ID: 382018
Sample Name: BnJvVt951o
Cookbook: default.jbs
Time: 18:47:44
Date: 05/04/2021
Version: 31.0.0 Emerald

Table of Contents

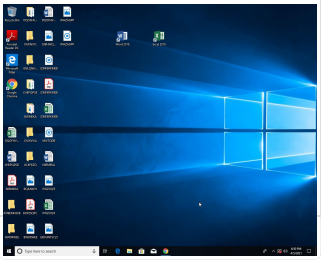
Analysis Report BnJvVt951o

Overview

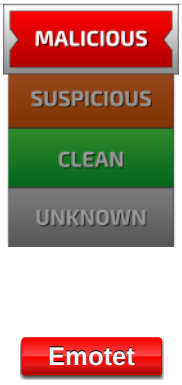
General Information

Sample Name:	BnJvVt951o (renamed file extension from none to exe)
Analysis ID:	382018
MD5:	ae03a6f8fb74d40..
SHA1:	6ee320cedc7749..
SHA256:	1ad1ff05930f27e…
Infos:	

Most interesting Screenshot:



Detection

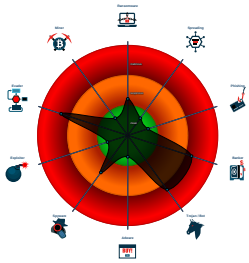


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected Emotet e-Banking trojan
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Drops executables to the windows d…
- Found evasive API chain (may stop…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- Antivirus or Machine Learning detec…
- Contains capabilities to detect virtua…
- Contains functionality to check if a w…

Classification



Startup

- **System is w10x64**
- BnJvVt951o.exe (PID: 7136 cmdline: 'C:\Users\user\Desktop\BnJvVt951o.exe' MD5: AE03A6F8FB74D401B403647D28E21574)
  - BnJvVt951o.exe (PID: 1572 cmdline: --132eeff2 MD5: AE03A6F8FB74D401B403647D28E21574)
- svchost.exe (PID: 6228 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- browserdialog.exe (PID: 4528 cmdline: C:\Windows\SysWOW64\browserdialog.exe MD5: AE03A6F8FB74D401B403647D28E21574)
  - browserdialog.exe (PID: 5168 cmdline: --39eda026 MD5: AE03A6F8FB74D401B403647D28E21574)
- svchost.exe (PID: 6484 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6864 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6868 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.903155910.0000000000540000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000004.00000002.903155910.0000000000540000.00000040.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0x18ec:$snippet2: 6A 13 68 01 00 01 00 FF 15 48 FA 40 00 85 C0 • 0x5a13:$snippet6: 33 C0 21 05 EC 10 41 00 A3 E8 10 41 00 39 05 A0 E3 40 00 74 18 40 A3 E8 10 41 00 83 3C C5 A0 E3 ...
00000001.00000002.655860929.0000000002380000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000002.655860929.0000000002380000.00000040.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0x18ec:$snippet2: 6A 13 68 01 00 01 00 FF 15 48 FA 40 00 85 C0 • 0x5a13:$snippet6: 33 C0 21 05 EC 10 41 00 A3 E8 10 41 00 39 05 A0 E3 40 00 74 18 40 A3 E8 10 41 00 83 3C C5 A0 E3 ...

Source	Rule	Description	Author	Strings
00000000.00000002.635756418.0000000002390000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

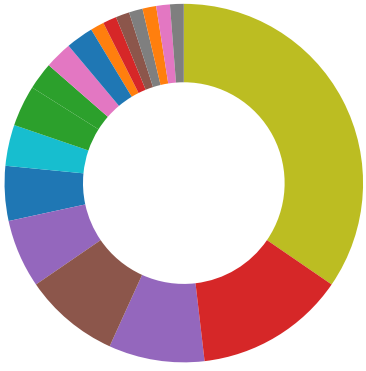
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.browserdialog.exe.54053f.1.raw.unpack	MAL_Emotet_Jan20_1	Detects Emotet malware	Florian Roth	• 0x3177:$op1: 03 FE 66 39 07 0F 85 2A FF FF FF 8B 4D F0 6A 20 • 0x315d:$op2: 8B 7D FC 0F 85 49 FF FF FF 85 DB 0F 84 D1
4.2.browserdialog.exe.54053f.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.browserdialog.exe.54053f.1.raw.unpack	Emotet	Emotet Payload	kevoreilly	• 0x13ad:$snippet2: 6A 13 68 01 00 01 00 FF 15 48 FA 40 00 85 C0 • 0x54d4:$snippet6: 33 C0 21 05 EC 10 41 00 A3 E8 10 41 00 39 05 A0 E3 40 00 74 18 40 A3 E8 10 41 00 83 3C C5 A0 E3 ...
4.2.browserdialog.exe.54053f.1.raw.unpack	Win32_Trojan_Emotet	unknown	ReversingLabs	• 0xe52:$decrypt_resource_v1: 55 8B EC 83 EC 18 53 8B D9 8B C2 56 57 89 45 F0 8B 3B 33 F8 8B C7 89 7D EC 83 E0 03 75 05 8D 77 ... • 0xb23e:$generate_filename_v1: 56 57 33 C0 BF 08 16 41 00 57 50 50 6A 1C 50 FF 15 68 04 41 00 BA 9A DB 40 5A B9 60 EE 40 00 E8 ...
1.2.BnJvVt951o.exe.238053f.1.unpack	MAL_Emotet_Jan20_1	Detects Emotet malware	Florian Roth	• 0x2577:$op1: 03 FE 66 39 07 0F 85 2A FF FF FF 8B 4D F0 6A 20 • 0x255d:$op2: 8B 7D FC 0F 85 49 FF FF FF 85 DB 0F 84 D1
Click to see the 23 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

E-Banking Fraud:

Detected Emotet e-Banking trojan

Yara detected Emotet

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Drops executables to the windows directory (C:\Windows) and starts them

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Found evasive API chain (may stop execution after checking mutex)

Stealing of Sensitive Information:

