ID: 778238
Sample Name: Stub.exe
Cookbook: default.jbs
Time: 09:15:14
Date: 05/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

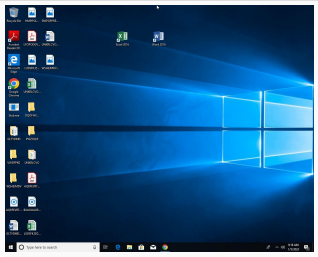
Windows Analysis Report

Stub.exe

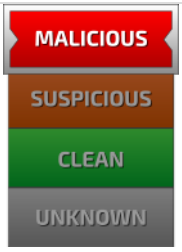
Overview

General Information

Sample Name:	Stub.exe
Analysis ID:	778238
MD5:	da5c4dbbc80ca5..
SHA1:	c6689884e4bf33..
SHA256:	4981bda443713f..
Tags:	AsyncRAT exe
Infos:	



Detection



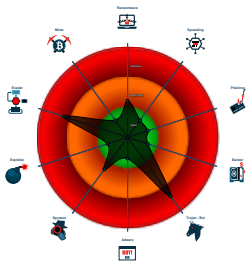
AsyncRAT

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Malicious sample detected (through…
- Yara detected AsyncRAT
- Snort IDS alert for network traffic
- Yara detected Generic Downloader
- C2 URLs / IPs found in malware con…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Uses 32bit PE files
- Found a high number of Window / U…
- AV process strings found (often use…

Classification



Process Tree

- **System is w10x64**
- Stub.exe (PID: 5484 cmdline: C:\Users\user\Desktop\Stub.exe MD5: DA5C4DBBC80CA5DA70237EF8BC281476)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT

```
{
  "Server": "egrh.linkpc.net",
  "Port": "5505",
  "Version": "| Edit 3LOSH RAT",
  "MutexName": "AsyncMutex_6SI8OkPnk",
  "Autorun": "false",
  "Group": "true"
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Stub.exe	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Stub.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Source	Rule	Description	Author	Strings
Stub.exe	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0xd0e6:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
Stub.exe	Windows_Trojan_Asyncrat_11a11ba1	unknown	unknown	• 0xd054:$a1: /c schtasks /create /f /sc onlogon /rl highest /tn " • 0xec38:$a2: Stub.exe • 0xecc8:$a2: Stub.exe • 0x940c:$a3: get_ActivatePong • 0xd26c:$a4: vmware • 0xd0e4:$a5: \nuR\noisreVtnerruC\swodniW\tfosorciM\erawtfoS • 0xa49d:$a6: get_SslClient

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x3ea:$x1: AsyncRAT • 0x428:$x1: AsyncRAT

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.510364745.0000000004966000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0xa7bb:$x1: AsyncRAT • 0xa7f9:$x1: AsyncRAT
00000000.00000003.474031615.0000000000633000.00000004.00000020.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x5a7:$x1: AsyncRAT • 0x5e5:$x1: AsyncRAT
00000000.00000002.505594690.0000000000633000.00000004.00000020.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x5a7:$x1: AsyncRAT • 0x5e5:$x1: AsyncRAT
00000000.00000000.237566508.0000000000052000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000000.00000000.237566508.0000000000052000.00000002.00000001.01000000.00000003.sdmp	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0xcee6:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.Stub.exe.50000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.0.Stub.exe.50000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
0.0.Stub.exe.50000.0.unpack	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0xd0e6:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
0.0.Stub.exe.50000.0.unpack	Windows_Trojan_Asyncrat_11a11ba1	unknown	unknown	• 0xd054:$a1: /c schtasks /create /f /sc onlogon /rl highest /tn " • 0xec38:$a2: Stub.exe • 0xecc8:$a2: Stub.exe • 0x940c:$a3: get_ActivatePong • 0xd26c:$a4: vmware • 0xd0e4:$a5: \nuR\noisreVtnerruC\swodniW\tfosorciM\erawtfoS • 0xa49d:$a6: get_SslClient

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Observed Malicious SSL Cert (AsyncRAT Server) - Source IP: 142.202.240.108 - Destination IP: 192.168.2.3

Timestamp:	142.202.240.108192.168.2.35505496892030673 01/05/23-09:16:11.192042
SID:	2030673
Source Port:	5505
Destination Port:	49689
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Generic AsyncRAT Style SSL Cert - Source IP: 142.202.240.108 - Destination IP: 192.168.2.3

Timestamp:	142.202.240.108192.168.2.35505496892035595 01/05/23-09:16:11.192042
SID:	2035595
Source Port:	5505
Destination Port:	49689
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected AsyncRAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Yara detected AsyncRAT

Malware Analysis System Evasion

Yara detected AsyncRAT

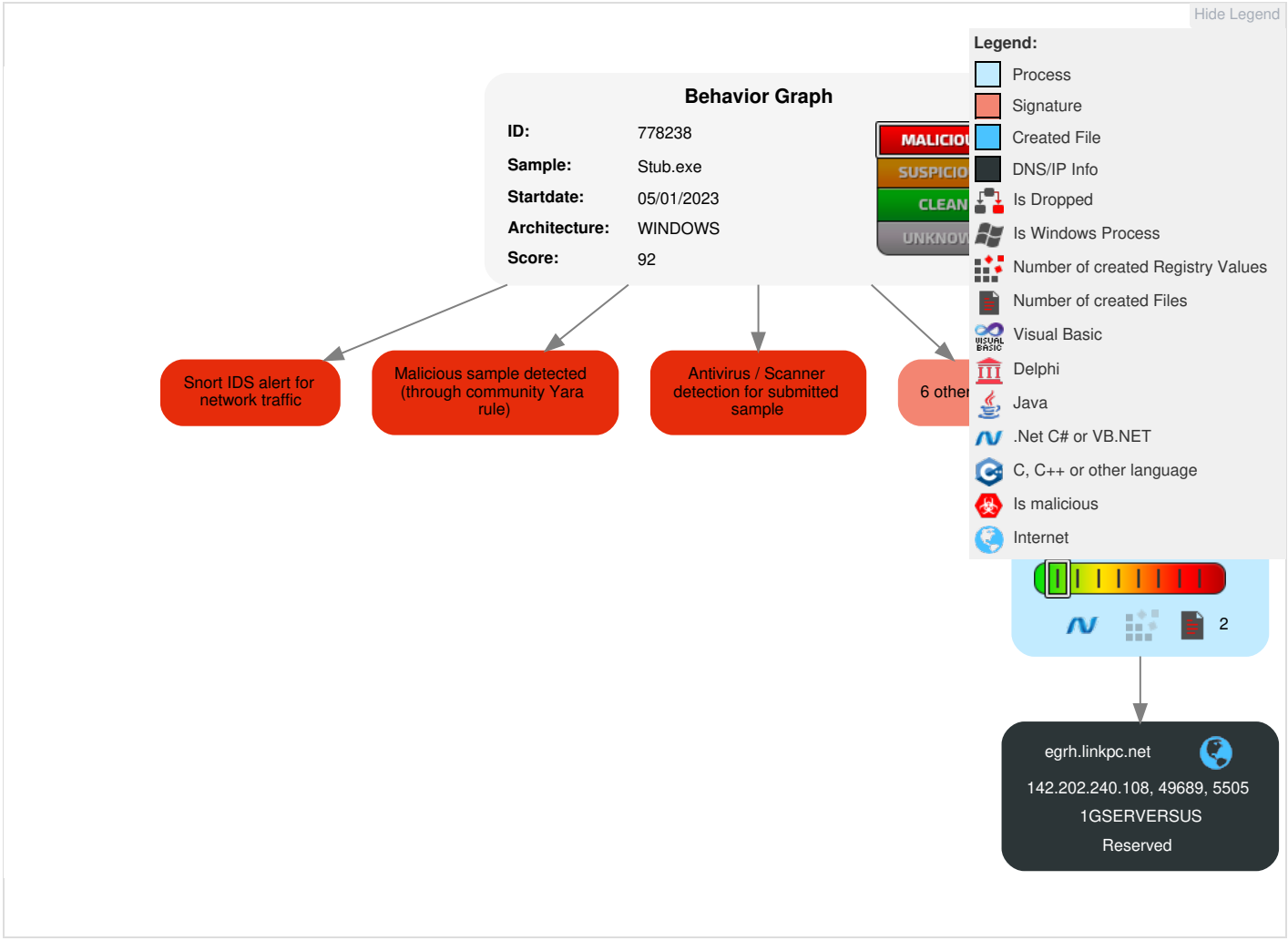
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Lowering of HIPS / PFW / Operating System Security Settings

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 Scheduled Task/Job	1 Process Injection	1 Disable or Modify Tools	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	2 1 Virtualization/Sandbox Evasion	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Obfuscated Files or Information	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Software Packing	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

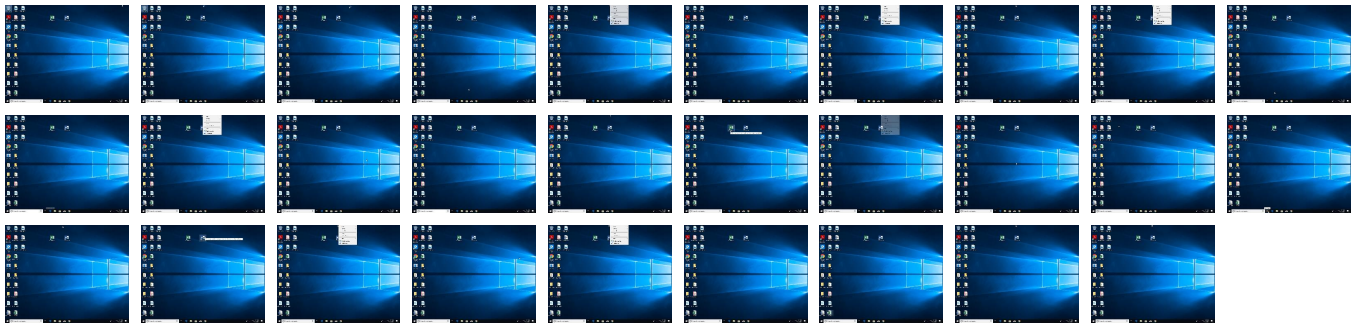
Behavior Graph



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

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Stub.exe.50000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
egrh.linkpc.net	142.202.240.108	true	false		high
windowsupdatebg.s.llnwi.net	41.63.96.128	true	false		unknown

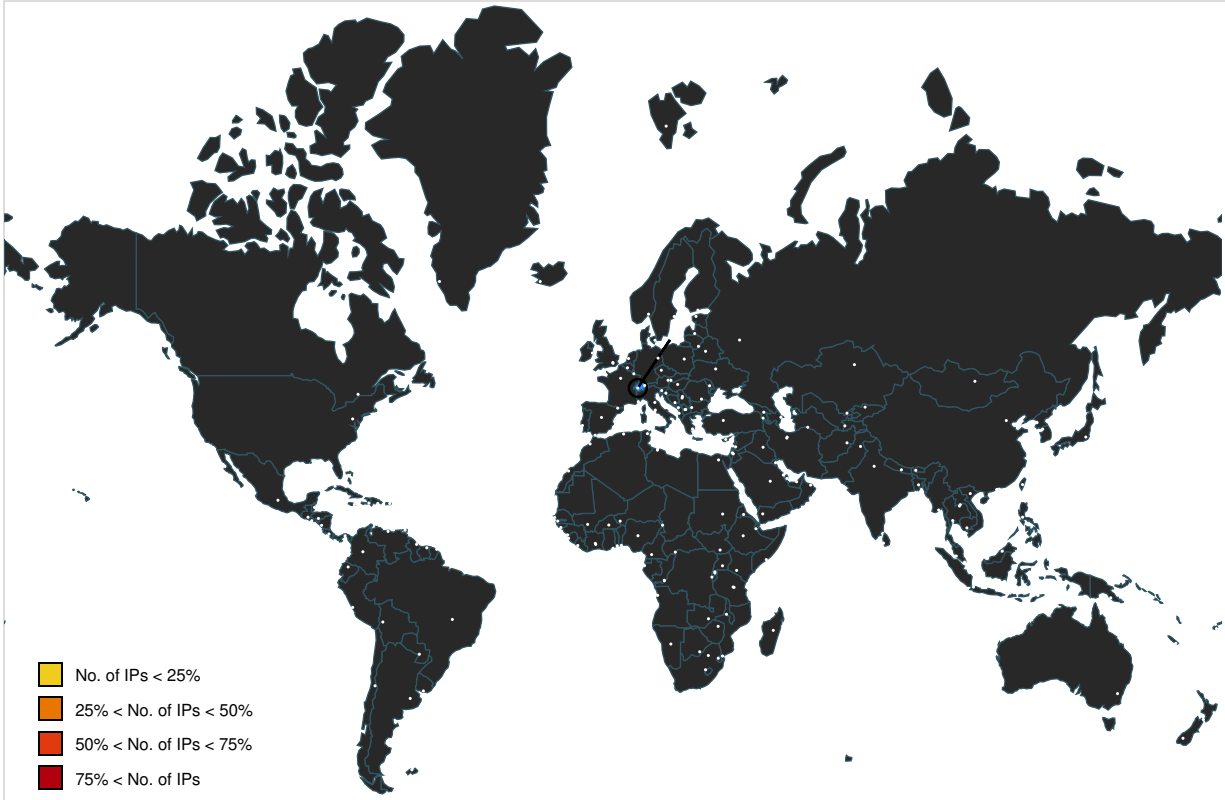
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
egrh.linkpc.net	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Stub.exe, 00000000.00000002.508243418.000000002511000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.202.240.108	egrh.linkpc.net	Reserved	?	14315	1GSERVERSUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	778238
Start date and time:	2023-01-05 09:15:14 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 55s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	Stub.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
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:	mal92.troj.evad.winEXE@1/2@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 8.238.88.254, 8.238.85.126, 8.253.207.121, 8.248.113.254, 8.238.85.254, 209.197.3.8, 93.184.221.240
- Excluded domains from analysis (whitelisted): www.bing.com, fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Not all processes where analyzed, report is missing behavior information
- 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: Stub.exe

Simulations

Behavior and APIs

Time	Type	Description
09:16:12	API Interceptor	2x Sleep call for process: Stub.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\Stub.exe
File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 62932 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	62932
Entropy (8bit):	**7.9958071285043335**
Encrypted:	**true**
SSDEEP:	1536:pvl2gmukMiArbge/oKIxf+Q9yNJLaRCfIElhUuDz:pvl2gmZhpehIxfJsJLawfIElhUu3
MD5:	FC4666CBCA561E864E7FDF883A9E6661
SHA1:	2F8D6094C7A34BF12EA0BBF0D51EE9C5BB7939A5
SHA-256:	10F3DEB6C452D749A7451B5D065F4C0449737E5EE8A44F4D15844B503141E65B
SHA-512:	C71F54B571E01F247F072BE4BBEBDF5D8410B67EB79A61E7E0D9853FE857AB9BD12F53E6AF3394B935560178107291FC4BE351B27DEB388EBA90BA949633D57D
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....oU.s .authroot.stl.....5..CK..8U[...q.yL;sf!d.D..."2."C...2....RRRHnT...\...!2.)QQ*2..nN.\7.....lgYk;.^.....}..h4.....Kc.cG.q.tY..Drg<..G.D....c.qnx..G.....r.8.....w...;.Q6..o.xf:f..:NL[.`..]I.@ ,W..J..Qf.z9.<.../.D.p:0R...#..I,.%.+."...B.n)...[Y=.,0...R.#..G5..2..]........$p..3.M.O...._L.....g.....?=.J..!...G~.#.J:.Wj.....9(:..g.8,.o.b...3..C..t.7L=..+~%pc...%..b(.q.....F.'...@~P .6CA.(d.Z~..6....=.).9.....A.....p...Gy....7U.L....S...^.R.T.p...R..:.hr./..8...a&p.l(....g.3a)...[.M..v.....g,.U..l.F..._kJv.4.rG.{.K.6.X.rz.8.r..&..G.j..p".z...L...EUX.....;...Y.....j}..FrT.,J3.d?T.T}Q..hn.?.4F...~K.....'...c...X,.v..yk..0._.j|.(.q4k1....^b..6...z..\9'}.%.*...S.[..D.k....J.../D$.#..O.o~%S.9u....|61.....~....Q+.w.e....7}..:.....^.p.mKm._9v.....'.3T..bY3..9a..p.'1..Lx.O.g..J5w+.r..K.R.P.....E0bf*r...c..;...`.j...i.;y.C..#|L.e.(.....w.X'...z../.-...c.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\Stub.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.1786749463541457
Encrypted:	false
SSDEEP:	6:kK3dh+qz7ksN+SkQlPlEGYRMY9z+4KlDA3RUe+OGNglcy:fTUkPlE99SNxAhUefblcy
MD5:	2E0F10B259BAF2EE99431DF49C886A0B
SHA1:	0708B9E03DE5A9A7637F4461D840EDC9E4414A6A
SHA-256:	1333401AA1A0F6D497C63B5B1D1E01F2595FD0380CB2A984102A65E6B26B6023
SHA-512:	76C6D7BDF682AEAB9104A81F0BE7E92EA452A68F4AC13741380DF10BCF878DC35895E16FAADD62C7437B41647A457E7E56C4FBDBF0E3EA6F1505D11BAAE0CD59
Malicious:	false
Reputation:	low
