ID: 412502
Sample Name:
Ko4zQgTBHv.exe
Cookbook: default.jbs
Time: 18:31:17
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

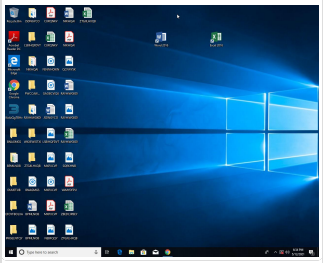
Analysis Report Ko4zQgTBHv.exe

Overview

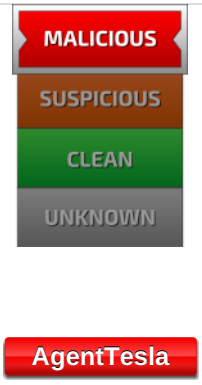
General Information

Sample Name:	Ko4zQgTBHv.exe
Analysis ID:	412502
MD5:	02bc365a934e55..
SHA1:	a7fcb0381c4f68e..
SHA256:	bd97a138f3c0b9b.
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



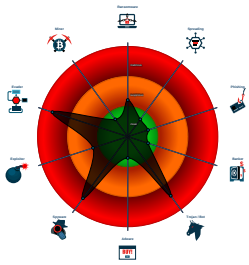
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- Ko4zQgTBHv.exe (PID: 6484 cmdline: 'C:\Users\user\Desktop\Ko4zQgTBHv.exe' MD5: 02BC365A934E558EB634E19DD2D33E64)
  - schtasks.exe (PID: 6660 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\vZvprBd' /XML 'C:\Users\user\AppData\Local\Temp\tmpF3F1.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6668 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Ko4zQgTBHv.exe (PID: 6704 cmdline: C:\Users\user\Desktop\Ko4zQgTBHv.exe MD5: 02BC365A934E558EB634E19DD2D33E64)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "jojo@glimpse-it.co@Mexico1.,mail.privateemail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.591708318.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.591708318.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.342175940.0000000002D4E000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.595056596.0000000002B01000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.595056596.0000000002B0 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Click to see the 8 entries				

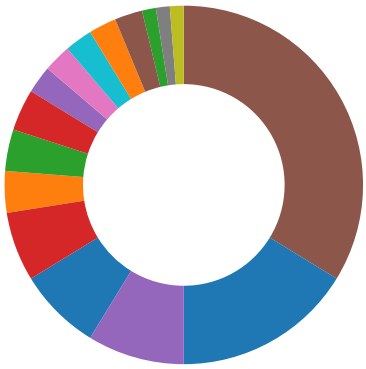
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Ko4zQgTBHv.exe.3daed20.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Ko4zQgTBHv.exe.3daed20.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.2.Ko4zQgTBHv.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.Ko4zQgTBHv.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Ko4zQgTBHv.exe.3daed20.3.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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

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)