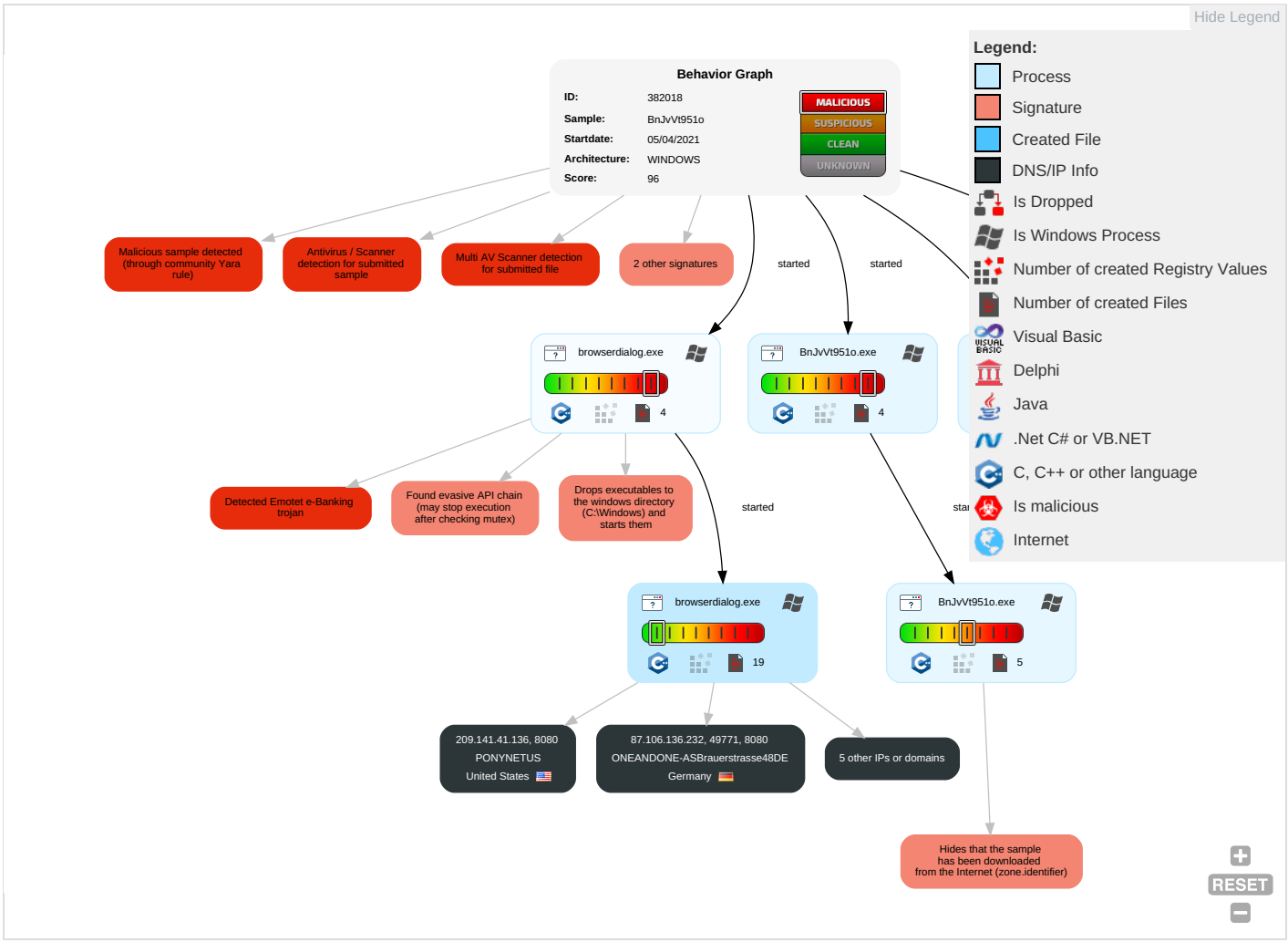
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts 1	Native API 1 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress To Transfer 1
Default Accounts	Service Execution 1 2	Windows Service 1 2	Access Token Manipulation 1	Obfuscated Files or Information 2	LSASS Memory	System Service Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 2
Domain Accounts	At (Linux)	Logon Script (Windows)	Windows Service 1 2	Software Packing 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Stand Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 1	File Deletion 1	NTDS	System Information Discovery 3 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 2 1	LSA Secrets	Security Software Discovery 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Process Discovery 2	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	Virtualization/Sandbox Evasion 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transf Protocols

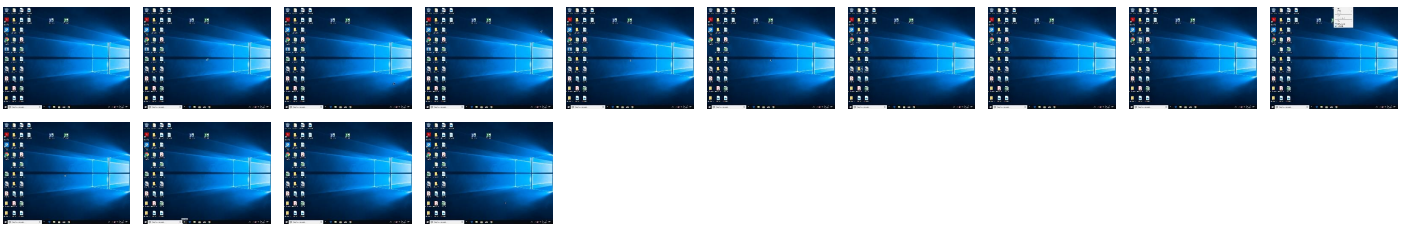
Behavior Graph



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
BnJvVt951o.exe	84%	Virustotal		Browse
BnJvVt951o.exe	96%	ReversingLabs	Win32.Trojan.Emotet	
BnJvVt951o.exe	100%	Avira	HEUR/AGEN.1111753	
BnJvVt951o.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.BnJvVt951o.exe.238053f.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.BnJvVt951o.exe.239053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.2.browserdialog.exe.62053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.BnJvVt951o.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
1.0.BnJvVt951o.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
0.0.BnJvVt951o.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
4.2.browserdialog.exe.54053f.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.0.browserdialog.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
3.2.browserdialog.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.BnJvVt951o.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
4.2.browserdialog.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
3.0.browserdialog.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://178.210.51.222/enabled/guids/free/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

