ID: 679246
Sample Name: Uhy4TvdjRw.exe
Cookbook: default.jbs
Time: 13:06:17
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

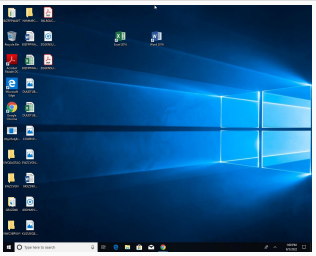
Windows Analysis Report

Uhy4TvdjRw.exe

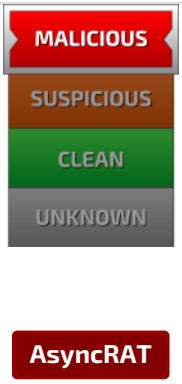
Overview

General Information

Sample Name:	Uhy4TvdjRw.exe
Analysis ID:	679246
MD5:	10135b39a4a6d8.
SHA1:	3669c101670b0b..
SHA256:	45e87ee0b025a7.
Tags:	AsyncRAT exe RAT
Infos:	



Detection



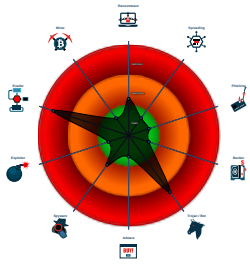
AsyncRAT

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: Schedule system p…
- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Yara detected AsyncRAT
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- Uhy4TvdjRw.exe (PID: 2508 cmdline: "C:\Users\user\Desktop\Uhy4TvdjRw.exe" MD5: 10135B39A4A6D8717BA8CEEC380EF060)
  - cmd.exe (PID: 5232 cmdline: "C:\Windows\System32\cmd.exe" /c schtasks /create /f /sc onlogon /rl highest /tn "svchost" /tr '"C:\Users\user\AppData\Roaming\svchost.exe"' & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 2936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - MpCmdRun.exe (PID: 3572 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
        - conhost.exe (PID: 4412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 4756 cmdline: schtasks /create /f /sc onlogon /rl highest /tn "svchost" /tr '"C:\Users\user\AppData\Roaming\svchost.exe"' MD5: 15FF7D8324231381BAD48A052F85DF04)
  - cmd.exe (PID: 5992 cmdline: C:\Windows\system32\cmd.exe /c '"C:\Users\user\AppData\Local\Temp\tmp93E6.tmp.bat"' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6052 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5132 cmdline: timeout 3 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - svchost.exe (PID: 4152 cmdline: "C:\Users\user\AppData\Roaming\svchost.exe" MD5: 10135B39A4A6D8717BA8CEEC380EF060)
- svchost.exe (PID: 5208 cmdline: C:\Users\user\AppData\Roaming\svchost.exe MD5: 10135B39A4A6D8717BA8CEEC380EF060)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT


```
{
  "Server": "127.0.0.1,61.14.233.88",
  "Ports": "6606,7707,8808",
  "Version": "0.5.7B",
  "Autorun": "true",
  "Install_Folder": "%AppData%"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Uhy4TvdjRw.exe	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Uhy4TvdjRw.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
Uhy4TvdjRw.exe	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0xa355:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x104bfb:$x1: AsyncRAT • 0x104c39:$x1: AsyncRAT

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\svchost.exe	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
