ID: 356642
Sample Name: uqoYt8EFEWQXAne.exe
Cookbook: default.jbs
Time: 13:53:10
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

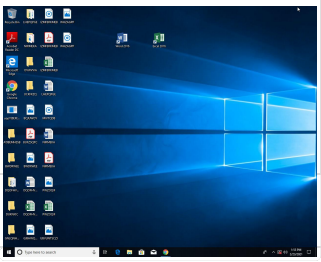
Analysis Report uqoYt8EFEWQXAne.exe

Overview

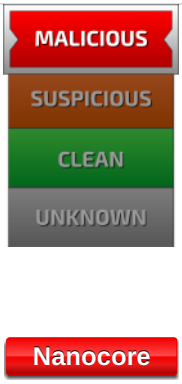
General Information

Sample Name:	uqoYt8EFEWQXAne.exe
Analysis ID:	356642
MD5:	c415765ef678428.
SHA1:	e5458ff58b98401..
SHA256:	c024e649afaafd4..
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection

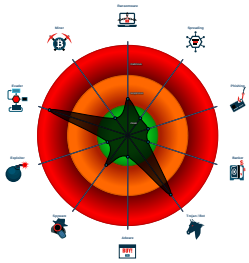


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code contains very larg…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- uqoYt8EFEWQXAne.exe (PID: 7160 cmdline: 'C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe' MD5: C415765EF678428F502B101039B7D495)
  - schtasks.exe (PID: 3984 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\krPtdhRIieabB' /XML 'C:\Users\user\AppData\Local\Temp\tmp975D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - uqoYt8EFEWQXAne.exe (PID: 3040 cmdline: C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe MD5: C415765EF678428F502B101039B7D495)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.661591930.000000000251 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.661683281.000000000259 9000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.662828873.000000000379 4000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3f54d:$x1: NanoCore.ClientPluginHost • 0x7258d:$x1: NanoCore.ClientPluginHost • 0x3f58a:$x2: IClientNetworkHost • 0x725ca:$x2: IClientNetworkHost • 0x430bd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x760fd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.662828873.000000000379 4000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.662828873.000000000379 4000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x3f2b5:$a: NanoCore • 0x3f2c5:$a: NanoCore • 0x3f4f9:$a: NanoCore • 0x3f50d:$a: NanoCore • 0x3f54d:$a: NanoCore • 0x722f5:$a: NanoCore • 0x72305:$a: NanoCore • 0x72539:$a: NanoCore • 0x7254d:$a: NanoCore • 0x7258d:$a: NanoCore • 0x3f314:$b: ClientPlugin • 0x3f516:$b: ClientPlugin • 0x3f556:$b: ClientPlugin • 0x72354:$b: ClientPlugin • 0x72556:$b: ClientPlugin • 0x72596:$b: ClientPlugin • 0x3f43b:$c: ProjectData • 0x7247b:$c: ProjectData • 0x3fe42:$d: DESCrypto • 0x72e82:$d: DESCrypto • 0x4780e:$e: KeepAlive
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.uqoYt8EFEWQXAne.exe.37c33c0.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.uqoYt8EFEWQXAne.exe.37c33c0.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.uqoYt8EFEWQXAne.exe.37c33c0.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.uqoYt8EFEWQXAne.exe.37c33c0.4.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
0.2.uqoYt8EFEWQXAne.exe.2546bb0.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 4 entries				

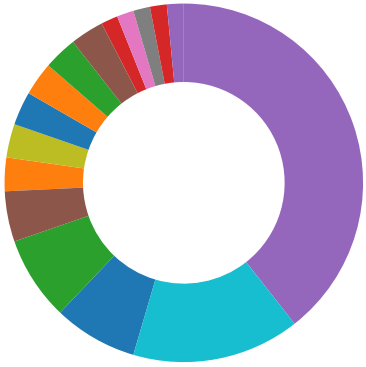
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Uses 32bit PE files
- Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

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

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- .NET source code contains very large strings