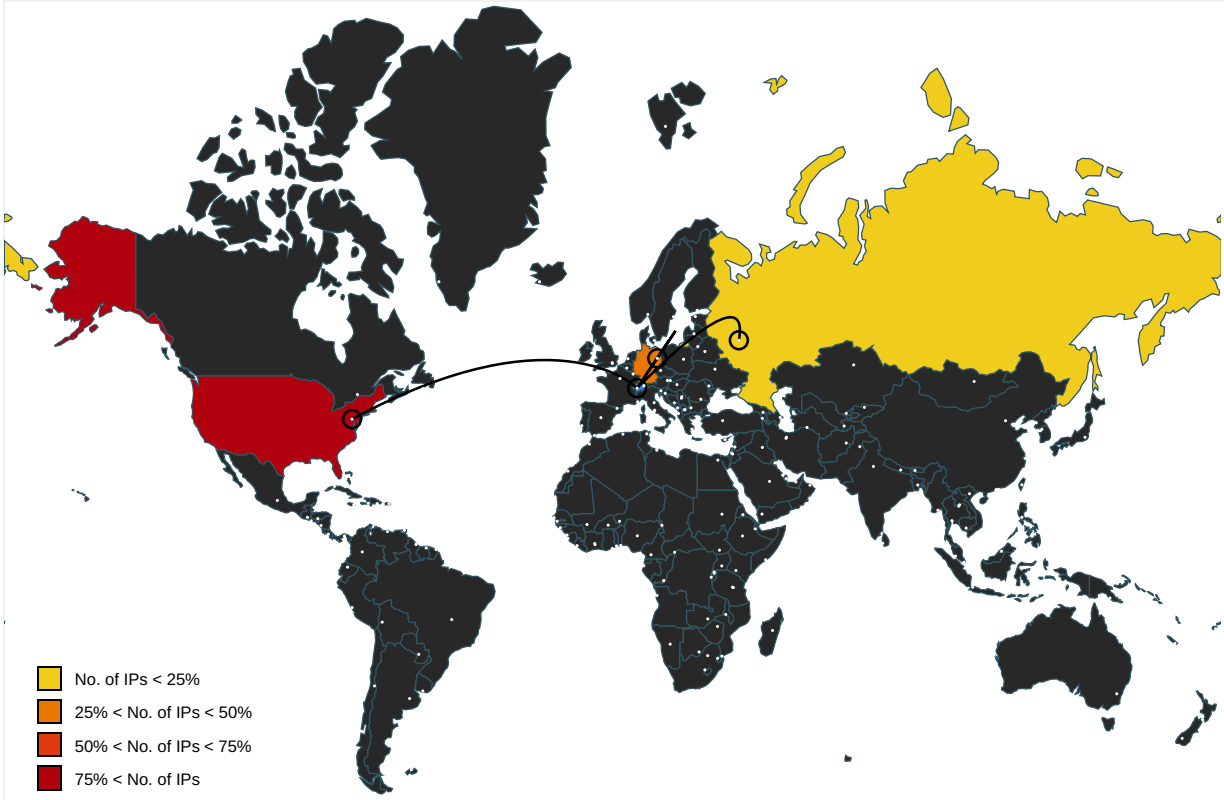
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.hulu.com/privacy	svchost.exe, 0000000B.00000003.727125544.0000025004155000.00000004.00000001.sdmp	false		high
http://www.g5e.com/G5_End_User_License_Supplemental_Terms	svchost.exe, 0000000B.00000003.728117612.000002500417A000.00000004.00000001.sdmp, svchost.exe, 0000000B.00000003.728325297.000002500419A000.00000004.00000001.sdmp	false		high
http://https://www.hulu.com/do-not-sell-my-info	svchost.exe, 0000000B.00000003.727125544.0000025004155000.00000004.00000001.sdmp	false		high
http://178.210.51.222/enabled/guids/free/	browserdialog.exe, 00000004.00000002.902979540.0000000000199000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hulu.com/terms	svchost.exe, 0000000B.00000003.727125544.0000025004155000.00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/contact/	svchost.exe, 0000000B.00000003.735526851.0000025004193000.00000004.00000001.sdmp, svchost.exe, 0000000B.00000003.735603672.0000025004177000.00000004.00000001.sdmp	false		high
http://https://www.roblox.com/develop	svchost.exe, 0000000B.00000003.735526851.0000025004193000.00000004.00000001.sdmp, svchost.exe, 0000000B.00000003.735603672.0000025004177000.00000004.00000001.sdmp	false		high
http://https://instagram.com/hiddencity_	svchost.exe, 0000000B.00000003.728117612.000002500417A000.00000004.00000001.sdmp, svchost.exe, 0000000B.00000003.728325297.000002500419A000.00000004.00000001.sdmp	false		high
http://https://www.roblox.com/info/privacy	svchost.exe, 0000000B.00000003.735526851.0000025004193000.00000004.00000001.sdmp, svchost.exe, 0000000B.00000003.735603672.0000025004177000.00000004.00000001.sdmp	false		high
http://www.g5e.com/termsofservice	svchost.exe, 0000000B.00000003.728117612.000002500417A000.00000004.00000001.sdmp, svchost.exe, 0000000B.00000003.728325297.000002500419A000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://en.help.roblox.com/hc/en-us	svchost.exe, 0000000B.00000003.735526851.0000025004193000.00000004.00000001.sdmp, svchost.exe, 0000000B.00000003.735603672.0000025004177000.00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/parents/	svchost.exe, 0000000B.00000003.735526851.0000025004193000.00000004.00000001.sdmp, svchost.exe, 0000000B.00000003.735603672.0000025004177000.00000004.00000001.sdmp, svchost.exe, 0000000B.00000003.735589105.0000025004166000.00000004.00000001.sdmp	false		high
http://https://www.hulu.com/ca-privacy-rights	svchost.exe, 0000000B.00000003.727125544.0000025004155000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
152.89.236.214	unknown	Germany		31400	ACCELERATED-ITDE	false
198.199.114.69	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
104.236.246.93	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
178.210.51.222	unknown	Russian Federation		43727	KVANT-TELECOMRU	false
45.33.54.74	unknown	United States		63949	LINODE-APLinodeLLCUS	false
209.141.41.136	unknown	United States		53667	PONYNETUS	false
87.106.136.232	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382018