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

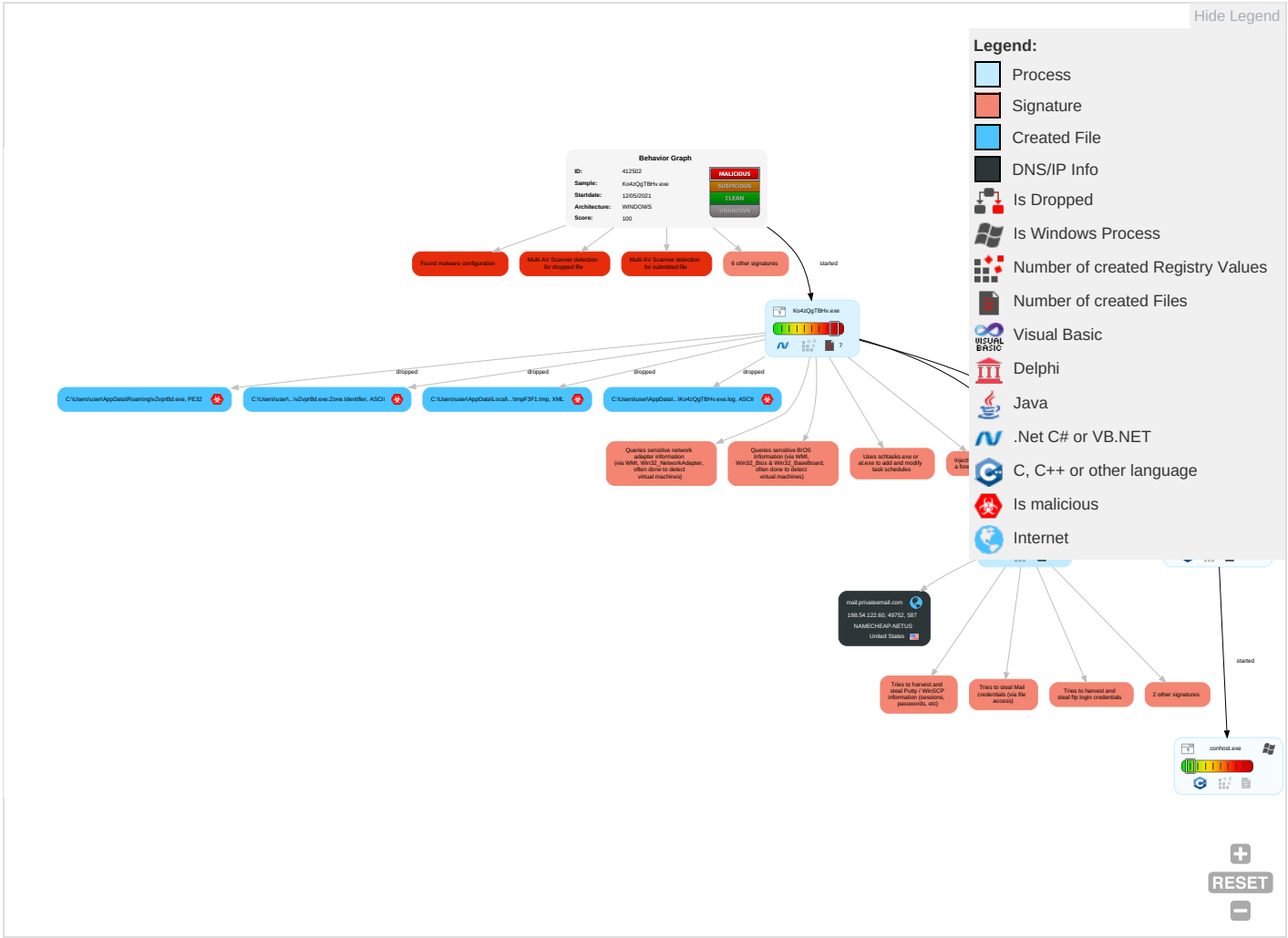
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Obfuscated Files or Information 3	Input Capture 1 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Software Packing 3	Credentials in Registry 1	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 2 1	SSH	Clipboard Data 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Virtualization/Sandbox Evasion 1 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscate Non-C2 Protocol

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
Ko4zQgTBHv.exe	22%	Virustotal		Browse
Ko4zQgTBHv.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
Ko4zQgTBHv.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\vZvprBd.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\vZvprBd.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.Ko4zQgTBHv.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	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://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://crt.sectigo.com/SectigoRSA	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.htmlk	0%	Avira URL Cloud	safe	
http://https://sectigo.c	0%	Avira URL Cloud	safe	
http://https://o3u5ap5OYRcXqxyqT.org8	0%	Avira URL Cloud	safe	
http://bplSZH.com	0%	Avira URL Cloud	safe	
http://https://o3u5ap5OYRcXqxyqT.org	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/hits/hit_index.php?k=1	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/E	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.html	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/report/reporter_index.php?name=	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/	0%	Avira URL Cloud	safe	
http://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://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