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 AntiVM_3

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

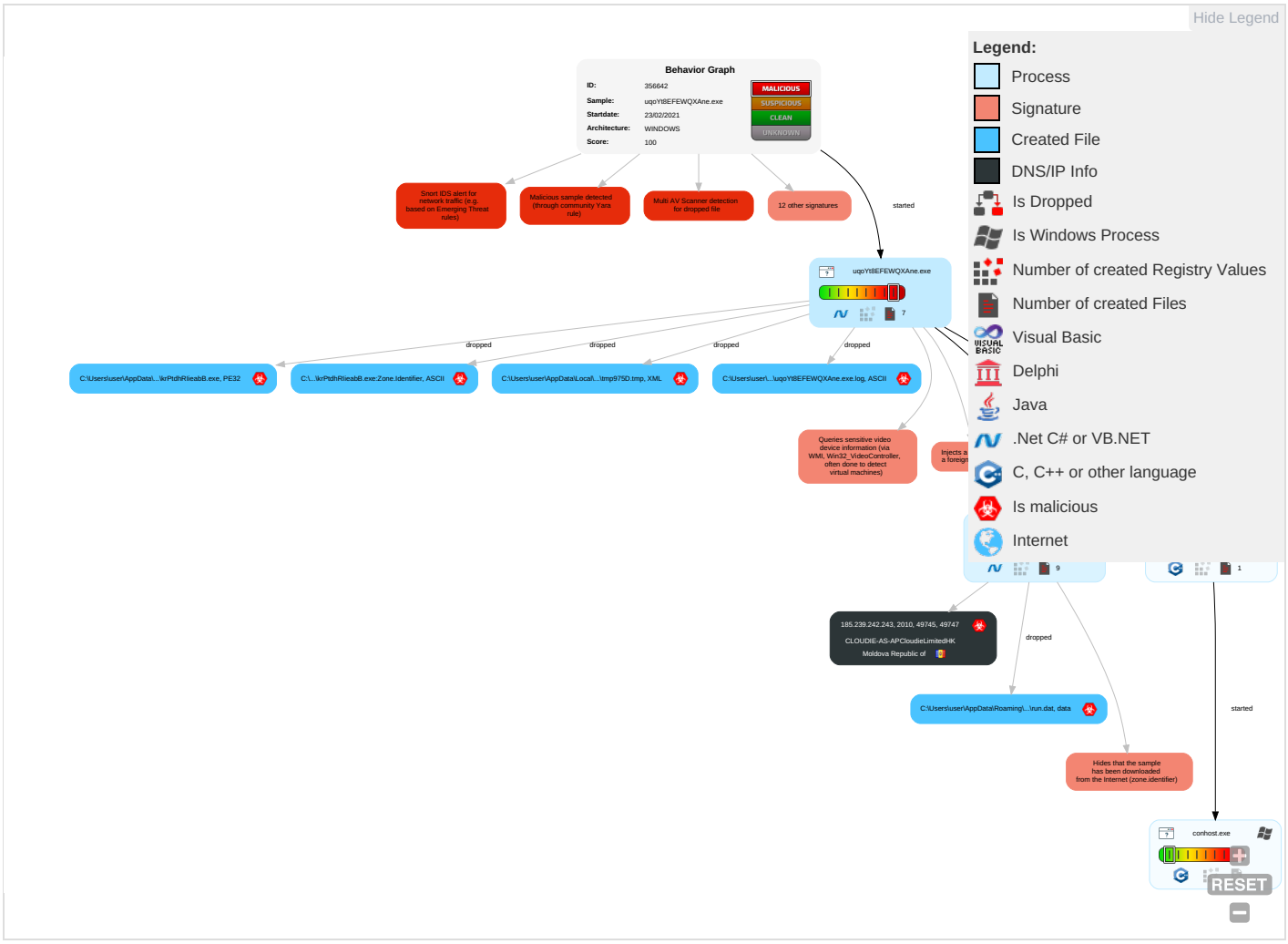
Detected Nanocore Rat

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	Net Effe
Valid Accounts	Windows Management Instrumentation 1 1	Scheduled Task/Job 1	Process Injection 1 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 3 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav Inse Net Cor
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 1 3	LSASS Memory	Virtualization/Sandbox Evasion 1 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exp Rec Cal
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exp Tra Loc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mar Dev Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Der Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc

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
uqoYt8EFEWQXAne.exe	43%	Virustotal		Browse
uqoYt8EFEWQXAne.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
uqoYt8EFEWQXAne.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\krPtdhRIieabB.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\krPtdhRIieabB.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://en.wxK	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnO	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnN	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnL	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgritaSOR	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm=OD	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cnmr_=	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.htmlmq	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.sajatypeworks.comZ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

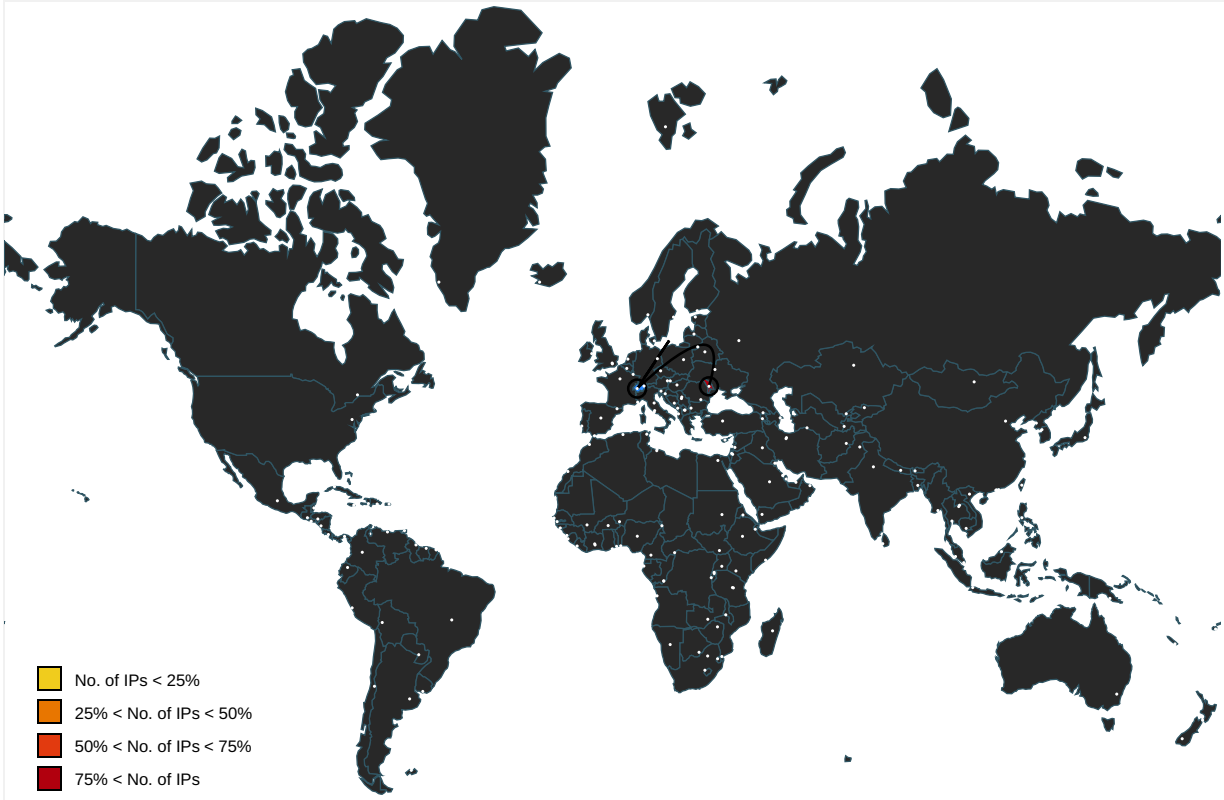
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://en.wxK	uqoYt8EFEWQXAne.exe, 00000000.00000003.638312128.00000000054D5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnO	uqoYt8EFEWQXAne.exe, 00000000.00000003.640183149.0000000000BAD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnN	uqoYt8EFEWQXAne.exe, 00000000.00000003.640183149.0000000000BAD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.0000000005640000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.0000000005640000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.0000000005640000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comF	uqoYt8EFEWQXAne.exe, 00000000.00000003.660725626.00000000054D0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.0000000005640000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.0000000005640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnL	uqoYt8EFEWQXAne.exe, 00000000.00000003.640371685.00000000054D7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comgritaSOR	uqoYt8EFEWQXAne.exe, 00000000.00000003.660725626.00000000054D0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.0000000005640000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comm=OD	uqoYt8EFEWQXAne.exe, 00000000.00000003.660725626.00000000054D0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.0000000005640000.00000002.00000001.sdmp, uqoYt8EFEWQXAne.exe, 00000000.00000003.639384165.00000000054EB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.0000000005640000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.0000000005640000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	uqoYt8EFEWQXAne.exe, 00000000.00000002.661591930.00000000025 11000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnmr_=	uqoYt8EFEWQXAne.exe, 00000000.00000003.640101915.00000000054 DE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	uqoYt8EFEWQXAne.exe, 00000000.00000003.637920168.00000000054 D3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	uqoYt8EFEWQXAne.exe, 00000000.00000003.640101915.00000000054 DE000.00000004.00000001.sdmp, uqoYt8EFEWQXAne.exe, 00000000.00000003.640686280.00000000054 D8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnn	uqoYt8EFEWQXAne.exe, 00000000.00000003.640371685.00000000054 D7000.00000004.00000001.sdmp	false		unknown
http://www.galapagosdesign.com/staff/dennis.htm	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false		high
http://www.ascendercorp.com/typedesigners.htmlmq	uqoYt8EFEWQXAne.exe, 00000000.00000003.642649855.00000000055 0D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	uqoYt8EFEWQXAne.exe, 00000000.00000003.644430876.00000000055 05000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comZ	uqoYt8EFEWQXAne.exe, 00000000.00000003.637920168.00000000054 D3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false		high
http://www.fonts.com	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	uqoYt8EFEWQXAne.exe, 00000000.00000002.661591930.00000000025 11000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.come	uqoYt8EFEWQXAne.exe, 00000000.00000003.637920168.00000000054 D3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	uqoYt8EFEWQXAne.exe, 00000000.00000002.667376898.00000000056 40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.239.242.243	unknown	Moldova Republic of		55933	CLOUDIE-AS-APCloudieLimitedHK	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356642
Start date:	23.02.2021
Start time:	13:53:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	uqoYt8EFEWQXAne.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/8@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 83% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • 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
13:54:00	API Interceptor	961x Sleep call for process: uqoYt8EFEWQXAne.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDIE-AS-APCloudieLimitedHK	New Order 2021.exe	Get hash	malicious	Browse	• 185.239.242.107
	SecuriteInfo.com.Variant.Bulz.361092.25830.exe	Get hash	malicious	Browse	• 185.239.242.107
	drWcfynA5k.exe	Get hash	malicious	Browse	• 185.239.242.107
	i5Z2XIR5k8.exe	Get hash	malicious	Browse	• 185.239.242.107
	receipt.doc	Get hash	malicious	Browse	• 185.239.242.107