Start date:	05.04.2021
Start time:	18:47:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BnJvVt951o (renamed file extension from none to 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:	19
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:	mal96.bank.troj.evad.winEXE@10/0@0/7
EGA Information:	• Successful, ratio: 33.3%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 91.1% • Quality standard deviation: 6.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 40.88.32.150, 52.255.188.83, 104.43.193.48, 20.82.210.154, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:49:08	API Interceptor	10x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
152.89.236.214	aEdlObiYav.exe	Get hash	malicious	Browse	
198.199.114.69	VYHauUUCLr.exe	Get hash	malicious	Browse	• 198.199.114.69:8080/badge/report/xian/
	http://infraturkey.com/deletecomment/parts_service/daaMnHeDzR/	Get hash	malicious	Browse	• 198.199.114.69:8080/jit/
	http://https://newwell.studio/test/DOC/NtnDpOmWbTdPEdBxrLyy/	Get hash	malicious	Browse	• 198.199.114.69:8080/json/
104.236.246.93	form.doc	Get hash	malicious	Browse	• 104.236.246.93:8080/hZhNeaDm/dcUDNcyqQW/niVKRU29uscA3Ju/
	UAr7Xz5JWr.exe	Get hash	malicious	Browse	• 104.236.246.93:8080/ZxZomdMT6G9XK/ghoypfynUN/
	invoice #865119.doc	Get hash	malicious	Browse	• 104.236.246.93:8080/XzlcYaBSUK0cswU/pzKYcLCk/PbvwO3hXkaN7W/WM9ZNIP/
	XY8707573112TQ.doc	Get hash	malicious	Browse	• 104.236.246.93:8080/att30xZ/YONUKbuNJ8IOQjL/G34JI8e3LEFl/jaWgrB/
	test-emotet.exe	Get hash	malicious	Browse	• 104.236.246.93/
178.210.51.222	SMtbg7yHyR.exe	Get hash	malicious	Browse	
	aEdlObiYav.exe	Get hash	malicious	Browse	
45.33.54.74	FA_36802305641_Oct2019.doc	Get hash	malicious	Browse	• 45.33.54.74:443/loadan/stubs/
209.141.41.136	SMtbg7yHyR.exe	Get hash	malicious	Browse	
	aEdlObiYav.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ACCELERATED-ITDE	SMtbg7yHyR.exe	Get hash	malicious	Browse	• 152.89.236.214
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	• 185.243.114.196
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 185.243.114.196
	document-1048628209.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1771131239.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1370071295.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69564892.xls	Get hash	malicious	Browse	• 185.243.114.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1320073816.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-184653858.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1729033050.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-540475316.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1456634656.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1376447212.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1813856412.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1776123548.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-684762271.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1590815978.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-66411652.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-415601328.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69633738.xls	Get hash	malicious	Browse	• 185.243.114.196
DIGITALOCEAN-ASNUS	0M53tHsUDg.dll	Get hash	malicious	Browse	• 161.35.99.181
	Sample.doc	Get hash	malicious	Browse	• 159.65.129.33
	Sample.doc	Get hash	malicious	Browse	• 159.65.129.33
	SMtbg7yHyR.exe	Get hash	malicious	Browse	• 104.236.246.93
	TW#9898748948-TZE.exe	Get hash	malicious	Browse	• 162.243.129.169
	xqtEOiEeHh.exe	Get hash	malicious	Browse	• 159.89.4.33
	5AKljISD4v.exe	Get hash	malicious	Browse	• 206.189.80.59
	nnrlOwKZlc.exe	Get hash	malicious	Browse	• 104.248.119.44
	documents-575751901.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	MIpyc881Ka.dll	Get hash	malicious	Browse	• 138.197.197.35
	278.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	1449.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	documents-1987093434.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	1737.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	492.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	3205.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	1984.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	2503.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	3032.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	937.xlsm	Get hash	malicious	Browse	• 138.197.197.35
DIGITALOCEAN-ASNUS	0M53tHsUDg.dll	Get hash	malicious	Browse	• 161.35.99.181
	Sample.doc	Get hash	malicious	Browse	• 159.65.129.33
	Sample.doc	Get hash	malicious	Browse	• 159.65.129.33
	SMtbg7yHyR.exe	Get hash	malicious	Browse	• 104.236.246.93
	TW#9898748948-TZE.exe	Get hash	malicious	Browse	• 162.243.129.169
	xqtEOiEeHh.exe	Get hash	malicious	Browse	• 159.89.4.33
	5AKljISD4v.exe	Get hash	malicious	Browse	• 206.189.80.59
	nnrlOwKZlc.exe	Get hash	malicious	Browse	• 104.248.119.44
	documents-575751901.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	MIpyc881Ka.dll	Get hash	malicious	Browse	• 138.197.197.35
	278.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	1449.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	documents-1987093434.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	1737.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	492.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	3205.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	1984.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	2503.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	3032.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	937.xlsm	Get hash	malicious	Browse	• 138.197.197.35

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.625638741868008
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	BnJvVt951o.exe
File size:	516346
MD5:	ae03a6f8fb74d401b403647d28e21574
SHA1:	6ee320cedc77499f5df9ae9c93ef42c0d91f3ce8
SHA256:	1ad1ff05930f27ef4b349c7a612235d1632ef7ceaa1a17adf7c7b3a97b40ca4d
SHA512:	ab2a30d32722419c72808032ae01b9443bfb8ea80ec52426aeb42ac21a84f0a2b04dd6f311c13b06bcaa37b7874b4e311ff8dc0c94ccfa42cbf6dcac0e2facab
SSDEEP:	6144:PebeJq15KNVIjux9tE9dVyAhwoajYPNo4ahRFPhpxOtYS0xefNPf+R6axxVccVPo:W5KNgux9t0VyAShUPCRdUi8cVRPw17i
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*1..Db..Db..Dbd..b..Db..]b..Db...b..Db..Kb..Db...ba.Db..cb..Dbd..b..Db..Eb..Db..$b..Db...b..Db...b..Db...b..DbRich..Db.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x419b95
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5D9A0326 [Sun Oct 6 15:07:18 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	92bdfd5dfdc574760c27f87d6f10fe98

Entrypoint Preview

Instruction
push 00000060h
push 0045C7A8h
call 00007F57B8F6A130h
mov edi, 00000094h
mov eax, edi
call 00007F57B8F6A288h
mov dword ptr [ebp-18h], esp
mov esi, esp
mov dword ptr [esi], edi
push esi
call dword ptr [004552A0h]
mov ecx, dword ptr [esi+10h]
mov dword ptr [0047B960h], ecx
mov eax, dword ptr [esi+04h]
mov dword ptr [0047B96Ch], eax
mov edx, dword ptr [esi+08h]
mov dword ptr [0047B970h], edx
mov esi, dword ptr [esi+0Ch]
and esi, 00007FFFh
mov dword ptr [0047B964h], esi
cmp ecx, 02h
je 00007F57B8F6AA9Eh
or esi, 00008000h
mov dword ptr [0047B964h], esi
shl eax, 08h
add eax, edx
mov dword ptr [0047B968h], eax
xor esi, esi
push esi
mov edi, dword ptr [00455320h]
call edi
cmp word ptr [eax], 5A4Dh
jne 00007F57B8F6AAB1h
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
cmp dword ptr [ecx], 00004550h
jne 00007F57B8F6AAA4h
movzx eax, word ptr [ecx+18h]
cmp eax, 0000010Bh
je 00007F57B8F6AAB1h
cmp eax, 0000020Bh
je 00007F57B8F6AA97h
mov dword ptr [ebp-1Ch], esi
jmp 00007F57B8F6AAB9h
cmp dword ptr [ecx+00000084h], 0Eh
jbe 00007F57B8F6AA84h
xor eax, eax
cmp dword ptr [ecx+000000F8h], esi
jmp 00007F57B8F6AAA0h
cmp dword ptr [ecx+74h], 0Eh
jbe 00007F57B8F6AA74h
xor eax, eax
cmp dword ptr [ecx+000000E8h], esi
setne al
mov dword ptr [ebp-1Ch], eax

Rich Headers

Programming Language:	• [ASM] VS2003 (.NET) build 3077 • [LNK] VS2003 (.NET) build 3077 • [RES] VS2003 (.NET) build 3077 • [EXP] VS2003 (.NET) build 3077 • [C++] VS2003 (.NET) build 3077 • [C] VS2003 (.NET) build 3077

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x68cf0	0x53	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x66224	0x104	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7e000	0x3ebc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x55880	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x60ed0	0x48	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x55000	0x878	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x66174	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x53ee9	0x54000	False	0.505048479353	DOS executable (COM)	6.50788658927	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x55000	0x13d43	0x14000	False	0.315026855469	data	5.20395932053	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x69000	0x14234	0x11000	False	0.795568129596	data	7.54511629913	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x3ebc	0x4000	False	0.259643554688	data	3.45842321085	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x7eb68	0x134	data	English	United States
RT_CURSOR	0x7ec9c	0xb4	data	English	United States
RT_CURSOR	0x7ed50	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x7ee84	0x134	data	English	United States
RT_CURSOR	0x7efb8	0x134	data	English	United States
RT_CURSOR	0x7f0ec	0x134	data	English	United States
RT_CURSOR	0x7f220	0x134	data	English	United States
RT_CURSOR	0x7f354	0x134	data	English	United States
RT_CURSOR	0x7f488	0x134	data	English	United States
RT_CURSOR	0x7f5bc	0x134	data	English	United States
RT_CURSOR	0x7f6f0	0x134	data	English	United States
RT_CURSOR	0x7f824	0x134	data	English	United States
RT_CURSOR	0x7f958	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x7fa8c	0x134	data	English	United States
RT_CURSOR	0x7fbc0	0x134	data	English	United States
RT_CURSOR	0x7fcf4	0x134	data	English	United States
RT_BITMAP	0x7fe28	0xb8	data	English	United States
RT_BITMAP	0x7fee0	0x144	data	English	United States
RT_DIALOG	0x80024	0x184	data	English	United States
RT_DIALOG	0x801a8	0xf4	data	English	United States
RT_DIALOG	0x8029c	0x100	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x8039c	0xe8	data	English	United States
RT_STRING	0x80484	0x44	data	English	United States
RT_STRING	0x804c8	0x48	data	English	United States
RT_STRING	0x80510	0x2c	data	English	United States
RT_STRING	0x8053c	0x38	data	English	United States
RT_STRING	0x80574	0x48	data	English	United States
RT_STRING	0x805bc	0x64	data	English	United States
RT_STRING	0x80620	0x46	data	English	United States
RT_STRING	0x80668	0x82	data	English	United States
RT_STRING	0x806ec	0x2a	data	English	United States
RT_STRING	0x80718	0x192	data	English	United States
RT_STRING	0x808ac	0x4e2	data	English	United States
RT_STRING	0x80d90	0x31a	data	English	United States
RT_STRING	0x810ac	0x2dc	data	English	United States
RT_STRING	0x81388	0x8a	data	English	United States
RT_STRING	0x81414	0xac	data	English	United States
RT_STRING	0x814c0	0xde	data	English	United States
RT_STRING	0x815a0	0x4c4	data	English	United States
RT_STRING	0x81a64	0x264	data	English	United States
RT_STRING	0x81cc8	0x2c	data	English	United States
RT_STRING	0x81cf4	0x42	data	English	United States
RT_STRING	0x81d38	0x48	data	English	United States
RT_GROUP_CURSOR	0x81d80	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x81da4	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81db8	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81dcc	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81de0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81df4	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e08	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e1c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e30	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e44	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e58	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e6c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e80	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e94	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81ea8	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States

Imports

DLL	Import
CRYPT32.dll	CertOpenStore

DLL	Import
KERNEL32.dll	GetStartupInfoA, GetCommandLineA, ExitProcess, HeapReAlloc, TerminateProcess, ExitThread, CreateThread, HeapSize, FatalAppExitA, HeapDestroy, HeapCreate, VirtualFree, IsBadWritePtr, GetStdHandle, UnhandledExceptionFilter, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetFileType, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, SetUnhandledExceptionFilter, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetTimeZoneInformation, IsBadReadPtr, IsBadCodePtr, GetTimeFormatA, GetDateFormatA, GetUserDefaultLCID, EnumSystemLocalesA, IsValidLocale, IsValidCodePage, SetConsoleCtrlHandler, RtlUnwind, GetLocaleInfoW, SetEnvironmentVariableA, InterlockedExchange, GetACP, GetLocaleInfoA, GetThreadLocale, GetVersionExA, MultiByteToWideChar, WideCharToMultiByte, GetLastError, GetVersion, lstrcmpiA, lstrlenW, lstrcmpiW, lstrlenA, CompareStringA, CompareStringW, GetEnvironmentVariableA, GetEnvironmentVariableW, GetStringTypeExA, GetStringTypeExW, SizeofResource, LockResource, LoadResource, FindResourceA, FreeResource, GlobalFree, GlobalUnlock, GlobalLock, LocalFree, lstrcpynA, FormatMessageA, GlobalAlloc, GlobalSize, MulDiv, CopyFileA, SetLastError, GetProcAddress, GetModuleHandleA, lstrcmpW, VirtualQuery, GetSystemInfo, VirtualAlloc, VirtualProtect, HeapFree, HeapAlloc, GetDiskFreeSpaceA, GetTempFileNameA, LocalLock, LocalUnlock, GetFileTime, GetFileAttributesA, SetFileAttributesA, SetFileTime, LocalFileTimeToFileTime, FileTimeToLocalFileTime, SetErrorMode, GetShortPathNameA, CreateFileA, GetFullPathNameA, GetVolumeInformationA, FindFirstFileA, FindClose, GetCurrentProcess, DuplicateHandle, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, DeleteFileA, MoveFileA, GetCurrentDirectoryA, GetPrivateProfileStringA, WritePrivateProfileStringA, GetPrivateProfileIntA, SystemTimeToFileTime, FileTimeToSystemTime, GetOEMCP, GetCPInfo, TlsFree, LocalReAlloc, TlsSetValue, TlsAlloc, TlsGetValue, EnterCriticalSection, GlobalHandle, GlobalReAlloc, LeaveCriticalSection, LocalAlloc, InterlockedIncrement, GlobalFlags, DeleteCriticalSection, InitializeCriticalSection, RaiseException, CreateEventA, SuspendThread, SetEvent, WaitForSingleObject, ResumeThread, SetThreadPriority, CloseHandle, GetCurrentThread, lstrcmpA, GetModuleFileNameA, lstrcatA, ConvertDefaultLocale, EnumResourceLanguagesA, lstrcpyA, InterlockedDecrement, GetCurrentThreadId, GlobalGetAtomNameA, GlobalAddAtomA, GlobalFindAtomA, GlobalDeleteAtom, LoadLibraryA, FreeLibrary, SetStdHandle
USER32.dll	IsClipboardFormatAvailable, MessageBeep, GetTabbedTextExtentA, GetDCEx, LockWindowUpdate, SetParent, InvalidateRect, InsertMenuItemA, CreatePopupMenu, SetRectEmpty, BringWindowToTop, SetMenu, TranslateAcceleratorA, DestroyIcon, DeleteMenu, wsprintfA, WaitMessage, GetWindowThreadProcessId, ReleaseCapture, WindowFromPoint, SetCapture, LoadCursorA, GetSysColorBrush, GetDialogBaseUnits, GetMessageA, TranslateMessage, GetCursorPos, ValidateRect, ShowOwnedPopups, SetCursor, PostQuitMessage, EndPaint, BeginPaint, GetWindowDC, ReleaseDC, GetDC, ClientToScreen, GrayStringA, DrawTextExA, DrawTextA, TabbedTextOutA, FillRect, DestroyMenu, GetMenuItemInfoA, InflateRect, SetMenuItemBitmaps, ModifyMenuA, EnableMenuItem, CheckMenuItem, GetMenuCheckMarkDimensions, LoadBitmapA, ScrollWindowEx, ShowWindow, MoveWindow, SetWindowTextA, IsDialogMessageA, IsDlgButtonChecked, SetDlgItemInt, GetDlgItemTextA, GetDlgItemInt, CheckRadioButton, CheckDlgButton, RegisterWindowMessageA, WinHelpA, GetCapture, CreateWindowExA, SetWindowsHookExA, CallNextHookEx, KillTimer, GetClassInfoExA, GetClassNameA, SetPropA, GetPropA, RemovePropA, SendDlgItemMessageA, GetFocus, SetFocus, IsChild, GetWindowTextLengthA, GetWindowTextA, GetForegroundWindow, GetLastActivePopup, DispatchMessageA, BeginDeferWindowPos, EndDeferWindowPos, GetTopWindow, UnhookWindowsHookEx, GetMessageTime, GetMessagePos, PeekMessageA, MapWindowPoints, ScrollWindow, MessageBoxA, TrackPopupMenuEx, TrackPopupMenu, GetKeyState, SetScrollRange, SetDlgItemTextA, CharLowerA, CharLowerW, CharUpperA, CharUpperW, SendMessageA, EnableWindow, DrawIcon, AppendMenuA, GetSystemMenu, IsIconic, GetClientRect, SetActiveWindow, LoadIconA, GetScrollRange, SetScrollPos, GetScrollPos, SetForegroundWindow, ShowScrollBar, IsWindowVisible, UpdateWindow, GetMenu, PostMessageA, GetSysColor, AdjustWindowRectEx, ScreenToClient, EqualRect, DeferWindowPos, GetScrollInfo, SetScrollInfo, SetTimer, SetRect, UnionRect, IsRectEmpty, MapVirtualKeyA, GetClassInfoA, RegisterClassA, UnregisterClassA, SetWindowPlacement, GetDlgCtrlID, DefWindowProcA, SetWindowLongA, SetWindowPos, OffsetRect, IntersectRect, SystemParametersInfoA, GetWindowPlacement, GetKeyNameTextA, LoadMenuA, UnpackDDElParam, ReuseDDElParam, GetClassLongA, LoadAcceleratorsA, CallWindowProcA, LoadStringW, GetSystemMetrics, EndDialog, GetNextDlgTabItem, GetParent, IsWindowEnabled, GetDlgItem, GetWindowLongA, IsWindow, DestroyWindow, CreateDialogIndirectParamA, GetActiveWindow, GetDesktopWindow, RemoveMenu, GetSubMenu, GetMenuItemCount, InsertMenuA, GetWindowRect, CopyRect, PtInRect, GetWindow, GetMenuState, GetMenuStringA, GetMenuItemID
GDI32.dll	SetMapperFlags, SetArcDirection, SetColorAdjustment, DeleteObject, SelectClipRgn, GetClipRgn, CreateRectRgn, SelectClipPath, GetViewportExtEx, GetWindowExtEx, GetPixel, StartDocA, PtVisible, RectVisible, TextOutA, Escape, SelectObject, SetViewportOrgEx, OffsetViewportOrgEx, SetViewportExtEx, ScaleViewportExtEx, SetWindowOrgEx, OffsetWindowOrgEx, SetWindowExtEx, ScaleWindowExtEx, GetCurrentPositionEx, ArcTo, PolyDraw, PolylineTo, PolyBezierTo, SetTextCharacterExtra, DeleteDC, CreateDIBPatternBrushPt, CreatePatternBrush, GetStockObject, SelectPalette, PlayMetaFileRecord, GetObjectType, EnumMetaFile, PlayMetaFile, CreatePen, ExtCreatePen, CreateSolidBrush, CreateHatchBrush, GetTextMetricsA, CreateRectRgnIndirect, SetRectRgn, CombineRgn, GetMapMode, PatBlt, DPtoLP, CreateCompatibleBitmap, StretchDIBits, GetCharWidthA, CreateFontA, GetBkColor, StartPage, EndPage, SetAbortProc, AbortDoc, EndDoc, SetTextJustification, SetTextAlign, MoveToEx, LineTo, OffsetClipRgn, IntersectClipRect, ExcludeClipRect, SetMapMode, SetStretchBltMode, SetROP2, SetPolyFillMode, SetBkMode, RestoreDC, SaveDC, GetTextExtentPoint32A, ExtTextOutA, BitBlt, CreateCompatibleDC, CreateFontIndirectA, CreateBitmap, GetObjectA, SetBkColor, SetTextColor, GetClipBox, GetDCOrgEx, CreateDCA, CopyMetaFileA, ExtSelectClipRgn, GetDeviceCaps
comdlg32.dll	PageSetupDlgA, FindTextA, ReplaceTextA, GetOpenFileNameA, CommDlgExtendedError, PrintDlgA, GetFileTitleA, GetSaveFileNameA
WINSPOOL.DRV	OpenPrinterA, DocumentPropertiesA, ClosePrinter, GetJobA
ADVAPI32.dll	GetFileSecurityA, RegCloseKey, RegSetValueA, RegOpenKeyA, RegQueryValueExA, RegOpenKeyExA, RegDeleteKeyA, RegEnumKeyA, RegQueryValueA, RegCreateKeyExA, RegSetValueExA, RegDeleteValueA, RegCreateKeyA, SetFileSecurityW, SetFileSecurityA
SHELL32.dll	SHGetFileInfoA, DragFinish, DragQueryFileA, ExtractIconA
COMCTL32.dll	ImageList_Draw, ImageList_GetImageInfo, ImageList_Read, ImageList_Write, ImageList_Destroy, ImageList_Create, ImageList_LoadImageA, ImageList_Merge
SHLWAPI.dll	PathRemoveExtensionA, PathFindFileNameA, PathStripToRootA, PathFindExtensionA, PathIsUNCA
ole32.dll	WriteClassStg, OleRegGetUserType, SetConvertStg, CoTaskMemFree, ReadFmtUserTypeStg, ReadClassStg, StringFromCLSID, CoTreatAsClass, CreateBindCtx, CoTaskMemAlloc, ReleaseStgMedium, OleDuplicateData, CoDisconnectObject, CoCreateInstance, StringFromGUID2, CLSIDFromString, WriteFmtUserTypeStg

DLL	Import
OLEAUT32.dll	VariantClear, VariantChangeType, VariantInit, SysAllocStringLen, SysFreeString, SysStringLen, SysAllocStringByteLen, SysStringByteLen, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayGetElemsize, SafeArrayGetDim, SafeArrayCreate, SafeArrayRedim, VariantCopy, SafeArrayAllocData, SafeArrayAllocDescriptor, SafeArrayCopy, SafeArrayGetElement, SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayLock, SafeArrayUnlock, SafeArrayDestroy, SafeArrayDestroyData, SafeArrayDestroyDescriptor, VariantTimeToSystemTime, SystemTimeToVariantTime, SysAllocString, SysReAllocStringLen, VarDateFromStr, VarBstrFromDec, VarDecFromStr, VarCyFromStr, VarBstrFromCy, VarBstrFromDate

Exports

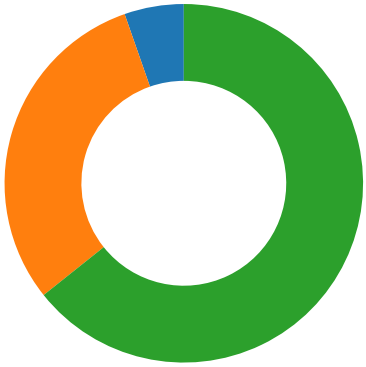
Name	Ordinal	Address
mcfGvgupamvngNBNmgO	1	0x401e04

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



Total Packets: 56

- 53 (DNS)
- 8080 undefined
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 18:48:55.969646931 CEST	49746	443	192.168.2.4	45.33.54.74
Apr 5, 2021 18:48:56.169734001 CEST	443	49746	45.33.54.74	192.168.2.4
Apr 5, 2021 18:48:56.684578896 CEST	49746	443	192.168.2.4	45.33.54.74
Apr 5, 2021 18:48:56.884747028 CEST	443	49746	45.33.54.74	192.168.2.4
Apr 5, 2021 18:48:57.387727022 CEST	49746	443	192.168.2.4	45.33.54.74
Apr 5, 2021 18:48:57.587728977 CEST	443	49746	45.33.54.74	192.168.2.4
Apr 5, 2021 18:49:02.440999985 CEST	49747	8080	192.168.2.4	209.141.41.136
Apr 5, 2021 18:49:05.450963974 CEST	49747	8080	192.168.2.4	209.141.41.136
Apr 5, 2021 18:49:11.467154026 CEST	49747	8080	192.168.2.4	209.141.41.136
Apr 5, 2021 18:49:27.320493937 CEST	49766	8080	192.168.2.4	104.236.246.93
Apr 5, 2021 18:49:30.327960014 CEST	49766	8080	192.168.2.4	104.236.246.93
Apr 5, 2021 18:49:36.344325066 CEST	49766	8080	192.168.2.4	104.236.246.93
Apr 5, 2021 18:49:53.059019089 CEST	49768	8080	192.168.2.4	198.199.114.69
Apr 5, 2021 18:49:56.064657927 CEST	49768	8080	192.168.2.4	198.199.114.69
Apr 5, 2021 18:50:02.080627918 CEST	49768	8080	192.168.2.4	198.199.114.69
Apr 5, 2021 18:50:17.470303059 CEST	49770	8080	192.168.2.4	152.89.236.214
Apr 5, 2021 18:50:17.508716106 CEST	8080	49770	152.89.236.214	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 18:50:18.019629002 CEST	49770	8080	192.168.2.4	152.89.236.214
Apr 5, 2021 18:50:18.058051109 CEST	8080	49770	152.89.236.214	192.168.2.4
Apr 5, 2021 18:50:18.566450119 CEST	49770	8080	192.168.2.4	152.89.236.214
Apr 5, 2021 18:50:18.604933023 CEST	8080	49770	152.89.236.214	192.168.2.4
Apr 5, 2021 18:50:23.470061064 CEST	49771	8080	192.168.2.4	87.106.136.232
Apr 5, 2021 18:50:23.513995886 CEST	8080	49771	87.106.136.232	192.168.2.4
Apr 5, 2021 18:50:24.020106077 CEST	49771	8080	192.168.2.4	87.106.136.232
Apr 5, 2021 18:50:24.063241005 CEST	8080	49771	87.106.136.232	192.168.2.4
Apr 5, 2021 18:50:24.567085028 CEST	49771	8080	192.168.2.4	87.106.136.232
Apr 5, 2021 18:50:24.609909058 CEST	8080	49771	87.106.136.232	192.168.2.4
Apr 5, 2021 18:50:29.480820894 CEST	49772	8080	192.168.2.4	178.210.51.222
Apr 5, 2021 18:50:32.489423990 CEST	49772	8080	192.168.2.4	178.210.51.222

UDP Packets

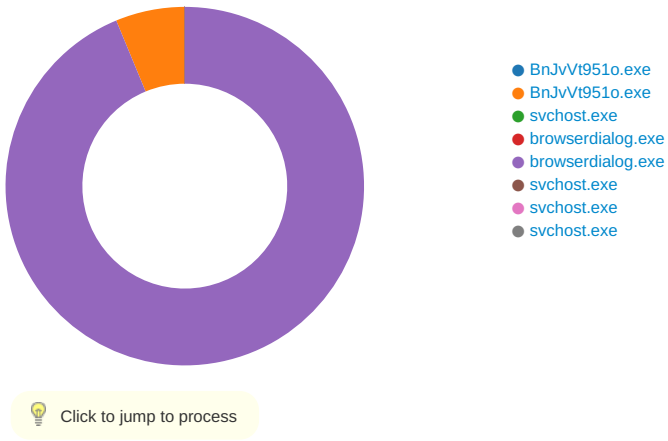
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 18:48:21.685017109 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:21.731705904 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:22.841021061 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:22.890100956 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:23.632489920 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:23.678728104 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:24.837585926 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:24.883778095 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:25.781883001 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:25.827970028 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:26.738219976 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:26.792751074 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:27.517906904 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:27.572283030 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:28.452128887 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:28.498586893 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:29.489063025 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:29.537909031 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:30.415146112 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:30.464212894 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:31.253196001 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:31.300744057 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:32.636662960 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:32.682801962 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:33.556579113 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:33.605434895 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:34.500181913 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:34.546494007 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:35.424271107 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:35.473685026 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:36.872258902 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:36.918473005 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:37.814790964 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:37.861109972 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:38.580564022 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:38.626775026 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:39.580365896 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:39.626697063 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:49.680862904 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:49.728504896 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 5, 2021 18:48:53.430675983 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:48:53.486592054 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:08.737860918 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:49:08.801525116 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:09.341824055 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:49:09.396652937 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:09.859584093 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:49:09.917459011 CEST	49285	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 18:49:09.927885056 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:09.979881048 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:10.355377913 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:49:10.413330078 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:10.960107088 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:49:11.014590979 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:11.632976055 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:49:11.690922976 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:12.148080111 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:49:12.208620071 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:12.921456099 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:49:12.978704929 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:13.796907902 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:49:13.851423025 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:14.328246117 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:49:14.385313988 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:24.833447933 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:49:24.882425070 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:25.167478085 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:49:25.230235100 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 5, 2021 18:49:27.097711086 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:49:27.152903080 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 5, 2021 18:50:00.396539927 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 5, 2021 18:50:00.442426920 CEST	53	55916	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: BnJvVt951o.exe PID: 7136 Parent PID: 6028

General

Start time:	18:48:26
Start date:	05/04/2021
Path:	C:\Users\user\Desktop\BnJvVt951o.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BnJvVt951o.exe'
Imagebase:	0x400000
File size:	516346 bytes
MD5 hash:	AE03A6F8FB74D401B403647D28E21574
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.635756418.0000000002390000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.635756418.0000000002390000.00000040.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.635771732.00000000023A1000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.635771732.00000000023A1000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: BnJvVt951o.exe PID: 1572 Parent PID: 7136

General

Start time:	18:48:26
Start date:	05/04/2021
Path:	C:\Users\user\Desktop\BnJvVt951o.exe
Wow64 process (32bit):	true
Commandline:	--132eeff2
Imagebase:	0x400000
File size:	516346 bytes
MD5 hash:	AE03A6F8FB74D401B403647D28E21574
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.655860929.0000000002380000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000001.00000002.655860929.0000000002380000.00000040.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.655881251.0000000002391000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000001.00000002.655881251.0000000002391000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\browserdialog.exe:Zone.Identifier	success or wait	1	2391126	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6228 Parent PID: 568

General

Start time:	18:48:26
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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

Analysis Process: browserdialog.exe PID: 4528 Parent PID: 568

General

Start time:	18:48:35
Start date:	05/04/2021
Path:	C:\Windows\SysWOW64\browserdialog.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\browserdialog.exe
Imagebase:	0x400000
File size:	516346 bytes
MD5 hash:	AE03A6F8FB74D401B403647D28E21574
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.654778661.0000000000620000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000003.00000002.654778661.0000000000620000.00000040.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.654794849.0000000000641000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000003.00000002.654794849.0000000000641000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: browserdialog.exe PID: 5168 Parent PID: 4528

General

Start time:	18:48:35
Start date:	05/04/2021
Path:	C:\Windows\SysWOW64\browserdialog.exe
Wow64 process (32bit):	true
Commandline:	--39eda026
Imagebase:	0x400000
File size:	516346 bytes
MD5 hash:	AE03A6F8FB74D401B403647D28E21574
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.903155910.0000000000540000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000004.00000002.903155910.0000000000540000.00000040.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.903347367.0000000000E01000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000004.00000002.903347367.0000000000E01000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E014A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E014A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E014A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E014A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\Content.IE5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E014A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E014A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E014A5	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E014A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E014A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E014A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E014A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E014A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E014A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E014A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\History\History.IE5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E014A5	HttpSendRequestW

Analysis Process: svchost.exe PID: 6484 Parent PID: 568

General

Start time:	18:48:49
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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

Analysis Process: svchost.exe PID: 6864 Parent PID: 568

General

Start time:	18:48:58
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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

Analysis Process: svchost.exe PID: 6868 Parent PID: 568

General

Start time:	18:49:07
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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 Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis