ID: 412223
Sample Name: aISbFyk4Lj.exe
Cookbook: default.jbs
Time: 14:09:05
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

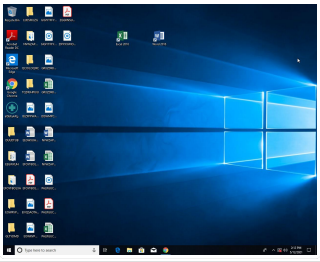
Analysis Report aISbFyk4Lj.exe

Overview

General Information

Sample Name:	aISbFyk4Lj.exe
Analysis ID:	412223
MD5:	167f0a829df709c..
SHA1:	a66caacf3bd0390..
SHA256:	12279e26650d58..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

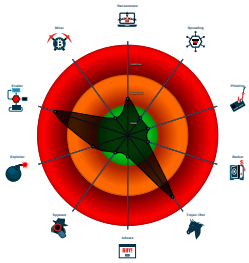
NanoCore

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- aISbFyk4Lj.exe (PID: 3288 cmdline: 'C:\Users\user\Desktop\aISbFyk4Lj.exe' MD5: 167F0A829DF709CC4107369ED23FBDFB)
  - schtasks.exe (PID: 2200 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\QxHKzIlUxTf' /XML 'C:\Users\user\AppData\Local\Temp\tmp8EF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5232 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 1724 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - RegSvcs.exe (PID: 5884 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": ".0.0.0,",
  "Mutex": "a7fa722b-7dae-45b1-afa6-302155a5",
  "Group": "Default",
  "Domain1": "wespeaktruthtoman.sytes.net",
  "Domain2": "wespeaktruthtoman12.sytes.net",
  "Port": 5600,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.227476170.000000000362D000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.227998353.00000000045E1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x279b45:$x1: NanoCore.ClientPluginHost • 0x2feb65:$x1: NanoCore.ClientPluginHost • 0x279b82:$x2: IClientNetworkHost • 0x2feba2:$x2: IClientNetworkHost • 0x27d6b5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x3026d5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.227998353.00000000045E1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.227998353.00000000045E1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2798ad:$a: NanoCore • 0x2798bd:$a: NanoCore • 0x279af1:$a: NanoCore • 0x279b05:$a: NanoCore • 0x279b45:$a: NanoCore • 0x2fe8cd:$a: NanoCore • 0x2fe8dd:$a: NanoCore • 0x2feb11:$a: NanoCore • 0x2feb25:$a: NanoCore • 0x2feb65:$a: NanoCore • 0x27990c:$b: ClientPlugin • 0x279b0e:$b: ClientPlugin • 0x279b4e:$b: ClientPlugin • 0x2fe92c:$b: ClientPlugin • 0x2feb2e:$b: ClientPlugin • 0x2feb6e:$b: ClientPlugin • 0x279a33:$c: ProjectData • 0x2fea53:$c: ProjectData • 0x447ba0:$c: ProjectData • 0x27a43a:$d: DESCrypto • 0x2ff45a:$d: DESCrypto
Process Memory Space: aISbFyk4Lj.exe PID: 3288	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.aISbFyk4Lj.exe.484a9b8.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
0.2.aISbFyk4Lj.exe.484a9b8.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.aISbFyk4Lj.exe.484a9b8.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.aISbFyk4Lj.exe.484a9b8.2.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
0.2.aISbFyk4Lj.exe.484a9b8.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x951ad:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x951ea:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x98d1d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 2 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

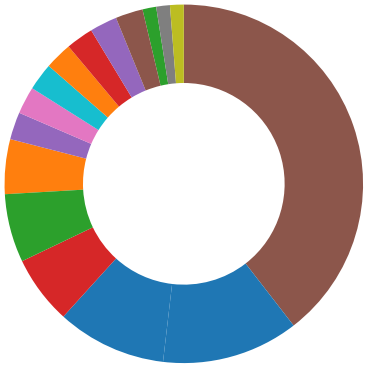
Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