C:\Users\user\AppData\Roaming\svchost.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
C:\Users\user\AppData\Roaming\svchost.exe	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0xa355:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.534018978.0000000005100000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x623f:$x1: AsyncRAT • 0x627d:$x1: AsyncRAT
0000000B.00000003.304436416.00000000051E6000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x9363:$x1: AsyncRAT • 0x93a1:$x1: AsyncRAT
00000000.00000002.280682459.0000000004F88000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x741b:$x1: AsyncRAT • 0x7459:$x1: AsyncRAT
00000000.00000003.269514411.0000000004F88000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x741b:$x1: AsyncRAT • 0x7459:$x1: AsyncRAT
00000000.00000002.278048476.0000000002B00000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.Uhy4TvdjRw.exe.6d0000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.0.Uhy4TvdjRw.exe.6d0000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
0.0.Uhy4TvdjRw.exe.6d0000.0.unpack	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0xa355:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
0.2.Uhy4TvdjRw.exe.2b00314.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.2.Uhy4TvdjRw.exe.2b00314.0.unpack	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0x8555:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
Click to see the 3 entries				

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Schedule system process

Snort Signatures

ET TROJAN Generic AsyncRAT Style SSL Cert - Source IP: 61.14.233.88 - Destination IP: 192.168.2.3 −

Timestamp:	61.14.233.88192.168.2.37707497392035595 08/05/22-13:07:46.244143
SID:	2035595
Source Port:	7707
Destination Port:	49739
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Observed Malicious SSL Cert (AsyncRAT Server) - Source IP: 61.14.233.88 - Destination IP: 192.168.2.3 −

Timestamp:	61.14.233.88192.168.2.37707497392030673 08/05/22-13:07:46.244143
SID:	2030673
Source Port:	7707
Destination Port:	49739
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

Yara detected Generic Downloader

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

Persistence and Installation Behavior

Drops PE files with benign system names

Boot Survival

Yara detected AsyncRAT

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

Malware Analysis System Evasion

Yara detected AsyncRAT

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

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Lowering of HIPS / PFW / Operating System Security Settings

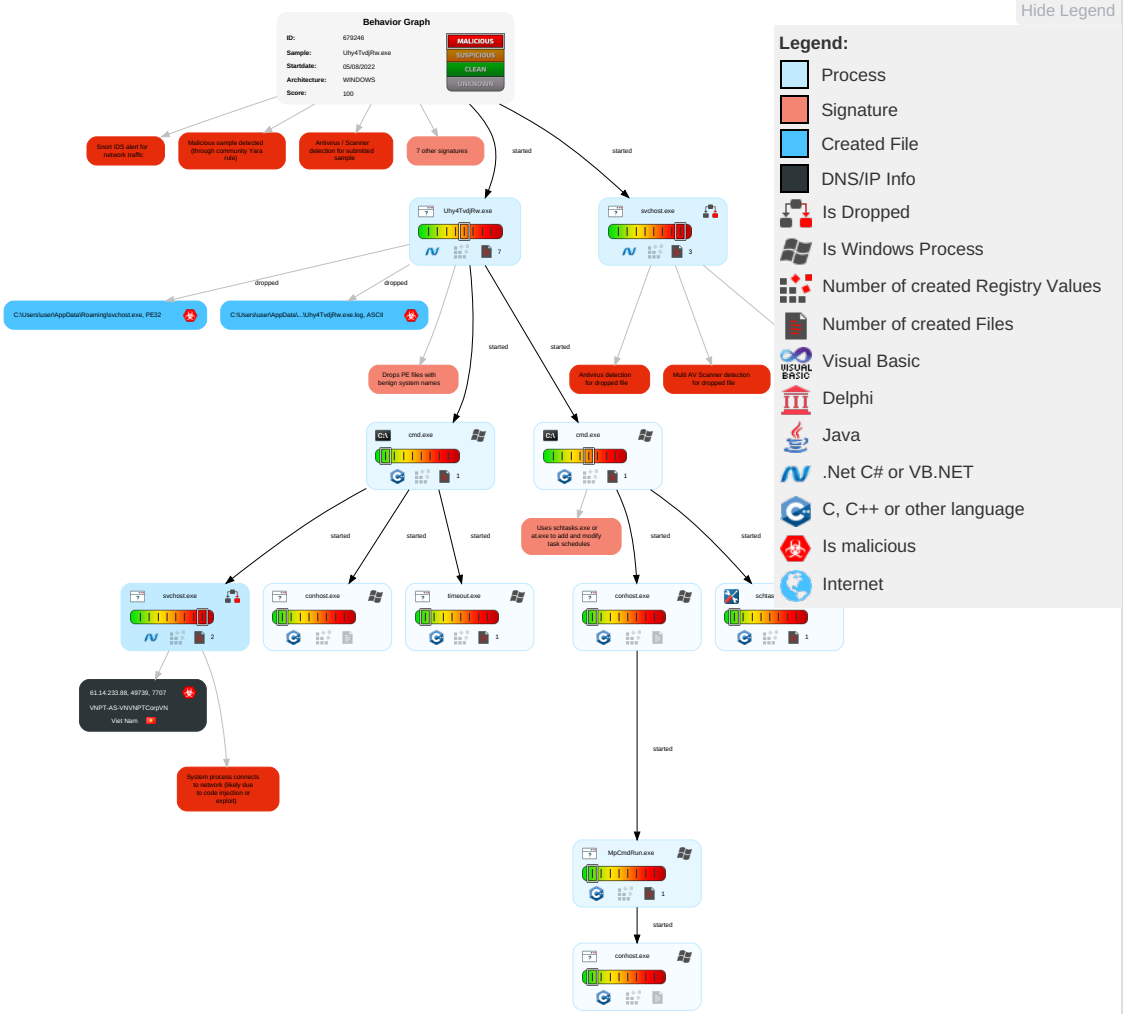