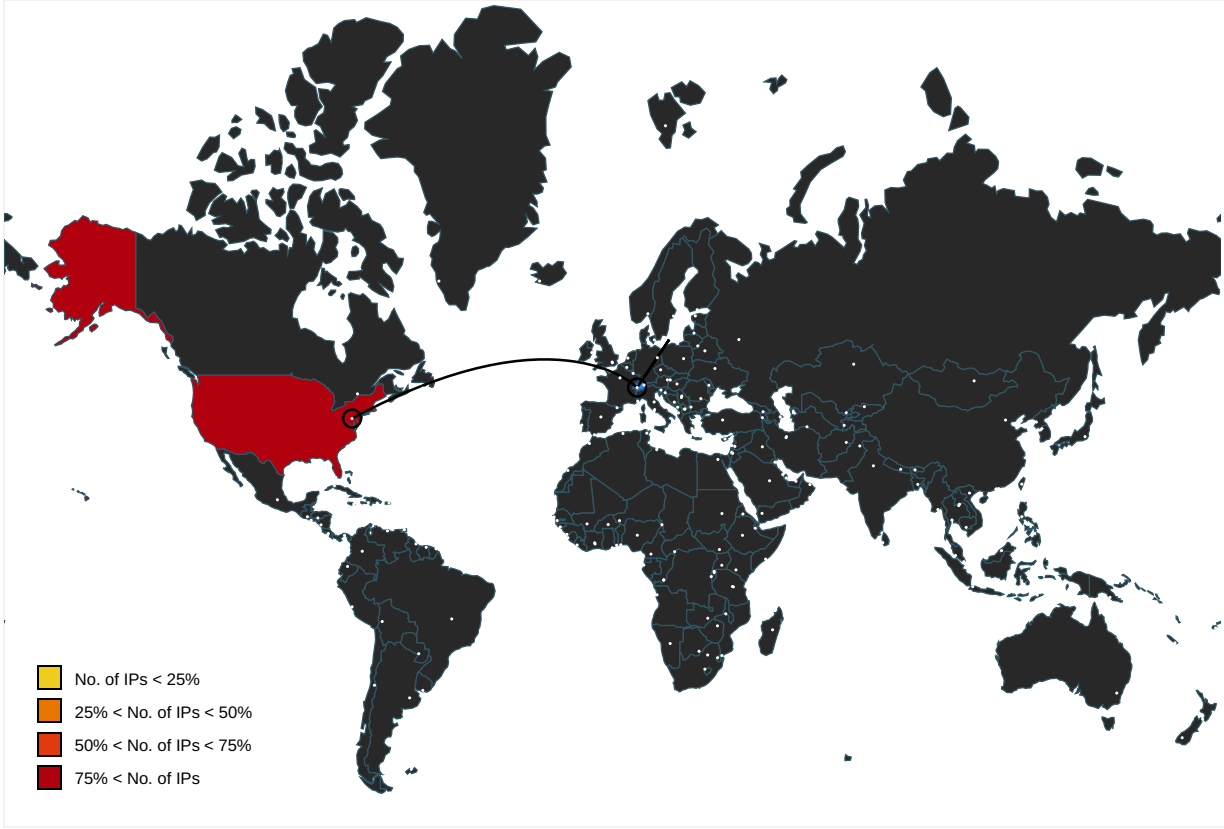
Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.privateemail.com	198.54.122.60	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	Ko4zQgTBHv.exe, 00000004.00000002.599388925.0000000006690000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	Ko4zQgTBHv.exe, 00000004.00000002.595056596.0000000002B01000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNS	Ko4zQgTBHv.exe, 00000004.00000002.595056596.0000000002B01000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	Ko4zQgTBHv.exe, 00000004.00000002.599388925.0000000006690000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	Ko4zQgTBHv.exe, 00000004.00000002.599388925.0000000006690000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Ko4zQgTBHv.exe, 00000004.00000002.595056596.0000000002B01000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSA	Ko4zQgTBHv.exe, 00000004.00000002.599388925.0000000006690000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.privateemail.com	Ko4zQgTBHv.exe, 00000004.00000002.596057980.0000000002C3C000.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/index_ru.htmlk	Ko4zQgTBHv.exe	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Ko4zQgTBHv.exe, 00000000.00000002.342175940.0000000002D4E000.00000004.00000001.sdmp	false		high
http://https://sectigo.c	Ko4zQgTBHv.exe, 00000004.00000002.599388925.0000000006690000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://o3u5ap5OYRcXqxyqT.org8	Ko4zQgTBHv.exe, 00000004.00000002.595643681.0000000002BB0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://bplSZH.com	Ko4zQgTBHv.exe, 00000004.00000002.595056596.0000000002B01000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://o3u5ap5OYRcXqxyqT.org	Ko4zQgTBHv.exe, 00000004.00000002.595643681.0000000002BB0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://checkip.dyndns.org/	Ko4zQgTBHv.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/hits/hit_index.php?k=1	Ko4zQgTBHv.exe	false	• Avira URL Cloud: safe	unknown
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC	Ko4zQgTBHv.exe	false		high
http://servermanager.miixit.org/E	Ko4zQgTBHv.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/index_ru.html	Ko4zQgTBHv.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/report/reporter_index.php?name=	Ko4zQgTBHv.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/	Ko4zQgTBHv.exe	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Ko4zQgTBHv.exe, 00000000.00000002.342093039.0000000002D01000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Ko4zQgTBHv.exe, 00000000.00000002.343072283.0000000003D01000.00000004.00000001.sdmp, Ko4zQgTBHv.exe, 00000004.00000002.591708318.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servermanager.miixit.org/downloads/	Ko4zQgTBHv.exe	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/hits/hit_index.php?k=	Ko4zQgTBHv.exe	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.122.60	mail.privateemail.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412502
Start date:	12.05.2021
Start time:	18:31:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ko4zQgTBHv.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/4@1/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 96% • 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 • Excluded IPs from analysis (whitelisted): 92.122.145.220, 13.88.21.125, 52.255.188.83, 131.253.33.200, 13.107.22.200, 20.49.157.6, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 2.20.143.16, 2.20.142.209, 20.82.210.154, 184.30.24.56 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.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, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, iris-de-ppe-azsc-uks.uksouth.cloudapp.azure.com, 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.

