ID: 356842
Sample Name: SWcNyi2YBj.exe
Cookbook: default.jbs
Time: 17:42:49
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

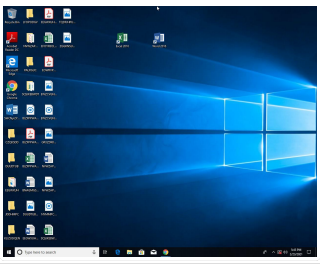
Analysis Report SWcNyi2YBj.exe

Overview

General Information

Sample Name:	SWcNyi2YBj.exe
Analysis ID:	356842
MD5:	413743f8b05dedc.
SHA1:	7b00081e08b834..
SHA256:	9b2db2aaf8c526d.
Tags:	AsyncRAT exe nVpn RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

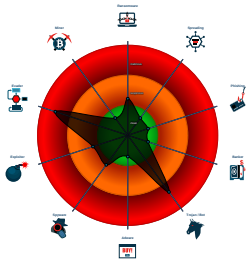
AsyncRAT

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

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected AsyncRAT
- .NET source code contains potentia…
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Uses dynamic DNS services
- Uses schtasks.exe or at.exe to add …
- Antivirus or Machine Learning detec…

Classification



Startup

- **System is w10x64**
- SWcNyi2YBj.exe (PID: 3468 cmdline: 'C:\Users\user\Desktop\SWcNyi2YBj.exe' MD5: 413743F8B05DEDC18E9D2D2FBE5D6528)
  - schtasks.exe (PID: 3412 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\mWSqBKhLOazUTy' /XML 'C:\Users\user\AppData\Local\Temp\tmp3DE4.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1156 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SWcNyi2YBj.exe (PID: 5080 cmdline: C:\Users\user\Desktop\SWcNyi2YBj.exe MD5: 413743F8B05DEDC18E9D2D2FBE5D6528)
  - SWcNyi2YBj.exe (PID: 4912 cmdline: C:\Users\user\Desktop\SWcNyi2YBj.exe MD5: 413743F8B05DEDC18E9D2D2FBE5D6528)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.479348490.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000000.00000002.240378798.00000000024C1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.240378798.00000000024C1000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Process Memory Space: SWcNyi2YBj.exe PID: 3468	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Process Memory Space: SWcNyi2YBj.exe PID: 3468	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Click to see the 1 entries

Unpacked PEs

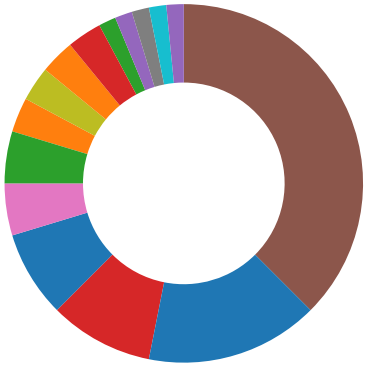
Source	Rule	Description	Author	Strings
7.2.SWcNyi2YBj.exe.400000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.2.SWcNyi2YBj.exe.26366d4.1.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.2.SWcNyi2YBj.exe.26366d4.1.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.2.SWcNyi2YBj.exe.25230cc.2.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.SWcNyi2YBj.exe.25230cc.2.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

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:

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

System Summary:

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Yara detected AsyncRAT

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

Yara detected AsyncRAT

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

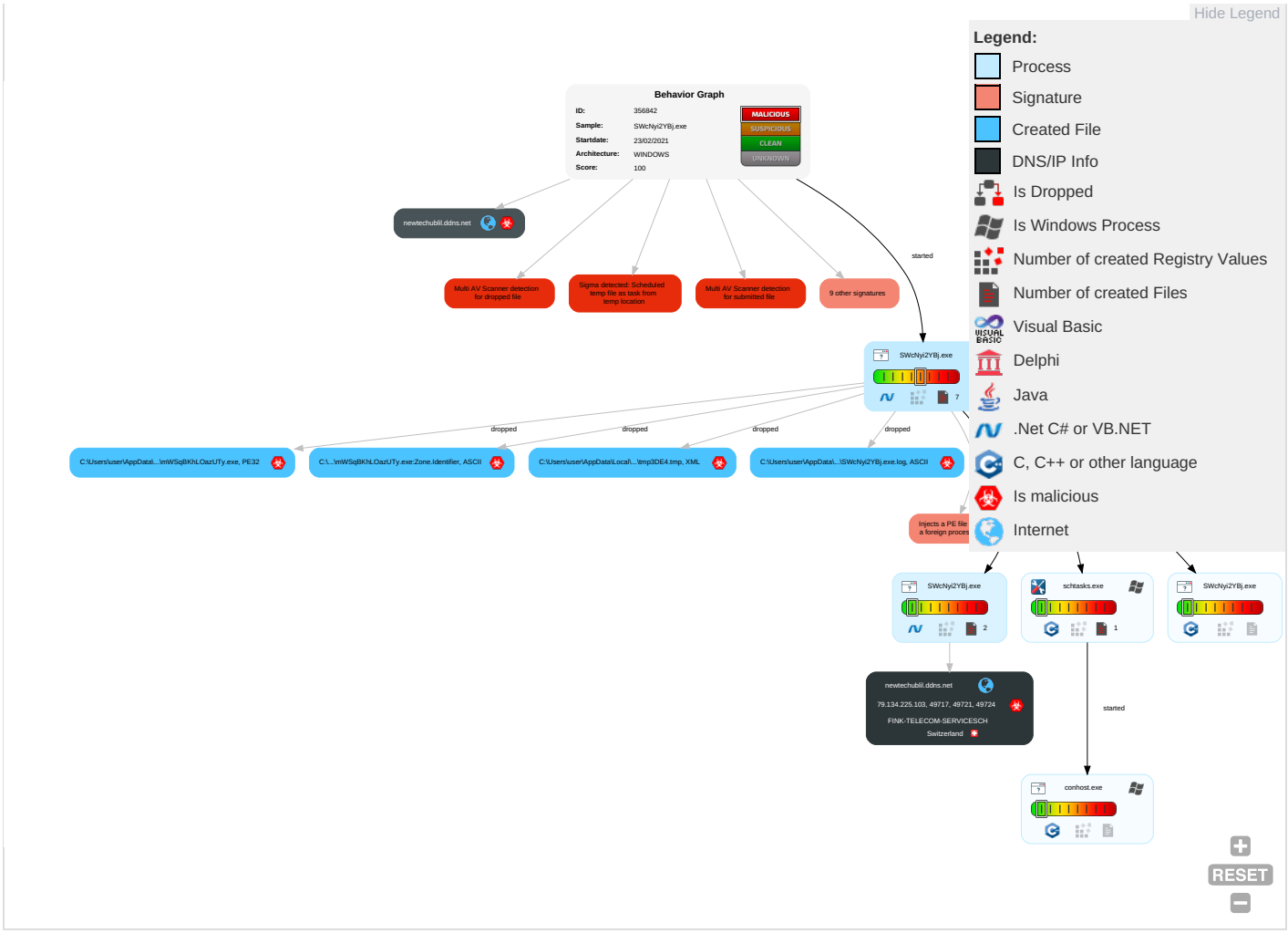
Lowering of HIPS / PFW / Operating System Security Settings:

Yara detected AsyncRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 2	Scheduled Task/Job 2	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 2	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1 3 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 2	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

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
SWcNyi2YBj.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
SWcNyi2YBj.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\mWSqBKhLOazUTy.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\mWSqBKhLOazUTy.exe	23%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.SWcNyi2YBj.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.SWcNyi2YBj.exe.26366d4.1.unpack	100%	Avira	HEUR/AGEN.1110362		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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	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.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/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.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	
http://www.zhongyicts.com.cn	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

Name	IP	Active	Malicious	Antivirus Detection	Reputation
newtechublil.ddns.net	79.134.225.103	true	true		unknown