Preview:	p..... .....i)!..(..... .....g.%.....&.....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...".8.0.a.1.6.7.1.3.2.5.4.d.9.1.:.0."...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.627060592579058
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:	Stub.exe
File size:	62464

MD5:	da5c4dbbc80ca5da70237ef8bc281476
SHA1:	c6689884e4bf3360fceacbdaff09d211cef3a49d
SHA256:	4981bda443713f5cecb9df4d163cd62f1bd038cb897895bb2f81015796676371
SHA512:	40210ddddaae84fa45d758831491cc3b609c3194862f8fad8938e713fa5033eaf473c44bb0bc345ea46fc302264f5628b6793339bf0cb5f2aea2c316a0c115f4
SSDEEP:	1536:+/KCnABwEttYQuT68QKzWbVSDRDZLbxx:+/KrBwEttYm8BabVSjLVx
TLSH:	EE532B043BE9C129F1BE8F709DF376444AB9F1677906DA0E1CD451DA0622BC68A427EF
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....7c............................^.... ... .@.. ....`............@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41075e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x633700E3 [Fri Sep 30 14:44:51 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1070c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x12000	0x7ff	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x14000	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	0xe764	0xe800	False	0.5357623922413793	data	5.673338999412451	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x12000	0x7ff	0x800	False	0.41650390625	data	4.884866150337139	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x14000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x120a0	0x2cc	data		
RT_MANIFEST	0x1236c	0x493	exported SGML document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

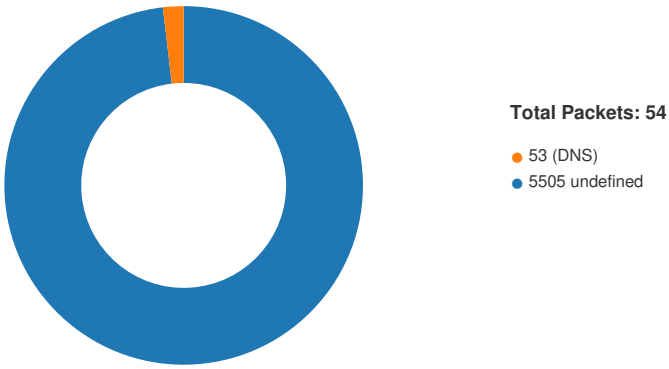
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
142.202.240.108192.168.2.35505496892030673 01/05/23-09:16:11.192042	TCP	2030673	ET TROJAN Observed Malicious SSL Cert (AsyncRAT Server)	5505	49689	142.202.240.108	192.168.2.3
142.202.240.108192.168.2.35505496892035595 01/05/23-09:16:11.192042	TCP	2035595	ET TROJAN Generic AsyncRAT Style SSL Cert	5505	49689	142.202.240.108	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:16:10.446110964 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:10.608800888 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:10.609150887 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:11.019267082 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:11.192042112 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:11.192109108 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:11.192358017 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:11.211710930 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:11.376323938 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:11.420284033 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:14.210656881 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:14.413397074 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:14.413630962 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:14.616478920 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:24.083786011 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:24.287956953 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:24.288218021 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:24.450222969 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:24.499444008 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:24.660866022 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:24.702743053 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:25.105531931 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:25.319370985 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:25.319547892 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:25.522351980 CET	5505	49689	142.202.240.108	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:16:33.945424080 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:34.147113085 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:34.147206068 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:34.309361935 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:34.359613895 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:34.520828962 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:34.556056976 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:34.771938086 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:34.774681091 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:34.990674973 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:37.736253977 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:37.781907082 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:37.943053961 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:37.985011101 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:43.769193888 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:43.974895954 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:43.975084066 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:44.137037039 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:44.188657999 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:44.349960089 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:44.367060900 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:44.568764925 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:44.568924904 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:44.771676064 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:53.594084978 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:53.802622080 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:53.802706003 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:53.964433908 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:54.017430067 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:54.178270102 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:54.220592976 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:54.596527100 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:54.802869081 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:16:54.803147078 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:16:55.005819082 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:03.475423098 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:03.677582026 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:03.677704096 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:03.840008974 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:03.893325090 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:04.054852962 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:04.086241007 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:04.302668095 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:04.305140018 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:04.521357059 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:07.741579056 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:07.784228086 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:07.945435047 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:08.003063917 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:13.312128067 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:13.521106005 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:13.521403074 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:13.684165955 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:13.737871885 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:13.899128914 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:13.941026926 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:14.171483040 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:14.380517960 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:14.382247925 CET	49689	5505	192.168.2.3	142.202.240.108

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:17:14.599172115 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:23.155992031 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:23.380219936 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:23.380513906 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:23.543056965 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:23.598146915 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:23.759288073 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:23.776537895 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:23.989550114 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:23.989643097 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:24.192562103 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:33.781151056 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:33.989244938 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:33.989427090 CET	49689	5505	192.168.2.3	142.202.240.108
Jan 5, 2023 09:17:34.164716005 CET	5505	49689	142.202.240.108	192.168.2.3
Jan 5, 2023 09:17:34.208254099 CET	49689	5505	192.168.2.3	142.202.240.108

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:16:10.250736952 CET	59869	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:16:10.373781919 CET	53	59869	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 5, 2023 09:16:10.250736952 CET	192.168.2.3	8.8.8.8	0xd24c	Standard query (0)	egrh.linkpc.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 09:16:10.373781919 CET	8.8.8.8	192.168.2.3	0xd24c	No error (0)	egrh.linkpc.net		142.202.240.108	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:16:23.498951912 CET	8.8.8.8	192.168.2.3	0x2082	No error (0)	windowsupdatebg.s.llnwi.net		41.63.96.128	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:16:23.973170042 CET	8.8.8.8	192.168.2.3	0x96f9	No error (0)	windowsupdatebg.s.llnwi.net		41.63.96.128	A (IP address)	IN (0x0001)	false

Statistics

No statistics

System Behavior

Analysis Process: Stub.exe PID: **5484**, Parent PID: **3452**

General

Target ID:	0
Start time:	09:16:03
Start date:	05/01/2023
Path:	C:\Users\user\Desktop\Stub.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\Desktop\Stub.exe
Imagebase:	0x50000
File size:	62464 bytes
MD5 hash:	DA5C4DBBC80CA5DA70237EF8BC281476
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000000.00000002.510364745.0000000004966000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000000.00000003.474031615.0000000000633000.00000004.00000020.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000000.00000002.505594690.0000000000633000.00000004.00000020.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000000.237566508.0000000000052000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000000.00000000.237566508.0000000000052000.00000002.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000000.00000003.384798750.000000000061D000.00000004.00000020.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000000.00000003.432092160.0000000000631000.00000004.00000020.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000002.508243418.0000000002511000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000000.00000002.508243418.0000000002511000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	low

File Activities

File Created

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

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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile

Disassembly

No disassembly