Simulations

Behavior and APIs

Time	Type	Description
18:32:11	API Interceptor	712x Sleep call for process: Ko4zQgTBHv.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.122.60	wed.doc	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ORDER CONFIRMATION.doc	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Packed2.43091.10004.exe	Get hash	malicious	Browse	
	6e5c05e1_by_Libranalysis.exe	Get hash	malicious	Browse	
	RFQ Plasma cutting machine.doc	Get hash	malicious	Browse	
	337840b9_by_Libranalysis.exe	Get hash	malicious	Browse	
	vy38Kw9qRh.exe	Get hash	malicious	Browse	
	ePj6KfzLBxh4vbe.exe	Get hash	malicious	Browse	
	zkXpISzeo3.exe	Get hash	malicious	Browse	
	yl9KgwwOXDZoGMw.exe	Get hash	malicious	Browse	
	8DL3LHg4SB6Q7z2.exe	Get hash	malicious	Browse	
	01217a79_by_Libranalysis.exe	Get hash	malicious	Browse	
	5iRqi4LmLF.exe	Get hash	malicious	Browse	
	6f37L7HNqo.exe	Get hash	malicious	Browse	
	IqRG5ZzYOH.exe	Get hash	malicious	Browse	
	PO 4302003683.doc	Get hash	malicious	Browse	
	Tender Overview 10052021.doc	Get hash	malicious	Browse	
	ORDER 10.05.doc	Get hash	malicious	Browse	
	purchase request.doc	Get hash	malicious	Browse	
	lBKwquZfBhdeO7D.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.privateemail.com	wed.doc	Get hash	malicious	Browse	• 198.54.122.60
	ORDER CONFIRMATION.doc	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Trojan.Packed2.43091.10004.exe	Get hash	malicious	Browse	• 198.54.122.60
	6e5c05e1_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	RFQ Plasma cutting machine.doc	Get hash	malicious	Browse	• 198.54.122.60
	337840b9_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	vy38Kw9qRh.exe	Get hash	malicious	Browse	• 198.54.122.60
	ePj6KfzLBxh4vbe.exe	Get hash	malicious	Browse	• 198.54.122.60
	zkXpISzeo3.exe	Get hash	malicious	Browse	• 198.54.122.60
	yl9KgwwOXDZoGMw.exe	Get hash	malicious	Browse	• 198.54.122.60
	8DL3LHg4SB6Q7z2.exe	Get hash	malicious	Browse	• 198.54.122.60
	01217a79_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	5iRqi4LmLF.exe	Get hash	malicious	Browse	• 198.54.122.60
	6f37L7HNqo.exe	Get hash	malicious	Browse	• 198.54.122.60
	IqRG5ZzYOH.exe	Get hash	malicious	Browse	• 198.54.122.60
	PO 4302003683.doc	Get hash	malicious	Browse	• 198.54.122.60
	Tender Overview 10052021.doc	Get hash	malicious	Browse	• 198.54.122.60
	ORDER 10.05.doc	Get hash	malicious	Browse	• 198.54.122.60
	purchase request.doc	Get hash	malicious	Browse	• 198.54.122.60
	New order.exe	Get hash	malicious	Browse	• 198.54.122.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	Purchase Order.exe	Get hash	malicious	Browse	• 198.54.126.165
	wed.doc	Get hash	malicious	Browse	• 198.54.122.60
	ORDER CONFIRMATION.doc	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Trojan.Packed2.43091.10004.exe	Get hash	malicious	Browse	• 198.54.122.60
	6e5c05e1_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	RFQ Plasma cutting machine.doc	Get hash	malicious	Browse	• 198.54.122.60
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 198.54.117.216
	main_setup_x86x64.exe	Get hash	malicious	Browse	• 162.255.11 9.164
	00098765123POIIU.exe	Get hash	malicious	Browse	• 199.192.23.253
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 185.61.154.27
	2021_May_Quotation_pdf.exe	Get hash	malicious	Browse	• 198.54.115.133
	337840b9_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	Citvonvhciktufwvyzyhistnewdjgsoqdr.exe	Get hash	malicious	Browse	• 198.54.117.212
	Updated Order list -804333.exe	Get hash	malicious	Browse	• 198.54.115.56
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	BELLOW FABRICATION Dwg.exe	Get hash	malicious	Browse	• 199.188.200.15

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	file.exe	Get hash	malicious	Browse	• 198.54.115.133
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 162.0.233.152
	vy38Kw9qRh.exe	Get hash	malicious	Browse	• 198.54.122.60
	copy of order 9119.xlsm	Get hash	malicious	Browse	• 162.0.233.152

JA3 Fingerprints

No context

Dropped Files

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

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Ko4zQgTBHv.exe.log	
Process:	C:\Users\user\Desktop\Ko4zQgTBHv.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..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,"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\tmpF3F1.tmp	
Process:	C:\Users\user\Desktop\Ko4zQgTBHv.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1652
Entropy (8bit):	5.156693657693423
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3vtn:cbha7JlNQV/rydbz9I3YODOLNdq3r
MD5:	9D4A23205956BC2E8DD228033AC5726E
SHA1:	7565F73DAB98820902B657E8C7DE52AAB948E3C7
SHA-256:	F12E060679B837A16C1F0D231F1B345125EE56C69858B4C9E44EDBBEF06EF4AD
SHA-512:	88F2BBFC08C1EC83DC5FF994995542D9C3752E2201C3557D20614CFF32DF100CFD3F90B358A877F8C2ED1F9EBD55ED83B4EA8A5A565726CA1D3221336C5BEFD
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>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\vZvprBd.exe	
Process:	C:\Users\user\Desktop\Ko4zQgTBHv.exe

C:\Users\user\AppData\Roaming\vZvprBd.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	971264
Entropy (8bit):	7.869815902345992
Encrypted:	false
SSDEEP:	12288:PYh5qL6Evo89A05qLcAwwhFsHF5xucMfz3fwXJ3CPBAEV4e1g5qLq:PY3I6jw9IcAyHFcfz3f8itCe1+Iq
MD5:	02BC365A934E558EB634E19DD2D33E64
SHA1:	A7FCB0381C4F68EBEA3DDA4508A789A23EB9F637
SHA-256:	BD97A138F3C0B9B078C119BCB59793CECA55120411C95635CC4D12C01406C2CD
SHA-512:	E261643D2BFEA93CE7A907D344F19AD995519F172DEE9E9F028DEDD8C9565CD92ACD53F571078B026C62FEF70F0561060CFA7A18800EEC2F833E4D84B057D02A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 34%
Joe Sandbox View:	• Filename: wed.doc, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....c.`.....P.....8.....6.... .....@.. ..... ..... ..@.....O.....4..... ..... ..H.....text...<.... ..... ..`.rsrc....4.....6.....@..@.reloc..... .....@..B.....H.....xr..<.....0.....(....(.....(.....o!....*.....("......(#.....($.....(%.....(&....*N..(....o....('....*&.. ((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0..<.....~.....(3.....,!r..p.....(4...o5...s6.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\vZvprBd.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Ko4zQgTBHv.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
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.869815902345992
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Ko4zQgTBHv.exe
File size:	971264
MD5:	02bc365a934e558eb634e19dd2d33e64
SHA1:	a7fcb0381c4f68ebea3dda4508a789a23eb9f637
SHA256:	bd97a138f3c0b9b078c119bcb59793ceca55120411c95635cc4d12c01406c2cd
SHA512:	e261643d2bfea93ce7a907d344f19ad995519f172dee9e9f028dedd8c9565cd92acd53f571078b026c62fef70f056106 0cfa7a18800eec2f833e4d84b057d02a
SSDEEP:	12288:PYh5qL6Evo89A05qLcAwwhFsHF5xucMfz3fwXJ3CPBAEV4e1g5qLq:PY3I6jw9IcAyHFcfz3f8itCe1+Iq

General

File Content Preview:	MZ......................@..!..L.!Th is program cannot be run in DOS mode....$.......PE..L.... c.`..............P......8......6.... ....@.. ....@................................