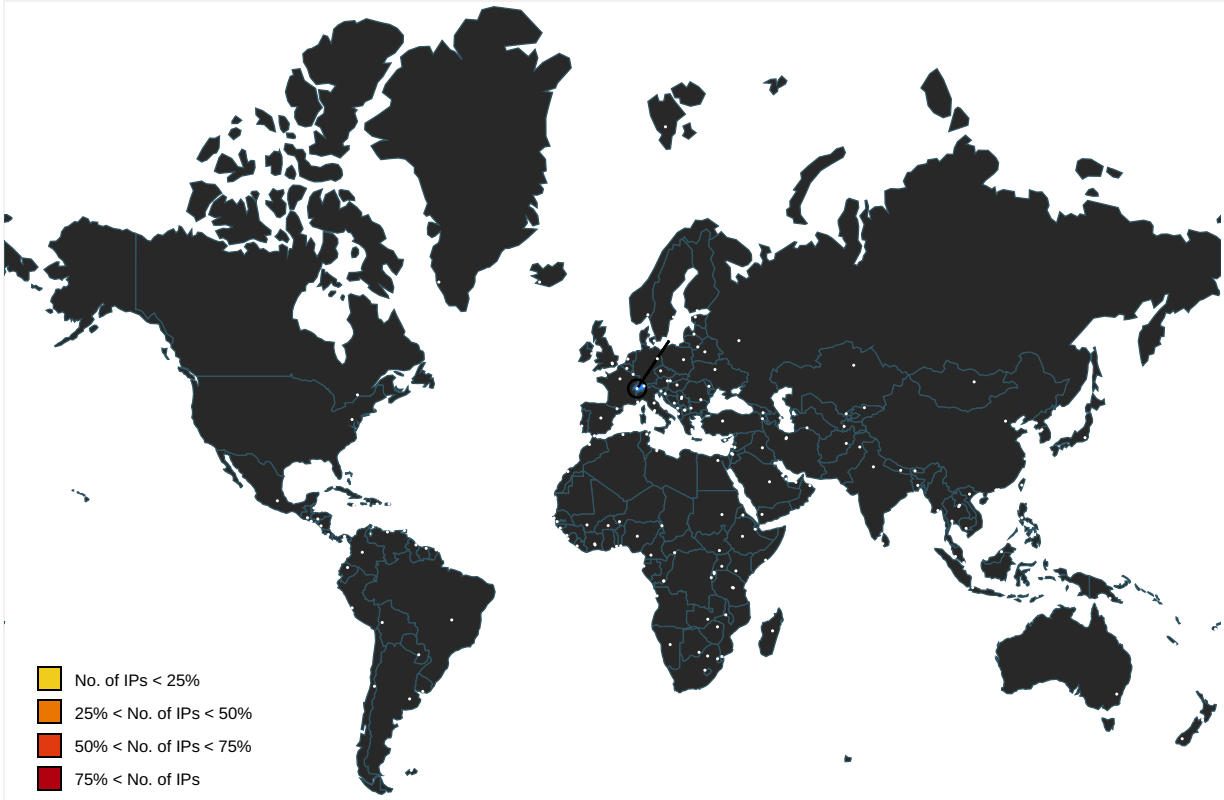
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false		high
http://www.tiro.com	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	SWcNyi2YBj.exe, 00000000.00000002.240378798.00000000024C1000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false		high
http://www.fonts.com	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SWcNyi2YBj.exe, 00000000.00000002.240378798.00000000024C1000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	SWcNyi2YBj.exe, 00000000.00000002.245240426.00000000054A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.103	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356842
Start date:	23.02.2021
Start time:	17:42:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SWcNyi2YBj.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:	31
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@8/4@18/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 52.147.198.201, 13.64.90.137, 104.42.151.234, 23.211.6.115, 184.30.20.56, 51.104.139.180, 8.250.157.254, 8.248.95.254, 8.238.27.126, 8.241.80.126, 8.248.123.254, 20.54.26.129, 92.122.213.194, 92.122.213.247, 51.11.168.160 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net • 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356842/sample/SWcNyi2YBj.exe

Simulations

Behavior and APIs

Time	Type	Description
17:43:49	API Interceptor	2x Sleep call for process: SWcNyi2YBj.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.103	dabs (1).exe	Get hash	malicious	Browse	
	dabsssss.exe	Get hash	malicious	Browse	
	PO UGT.exe	Get hash	malicious	Browse	
	feTtSsyXeBsJZUl.exe	Get hash	malicious	Browse	
	zAlNQ6GMGIHd4EB.exe	Get hash	malicious	Browse	
	I6sSftkh08BcVNE.exe	Get hash	malicious	Browse	
	t7Beia0TdGFsj4p.exe	Get hash	malicious	Browse	
	4paH8ucrAcKqEss.exe	Get hash	malicious	Browse	
	N9dbGzB9HSZWe4S.exe	Get hash	malicious	Browse	
	bedrapes.exe	Get hash	malicious	Browse	
	6PO.exe	Get hash	malicious	Browse	
	OFFICE.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
newtechublil.ddns.net	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 79.134.225.76
	RFQ.exe	Get hash	malicious	Browse	• 91.193.75.17
	ulY3ZgnMai.exe	Get hash	malicious	Browse	• 79.134.225.8