Yara detected AsyncRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	2 Scheduled Task/Job	1 1 2 Process Injection	1 1 Masquerading	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	2 Scheduled Task/Job	Boot or Logon Initialization Scripts	2 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	2 2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scripting	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	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 2 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Scripting	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	1 1 Obfuscated Files or Information	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	1 Software Packing	DCSync	1 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 3 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph

Hide Legend



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
Uhy4TvdjRw.exe	68%	Virustotal		Browse
Uhy4TvdjRw.exe	57%	Metadefender		Browse
Uhy4TvdjRw.exe	96%	ReversingLabs	ByteCode-MSIL.Backdoor.AsyncRAT	
Uhy4TvdjRw.exe	100%	Avira	HEUR/AGEN.1202836	
Uhy4TvdjRw.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\svchost.exe	100%	Avira	HEUR/AGEN.1202836	
C:\Users\user\AppData\Roaming\svchost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\svchost.exe	68%	Virustotal		Browse
C:\Users\user\AppData\Roaming\svchost.exe	57%	Metadefender		Browse
C:\Users\user\AppData\Roaming\svchost.exe	96%	ReversingLabs	ByteCode-MSIL.Backdoor.AsyncRAT	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Uhy4TvdjRw.exe.6d0000.0.unpack	100%	Avira	HEUR/AGEN.1202836		Download File

Domains

Source	Detection	Scanner	Label	Link
windowsupdatebg.s.llnwi.net	0%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

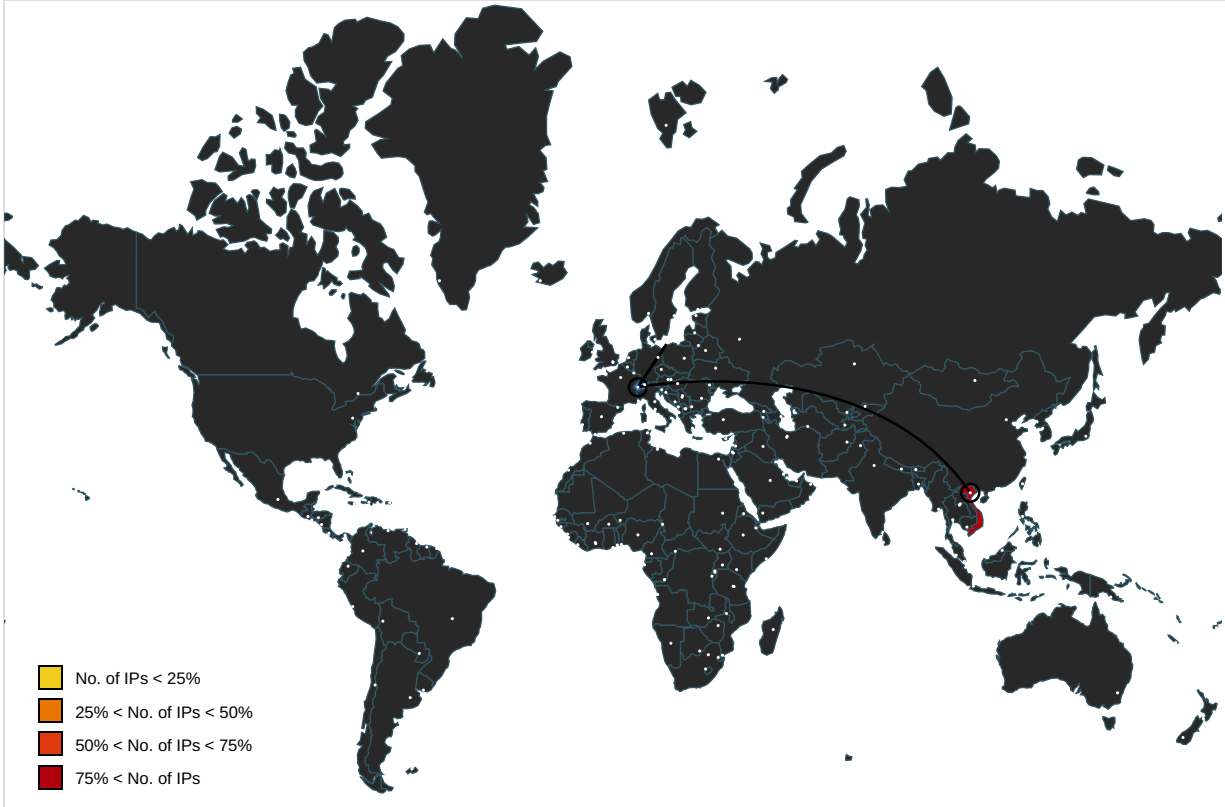
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
windowsupdatebg.s.llnwi.net	95.140.230.192	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Uhy4TvdjRw.exe, 00000000.00000002.278002213.0000000002AC7000.00000004.00000800.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.528272233.00000000029A4000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
61.14.233.88	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679246
Start date and time: 05/08/202213:06:17	2022-08-05 13:06:17 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Uhy4TvdjRw.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:	34
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@17/8@0/1
EGA Information:	• Successful, ratio: 33.3%
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 • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 95.140.230.192, 8.238.189.126, 8.238.190.126, 8.248.141.254, 8.248.117.254, 67.26.139.254
- Excluded domains from analysis (whitelisted): www.bing.com, fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, client-office365-tas.msedge.net, store-images.s-microsoft.com-c.edgekey.net, ctldl.windowsupdate.com, arc.msn.com, wu-bg-shim.trafficmanager.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, config.edge.skype.com
- Execution Graph export aborted for target Uhy4TvdjRw.exe, PID 2508 because it is empty
- Execution Graph export aborted for target svchost.exe, PID 5208 because it is empty
- 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.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:07:36	Task Scheduler	Run new task: svchost path: "C:\Users\user\AppData\Roaming\svchost.exe"
13:07:47	API Interceptor	1x Sleep call for process: svchost.exe modified
13:08:49	API Interceptor	1x Sleep call for process: MpCmdRun.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\AppData\Roaming\svchost.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C.....`h!0.I.(C..1Q*L.p.."s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<.....3....s.T...._.'...%{v...s.....KgV.0..X=.A.9w9.Ea.x.....\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....uI.....}.....d....M.....6q.Q~.0.\.'U^)`.u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.l.E.6..a8.6..nq..x.r4..1t.....,..u.O..O.L...Uf...X.u.F .(.(....."..q...n{%U.-u....l6!....Z....~o0.}Q'.s.i....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

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

Process:	C:\Users\user\AppData\Roaming\svchost.exe
File Type:	data
Category:	modified
Size (bytes):	290
Entropy (8bit):	2.947388251222562
Encrypted:	false
SSDEEP:	6:kKf11+N+SkQlPlEGYRMY9z+4KlDA3RUe/:311NkPlE99SNxAhUe/
MD5:	AA449CC3E819D614B28CB03C1D01D8BF
SHA1:	782EF6F88E4BF68E6D5B823AE7DCFA73B3DB4DA5
SHA-256:	1477C8430F191DAD859F18B5B1511440B7E331BEED1A1BB18B7506A964D8FB76
SHA-512:	1DC5EC42331021DC9C8F27EE6DE63B1CF83485EDA11F5E46CBC1E64811579E89C518FFBFC05FC6C0CB56497AAD9505962C048A977A67C1D60BBC734E0A6F85AF
Malicious:	false

Preview:	p..... .....(..... .....L.....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...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Uhy4TvdjRw.exe.log

Process:	C:\Users\user\Desktop\Uhy4TvdjRw.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.348034597186669
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat92n4M6:ML9E4Ks2wKDE4KhK3VZ9pKhg84j
MD5:	07FC10473CB7F0DEC42EE8079EB0DF28
SHA1:	90FA6D0B604991B3E5E8F6DB041651B10FD4284A
SHA-256:	A42B61DFB4AF366D05CE1815C88E2392C7C4AA9B6B17604234BEB7A7DADA7E4C
SHA-512:	D7240EE88D207E631990907AFA96C8384FB51729A16247BD4BDB96CBA3C4CDB9A68ADCD07819B2242A0F395690AD831B1B547EC91E988CBE39398F472055D56F
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

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

Process:	C:\Users\user\AppData\Roaming\svchost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD3D
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp93E6.tmp.bat

Process:	C:\Users\user\Desktop\Uhy4TvdjRw.exe
File Type:	DOS batch file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	151
Entropy (8bit):	5.102625473568323
Encrypted:	false
SSDEEP:	3:mKDDCMNqTtvL5oWXp5cViEaKC5ZACSmqRDWXp5cViE2J5xAlnTRI2WjVZPy:hWKqTtT6WXp+NaZ5Omq1WXp+N23fTXWq
MD5:	6D013B1CAFE4160FDC1F7B36C3145E1A
SHA1:	C80E8E5E33E867683564C8E649DB78ED5ED6A1D2
SHA-256:	254D27DCF87576D5221575F043F5BB32F4A2E508B4B7A98244AF933C678D7226
SHA-512:	301C4B0635C31D563B6286239A0711B753A453B02BC4623E21FF6A896186602F147E74956CD7B879EA0ECE8593F6A391C5C0FD87F66DCF98C6CF1988DE2631B4
Malicious:	false
Preview:	@echo off..timeout 3 > NUL..START "" "C:\Users\user\AppData\Roaming\svchost.exe"..CD C:\Users\user\AppData\Local\Temp\..DEL "tmp93E6.tmp.bat" /f /q..

C:\Users\user\AppData\Roaming\svchost.exe

Process:	C:\Users\user\Desktop\Uhy4TvdjRw.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	49152

Entropy (8bit):	5.575530706715254
Encrypted:	false
SSDEEP:	768:wuK49TH4EjZWUR+ejmo2qrw8sJrKKIixPIAoqVcg0b1G24HftYUpG5ilsga8yBDu:wuK49THf52HtuAo9rbMNYUpnfMdh+
MD5:	10135B39A4A6D8717BA8CEEC380EF060
SHA1:	3669C101670B0B373DEA1C7729718340196DA4BC
SHA-256:	45E87EE0B025A7E4A783A6786564982E7735C8C50D0B3D84A3D5DD90CE735CFE
SHA-512:	71CC73FBB213529A14FB94C56F1A056AE5DB940A7AAC22079AE9A238A9633DDD64B7D8FF9B3A023051C9D6CFBBED48E90F14F2E17A2F6893AE9B3B6F46DD31 EE
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Roaming\svchost.exe, Author: Joe Security • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Users\user\AppData\Roaming\svchost.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: C:\Users\user\AppData\Roaming\svchost.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 68%, Browse • Antivirus: Metadefender, Detection: 57%, Browse • Antivirus: ReversingLabs, Detection: 96%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...#..^................................. ....@.. ....@................................\...O... ....H............text........ ....`.rsrc...............................@..@.reloc........ ......................@..B........................H........Y..`v...V..;...$0.xC.=VD..b......9A../.\.....(....*.~....*.......*.~....*.......*.~....*.......*.~....*.......*.~ ....*.......*.~....*.......*.~....*.......*.~....*.~....*.......*.~....*.......*.~....*.......**.(>......*2~.....o?...*.s.........*.()...:(...(*...:....(+...:....('...:....((...9.....(v...*V(....s.... ...o....*n~....9....~....o.. ....*~~....(....9....(0...9....(@...*Vr.%.p~....(o....#...*.s...

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log

Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.1650995689703207
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zq+F:j+s+v+b+P+m+0+Q+q+5+F
MD5:	78B72556A96E740F02ADAB636DC17FB1
SHA1:	5382CFD5A6C1DE0541DE9CC4EE515CC2F63654F4
SHA-256:	915A96B1B706C95F06CF841A202296F34942DD69E7C7C83EDA9B2A79F93BF435
SHA-512:	1217A1B06E44EEF2BCC63BDC27C130932FEC307277722FD4E3DCDBA0A225918953BE239BCF19E0C2C35C5CD5B4E004893ACABB96F15A893B4D089DB2E0C5C E77
Malicious:	false
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....- .-.............-.

\Device\Null

Process:	C:\Windows\SysWOW64\timeout.exe
File Type:	ASCII text, with CRLF line terminators, with overstriking
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.41440934524794
Encrypted:	false
SSDEEP:	3:hYFqdLGAR+mQRKVxLZXt0sn:hYFqGaNZKsn
MD5:	3DD7DD37C304E70A7316FE43B69F421F
SHA1:	A3754CFC33E9CA729444A95E95BCB53384CB51E4
SHA-256:	4FA27CE1D904EA973430ADC99062DCF4BAB386A19AB0F8D9A4185FA99067F3AA
SHA-512:	713533E973CF0FD359AC7DB22B1399392C86D9FD1E715248F5724AAFBBF0EEB5EAC0289A0E892167EB559BE976C2AD0A0A0D8EFC407FFAF5B3C3A32AA9A0A AA4
Malicious:	false
Preview:	..Waiting for 3 seconds, press a key to continue ....2.1.0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.575530706715254
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:	Uhy4TvdjRw.exe
File size:	49152
MD5:	10135b39a4a6d8717ba8ceec380ef060
SHA1:	3669c101670b0b373dea1c7729718340196da4bc
SHA256:	45e87ee0b025a7e4a783a6786564982e7735c8c50d0b3d84a3d5dd90ce735cfe
SHA512:	71cc73fbb213529a14fb94c56f1a056ae5db940a7aac22079ae9a238a9633ddd64b7d8ff9b3a023051c9d6cfbbed48e90f14f2e17a2f6893ae9b3b6f46dd31ee
SSDEEP:	768:wuK49TH4EjZWUR+ejmo2qrw8sJrKKIixPIAoqVcg0b1G24HftYUpG5ilsga8yBDu:wuK49THf52HtuAo9rbMNYUpnfMdh+
TLSH:	61233B003BE9822BF2BE4F789DF22145467AB1673607D64E6CC441D75A13FC19A42AFE
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:	0x40d0ae
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:	0x5EB79023 [Sun May 10 05:24:51 2020 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

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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0xd05c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe000	0x8c8	.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	0xb0b4	0xb200	False	0.5427273525280899	data	5.624119295582564	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xe000	0x8c8	0xa00	False	0.3765625	data	5.0748901103993935	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10000	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	0xe0a0	0x394	data		
RT_MANIFEST	0xe434	0x493	exported SGML document, UTF-8 Unicode (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
61.14.233.88192.168.2.37707497392035595 08/05/22-13:07:46.244143	TCP	2035595	ET TROJAN Generic AsyncRAT Style SSL Cert	7707	49739	61.14.233.88	192.168.2.3
61.14.233.88192.168.2.37707497392030673 08/05/22-13:07:46.244143	TCP	2030673	ET TROJAN Observed Malicious SSL Cert (AsyncRAT Server)	7707	49739	61.14.233.88	192.168.2.3

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 13:07:45.648207903 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:07:45.930344105 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:07:45.930579901 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:07:45.962605953 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:07:46.244143009 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:07:46.244194984 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:07:46.244291067 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:07:46.248120070 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:07:46.566440105 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:07:46.643579960 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:07:49.418629885 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:07:49.902847052 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:07:49.903542042 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:07:50.386825085 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:01.679904938 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:02.169430017 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:02.169563055 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:02.451380968 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:02.535649061 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:02.816046000 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:02.921156883 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:03.402391911 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:03.402510881 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:03.887619019 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:14.365777969 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:14.855849981 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:14.855950117 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:15.136513948 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:15.177320004 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:15.457210064 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:15.521085024 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:15.538252115 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:15.800976992 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:15.801150084 CEST	49739	7707	192.168.2.3	61.14.233.88

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 13:08:16.029189110 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:16.293257952 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:26.633465052 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:27.121565104 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:27.125171900 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:27.408021927 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:27.506469011 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:27.786192894 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:27.793873072 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:28.277340889 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:28.277441978 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:28.777179003 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:38.933715105 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:39.417967081 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:39.418081045 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:39.699002028 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:39.741934061 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:40.021214962 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:40.026793003 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:40.512087107 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:40.512187958 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:40.998488903 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:45.606575012 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:45.851788044 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:46.131325006 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:46.242445946 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:51.230092049 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:51.714715004 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:51.714873075 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:51.996316910 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:52.055486917 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:52.335429907 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:52.348324060 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:52.839986086 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:08:52.840198040 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:08:53.324326038 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:03.528692961 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:04.011859894 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:04.011940002 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:04.293437958 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:04.337769985 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:04.617676020 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:04.665924072 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:04.842731953 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:05.324264050 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:05.324431896 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:05.808985949 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:15.584073067 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:15.635601044 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:15.831409931 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:15.914891958 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:15.915205956 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:16.194834948 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:16.195557117 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:16.245033026 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:16.524821997 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:16.529345989 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:17.011609077 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:17.011742115 CEST	49739	7707	192.168.2.3	61.14.233.88

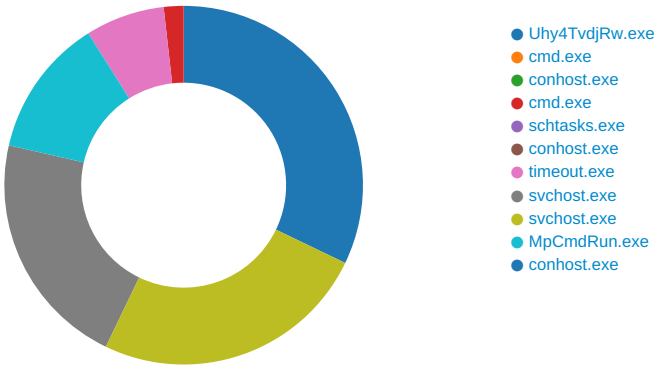
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 13:09:17.496249914 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:28.139405012 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:28.636779070 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:28.636989117 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:28.917084932 CEST	7707	49739	61.14.233.88	192.168.2.3
Aug 5, 2022 13:09:28.964931011 CEST	49739	7707	192.168.2.3	61.14.233.88
Aug 5, 2022 13:09:29.244489908 CEST	7707	49739	61.14.233.88	192.168.2.3

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 13:07:47.267018080 CEST	8.8.8.8	192.168.2.3	0xd471	No error (0)	windowsupdatebg.s.llnwi.net		95.140.230.192	A (IP address)	IN (0x0001)
Aug 5, 2022 13:07:47.267018080 CEST	8.8.8.8	192.168.2.3	0xd471	No error (0)	windowsupdatebg.s.llnwi.net		178.79.225.0	A (IP address)	IN (0x0001)

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Uhy4TvdjRw.exe PID: **2508**, Parent PID: **5148**

General

Target ID:	0
Start time:	13:07:25
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\Uhy4TvdjRw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Uhy4TvdjRw.exe"
Imagebase:	0x6d0000
File size:	49152 bytes
MD5 hash:	10135B39A4A6D8717BA8CEEC380EF060
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: 00000000.00000002.280682459.0000000004F88000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000000.00000003.269514411.0000000004F88000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000002.278048476.0000000002B00000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000000.00000002.278048476.0000000002B00000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000000.257007882.00000000006D2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000000.00000000.257007882.00000000006D2000.00000002.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000000.00000002.277813823.0000000002A71000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000000.00000002.277813823.0000000002A71000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	low

File Activities

Analysis Process: cmd.exe PID: 5232, Parent PID: 2508

General

Target ID:	4
Start time:	13:07:33