File Icon

	
Icon Hash:	f2d2e9fcc4ead362

Static PE Info

General

Entrypoint:	0x4eb636
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609B63E3 [Wed May 12 05:13:07 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 [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xeb5e4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xec000	0x34d4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xeb4ac	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe963c	0xe9800	False	0.909726520677	data	7.89033690485	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xec000	0x34d4	0x3600	False	0.361689814815	data	5.25516289643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xec100	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	0xee6b8	0x14	data		
RT_VERSION	0xee6dc	0x37c	data		
RT_MANIFEST	0xeea68	0xa65	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

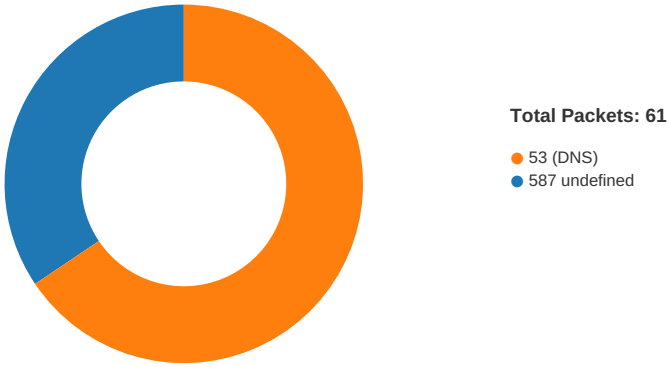
Version Infos

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

Description	Data
OriginalFilename	ScopelessEnumAttribute.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:33:57.590287924 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:57.782218933 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:57.782362938 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:57.973872900 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:57.974586010 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:58.164808035 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:58.165076017 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:58.169214010 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:58.359529018 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:58.402468920 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:58.430995941 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:58.622334957 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:58.623831987 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:58.623858929 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:58.623883009 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:58.623905897 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:58.624061108 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:58.624207973 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:58.675378084 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:58.865664005 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:58.866667986 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:58.918052912 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:59.144306898 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:59.334512949 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:59.336196899 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:59.341310024 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:59.531418085 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:59.534073114 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:59.535981894 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:59.728559971 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:59.731681108 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:59.732639074 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:33:59.922954082 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:59.925484896 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:33:59.926291943 CEST	49752	587	192.168.2.6	198.54.122.60

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:34:00.116590023 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:34:00.157192945 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:34:00.158485889 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:34:00.348891020 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:34:00.349466085 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:34:00.352077007 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:34:00.352103949 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:34:00.353277922 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:34:00.353303909 CEST	49752	587	192.168.2.6	198.54.122.60
May 12, 2021 18:34:00.542407036 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:34:00.542478085 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:34:00.544215918 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:34:00.632358074 CEST	587	49752	198.54.122.60	192.168.2.6
May 12, 2021 18:34:00.683339119 CEST	49752	587	192.168.2.6	198.54.122.60

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:32:01.505918980 CEST	54513	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:01.567689896 CEST	53	54513	8.8.8.8	192.168.2.6
May 12, 2021 18:32:01.654706001 CEST	62044	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:01.708113909 CEST	53	62044	8.8.8.8	192.168.2.6
May 12, 2021 18:32:02.769505978 CEST	63791	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:02.831269979 CEST	53	63791	8.8.8.8	192.168.2.6
May 12, 2021 18:32:03.903897047 CEST	64267	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:03.955429077 CEST	53	64267	8.8.8.8	192.168.2.6
May 12, 2021 18:32:05.422872066 CEST	49448	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:05.471720934 CEST	53	49448	8.8.8.8	192.168.2.6
May 12, 2021 18:32:06.750407934 CEST	60342	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:06.799278021 CEST	53	60342	8.8.8.8	192.168.2.6
May 12, 2021 18:32:07.854561090 CEST	61346	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:07.903265953 CEST	53	61346	8.8.8.8	192.168.2.6
May 12, 2021 18:32:08.032258987 CEST	51774	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:08.102324009 CEST	53	51774	8.8.8.8	192.168.2.6
May 12, 2021 18:32:08.895251036 CEST	56023	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:08.946938038 CEST	53	56023	8.8.8.8	192.168.2.6
May 12, 2021 18:32:10.643033981 CEST	58384	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:10.693039894 CEST	53	58384	8.8.8.8	192.168.2.6
May 12, 2021 18:32:12.426206112 CEST	60261	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:12.476443052 CEST	53	60261	8.8.8.8	192.168.2.6
May 12, 2021 18:32:13.700006008 CEST	56061	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:13.751530886 CEST	53	56061	8.8.8.8	192.168.2.6
May 12, 2021 18:32:14.812074900 CEST	58336	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:14.860830069 CEST	53	58336	8.8.8.8	192.168.2.6
May 12, 2021 18:32:16.004043102 CEST	53781	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:16.052792072 CEST	53	53781	8.8.8.8	192.168.2.6
May 12, 2021 18:32:17.855899096 CEST	54064	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:17.907633066 CEST	53	54064	8.8.8.8	192.168.2.6
May 12, 2021 18:32:18.961852074 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:19.010551929 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 18:32:20.196566105 CEST	55299	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:20.245496988 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 18:32:21.418642044 CEST	63745	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:21.471422911 CEST	53	63745	8.8.8.8	192.168.2.6
May 12, 2021 18:32:22.550496101 CEST	50055	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:22.602402925 CEST	53	50055	8.8.8.8	192.168.2.6
May 12, 2021 18:32:35.321342945 CEST	61374	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:35.395571947 CEST	53	61374	8.8.8.8	192.168.2.6
May 12, 2021 18:32:39.164099932 CEST	50339	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:39.225599051 CEST	53	50339	8.8.8.8	192.168.2.6
May 12, 2021 18:32:54.132843971 CEST	63307	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:54.192929029 CEST	53	63307	8.8.8.8	192.168.2.6
May 12, 2021 18:32:54.744596958 CEST	49694	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:54.795043945 CEST	53	49694	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:32:55.451318026 CEST	54982	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:55.500478029 CEST	53	54982	8.8.8.8	192.168.2.6
May 12, 2021 18:32:55.809406042 CEST	50010	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:55.882838964 CEST	53	50010	8.8.8.8	192.168.2.6
May 12, 2021 18:32:55.922677994 CEST	63718	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:55.984842062 CEST	53	63718	8.8.8.8	192.168.2.6
May 12, 2021 18:32:56.285636902 CEST	62116	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:56.347177029 CEST	53	62116	8.8.8.8	192.168.2.6
May 12, 2021 18:32:56.502953053 CEST	63816	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:56.551727057 CEST	53	63816	8.8.8.8	192.168.2.6
May 12, 2021 18:32:57.149645090 CEST	55014	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:57.201231003 CEST	53	55014	8.8.8.8	192.168.2.6
May 12, 2021 18:32:57.670654058 CEST	62208	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:57.729873896 CEST	53	62208	8.8.8.8	192.168.2.6
May 12, 2021 18:32:58.704262972 CEST	57574	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:58.763200998 CEST	53	57574	8.8.8.8	192.168.2.6
May 12, 2021 18:32:59.693232059 CEST	51818	53	192.168.2.6	8.8.8.8
May 12, 2021 18:32:59.750224113 CEST	53	51818	8.8.8.8	192.168.2.6
May 12, 2021 18:33:00.341689110 CEST	56628	53	192.168.2.6	8.8.8.8
May 12, 2021 18:33:00.390507936 CEST	53	56628	8.8.8.8	192.168.2.6
May 12, 2021 18:33:09.605097055 CEST	60778	53	192.168.2.6	8.8.8.8
May 12, 2021 18:33:09.677778959 CEST	53	60778	8.8.8.8	192.168.2.6
May 12, 2021 18:33:10.886634111 CEST	53799	53	192.168.2.6	8.8.8.8
May 12, 2021 18:33:10.946465015 CEST	53	53799	8.8.8.8	192.168.2.6
May 12, 2021 18:33:12.776998997 CEST	54683	53	192.168.2.6	8.8.8.8
May 12, 2021 18:33:12.836379051 CEST	53	54683	8.8.8.8	192.168.2.6
May 12, 2021 18:33:39.965634108 CEST	59329	53	192.168.2.6	8.8.8.8
May 12, 2021 18:33:40.040384054 CEST	53	59329	8.8.8.8	192.168.2.6
May 12, 2021 18:33:44.842503071 CEST	64021	53	192.168.2.6	8.8.8.8
May 12, 2021 18:33:44.916666985 CEST	53	64021	8.8.8.8	192.168.2.6
May 12, 2021 18:33:46.437069893 CEST	56129	53	192.168.2.6	8.8.8.8
May 12, 2021 18:33:46.505568027 CEST	53	56129	8.8.8.8	192.168.2.6
May 12, 2021 18:33:57.399168015 CEST	58177	53	192.168.2.6	8.8.8.8
May 12, 2021 18:33:57.461641073 CEST	53	58177	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 18:33:57.399168015 CEST	192.168.2.6	8.8.8.8	0x7f74	Standard query (0)	mail.privateemail.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 18:33:57.461641073 CEST	8.8.8.8	192.168.2.6	0x7f74	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)