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	Confirmation Transfer Note Ref Number0002636.exe	Get hash	malicious	Browse	• 79.134.225.8
	TdX45jQWjj.exe	Get hash	malicious	Browse	• 79.134.225.43
	e92b274943f4a3a557881ee0dd57772d.exe	Get hash	malicious	Browse	• 79.134.225.105
	WxTm2cWLHF.exe	Get hash	malicious	Browse	• 79.134.225.71
	Payment Confirmation.exe	Get hash	malicious	Browse	• 79.134.225.30
	rjHlt1zz28.exe	Get hash	malicious	Browse	• 79.134.225.49
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 79.134.225.49
	document.exe	Get hash	malicious	Browse	• 79.134.225.122
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 79.134.225.105
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 79.134.225.105
	256ec8f8f67b59c5e085b0bb63afcd13.exe	Get hash	malicious	Browse	• 79.134.225.105
	JOIN.exe	Get hash	malicious	Browse	• 79.134.225.30
	Delivery pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 79.134.225.105
	fnfqzfwC44.exe	Get hash	malicious	Browse	• 79.134.225.25
	Solicitud de oferta 6100003768.exe	Get hash	malicious	Browse	• 79.134.225.96
	Nrfgylra.exe	Get hash	malicious	Browse	• 79.134.225.96
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SWcNyi2YBj.exe.log	
Process:	C:\Users\user\Desktop\SWcNyi2YBj.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	moderate, very likely benign file
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\Temp\tmp3DE4.tmp	
Process:	C:\Users\user\Desktop\SWcNyi2YBj.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.198515785095118
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBYtn:cbh47TlNQ//rydbz9I3YODOLNdq3g
MD5:	F673893CB70D0D66CFF6A2C9EFCC203A
SHA1:	3ABA1096F1DC32391C67402EA3B144034FF468CC
SHA-256:	728E077C3F91752E5653161656169D61323C80C2A1BBA5FF6AE465A49354ADC7
SHA-512:	7185A9F6388406E9626FA7DFBC809F2A760D3526FF5F60980CB63B5B7A98F508AC1273758F96D608815CB7EE512A4E506CC98034E086CD94DB0155FE7358CECE
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\mWSqBKhLOazUTy.exe	
Process:	C:\Users\user\Desktop\SWcNyi2YBj.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	724992
Entropy (8bit):	6.611620887453061
Encrypted:	false
SSDEEP:	12288:pG/bvRU9z7ZB2uXI5tARzjnOeX6nKAZgDpaSO3nMJibf41y99zzSl+XoEzz1w5Uy:pG/+9zf2gKrB9zztzzK
MD5:	413743F8B05DEDC18E9D2D2FBE5D6528
SHA1:	7B00081E08B8348DF7D0940B73FFBECD7DE249DA
SHA-256:	9B2DB2AAF8C526DFF498520E35898C5F3EF718EC198E267A40BFADD926BD358A
SHA-512:	C3306C58CED2C58BA765116A07192D03424FD4568C1AE5F99359CB0ECB504CA109AFBD082DA00A665096F2EC330CBEE55DF655D557F1B12AB37F0C957707128
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 23%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....3`.....P..^.....j|... .....@.. .....`.....@.....|..O.....@..... ....H.....text...p\... ...^..... ..`.rsrc.....`.....@..@.reloc.....@.....@..B.....L|.....H.....8Y...T.....H.....(...*&..(!....*.s".....s#.....s$.....s%.....s&.....*...0.....~....o'....+..*.0.....~....o(....+..*.0.....~....o).....+..*.0.....~....o*....+..*.0.....~....o+....+..*.0..<.....~.....(,.....,!r...p.....(-...o....s/.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r)..p~....o0...(1.....t$....+..*Vs....(2...t.....*..(3...*.0.....

C:\Users\user\AppData\Roaming\mWSqBKhLOazUTy.exe:Zone.Identifier	

C:\Users\user\AppData\Roaming\mWSqBKhLOazUTy.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SWcNyi2YBj.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
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.611620887453061
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:	SWcNyi2YBj.exe
File size:	724992
MD5:	413743f8b05dedc18e9d2d2fbe5d6528
SHA1:	7b00081e08b8348df7d0940b73ffbecd7de249da
SHA256:	9b2db2aaf8c526dff498520e35898c5f3ef718ec198e267a40bfadd926bd358a
SHA512:	c3306c58ced2c58ba765116a07192d03424fd4568c1ae5f99359cb0ecb504ca109afbd082da00a665096f2ec330cbee55df655d557f1b12ab37f0c9577071280
SSDEEP:	12288:pG/bvRU9z7ZB2uXl5tARzjnOeX6nKAZgDpaSO3nMJibf41y99zzSl+XoEzz1w5Uy:pG/+9zf2gKrB9zztzzK
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....3`.....P..^.....j|... .....@.. .....`.....@.....

File Icon

Icon Hash:	f08f888c8e8e8730

Static PE Info

General

Entrypoint:	0x457c6a
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:	0x6033D2E6 [Mon Feb 22 15:51:02 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x57c18	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x58000	0x5acd0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb4000	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

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x55c70	0x55e00	False	0.674169282205	data	7.13520516596	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x58000	0x5acd0	0x5ae00	False	0.101229367263	data	5.55258821771	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb4000	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_ICON	0x58220	0x42028	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x9a248	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x9a6b0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x9cc58	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x9dd00	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xae528	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xb2750	0x5a	data		
RT_VERSION	0xb27ac	0x338	data		
RT_MANIFEST	0xb2ae4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

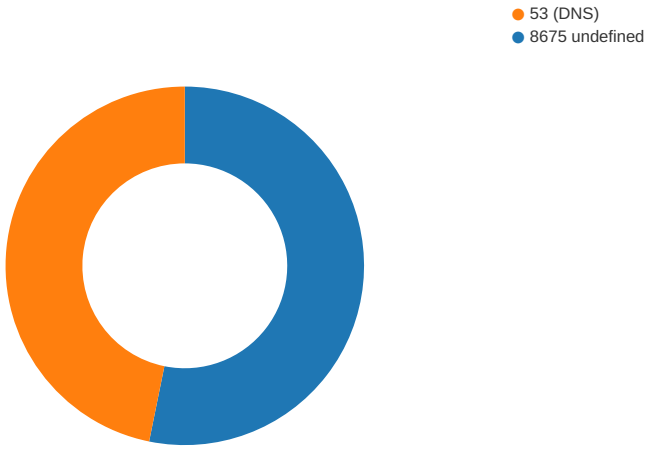
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Microsoft 2014
Assembly Version	1.0.0.0
InternalName	SHA384.exe
FileVersion	1.0.0.0
CompanyName	Microsoft
LegalTrademarks	
Comments	
ProductName	WinClient
ProductVersion	1.0.0.0
FileDescription	WinClient
OriginalFilename	SHA384.exe

Network Behavior

Network Port Distribution

Total Packets: 94



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:44:03.105317116 CET	49717	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:03.191925049 CET	8675	49717	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:03.863028049 CET	49717	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:03.950175047 CET	8675	49717	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:04.472395897 CET	49717	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:04.559859991 CET	8675	49717	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:09.652251005 CET	49721	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:09.740115881 CET	8675	49721	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:10.363591909 CET	49721	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:10.449055910 CET	8675	49721	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:10.972980022 CET	49721	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:11.058640003 CET	8675	49721	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:16.228962898 CET	49724	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:16.311551094 CET	8675	49724	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:16.817193985 CET	49724	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:16.902813911 CET	8675	49724	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:17.504775047 CET	49724	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:17.592001915 CET	8675	49724	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:22.903727055 CET	49725	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:22.987723112 CET	8675	49725	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:23.520935059 CET	49725	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:23.605128050 CET	8675	49725	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:24.208554029 CET	49725	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:24.293292046 CET	8675	49725	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:29.396760941 CET	49726	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:29.482269049 CET	8675	49726	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:29.990196943 CET	49726	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:30.075594902 CET	8675	49726	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:30.584013939 CET	49726	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:30.670018911 CET	8675	49726	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:35.748512030 CET	49728	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:35.831305981 CET	8675	49728	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:36.334497929 CET	49728	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:36.494031906 CET	8675	49728	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:37.006361008 CET	49728	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:37.089211941 CET	8675	49728	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:42.206016064 CET	49730	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:42.290887117 CET	8675	49730	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:42.803889990 CET	49730	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:42.890052080 CET	8675	49730	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:43.397552967 CET	49730	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:43.480703115 CET	8675	49730	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:48.562206984 CET	49731	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:48.646739006 CET	8675	49731	79.134.225.103	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:44:49.148060083 CET	49731	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:49.232023001 CET	8675	49731	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:49.741868973 CET	49731	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:49.828656912 CET	8675	49731	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:54.907299995 CET	49735	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:54.994627953 CET	8675	49735	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:55.508002996 CET	49735	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:55.593450069 CET	8675	49735	79.134.225.103	192.168.2.3
Feb 23, 2021 17:44:56.101721048 CET	49735	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:44:56.190965891 CET	8675	49735	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:01.309381962 CET	49741	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:01.392326117 CET	8675	49741	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:01.899068117 CET	49741	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:01.983769894 CET	8675	49741	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:02.492978096 CET	49741	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:02.575634003 CET	8675	49741	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:07.658233881 CET	49742	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:07.743900061 CET	8675	49742	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:08.258971930 CET	49742	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:08.346327066 CET	8675	49742	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:08.852788925 CET	49742	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:08.938304901 CET	8675	49742	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:14.017774105 CET	49743	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:14.105139971 CET	8675	49743	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:14.618869066 CET	49743	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:14.704482079 CET	8675	49743	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:15.226310015 CET	49743	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:15.315165997 CET	8675	49743	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:20.440475941 CET	49744	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:20.523124933 CET	8675	49744	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:21.025955915 CET	49744	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:21.108951092 CET	8675	49744	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:21.619462967 CET	49744	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:21.702661991 CET	8675	49744	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:26.783905983 CET	49745	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:26.869257927 CET	8675	49745	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:27.369971037 CET	49745	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:27.457417965 CET	8675	49745	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:27.963754892 CET	49745	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:28.051026106 CET	8675	49745	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:33.125773907 CET	49748	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:33.208446026 CET	8675	49748	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:33.714291096 CET	49748	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:33.797103882 CET	8675	49748	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:34.308130980 CET	49748	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:34.390979052 CET	8675	49748	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:39.499028921 CET	49749	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:39.581712961 CET	8675	49749	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:40.089854956 CET	49749	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:40.174037933 CET	8675	49749	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:40.683594942 CET	49749	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:40.768460989 CET	8675	49749	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:45.849132061 CET	49750	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:45.931723118 CET	8675	49750	79.134.225.103	192.168.2.3
Feb 23, 2021 17:45:46.434417963 CET	49750	8675	192.168.2.3	79.134.225.103
Feb 23, 2021 17:45:46.517024994 CET	8675	49750	79.134.225.103	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:43:35.327290058 CET	51281	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:35.379692078 CET	53	51281	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:36.108521938 CET	49199	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:36.160074949 CET	53	49199	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:43:36.971259117 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:37.043848991 CET	53	50620	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:38.186973095 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:38.238607883 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:38.541035891 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:38.607603073 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:39.498251915 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:39.547049046 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:40.867343903 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:40.918814898 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:42.044867039 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:42.093602896 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:43.429733038 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:43.489700079 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:44.706145048 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:44.755294085 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:45.675206900 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:45.724040031 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:46.575237036 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:46.623881102 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:47.815298080 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:47.863918066 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:49.237941980 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:49.286633015 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:50.495012999 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:50.553633928 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:51.710032940 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:51.758600950 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:52.886774063 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:52.946746111 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 17:43:54.075249910 CET	51352	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:43:54.128885984 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:03.032732010 CET	59349	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:03.091830969 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:07.196192980 CET	57084	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:07.255497932 CET	53	57084	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:09.591444969 CET	58823	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:09.650608063 CET	53	58823	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:13.450990915 CET	57568	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:13.499706030 CET	53	57568	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:16.092787027 CET	50540	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:16.152749062 CET	53	50540	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:22.840045929 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:22.901628017 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:29.336308956 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:29.393642902 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:30.755537033 CET	57762	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:30.817784071 CET	53	57762	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:35.687403917 CET	55435	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:35.746407032 CET	53	55435	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:40.642918110 CET	50713	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:40.712431908 CET	53	50713	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:42.143765926 CET	56132	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:42.203774929 CET	53	56132	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:48.508322954 CET	58987	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:48.560257912 CET	53	58987	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:54.448518038 CET	56579	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:54.501279116 CET	53	56579	8.8.8.8	192.168.2.3
Feb 23, 2021 17:44:54.845721006 CET	60633	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:44:54.905570984 CET	53	60633	8.8.8.8	192.168.2.3
Feb 23, 2021 17:45:00.655599117 CET	61292	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:45:00.714571953 CET	53	61292	8.8.8.8	192.168.2.3
Feb 23, 2021 17:45:01.259339094 CET	63619	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:45:01.307837009 CET	53	63619	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:45:07.595879078 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:45:07.655770063 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 17:45:13.956756115 CET	61946	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:45:14.015863895 CET	53	61946	8.8.8.8	192.168.2.3
Feb 23, 2021 17:45:20.381505966 CET	64910	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:45:20.438465118 CET	53	64910	8.8.8.8	192.168.2.3
Feb 23, 2021 17:45:26.723320961 CET	52123	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:45:26.782072067 CET	53	52123	8.8.8.8	192.168.2.3
Feb 23, 2021 17:45:30.229089975 CET	56130	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:45:30.280635118 CET	53	56130	8.8.8.8	192.168.2.3
Feb 23, 2021 17:45:31.795489073 CET	56338	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:45:31.860456944 CET	53	56338	8.8.8.8	192.168.2.3
Feb 23, 2021 17:45:33.067162991 CET	59420	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:45:33.124275923 CET	53	59420	8.8.8.8	192.168.2.3
Feb 23, 2021 17:45:39.438234091 CET	58784	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:45:39.497051954 CET	53	58784	8.8.8.8	192.168.2.3
Feb 23, 2021 17:45:45.786523104 CET	63978	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:45:45.846759081 CET	53	63978	8.8.8.8	192.168.2.3
Feb 23, 2021 17:45:52.123995066 CET	62938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:45:52.181025028 CET	53	62938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:44:03.032732010 CET	192.168.2.3	8.8.8.8	0x7f48	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:09.591444969 CET	192.168.2.3	8.8.8.8	0x3df	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:16.092787027 CET	192.168.2.3	8.8.8.8	0x4586	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:22.840045929 CET	192.168.2.3	8.8.8.8	0xa9d6	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:29.336308956 CET	192.168.2.3	8.8.8.8	0x7b92	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:35.687403917 CET	192.168.2.3	8.8.8.8	0xd4fa	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:42.143765926 CET	192.168.2.3	8.8.8.8	0x9d28	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:48.508322954 CET	192.168.2.3	8.8.8.8	0x1b71	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:54.845721006 CET	192.168.2.3	8.8.8.8	0xa1ef	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:01.259339094 CET	192.168.2.3	8.8.8.8	0xd19d	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:07.595879078 CET	192.168.2.3	8.8.8.8	0x233	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:13.956756115 CET	192.168.2.3	8.8.8.8	0x3bd1	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:20.381505966 CET	192.168.2.3	8.8.8.8	0x373f	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:26.723320961 CET	192.168.2.3	8.8.8.8	0x4996	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:33.067162991 CET	192.168.2.3	8.8.8.8	0xfecb	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:39.438234091 CET	192.168.2.3	8.8.8.8	0x6506	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:45.786523104 CET	192.168.2.3	8.8.8.8	0x19ac	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:52.123995066 CET	192.168.2.3	8.8.8.8	0x416d	Standard query (0)	newtechubl il.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

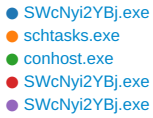
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:44:03.091830969 CET	8.8.8.8	192.168.2.3	0x7f48	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:09.650608063 CET	8.8.8.8	192.168.2.3	0x3df	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)

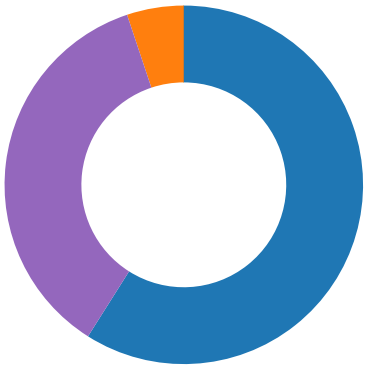
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:44:16.152749062 CET	8.8.8.8	192.168.2.3	0x4586	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:22.901628017 CET	8.8.8.8	192.168.2.3	0xa9d6	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:29.393642902 CET	8.8.8.8	192.168.2.3	0x7b92	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:35.746407032 CET	8.8.8.8	192.168.2.3	0xd4fa	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:42.203774929 CET	8.8.8.8	192.168.2.3	0x9d28	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:48.560257912 CET	8.8.8.8	192.168.2.3	0x1b71	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:44:54.905570984 CET	8.8.8.8	192.168.2.3	0xa1ef	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:01.307837009 CET	8.8.8.8	192.168.2.3	0xd19d	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:07.655770063 CET	8.8.8.8	192.168.2.3	0x233	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:14.015863895 CET	8.8.8.8	192.168.2.3	0x3bd1	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:20.438465118 CET	8.8.8.8	192.168.2.3	0x373f	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:26.782072067 CET	8.8.8.8	192.168.2.3	0x4996	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:33.124275923 CET	8.8.8.8	192.168.2.3	0xfecb	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:39.497051954 CET	8.8.8.8	192.168.2.3	0x6506	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:45.846759081 CET	8.8.8.8	192.168.2.3	0x19ac	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)
Feb 23, 2021 17:45:52.181025028 CET	8.8.8.8	192.168.2.3	0x416d	No error (0)	newtechubl il.ddns.net		79.134.225.103	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: SWcNyi2YBj.exe PID: 3468 Parent PID: 5564

General

Start time:	17:43:42
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SWcNyi2YBj.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SWcNyi2YBj.exe'
Imagebase:	0xd0000
File size:	724992 bytes
MD5 hash:	413743F8B05DEDC18E9D2D2FBE5D6528
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: 00000000.00000002.240378798.00000000024C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000002.240378798.00000000024C1000.00000004.00000001.sdmp, Author: Joe Security
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	6E0ACF06	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	6E0ACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\mWSqBKhLOazUTy.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	6CEFDD66	CopyFileW
C:\Users\user\AppData\Roaming\mWSqBKhLOazUTy.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CEFDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp3DE4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEF7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SWcNyi2YBj.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3DE4.tmp	success or wait	1	6CEF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\mWSqBKhLOazUTy.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 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 e6 d2 33 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 5e 05 00 00 b0 05 00 00 00 00 00 6a 7c 05 00 00 20 00 00 00 80 05 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 0b 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.....3`.......... ....P..^..........j|... ........@.. .......................` ....@................	success or wait	3	6CEFDD66	CopyFileW
C:\Users\user\AppData\Roaming\mWSqBKhLOazUTy.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	6CEFDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3DE4.tmp	unknown	1647	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 68 61 72 64 7a 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	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SWcNyi2YBj.exe.log	unknown	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",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_v4.0.3	success or wait	1	6E3BC907	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Analysis Process: schtasks.exe PID: 3412 Parent PID: 3468

General

Start time:	17:43:52
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\mWSqBKhLOazUTy' /XML 'C: \Users\user\AppData\Local\Temp\tmp3DE4.tmp'
Imagebase:	0xf20000
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\tmp3DE4.tmp	unknown	2	success or wait	1	F2AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3DE4.tmp	unknown	1648	success or wait	1	F2ABD9	ReadFile

Analysis Process: conhost.exe PID: 1156 Parent PID: 3412

General

Start time:	17:43:52
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SWcNyi2YBj.exe PID: 5080 Parent PID: 3468

General

Start time:	17:43:53
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SWcNyi2YBj.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SWcNyi2YBj.exe
Imagebase:	0x230000
File size:	724992 bytes
MD5 hash:	413743F8B05DEDC18E9D2D2FBE5D6528
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SWcNyi2YBj.exe PID: 4912 Parent PID: 3468

General

Start time:	17:43:53
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SWcNyi2YBj.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SWcNyi2YBj.exe
Imagebase:	0x830000
File size:	724992 bytes
MD5 hash:	413743F8B05DEDC18E9D2D2FBE5D6528
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000007.00000002.479348490.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
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	6E0ACF06	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	6E0ACF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	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	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Disassembly

Code Analysis