ID: 358594
Sample Name: jvHSccqW.exe
Cookbook: default.jbs
Time: 22:03:17
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

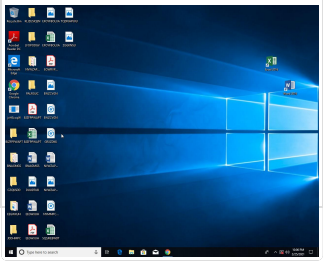
Analysis Report jvHSccqW.exe

Overview

General Information

Sample Name:	jvHSccqW.exe
Analysis ID:	358594
MD5:	efeff4b4242776d…
SHA1:	557fa8532f5340e..
SHA256:	2399e5acd8e6fec..
Tags:	AsyncRAT exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

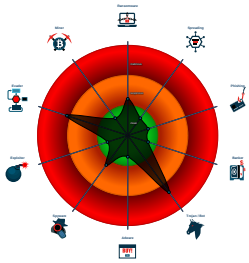
AsyncRAT

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Yara detected AsyncRAT
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- AV process strings found (often use…
- Antivirus or Machine Learning detec…
- Checks if Antivirus/Antispyware/Fire…
- Contains long sleeps (>= 3 min)
- Detected TCP or UDP traffic on non…
- Detected potential crypto function

Classification



Startup

- **System is w10x64**
- jvHSccqW.exe (PID: 6356 cmdline: 'C:\Users\user\Desktop\jvHSccqW.exe' MD5: EFEFF4B4242776D6576B0FB18F35D52C)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT


```
{
  "Server": "newss.myq-see.com",
  "Ports": "1177",
  "Version": "0.5.7B",
  "Autorun": "false",
  "Install_Folder": "%AppData%",
  "Install_File": "",
  "AES_key": "HMaZiL8g7SjFAvgHIXWZdtT729qvTY9R",
  "Mutex": "AsyncMutex_6SI8OkPnk",
  "AntiDetection": "false",
  "External_config_on_Pastebin": "null",
  "BDOS": "false",
  "Startup_Delay": "3",
  "HWID": "null",
  "Certificate":
"MIIE3DCCAsSgAwIBAgIQAMDC8f2wXucoHHZWb62H+zANBgkqhkiG9w0BAQ0FADAPMQ0wCwYDVQQDDARmdWtlMCAXDTIxMDEwMzAwMDk1MFoYDzk5OTkxMjMxMjM1OTU5WjAPMQ0wCwYDVQQDDARmdWtlMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEApN6Lx96xgRB2ew7bmjJo+AirgsTz5e47pySUi2lxHrb6HydPSeIMWx1FkowQbDiu9waY3LN+b3HZT0XWf8Ls6khK0RvqPdBU4PA3x5AygSP6UVox2pzxMuIEDWD5qabMZtf3Wf+yZXI6D4uYNBtc2vC3jiYLfzE24U0JCRWMB5rP8gbfWqna2o1d8gY+Q0HJw1p4xkq6k3y7rBRr5tdNdGzkP6Dn3o+YLaCr4O6sVeMC+MNbcAFNHEc7K+5txH/1YgnJ9l32wIHxTVjBsaeyf7P6zYbVhYvGkGWbQIdF3f5e1tys1NK4taEzVuHnCzdSCH+Ho0L8mVIHjqtAiqvskZxCplT0eh94b50iDmevZgdkFMN0wPloUdUrfHobL9y637Ni5Et8Jgmouw6GG3DUO3pOOCI88SsjnmLnKJauj1dYCp35FI4WdTLov1cv+gtdHxJqG8TroCjJ+p2aQ/AmsHaZbRGShu2V7eHti/JPvWuhaGm+wD8zo9pf+czwVEvv7T21haZlWMtNxiS3UUaTQkfmI10V37sOXEXbcpaEVAchD3QcL8DvpuTApmYL/nhnHPlA6ln21ty0sn2rvoTr4yUCfS0jjZNGK3rN3Z/YJkEZQ5myJ/4ONFxhQhgRx+0LC7TH0jLL9x6UexjZNdN51dhOU6vxfYFFVKW9cnKGZ0kCAwEAAaMyMDAwHQYDVR0OBBYEFGwlNXg0Bwn+JqaeWIOfs0fXpFeIMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQENBQADggIBAEQItDXUfGw7/MGuEqw8skKgfI58JL5L/oJsvST3FeFD1JzIa9X4wIzhbXT3OqGsDn5AfJZ0I+cmmz6hSkbLbEaF3aN3vsXGSLaatftjB6Ek2JgGEHBeVxKKwJuNtfK83kpanZ4TKvMnLhqUTmEMMl2k8SIN8pO3MrYTHmzOVIJtYpEyXOnUH6PftjM4atDTrlS05jlgpPFXUhm9GSqcTcCjTNihXZdU+rMc9ruoSyd5AdsuJaeM0yKQNGw/p6p+2RpMEUqgVRz1XW61NOPQSubAwZJqHgoy0pthfsCNxu0s/0SfwvCoqWzcFsoQs/eX4KALk8ThrTfP+PW3nNuXjLymGGkww1Env/xCF4h3wqa4IKkyBYpatMEhqyyXPtuhQmDuk2lXbGrJQwDydFMm9nBbUB1FO/7vBege8cZvVJ+y2/6TYkimJZ/WMTSrcbHD5FgT9QbvfXO1vitvDxcSwhT1cfgIQwT40CgzpdswCkWsP6/CA8RLKZcerJEIW1c/Y0dCaT4dpPetC0lXmIBFU5eCD0FlOtBAigoHVqWBkIlE8morqQedXgPe9gXH6AWVxExDjqITOrDweETVpVvFY8q7TB7XhZPcEHvJFH0/3D9nBwObkxjv5HZx1kYCilHAkCbAU714DIN0nKdgY6km9Ntpp52wqrtbeY2V9YQ9w5Dk",
  "ServerSignature":
"MTAsavgxOutIMsaUSguW3Z+vRa7Czv4HK1F4b5ydoIcOoRYF06jsDGYbw2TAG4BXSn2zVnQhvNK4tFeH5qvxVSiGY2dIfW4h4BOb5+fbWBQ5WikeA72thrnmb/lJVQKnbs/jQSxZXrdIbD9i74whKkiA1VBJin26yQuvSa1s6d+x9I3DLsrylv5yW3LPtHu+TOjAyWJSIadsk1O1vkpN9aWpf6BQeNLbtzSD6btb7Y5X+rHoCyROyasfR8tW/dYlsBtk98dCjKaAERKdh71Vw7ekm7Jj4S+dbaeQtuCUIDevWuA+QcqcuP+WaWEgrCMhAoEoqj65M/sIymI0dvxYk15N72icZIsyFCCUuDDqdpF+ykOxyieGYTcZeU6/0toOS4zRGRwFQ4Y5bQPzODNlkdLdLZPEvOgH8hgUY/AyhWrx4Ok8r2acKwM6t2xhgQR6PCrNWHDHrzdjUqrTFmsn9C7asP0+lzrB/VDe9CVnWm0MN5pNAYS3IEGYZAmKU/3H3YIiLWoEb3UMyJckPoR8AlPmLhdkrGCu50K+Jp0b1GwLlF5cItQGrxsUXQeZdGEswNU1Q5SrGI45La3/IjsI/ODQbQEI+lu64ZFUj3HsqMN1TCAlNgKd44R6t1Cuf/rYkUaHdRVIufxMUqiuX6YcgxHpBENYgi4aylBXTuPBCkw=",
  "Group": "Default"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
jvHSccqW.exe	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.219246907.0000000000FE2000.00000002.00020000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000000.00000002.484166821.0000000000FE2000.00000002.00020000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Process Memory Space: jvHSccqW.exe PID: 6356	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

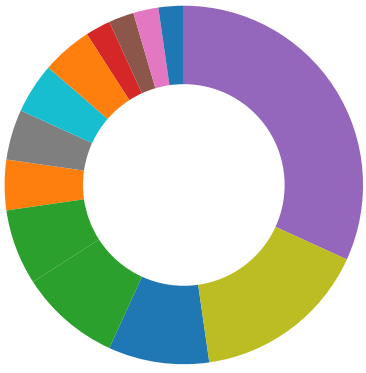
Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.jvHSccqW.exe.fe0000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.2.jvHSccqW.exe.fe0000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- 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

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

Boot Survival:

Yara detected AsyncRAT

Malware Analysis System Evasion:

Yara detected AsyncRAT

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

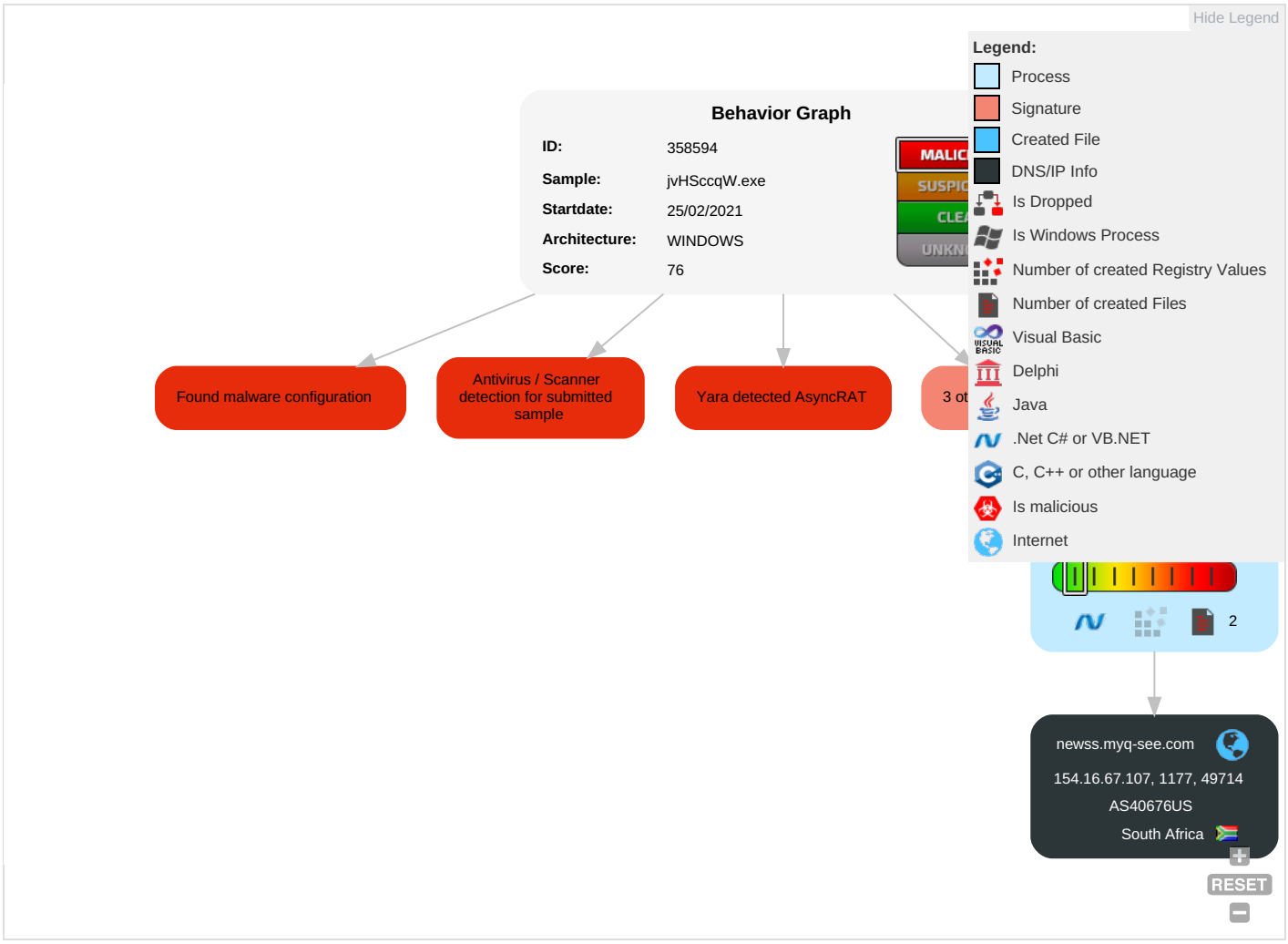
Lowering of HIPS / PFW / Operating System Security Settings:

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	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1	Virtualization/Sandbox Evasion 2	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop c Insecure Network Communica
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 2 1	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)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Virtualization/Sandbox Evasion 2	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)	Obfuscated Files or Information 1 1 1	NTDS	Process 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	Software Packing 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System 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	Compile After Delivery	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir

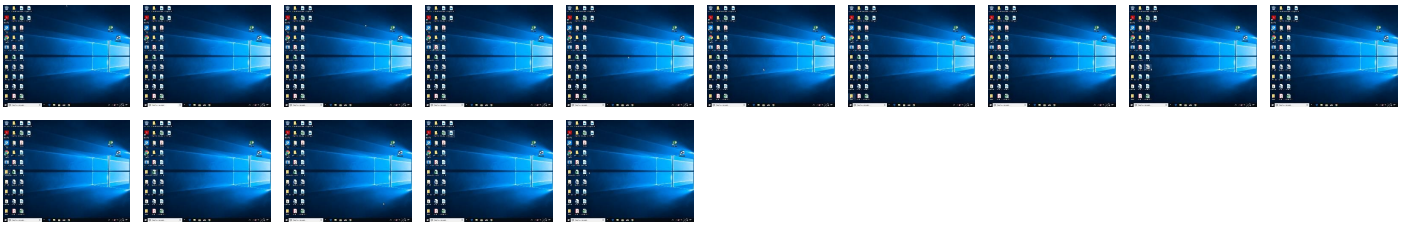
Behavior Graph



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
jvHSccqW.exe	100%	Avira	TR/Dropper.Gen	
jvHSccqW.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.jvHSccqW.exe.fe0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.jvHSccqW.exe.fe0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ctldl.windows	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
newss.myq-see.com	154.16.67.107	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
newss.myq-see.com	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ctldl.windows	jvHSccqW.exe, 00000000.00000003.295949209.000000000582F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	jvHSccqW.exe, 00000000.00000002.485611389.0000000003351000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.16.67.107	unknown	South Africa		40676	AS40676US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald

Analysis ID:	358594
Start date:	25.02.2021
Start time:	22:03:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	jvHSccqW.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:	24
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:	mal76.troj.evad.winEXE@1/2@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.7% (good quality ratio 0.3%) • Quality average: 16.8% • Quality standard deviation: 22.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 51.103.5.159, 204.79.197.200, 13.107.21.200, 40.88.32.150, 51.11.168.160, 93.184.220.29, 13.64.90.137, 23.54.113.53, 52.255.188.83, 52.147.198.201, 67.26.73.254, 67.27.158.126, 8.253.95.249, 8.248.147.254, 8.253.207.121, 184.30.20.56, 20.54.26.129, 2.20.142.210, 2.20.142.209, 92.122.213.194, 92.122.213.247, 51.104.144.132 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, cs9.wac.phicdn.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.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, au-bg-shim.trafficmanager.net, www.bing.com, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net • 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/358594/sample/jvHSccqW.exe

Simulations

Behavior and APIs

Time	Type	Description
22:04:11	API Interceptor	2x Sleep call for process: jvHSccqW.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS40676US	N5eld3tiba.exe	Get hash	malicious	Browse	• 172.107.43.174
	shed.exe	Get hash	malicious	Browse	• 172.106.24 2.148
	urgent specification request.exe	Get hash	malicious	Browse	• 23.228.252.187
	SecuriteInfo.com.Trojan.GenericKD.45746214.12120.exe	Get hash	malicious	Browse	• 45.61.139.76
	SecuriteInfo.com.BehavesLike.Win32.Generic.dc.exe	Get hash	malicious	Browse	• 45.61.139.76
	NF54.vbs	Get hash	malicious	Browse	• 88.214.59.150
	XE54.vbs	Get hash	malicious	Browse	• 88.214.59.150
	PA71.vbs	Get hash	malicious	Browse	• 88.214.59.150
	WI57.vbs	Get hash	malicious	Browse	• 88.214.59.150
	QD63.vbs	Get hash	malicious	Browse	• 88.214.59.150
	MV55.vbs	Get hash	malicious	Browse	• 88.214.59.150
	HL66.vbs	Get hash	malicious	Browse	• 88.214.59.150
	zSDBuG8gDl.exe	Get hash	malicious	Browse	• 185.229.243.67
	03728d6617cd13b19bd69625f7ead202.exe	Get hash	malicious	Browse	• 185.229.243.67
	AANK5mcsUZ.exe	Get hash	malicious	Browse	• 104.217.200.38
	mh47fywu0o.exe	Get hash	malicious	Browse	• 104.217.14 1.196
	P020433098747993990.PDF.exe	Get hash	malicious	Browse	• 185.162.88.26
	sample catalog_copy.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	210127.exe	Get hash	malicious	Browse	• 172.107.55.21
	DHL-#AWB130501923096PDF.exe	Get hash	malicious	Browse	• 185.162.88.26

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\jvHSccqW.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5 X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/I\.cDB0.'.Y...r.[.....vM...o.=....zK..r.. I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\jvHSccqW.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.084754685484954

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Encrypted:	false
SSDEEP:	6:kK5bqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:43kPlE99SNxAhUeo+aKt
MD5:	246BEC775D58E976C2E5A9367B1E0B71
SHA1:	1D3EFCA090254B07E9E8407257D9E6DCCCED7755
SHA-256:	65397B6692B8A7BB9E00260AD65276CDE902A51E2D06DA53828E4AA091BA67C9
SHA-512:	7AC1DE3B3C3DAB30925631439ABD5D5888705EDA5FC9E8BA590C93CDB08AC1D6FBD87D114FE009E35B89A9AA12F3B054DCE19EEE02309E1CCEC9FA8771D6C39
Malicious:	false
Reputation:	low
Preview:	p..... .....@B.3....(..... .....&.....h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.444852828545967
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	jvHSccqW.exe
File size:	46080
MD5:	efeff4b4242776d6576b0fb18f35d52c
SHA1:	557fa8532f5340ee628df64cb9a199ef935f1dc5
SHA256:	2399e5acd8e6fec2e83de445cf83b598676f57fdfedd1f67a7872a5009866591
SHA512:	ba28499ff3baf5fc56d4b77342095122a0c4dfabee6d639fa5f6f474ad0415f7a6de2668c5a41dea7faa1eb8835d7e81b01dd1a892db6619a8a6a3d4892459b7
SSDEEP:	768:4uwHvTpY8oiWUUGyKmo2q8zKjGKG6PlyzjbFgX3ioP6mfoZXBDZyx:4uwHvTpTf23KYDy3bCXSQf4dyx
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...#..^..... .....@.. .... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40c6ee
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:	0x5EB79023 [Sun May 10 05:24:51 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0

General

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc694	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe000	0x7ff	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x10000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa6f4	0xa800	False	0.499465215774	data	5.4994123035	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe000	0x7ff	0x800	False	0.41748046875	data	4.88506844918	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe0a0	0x2cc	data		
RT_MANIFEST	0xe36c	0x493	exported SGML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

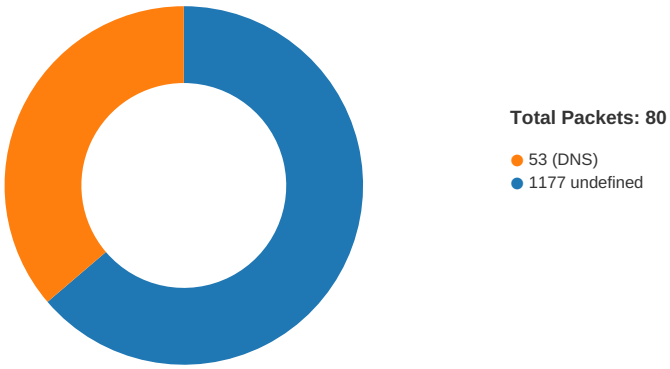
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:04:10.320004940 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:10.482769012 CET	1177	49714	154.16.67.107	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:04:10.482872009 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:10.527359009 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:10.702203989 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:10.702227116 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:10.702370882 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:10.706372023 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:10.870584011 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:10.971750021 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:12.691809893 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:12.910052061 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:12.910321951 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:13.128930092 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:26.430538893 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:26.654350996 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:26.654511929 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:26.825553894 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:26.973553896 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:27.144078016 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:27.215955019 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:27.451097965 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:27.451172113 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:27.685641050 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:40.216777086 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:40.451437950 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:40.451858997 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:40.623414040 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:40.818084002 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:40.989783049 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:41.012784958 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:41.248166084 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:41.248289108 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:41.482537985 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:53.941447973 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:54.170099020 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:54.172399998 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:54.346194983 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:54.397264957 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:54.568160057 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:54.598596096 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:54.826316118 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:54.826509953 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:55.060729980 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:57.112668037 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:57.163088083 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:04:57.333658934 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:04:57.381860971 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:07.718311071 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:07.951443911 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:07.951662064 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:08.123596907 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:08.179764986 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:08.351942062 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:08.375176907 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:08.611773968 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:08.611918926 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:08.843782902 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:21.453201056 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:21.685910940 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:21.686032057 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:21.859544992 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:21.899708033 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:22.070270061 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:22.089847088 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:22.311014891 CET	1177	49714	154.16.67.107	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:05:22.311285973 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:22.545649052 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:27.113698006 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:27.165659904 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:27.336261034 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:27.384622097 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:35.183702946 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:35.404809952 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:35.404905081 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:35.576008081 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:35.619482040 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:35.790024042 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:35.815161943 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:36.045651913 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:36.045840025 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:36.280075073 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:48.929539919 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:49.155081987 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:49.155215025 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:49.328382969 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:49.386205912 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:49.556647062 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:49.579850912 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:49.811225891 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:49.811405897 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:50.045640945 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:57.115108013 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:57.168124914 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:05:57.338890076 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:05:57.386899948 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:06:02.681866884 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:06:02.905075073 CET	1177	49714	154.16.67.107	192.168.2.5
Feb 25, 2021 22:06:02.905217886 CET	49714	1177	192.168.2.5	154.16.67.107
Feb 25, 2021 22:06:03.077801943 CET	1177	49714	154.16.67.107	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:03:56.743313074 CET	52212	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:03:56.809534073 CET	53	52212	8.8.8.8	192.168.2.5
Feb 25, 2021 22:03:57.711662054 CET	54302	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:03:57.726392984 CET	53784	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:03:57.760504007 CET	53	54302	8.8.8.8	192.168.2.5
Feb 25, 2021 22:03:57.775048018 CET	53	53784	8.8.8.8	192.168.2.5
Feb 25, 2021 22:03:57.817925930 CET	65307	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:03:57.821000099 CET	64344	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:03:57.869700909 CET	53	65307	8.8.8.8	192.168.2.5
Feb 25, 2021 22:03:57.871443033 CET	53	64344	8.8.8.8	192.168.2.5
Feb 25, 2021 22:03:57.901843071 CET	62060	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:03:57.906250954 CET	61805	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:03:57.950452089 CET	53	62060	8.8.8.8	192.168.2.5
Feb 25, 2021 22:03:57.954894066 CET	53	61805	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:00.116924047 CET	54795	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:00.179063082 CET	53	54795	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:00.717344046 CET	49557	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:00.776315928 CET	53	49557	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:01.398634911 CET	61733	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:01.455738068 CET	53	61733	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:02.309930086 CET	65447	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:02.369333982 CET	53	65447	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:03.224991083 CET	52441	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:03.276603937 CET	53	52441	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:04.140477896 CET	62176	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:04.188950062 CET	53	62176	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:04:05.006977081 CET	59596	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:05.056700945 CET	53	59596	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:05.870940924 CET	65296	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:05.919836998 CET	53	65296	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:06.792341948 CET	63183	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:06.886455059 CET	53	63183	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:08.029510021 CET	60151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:08.078099966 CET	53	60151	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:10.038857937 CET	56969	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:10.313076019 CET	53	56969	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:11.277034998 CET	55161	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:11.325793028 CET	53	55161	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:13.076601028 CET	54757	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:13.125665903 CET	53	54757	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:25.570389032 CET	49992	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:25.621350050 CET	53	49992	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:34.125613928 CET	60075	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:34.174144030 CET	53	60075	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:52.387094975 CET	55016	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:52.444765091 CET	53	55016	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:52.757637978 CET	64345	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:52.809149027 CET	53	64345	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:53.096856117 CET	57128	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:53.158231020 CET	53	57128	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:58.394128084 CET	54791	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:58.447798014 CET	53	54791	8.8.8.8	192.168.2.5
Feb 25, 2021 22:04:59.853595972 CET	50463	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:04:59.902231932 CET	53	50463	8.8.8.8	192.168.2.5
Feb 25, 2021 22:05:00.350521088 CET	50394	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:05:00.408370972 CET	53	50394	8.8.8.8	192.168.2.5
Feb 25, 2021 22:05:31.741476059 CET	58530	53	192.168.2.5	8.8.8.8
Feb 25, 2021 22:05:31.792717934 CET	53	58530	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 22:04:10.038857937 CET	192.168.2.5	8.8.8.8	0xdefc	Standard query (0)	newss.myq-see.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 22:04:10.313076019 CET	8.8.8.8	192.168.2.5	0xdefc	No error (0)	newss.myq-see.com		154.16.67.107	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: jvHSccqW.exe PID: 6356 Parent PID: 5704

General

Start time:	22:04:04
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\jvHSccqW.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\jvHSccqW.exe'
Imagebase:	0xfe0000
File size:	46080 bytes
MD5 hash:	EFEFF4B4242776D6576B0FB18F35D52C
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: 00000000.00000000.219246907.0000000000FE2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000002.484166821.0000000000FE2000.00000002.00020000.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	6DABCF06	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	6DABCF06	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile

Disassembly

Code Analysis