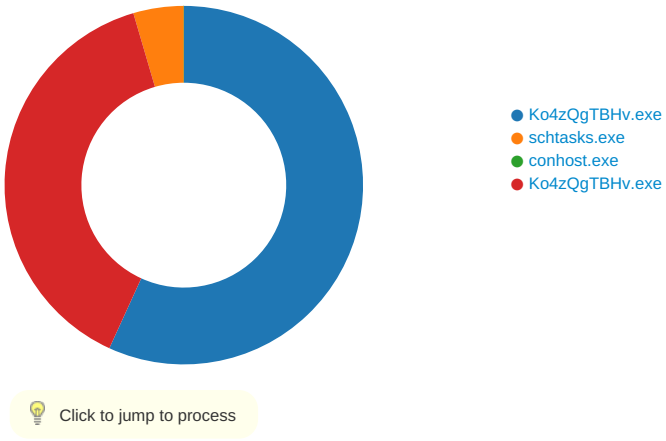
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 18:33:57.973872900 CEST	587	49752	198.54.122.60	192.168.2.6	220 PrivateEmail.com Mail Node
May 12, 2021 18:33:57.974586010 CEST	49752	587	192.168.2.6	198.54.122.60	EHLO 088753
May 12, 2021 18:33:58.165076017 CEST	587	49752	198.54.122.60	192.168.2.6	250-MTA-09.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 STARTTLS
May 12, 2021 18:33:58.169214010 CEST	49752	587	192.168.2.6	198.54.122.60	STARTTLS
May 12, 2021 18:33:58.359529018 CEST	587	49752	198.54.122.60	192.168.2.6	220 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Ko4zQgTBHv.exe PID: 6484 Parent PID: 5876

General

Start time:	18:32:09
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Ko4zQgTBHv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Ko4zQgTBHv.exe'
Imagebase:	0x800000
File size:	971264 bytes
MD5 hash:	02BC365A934E558EB634E19DD2D33E64
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.342175940.0000000002D4E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.343072283.0000000003D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.343072283.0000000003D01000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6E0CCF06	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	6E0CCF06	unknown
C:\Users\user\AppData\Roaming\vZvprBd.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	6CF1DD66	CopyFileW
C:\Users\user\AppData\Roaming\vZvprBd.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CF1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF3F1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF17038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Ko4zQgTBHv.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF3F1.tmp	success or wait	1	6CF16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\vZvprBd.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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 e3 63 9b 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 98 0e 00 00 38 00 00 00 00 00 00 36 b6 0e 00 00 20 00 00 00 c0 0e 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 20 0f 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....c.`.......... ....P......8......6.... ....@.. ....@.................	success or wait	4	6CF1DD66	CopyFileW
C:\Users\user\AppData\Roaming\vZvprBd.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	6CF1DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF3F1.tmp	unknown	1652	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 65 6e 67 69 6e 65 65 72 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	<?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>.. </Registratio	success or wait	1	6CF11B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Ko4zQgTBHv.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 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 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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..3,"System, Version=4.	success or wait	1	6E3DC907	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	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile

Analysis Process: schtasks.exe PID: 6660 Parent PID: 6484

General

Start time:	18:32:13
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\vZvprBd' /XML 'C:\Users\ user\AppData\Local\Temp\tmpF3F1.tmp'
Imagebase:	0x340000
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\tmpF3F1.tmp	unknown	2	success or wait	1	34AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF3F1.tmp	unknown	1653	success or wait	1	34ABD9	ReadFile

Analysis Process: conhost.exe PID: 6668 Parent PID: 6660

General

Start time:	18:32:14
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: Ko4zQgTBHv.exe PID: 6704 Parent PID: 6484

General

Start time:	18:32:14
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Ko4zQgTBHv.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Ko4zQgTBHv.exe
Imagebase:	0x6c0000
File size:	971264 bytes
MD5 hash:	02BC365A934E558EB634E19DD2D33E64
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: 00000004.00000002.591708318.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.591708318.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.595056596.0000000002B01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.595056596.0000000002B01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.595643681.0000000002BB0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.595643681.0000000002BB0000.00000004.00000001.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	6E0CCF06	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	6E0CCF06	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	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF11B4F	ReadFile

Disassembly

Code Analysis