6E46D72F	unknown
C:\Users\user\Desktop\5JbQqP8SDG.exe	unknown	512	success or wait	1	6E46D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6CA9646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **1408**, Parent PID: **4676**

General	
Target ID:	9
Start time:	20:25:20
Start date:	10/05/2022
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\tmpFEC7.tmp
Imagebase:	0xd30000
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\tmpFEC7.tmp	unknown	2	success or wait	1	D3AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFEC7.tmp	unknown	1302	success or wait	1	D3ABD9	ReadFile

Analysis Process: conhost.exe PID: **6608**, Parent PID: **1408**

General	
Target ID:	10
Start time:	20:25:21
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: 5JbQqP8SDG.exe PID: **5976**, Parent PID: **1040**

General	
Target ID:	11
Start time:	20:25:23
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\5JbQqP8SDG.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\5JbQqP8SDG.exe 0
Imagebase:	0x1a0000
File size:	611328 bytes
MD5 hash:	250D122F4AF32B52435A02787689EBBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.597428271.0000000003639000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.597428271.0000000003639000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.597428271.0000000003639000.00000004.00000800.00020000.00000000.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	6E4ACF06	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	6E4ACF06	unknown
C:\Users\user\AppData\Local\Temp\tmp3E23.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CA97038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3E23.tmp	success or wait	1	6CA96A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3E23.tmp	0	1643	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationI	success or wait	1	6CA91B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E485705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E48CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3E03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA91B4F	ReadFile

Analysis Process: schtasks.exe PID: **5564**, Parent PID: **4676**

General

Target ID:	12
Start time:	20:25:23
Start date:	10/05/2022
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\tmpBD8.tmp
Imagebase:	0xd30000
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\tmpBD8.tmp	unknown	2	success or wait	1	D3AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBD8.tmp	unknown	1311	success or wait	1	D3ABD9	ReadFile

Analysis Process: conhost.exe PID: **6652**, Parent PID: **5564**

General

Target ID:	13
Start time:	20:25:24
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: **6388**, Parent PID: **1040**

General

Target ID:	14
Start time:	20:25:26
Start date:	10/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xda0000
File size:	611328 bytes
MD5 hash:	250D122F4AF32B52435A02787689EBBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.604549457.0000000004159000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.604549457.0000000004159000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.604549457.0000000004159000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 63%, ReversingLabs
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	6E4ACF06	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	6E4ACF06	unknown
C:\Users\user\AppData\Local\Temp\tmp5777.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CA97038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E7BC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5777.tmp	success or wait	1	6CA96A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5777.tmp	0	1643	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationI	success or wait	1	6CA91B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 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 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E7BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E485705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E48CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E485705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E485705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA91B4F	ReadFile

Disassembly

No disassembly