- AV Detection
- Compliance
- Software Vulnerabilities
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

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

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

- Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

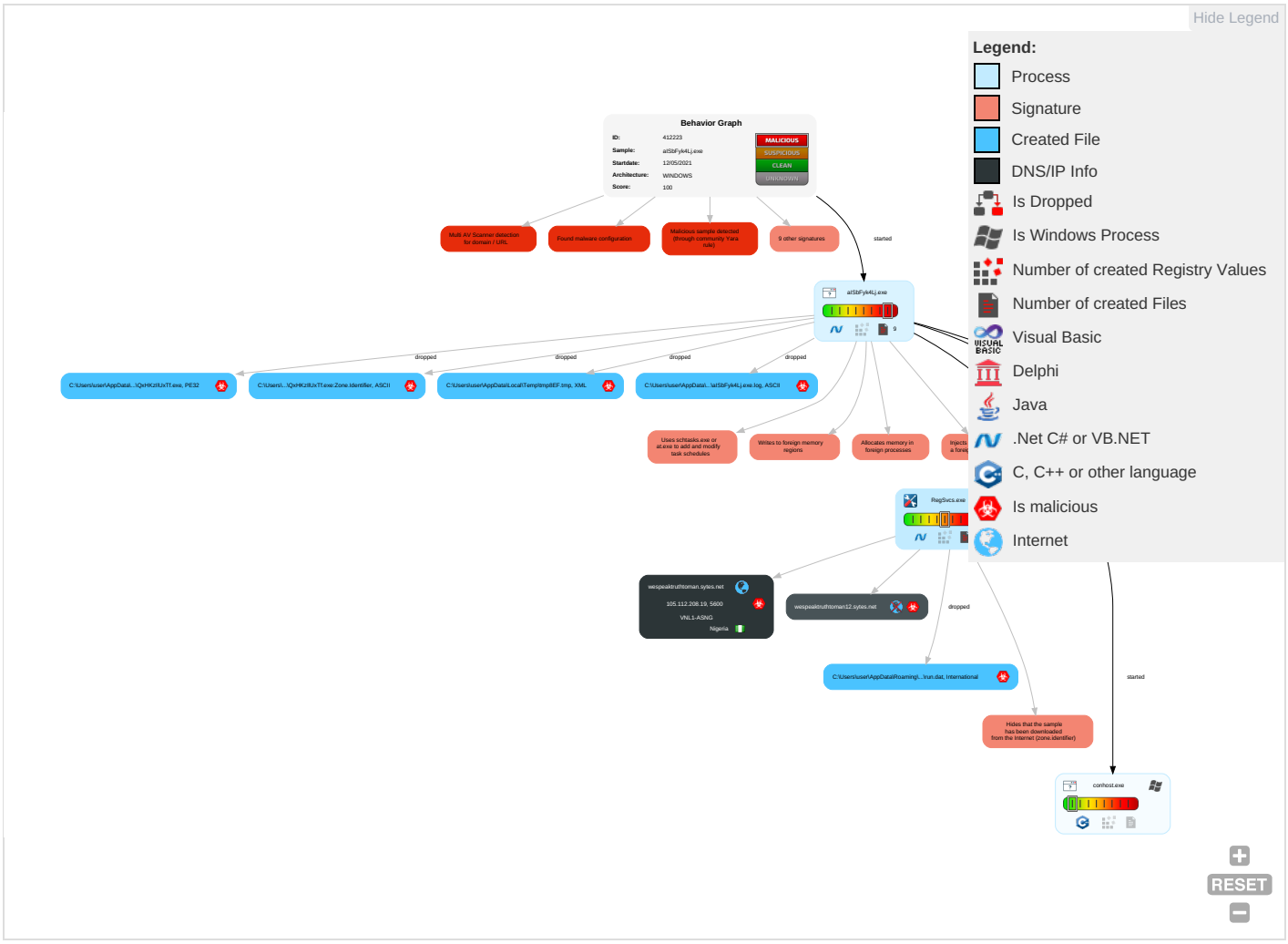
Remote Access Functionality:

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	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 Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window 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	Process Injection 3 1 2	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	System Information Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

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
aISbFyk4Lj.exe	24%	Virustotal		Browse
aISbFyk4Lj.exe	28%	ReversingLabs	Win32.Trojan.Wacatac	
aISbFyk4Lj.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\QxHKzIlUxTf.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\QxHKzIlUxTf.exe	28%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
wespeaktruthtoman.sytes.net	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://checkip.dyndns.org/	0%	Virustotal		Browse
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
wespeaktruthtoman.sytes.net	8%	Virustotal		Browse
wespeaktruthtoman.sytes.net	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/hits/hit_index.php?k=1	0%	Avira URL Cloud	safe	
wespeaktruthtoman12.sytes.net	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/E	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.html	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/report/reporter_index.php?name=	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.htmlk	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/downloads/	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/hits/hit_index.php?k=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wespeaktruthtoman.sytes.net	105.112.208.19	true	true	• 8%, Virustotal, Browse	unknown
wespeaktruthtoman12.sytes.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
wespeaktruthtoman.sytes.net	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown
wespeaktruthtoman12.sytes.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	aISbFyk4Lj.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/hits/hit_index.php?k=1	aISbFyk4Lj.exe	false	• Avira URL Cloud: safe	unknown
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC	aISbFyk4Lj.exe	false		high
http://servermanager.miixit.org/E	aISbFyk4Lj.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/index_ru.html	aISbFyk4Lj.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/report/reporter_index.php?name=	aISbFyk4Lj.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/	aISbFyk4Lj.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/index_ru.htmlk	aISbFyk4Lj.exe	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	aISbFyk4Lj.exe, 00000000.00000002.227476170.000000000362D000.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/downloads/	aISbFyk4Lj.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/hits/hit_index.php?k=	aISbFyk4Lj.exe	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
105.112.208.19	wespeaktruthtoman.sytes.net	Nigeria		36873	VNL1-ASNG	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412223
Start date:	12.05.2021
Start time:	14:09:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	aISbFyk4Lj.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:	17
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@8/5@15/1
EGA Information:	Failed

HDC Information:	Failed
HCA Information:	• Successful, ratio: 90% • 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. • Excluded IPs from analysis (whitelisted): 168.61.161.212, 52.147.198.201, 13.88.21.125, 184.30.20.56, 2.20.143.16, 2.20.142.209 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, fs.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcoleus16.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.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.

Simulations

Behavior and APIs

Time	Type	Description
14:10:00	API Interceptor	1x Sleep call for process: aISbFyk4Lj.exe modified
14:10:05	API Interceptor	967x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wespeaktruthtoman.sytes.net	cXyHZtgrFS.exe	Get hash	malicious	Browse	• 79.134.225.47
	13efMb6ayq.exe	Get hash	malicious	Browse	• 79.134.225.47
	s65eJyjKga.exe	Get hash	malicious	Browse	• 79.134.225.47
	new order.xlsx	Get hash	malicious	Browse	• 79.134.225.47
	Ot3srIM10B.exe	Get hash	malicious	Browse	• 79.134.225.47
	kwK4iGa9DL.exe	Get hash	malicious	Browse	• 79.134.225.47
	4z9Saf2vu3.exe	Get hash	malicious	Browse	• 79.134.225.47
	ORDER 4553241.xlsx	Get hash	malicious	Browse	• 105.112.101.86
	Pu5UMH4fWK.exe	Get hash	malicious	Browse	• 79.134.225.14

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNL1-ASNG	w85rzxid7y.exe	Get hash	malicious	Browse	• 105.112.102.199
	ORDER 4553241.xlsx	Get hash	malicious	Browse	• 105.112.101.86
	akclienttues.exe	Get hash	malicious	Browse	• 105.112.53.147
	Spec_PDF.vbs	Get hash	malicious	Browse	• 105.112.11.245
	6GCAm7DuOd.exe	Get hash	malicious	Browse	• 105.112.36.184
	Scan.Invoice0909206606.exe	Get hash	malicious	Browse	• 105.112.39.176
	kYXjS6Oc3S.exe	Get hash	malicious	Browse	• 105.112.99.190
	eK1KiJlz3l.exe	Get hash	malicious	Browse	• 105.112.99.190
	80tzo8FG3d.exe	Get hash	malicious	Browse	• 105.112.98.238
	Stub.exe	Get hash	malicious	Browse	• 105.112.78.3
	nyrXbOodFH.exe	Get hash	malicious	Browse	• 105.112.37.156
	3aDHivUqWtumbXb.exe	Get hash	malicious	Browse	• 105.112.99.199
	ld7EYHHTT6.exe	Get hash	malicious	Browse	• 105.112.148.62
	SecuriteInfo.com.Variant.Bulz.394792.29952.exe	Get hash	malicious	Browse	• 105.112.98.171
	SecuriteInfo.com.Trojan.PackedNET.578.18498.exe	Get hash	malicious	Browse	• 105.112.98.171
	yPLbA6JwCR.exe	Get hash	malicious	Browse	• 105.112.156.57
	m1UDslBq6j.exe	Get hash	malicious	Browse	• 105.112.107.123
	hjCQmeI243.exe	Get hash	malicious	Browse	• 105.112.36.173
	lxli7b5j6A.exe	Get hash	malicious	Browse	• 105.112.106.26
	Ircg423Akc.exe	Get hash	malicious	Browse	• 105.112.97.251

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\aISbFyk4Lj.exe.log

Process:	C:\Users\user\Desktop\aISbFyk4Lj.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	916
Entropy (8bit):	5.282390836641403
Encrypted:	false
SSDEEP:	24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2+:MwLLD2Y9h3go2rxxAcAO6ox+g2+
MD5:	5AD8E7ABEADADAC4CE06FF693476581A
SHA1:	81E42A97BBE3D7DE8B1E8B54C2B03C48594D761E
SHA-256:	BAA1A28262BA27D51C3A1FA7FB0811AD1128297ABB2EDCCC785DC52667D2A6FD
SHA-512:	7793E78E84AD36CE65B5B1C015364E340FB9110FAF199BC0234108CE9BCB1AEDACBD25C6A012AC99740E08BEA5E5C373A88E553E47016304D8AE6AEEAB58EEFF
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a9099237864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp8EF.tmp

Process:	C:\Users\user\Desktop\aISbFyk4Lj.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644

C:\Users\user\AppData\Local\Temp\tmp8EF.tmp	
Entropy (8bit):	5.1944478973860955
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBPtn:cbh47TlNQ//rydbz9I3YODOLNdq3n
MD5:	E38027EBC37002B1FE092464B6C50B95
SHA1:	69AA7795D3B11A6A00287E52B32922D8E709A90E
SHA-256:	1E9883662C67947499313FE57C066D600B86E342D05E38D3BBCA11D18057178B
SHA-512:	510EA110A11A2FCC43DEC5D7949AF1D521DE0E90312F9B85A2F599368670357D100D5F581E76B6345458E44DFA02094A3F9A604F755743199DBF63AFDBA5E1ED
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\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	International EBCDIC text, with NEL line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:KlN:KT
MD5:	E53DF14406EA51F6AD5310C94FEA9653
SHA1:	5BD800A65855F236146D932FBD4770D50E73F469
SHA-256:	5B4ECA88318B72851EFEE98C61006C852B7F468802C1D12D6B4FB0E611BEEA49
SHA-512:	BF9F3C5062392F727ACA1E3B1A277131F840AAAA6E398F16E6C8A717BA04D1B72296B92E9662EBAB399807BEF7C2A0F02024231BF306FDA4BA0D33F00A3BBD54
Malicious:	**true**
Reputation:	low
Preview:	..P...H

C:\Users\user\AppData\Roaming\QxHKzIlUxTf.exe	
Process:	C:\Users\user\Desktop\aISbFyk4Lj.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1476608
Entropy (8bit):	7.772479880770275
Encrypted:	false
SSDEEP:	24576:MvI4jwLI3Z/kneMTMoiKc4MUVLUFJ6VAsqbuQjrFQLIrH:MAa3Z/keMs5UUwWsqb/jr5
MD5:	167F0A829DF709CC4107369ED23FBDFB
SHA1:	A66CAACF3BD0390912AB789B7E773E805172BA4C
SHA-256:	12279E26650D5826758AE344BC6FFEF54A438D4782A42F0D369403AE41F3914B
SHA-512:	BFE66CD5BE80F3912041B504BF20A05EFE510C7ABB3CB653E03E1F25F5CF193BA5338A007A688C718A6AE97F51886C020ABB853A39A020DA7C880AA81C4C7E23
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....~.... .....@.. ..... ..@.....,...O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....`.....H.....pr.....X.....0.....(....(.....(.....o ....*.....(!.....("....(#.....($.....(%....*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\QxHKzIlUxTf.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\aISbFyk4Lj.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

C:\Users\user\AppData\Roaming\QxHKzIlUxTf.exe:Zone.Identifier	
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):	7.772479880770275
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:	aISbFyk4Lj.exe
File size:	1476608
MD5:	167f0a829df709cc4107369ed23fbdfb
SHA1:	a66caacf3bd0390912ab789b7e773e805172ba4c
SHA256:	12279e26650d5826758ae344bc6ffef54a438d4782a42f0d369403ae41f3914b
SHA512:	bfe66cd5be80f3912041b504bf20a05efe510c7abb3cb653e03e1f25f5cf193ba5338a007a688c718a6ae97f51886c020abb853a39a020da7c880aa81c4c7e23
SSDEEP:	24576:MvI4jwLI3Z/kneMTMoiKc4MUVLUFJ6VAsqbuQjrFQLIrH:MAa3Z/keMs5UUwWsqb/jr5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....~.... .....@.. .....@.....

File Icon

Icon Hash:	cc92316d713396e8

Static PE Info

General

Entrypoint:	0x54f67e
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:	0x609BBDAF [Wed May 12 11:36:15 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x14f62c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x150000	0x1abb0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x16c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x14f4f4	0x1c	.text
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	0x14d684	0x14d800	False	0.937049053598	data	7.93424696113	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x150000	0x1abb0	0x1ac00	False	0.146274459696	data	3.15106465863	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x16c000	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	0x150250	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1506b8	0x162a	PNG image data, 256 x 256, 8-bit colormap, non-interlaced		
RT_ICON	0x151ce4	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x15428c	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x155334	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x165b5c	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	0x169d84	0x5a	data		
RT_GROUP_ICON	0x169de0	0x14	data		
RT_VERSION	0x169df4	0x354	data		
RT_MANIFEST	0x16a148	0xa65	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

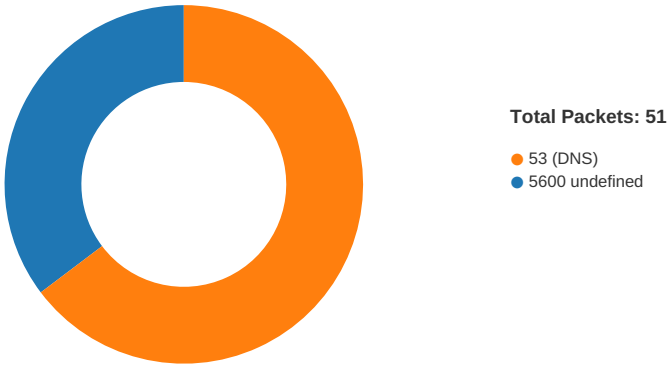
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2013
Assembly Version	3.0.0.0
InternalName	getClaimsd95.exe
FileVersion	3.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ServerManager_Core
ProductVersion	3.0.0.0
FileDescription	ServerManager_Core
OriginalFilename	getClaimsd95.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 14:10:07.926372051 CEST	49694	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:10:10.927815914 CEST	49694	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:10:16.928287029 CEST	49694	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:10:27.812267065 CEST	49705	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:10:30.820108891 CEST	49705	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:10:36.867598057 CEST	49705	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:10:47.904078007 CEST	49706	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:10:50.899920940 CEST	49706	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:10:57.072427034 CEST	49706	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:11:22.187241077 CEST	49708	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:11:25.199759007 CEST	49708	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:11:31.200397968 CEST	49708	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:11:40.734610081 CEST	49709	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:11:43.748296976 CEST	49709	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:11:49.764352083 CEST	49709	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:11:57.417399883 CEST	49710	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:12:00.421408892 CEST	49710	5600	192.168.2.3	105.112.208.19
May 12, 2021 14:12:06.422015905 CEST	49710	5600	192.168.2.3	105.112.208.19

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 14:09:52.197921038 CEST	56961	53	192.168.2.3	8.8.8.8
May 12, 2021 14:09:52.249525070 CEST	53	56961	8.8.8.8	192.168.2.3
May 12, 2021 14:09:53.094300985 CEST	59353	53	192.168.2.3	8.8.8.8
May 12, 2021 14:09:53.151433945 CEST	53	59353	8.8.8.8	192.168.2.3
May 12, 2021 14:09:54.402956009 CEST	52238	53	192.168.2.3	8.8.8.8
May 12, 2021 14:09:54.454456091 CEST	53	52238	8.8.8.8	192.168.2.3
May 12, 2021 14:09:55.308458090 CEST	49873	53	192.168.2.3	8.8.8.8
May 12, 2021 14:09:55.362652063 CEST	53	49873	8.8.8.8	192.168.2.3
May 12, 2021 14:10:01.325623035 CEST	53196	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:01.377830982 CEST	53	53196	8.8.8.8	192.168.2.3
May 12, 2021 14:10:02.353259087 CEST	56777	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:02.402128935 CEST	53	56777	8.8.8.8	192.168.2.3
May 12, 2021 14:10:04.487103939 CEST	58643	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:04.538048983 CEST	53	58643	8.8.8.8	192.168.2.3
May 12, 2021 14:10:05.972115040 CEST	60985	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:06.020780087 CEST	53	60985	8.8.8.8	192.168.2.3
May 12, 2021 14:10:06.890644073 CEST	50200	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:06.939263105 CEST	53	50200	8.8.8.8	192.168.2.3
May 12, 2021 14:10:07.797035933 CEST	51281	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:07.856506109 CEST	53	51281	8.8.8.8	192.168.2.3
May 12, 2021 14:10:08.141349077 CEST	49199	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:08.191653967 CEST	53	49199	8.8.8.8	192.168.2.3
May 12, 2021 14:10:08.925841093 CEST	50620	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:08.977776051 CEST	53	50620	8.8.8.8	192.168.2.3
May 12, 2021 14:10:09.719042063 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:09.769270897 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 14:10:10.492587090 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:10.541302919 CEST	53	60152	8.8.8.8	192.168.2.3
May 12, 2021 14:10:11.335540056 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:11.395431995 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 14:10:12.158965111 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:12.220136881 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 14:10:13.261647940 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:13.311885118 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 14:10:22.907243967 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:22.969291925 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 14:10:27.748070955 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:27.810220003 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 14:10:47.850631952 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 14:10:47.862081051 CEST	60831	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 14:10:47.902456999 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 14:10:47.922029972 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 14:11:07.928497076 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 14:11:07.985506058 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 14:11:08.167423010 CEST	53195	53	192.168.2.3	8.8.4.4
May 12, 2021 14:11:08.228714943 CEST	53	53195	8.8.4.4	192.168.2.3
May 12, 2021 14:11:08.287180901 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 14:11:08.348562002 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 14:11:12.555984974 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 14:11:12.613117933 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 14:11:13.215193987 CEST	49563	53	192.168.2.3	8.8.4.4
May 12, 2021 14:11:13.272510052 CEST	53	49563	8.8.4.4	192.168.2.3
May 12, 2021 14:11:13.365533113 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 14:11:13.422804117 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 14:11:17.661933899 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 14:11:17.719084978 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 14:11:17.753895044 CEST	57084	53	192.168.2.3	8.8.4.4
May 12, 2021 14:11:17.815638065 CEST	53	57084	8.8.4.4	192.168.2.3
May 12, 2021 14:11:17.981719017 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 14:11:18.042107105 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 14:11:22.121907949 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 14:11:22.185769081 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 14:11:40.674099922 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 14:11:40.733225107 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 14:11:57.362112999 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 14:11:57.415962934 CEST	53	54366	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 14:10:07.797035933 CEST	192.168.2.3	8.8.8.8	0xee82	Standard query (0)	wespeaktru thtoman.sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:10:27.748070955 CEST	192.168.2.3	8.8.8.8	0x9d3c	Standard query (0)	wespeaktru thtoman.sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:10:47.850631952 CEST	192.168.2.3	8.8.8.8	0xb13b	Standard query (0)	wespeaktru thtoman.sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:11:07.928497076 CEST	192.168.2.3	8.8.8.8	0x187e	Standard query (0)	wespeaktru thtoman12. sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:11:08.167423010 CEST	192.168.2.3	8.8.4.4	0x7021	Standard query (0)	wespeaktru thtoman12. sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:11:08.287180901 CEST	192.168.2.3	8.8.8.8	0x8e6a	Standard query (0)	wespeaktru thtoman12. sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:11:12.555984974 CEST	192.168.2.3	8.8.8.8	0xd0ae	Standard query (0)	wespeaktru thtoman12. sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:11:13.215193987 CEST	192.168.2.3	8.8.4.4	0x4bf6	Standard query (0)	wespeaktru thtoman12. sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:11:13.365533113 CEST	192.168.2.3	8.8.8.8	0x757b	Standard query (0)	wespeaktru thtoman12. sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:11:17.661933899 CEST	192.168.2.3	8.8.8.8	0xca1a	Standard query (0)	wespeaktru thtoman12. sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:11:17.753895044 CEST	192.168.2.3	8.8.4.4	0xa13f	Standard query (0)	wespeaktru thtoman12. sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:11:17.981719017 CEST	192.168.2.3	8.8.8.8	0xa420	Standard query (0)	wespeaktru thtoman12. sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:11:22.121907949 CEST	192.168.2.3	8.8.8.8	0x6731	Standard query (0)	wespeaktru thtoman.sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:11:40.674099922 CEST	192.168.2.3	8.8.8.8	0x3e28	Standard query (0)	wespeaktru thtoman.sytes.net	A (IP address)	IN (0x0001)
May 12, 2021 14:11:57.362112999 CEST	192.168.2.3	8.8.8.8	0x4eb1	Standard query (0)	wespeaktru thtoman.sytes.net	A (IP address)	IN (0x0001)

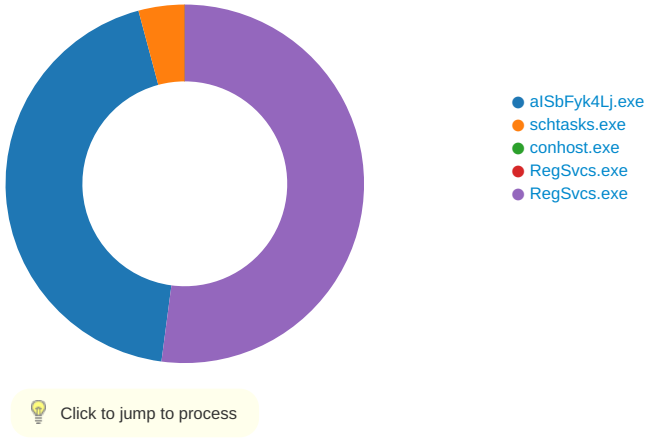
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 14:10:07.856506109 CEST	8.8.8.8	192.168.2.3	0xee82	No error (0)	wespeaktruthtoman.systes.net		105.112.208.19	A (IP address)	IN (0x0001)
May 12, 2021 14:10:27.810220003 CEST	8.8.8.8	192.168.2.3	0x9d3c	No error (0)	wespeaktruthtoman.systes.net		105.112.208.19	A (IP address)	IN (0x0001)
May 12, 2021 14:10:47.902456999 CEST	8.8.8.8	192.168.2.3	0xb13b	No error (0)	wespeaktruthtoman.systes.net		105.112.208.19	A (IP address)	IN (0x0001)
May 12, 2021 14:11:22.185769081 CEST	8.8.8.8	192.168.2.3	0x6731	No error (0)	wespeaktruthtoman.systes.net		105.112.208.19	A (IP address)	IN (0x0001)
May 12, 2021 14:11:40.733225107 CEST	8.8.8.8	192.168.2.3	0x3e28	No error (0)	wespeaktruthtoman.systes.net		105.112.208.19	A (IP address)	IN (0x0001)
May 12, 2021 14:11:57.415962934 CEST	8.8.8.8	192.168.2.3	0x4eb1	No error (0)	wespeaktruthtoman.systes.net		105.112.208.19	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: aISbFyk4Lj.exe PID: 3288 Parent PID: 5492

General

Start time:	14:09:59
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\aISbFyk4Lj.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\aISbFyk4Lj.exe'
Imagebase:	0xec0000
File size:	1476608 bytes
MD5 hash:	167F0A829DF709CC4107369ED23FBDFB
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: 00000000.00000002.227476170.000000000362D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.227998353.00000000045E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.227998353.00000000045E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.227998353.00000000045E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\QxHKzlIUxTf.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	59706E8	CopyFileW
C:\Users\user\AppData\Roaming\QxHKzlIUxTf.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	59706E8	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8EF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5970F2C	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\aISbFyk4Lj.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8EF.tmp	success or wait	1	5971242	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QxHKzIlUxTf.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 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 af bd 9b 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 d8 14 00 00 ae 01 00 00 00 00 00 7e f6 14 00 00 20 00 00 00 00 15 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 e0 16 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......`.......... ....P............~.... ....@.. ....@................	success or wait	6	59706E8	CopyFileW
C:\Users\user\AppData\Roaming\QxHKzIlUxTf.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	59706E8	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8EF.tmp	unknown	1644	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 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	18FBBDB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\aISbFyk4Lj.exe.log	unknown	916	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e 65	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	18FBBDB	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	18FBBDB	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	18FBBDB	ReadFile

Analysis Process: schtasks.exe PID: 2200 Parent PID: 3288

General

Start time:	14:10:02
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\QxHKzIlUxTf' /XML 'C:\Users\user\AppData\Local\Temp\tmp8EF.tmp'
Imagebase:	0xc70000
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\tmp8EF.tmp	unknown	2	success or wait	1	C7AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8EF.tmp	unknown	1645	success or wait	1	C7ABD9	ReadFile

Analysis Process: conhost.exe PID: 5232 Parent PID: 2200

General

Start time:	14:10:02
Start date:	12/05/2021
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: RegSvcs.exe PID: 1724 Parent PID: 3288

General

Start time:	14:10:03
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0x1e0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegSvcs.exe PID: 5884 Parent PID: 3288

General

Start time:	14:10:03
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0x4d0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4D107A1	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	4D1089B	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	4D107A1	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	4D107A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File 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	ed 92 c0 50 8a 15 d9 48	...P...H	success or wait	1	4D10A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4D10A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	4D10A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	4D10A53	ReadFile

Disassembly

Code Analysis