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order KVRQ-743012021.doc	Get hash	malicious	Browse	• 185.239.242.107
	902178.rtf	Get hash	malicious	Browse	• 185.239.242.107
	22urmvdx0H.exe	Get hash	malicious	Browse	• 185.239.242.107
	Vendor from.doc	Get hash	malicious	Browse	• 185.239.242.107
	Proforma Invoice.doc	Get hash	malicious	Browse	• 185.239.242.107
	order170221.exe	Get hash	malicious	Browse	• 185.239.242.107
	SecuriteInfo.com.Variant.Bulz.361092.7175.exe	Get hash	malicious	Browse	• 185.239.242.107
	SWIFT COPY $27,078.exe	Get hash	malicious	Browse	• 185.239.242.107
	kellyx.exe	Get hash	malicious	Browse	• 185.239.242.107
	SWIFT COPY 27078.exe	Get hash	malicious	Browse	• 185.239.242.107
	Payment Advice 170221.exe	Get hash	malicious	Browse	• 185.239.242.107
	ENQUIRY.doc	Get hash	malicious	Browse	• 185.239.242.107
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 185.239.242.107
	Payment Receipt.jar	Get hash	malicious	Browse	• 185.239.242.107
	Paymentadvise.doc	Get hash	malicious	Browse	• 185.239.242.107

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\uqoYt8EFEWQXAne.exe.log

Process:	C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1406
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHg
MD5:	E5FA1A53BA6D70E18192AF6AF7CFDBFA
SHA1:	1C076481F11366751B8DA795C98A54DE8D1D82D5
SHA-256:	1D7BAA6D3EB5A504FD4652BC01A0864DEE898D35D9E29D03EB4A60B0D6405D83
SHA-512:	77850814E24DB48E3DDF9DF5B6A8110EE1A823BAABA800F89CD353EAC7F72E48B13F3F4A4DC8E5F0FAA707A7F14ED90577CF1CB106A0422F0BEDD1EFD2E94(E4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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..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\Temp\tmp975D.tmp

Process:	C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe

C:\Users\user\AppData\Local\Temp\tmp975D.tmp	
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.174690949576107
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGNtn:cbhK79lNQR/rydbz9I3YODOLNdq3W
MD5:	126E3B613474ECAA1D9907447AB29E73
SHA1:	484AA9F88B924751F236851738B17072A41FAB62
SHA-256:	6A3C2131197E5AF173FBE5A0211853F0E6AFED2B1ABDE4129151564B99E60A9F
SHA-512:	38C29CE66994092539C130FDF57548FB8B328612F904F59E66BFC120A49C0189B8DD7F600F74B7D2FAD1840440456D0E910382C91B31113ED23EEF06118EA893
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe
File Type:	data
Category:	dropped
Size (bytes):	1624
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC08
MD5:	0D79388CEC6619D612C2088173BB6741
SHA1:	8A312E3198009C545D0CF3254572189D29A03EA7
SHA-256:	D7D423B23D932E306F3CCB2F7A984B7036A042C007A43FD655C6B57B960BB8DF
SHA-512:	53BB3E9263DFD746E7E8159466E220E6EC9D81E9D3F0E1D191E09CD511B7EB93B0BA65D13CE0C97C652ECD0F69BB991E6B1840F961BC65003C4DD7AA93EED13
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:qi:qi
MD5:	BF504F3876526A01296886A5B4AEE886
SHA1:	56FCA050A19081209B611D03FFC486A68B9C368F
SHA-256:	DE7C120694DBBFA99B23C197184A0EB2E427EB8934FAD9A699FFC25741118CCC
SHA-512:	8D33452D421AEDB9C81F051DAD52A6E1B807FF26779D77790CD57E93E7772CE3AEBCE8067F1F1124B9B7C6AD82CF89EDBDD3F1F37FBD0FA0C9637000FF493FDD
Malicious:	**true**
Reputation:	low
Preview:	7.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i..........J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\krPtdhRlieabB.exe	
Process:	C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	527872
Entropy (8bit):	7.482730571721643
Encrypted:	false
SSDEEP:	12288:r+3HmKMLTOvaFESR5s87FvE4N4zjtx0qm5eINJPvu:aH4L5dR5s87FvOjtxhm5eIrnu
MD5:	C415765EF678428F502B101039B7D495
SHA1:	E5458FF58B98401D715A68A67AFABDEFAAF2EDC3
SHA-256:	C024E649AFAAFD4D1A1EBC2C5A2C457EECD2B5994C2B78E32312EB5289B5C093
SHA-512:	859DEB240D2E8EE1B5CC057AA63B0F8D49FEC83619B4C346821B09EFA5B9FCA01FB8539604565886046810 7F9A19A8710DB85C2C7B299351F6225C64034F2D8C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 32%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... .4`.....P..... ... ....@.. .....`..... ..@.....h...O.... ..P.....@..... ....H.....text..... ....`.rsrc...P.... .....@..@.rel oc.....@.....@..B.....H.....x...S.....J.....0.....(....(.....(.....o ...*.....(!.....("....(#.....($.....(%....*N..(. ...o....(&...*&..('....*.s(.....s).....s*.....s+.....s,.....*....0.....~....o-....+..*.0.....~....o....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0..<..... ...~.....(2.....,!r...p.....(3...o4...s5.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\krPtdhRlieabB.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\uqoYt8EFEWQXAne.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Roaming\krPtdhRlieabB.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.482730571721643
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	uqoYt8EFEWQXAne.exe
File size:	527872
MD5:	c415765ef678428f502b101039b7d495
SHA1:	e5458ff58b98401d715a68a67afabdefaaf2edc3
SHA256:	c024e649afaafd4d1a1ebc2c5a2c457eecd2b5994c2b78e32312eb5289b5c093
SHA512:	859deb240d2e8ee1b5cc057aa63b0f8d49fec83619b4c346821b09efa5b9fca01fb85396045658860468107f9a19a8710db85c2c7b299351f6225c64034f2d8c
SSDEEP:	12288:r+3HmKMLTOvaFESR5s87FvE4N4zjtx0qm5eINJPvu:aH4L5dR5s87FvOjtxhm5eIrnu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... .4`.....P..... ... ....@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4816ba
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:	0x60349B20 [Tue Feb 23 06:05:20 2021 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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0x81668	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x82000	0x1050	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x84000	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	0x7f6c0	0x7f800	False	0.772669653799	data	7.49785747568	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x1050	0x1200	False	0.361979166667	data	4.73273150028	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x84000	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	0x82090	0x39c	data		
RT_MANIFEST	0x8243c	0xc0f	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	IsolatedStorageFilePermissionAttribute.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	RegisterVB
ProductVersion	1.0.0.0
FileDescription	RegisterVB
OriginalFilename	IsolatedStorageFilePermissionAttribute.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-13:54:08.510703	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	2010	192.168.2.4	185.239.242.243
02/23/21-13:54:15.977491	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	2010	192.168.2.4	185.239.242.243
02/23/21-13:54:22.849012	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	2010	192.168.2.4	185.239.242.243
02/23/21-13:54:28.855800	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	2010	192.168.2.4	185.239.242.243
02/23/21-13:54:34.873087	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	2010	192.168.2.4	185.239.242.243
02/23/21-13:54:41.879231	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	2010	192.168.2.4	185.239.242.243
02/23/21-13:54:49.259735	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49766	2010	192.168.2.4	185.239.242.243
02/23/21-13:54:55.260046	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	2010	192.168.2.4	185.239.242.243
02/23/21-13:55:01.369094	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	2010	192.168.2.4	185.239.242.243
02/23/21-13:55:07.366934	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	2010	192.168.2.4	185.239.242.243
02/23/21-13:55:13.420841	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	2010	192.168.2.4	185.239.242.243
02/23/21-13:55:20.360587	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	2010	192.168.2.4	185.239.242.243
02/23/21-13:55:25.416649	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	2010	192.168.2.4	185.239.242.243
02/23/21-13:55:30.452441	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	2010	192.168.2.4	185.239.242.243
02/23/21-13:55:36.509869	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	2010	192.168.2.4	185.239.242.243
02/23/21-13:55:43.477164	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	2010	192.168.2.4	185.239.242.243
02/23/21-13:55:49.502138	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	2010	192.168.2.4	185.239.242.243
02/23/21-13:55:56.520609	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49787	2010	192.168.2.4	185.239.242.243

TCP Packets

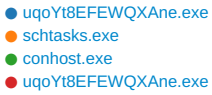
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 13:54:08.235266924 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:08.401680946 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:08.401907921 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:08.510703087 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:08.689546108 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:08.701209068 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:08.864763975 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:08.917184114 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.171945095 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.381033897 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.381109953 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.419231892 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.419270992 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.419301987 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.419316053 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.419328928 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.419353008 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.419373035 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.419378042 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.419401884 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.419403076 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.419426918 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.419430017 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.419450045 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.419464111 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.419475079 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.419506073 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.419536114 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.582185984 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582245111 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582283974 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582321882 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582343102 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.582360029 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582375050 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.582410097 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582453966 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582468033 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.582495928 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582535028 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582572937 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582604885 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.582611084 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582628012 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.582652092 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582690954 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582709074 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.582740068 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582787991 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582824945 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582834959 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.582865000 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582878113 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.582906961 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582945108 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.582957983 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.582986116 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.583064079 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.745871067 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.745958090 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746004105 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746042967 CET	2010	49745	185.239.242.243	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 13:54:09.746038914 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.746082067 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.746083975 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746124983 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746161938 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746172905 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.746202946 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746243000 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746289015 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.746292114 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746330976 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.746335983 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746378899 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746417046 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746450901 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.746454954 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746490002 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.746495008 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746535063 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746573925 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746611118 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.746620893 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746656895 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.746665001 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746702909 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746750116 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746788025 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746788979 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.746824026 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.746826887 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746866941 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746906042 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746942043 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.746953964 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.746992111 CET	49745	2010	192.168.2.4	185.239.242.243
Feb 23, 2021 13:54:09.746998072 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.747036934 CET	2010	49745	185.239.242.243	192.168.2.4
Feb 23, 2021 13:54:09.747076035 CET	2010	49745	185.239.242.243	192.168.2.4

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: uqoYt8EFEWQXAne.exe PID: 7160 Parent PID: 6084

General

Start time:	13:53:52
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe'
Imagebase:	0x150000
File size:	527872 bytes
MD5 hash:	C415765EF678428F502B101039B7D495
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.661591930.0000000002511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.661683281.0000000002599000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.662828873.0000000003794000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.662828873.0000000003794000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.662828873.0000000003794000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D17CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D17CF06	unknown
C:\Users\user\AppData\Roaming\krPtdhRIieabB.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	6BFCDD66	CopyFileW
C:\Users\user\AppData\Roaming\krPtdhRIieabB.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6BFCDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp975D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFC7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\uqoYt8EFEWQXAne.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp975D.tmp	success or wait	1	6BFC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\krPtdhRIieabB.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 20 9b 34 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 f8 07 00 00 14 00 00 00 00 00 00 ba 16 08 00 00 20 00 00 00 20 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode....$.......PE..L... .4`..............P.................. ... ....@.. .......................` ....@................	success or wait	3	6BFCDD66	CopyFileW
C:\Users\user\AppData\Roaming\krPtdhRIieabB.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	6BFCDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp975D.tmp	unknown	1646	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 6a 6f 6e 65 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 6e	<?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>.. </RegistrationIn	success or wait	1	6BFC1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\uqoYt8EFEWQXAne.exe.log	unknown	1406	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D48C907	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile

Analysis Process: schtasks.exe PID: 3984 Parent PID: 7160

General

Start time:	13:54:03
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\krPtdhRIieabB' /XML 'C:\Users\user\AppData\Local\Temp\tmp975D.tmp'
Imagebase:	0xa00000
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\tmp975D.tmp	unknown	2	success or wait	1	A0AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp975D.tmp	unknown	1647	success or wait	1	A0ABD9	ReadFile

Analysis Process: conhost.exe PID: 4680 Parent PID: 3984

General

Start time:	13:54:03
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: uqoYt8EFEWQXAne.exe PID: 3040 Parent PID: 7160

General

Start time:	13:54:04
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe
Imagebase:	0x700000
File size:	527872 bytes
MD5 hash:	C415765EF678428F502B101039B7D495
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D17CF06	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	6D17CF06	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	6BFCBEFF	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	6BFC1E60	CreateFileW
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	6BFCBEFF	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	6BFCBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	15	6BFC1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BFC1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BFC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe:Zone.Identifier	success or wait	1	6BF42935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	37 a5 a7 1a fa d7 d8 48	7.....H	success or wait	1	6BFC1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	7	6BFC1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wp K .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_....Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6BFC1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6BFC1B4F	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe	unknown	4096	success or wait	1	6D13D72F	unknown
C:\Users\user\Desktop\uqoYt8EFEWQXAne.exe	unknown	512	success or wait	1	6D13D72F	unknown

Disassembly

Code Analysis