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c schtasks /create /f /sc onlogon /rl highest /tn "svchost" /tr "'C:\Users\user\AppData\Roaming\svchost.exe'" & exit
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 2936, Parent PID: 5232

General

Target ID:	5
Start time:	13:07:33
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: cmd.exe PID: 5992, Parent PID: 2508

General

Target ID:	6
Start time:	13:07:34
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\tmp93E6.tmp.bat""
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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\tmp93E6.tmp.bat	unknown	8191	success or wait	5	C2FB07	ReadFile

Analysis Process: schtasks.exe PID: **4756**, Parent PID: **5232**

General

Target ID:	7
Start time:	13:07:34
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /f /sc onlogon /rl highest /tn "svchost" /tr "'C:\Users\user\AppData\Roaming\svchost.exe'"
Imagebase:	0x9e0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6052**, Parent PID: **5992**

General

Target ID:	8
Start time:	13:07:35
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: timeout.exe PID: **5132**, Parent PID: **5992**

General

Target ID:	9
Start time:	13:07:35
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 3
Imagebase:	0x80000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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 Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\Null	15	15	20 73 65 63 6f 6e 64 73 2c 20 70 72 65 73 73	seconds, press	success or wait	1	82DA7	fprintf
\Device\Null	52	37	08 32 08 31 08 30 0d 0a	210	success or wait	1	82DA7	fprintf
\Device\Null	54	2	08 31	1	success or wait	3	82DA7	fprintf
\Device\Null	60	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	82DA7	fprintf

Analysis Process: svchost.exe PID: **5208**, Parent PID: **848**

General

Target ID:	10
Start time:	13:07:36
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Roaming\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\svchost.exe
Imagebase:	0xc00000
File size:	49152 bytes
MD5 hash:	10135B39A4A6D8717BA8CEEC380EF060
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: 0000000A.00000002.304518771.0000000001439000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 0000000A.00000002.305975314.0000000003341000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Roaming\svchost.exe, Author: Joe Security • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Users\user\AppData\Roaming\svchost.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: C:\Users\user\AppData\Roaming\svchost.exe, Author: ditekSHen

Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 68%, Virustotal, Browse • Detection: 57%, Metadefender, Browse • Detection: 96%, ReversingLabs
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 | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\svchost.exe.log	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6D0FC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\svchost.exe.log	0	425	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6D0FC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD203DE	ReadFile

Analysis Process: svchost.exe PID: **4152**, Parent PID: **5992**

General

Target ID:	11
Start time:	13:07:38
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Roaming\svchost.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\svchost.exe"
Imagebase:	0x260000
File size:	49152 bytes
MD5 hash:	10135B39A4A6D8717BA8CEEC380EF060
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: 0000000B.00000002.534018978.0000000005100000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 0000000B.00000003.304436416.00000000051E6000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 0000000B.00000002.526007263.0000000000A3A000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 0000000B.00000003.304383142.00000000051DA000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000002.528272233.00000000029A4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 0000000B.00000002.528272233.00000000029A4000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 0000000B.00000002.528272233.00000000029A4000.00000004.00000800.00020000.00000000.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 | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDECF06	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	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC31B4F	ReadFile

Analysis Process: MpCmdRun.exe PID: 3572, Parent PID: 2936

General

Target ID:	29
Start time:	13:08:48
Start date:	05/08/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7b0320000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8156	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF7B034BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8338	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 46 00 72 00 69 00 20 00 0e 20 41 00 75 00 67 00 20 00 0e 20 30 00 35 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 31 00 33 00 3a 00 30 00 38 00 3a 00 34 00 39 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Fri Aug 05 2022 13:08:49	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8596	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8682	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8702	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8788	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 46 00 72 00 69 00 20 00 0e 20 41 00 75 00 67 00 20 00 0e 20 30 00 35 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 31 00 33 00 3a 00 30 00 38 00 3a 00 34 00 39 00 0d 00 0a 00	MpCmdRun: End Time: Fri Aug 05 2022 13:08:49	success or wait	1	7FF7B034BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8888	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF7B034BC96	WriteFile

Analysis Process: conhost.exe PID: **4412**, Parent PID: **3572**

General

Target ID:	30
Start time:	13:08:49
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly