ID: 671666
Sample Name: 5CUFfVMSaQ.dll
Cookbook: default.jbs
Time: 13:26:18
Date: 22/07/2022
Version: 35.0.0 Citrine

Table of Contents

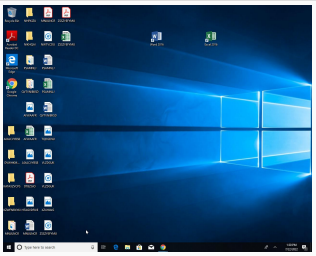
Windows Analysis Report

5CUFfVMSaQ.dll

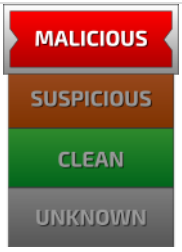
Overview

General Information

Sample Name:	5CUFfVMSaQ.dll
Analysis ID:	671666
MD5:	5d4728494832d0.
SHA1:	abcbd283801a05..
SHA256:	caa60b9025dfba..
Tags:	exe OpenCTIBR Sandboxed
Infos:	



Detection



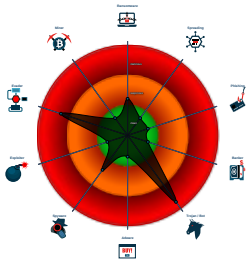
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query local…
- Deletes files inside the Windows fol…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6804 cmdline: loaddll64.exe "C:\Users\user\Desktop\5CUFfVMSaQ.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6812 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\5CUFfVMSaQ.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6856 cmdline: rundll32.exe "C:\Users\user\Desktop\5CUFfVMSaQ.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 6844 cmdline: regsvr32.exe /s C:\Users\user\Desktop\5CUFfVMSaQ.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 6964 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZJPGATOTIe\uLEHsZT.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 6880 cmdline: rundll32.exe C:\Users\user\Desktop\5CUFfVMSaQ.dll,ABeFtrnwmgAedx MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6924 cmdline: rundll32.exe C:\Users\user\Desktop\5CUFfVMSaQ.dll,AEjATaIExpQg MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6980 cmdline: rundll32.exe C:\Users\user\Desktop\5CUFfVMSaQ.dll,AbfBlUFQKbpevAFdaCpElBdscB MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 4376 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6864 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4724 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5144 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "188.165.79.151:443",
    "93.104.209.107:8080",
    "83.229.80.93:8080",
    "196.44.98.190:8080",
    "165.232.185.110:8080",
    "46.101.234.246:8080",
    "5.253.30.17:7080",
    "103.224.241.74:8080",
    "88.217.172.165:8080",
    "198.199.70.22:8080",
    "36.67.23.59:443",
    "157.245.111.0:8080",
    "128.199.242.164:8080",
    "139.196.72.155:8080",
    "202.29.239.162:443",
    "37.44.244.177:8080",
    "104.248.225.227:8080",
    "103.56.149.105:8080",
    "175.126.176.79:8080",
    "118.98.72.86:443",
    "157.230.99.206:8080",
    "103.85.95.4:8080",
    "103.71.99.57:8080",
    "104.244.79.94:443",
    "85.214.67.203:8080",
    "46.101.98.60:8080",
    "54.37.106.167:8080",
    "128.199.217.206:443",
    "178.62.112.199:8080",
    "103.41.204.169:8080",
    "103.254.12.236:7080",
    "116.124.128.206:8080",
    "54.37.228.122:443",
    "210.57.209.142:8080",
    "195.77.239.39:8080",
    "165.22.254.236:8080",
    "37.187.114.15:8080",
    "85.25.120.45:8080",
    "190.107.19.179:443",
    "62.171.178.147:8080",
    "87.106.97.83:7080",
    "139.59.80.108:8080",
    "103.126.216.86:443",
    "188.225.32.231:4143",
    "64.227.55.231:8080",
    "43.129.209.178:443",
    "202.134.4.210:7080",
    "202.28.34.99:8080",
    "190.145.8.4:443",
    "78.47.204.80:443"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0F12ZrwACAIg=",
    "RUNLMSAAAADYNZPXV4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCWSV3XrwAMAIg="
  ]
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
5CUFfVMSaQ.dll	JoeSecurity_Emotet_2	Yara detected Emotet	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.783905665.0000000000EE8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Emotet_3		Joe Security	
00000003.00000002.404900294.0000000002681000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.404253356.0000026BAB700000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.398318822.000001ED72500000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.399047583.000001766C2B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.rundll32.exe.26bab700000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.regsvr32.exe.e50000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.1766c2b0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.rundll32.exe.26bab700000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.1766c2b0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 7 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 11 - Source IP: 192.168.2.5 - Destination IP: 188.165.79.151

Timestamp:	192.168.2.5188.165.79.151497724432404320 07/22/22-13:16:45.923727
SID:	2404320
Source Port:	49772
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

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

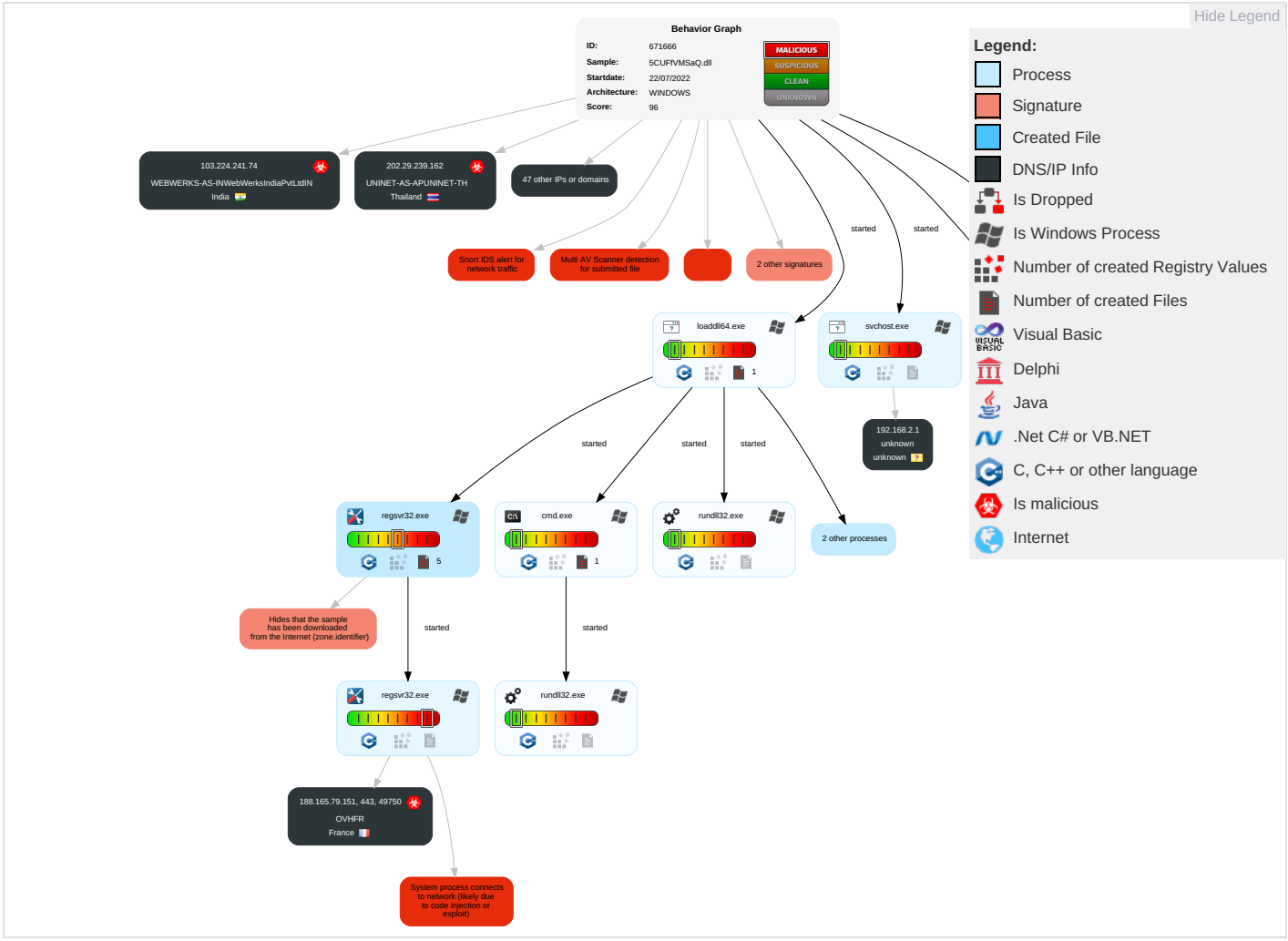
Stealing of Sensitive Information

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	LSASS Memory	3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 1 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	3 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Regsvr32	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

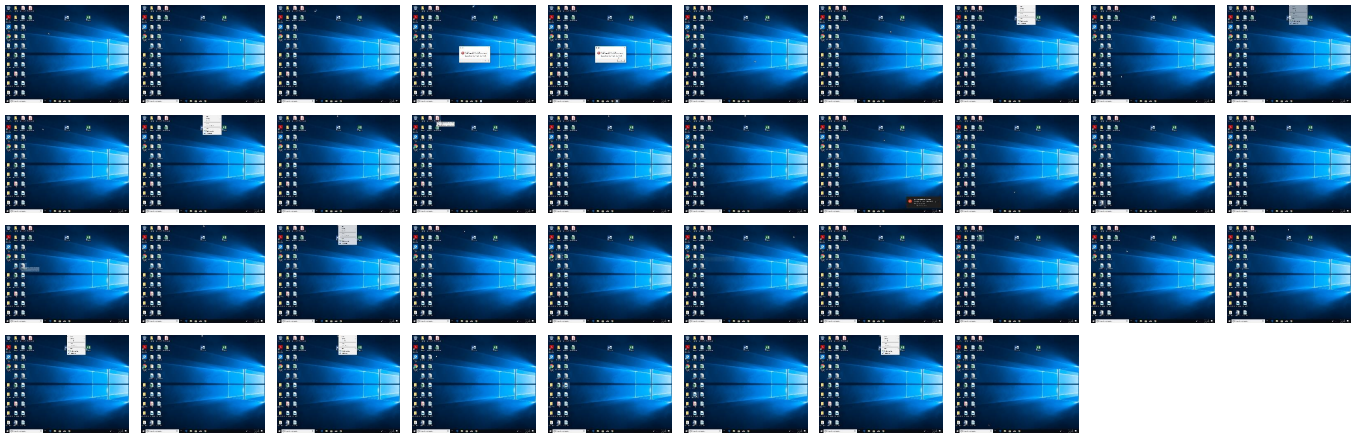
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
5CUFfVMSaQ.dll	21%	Virustotal		Browse
5CUFfVMSaQ.dll	46%	Metadefender		Browse
5CUFfVMSaQ.dll	81%	ReversingLabs	Win64.Trojan.Emotet	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://188.165.79.151/6S#	0%	Avira URL Cloud	safe	
http://https://188.165.79.151/	0%	URL Reputation	safe	
http://crl.v	0%	URL Reputation	safe	
http://https://188.165.79.151/~r	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

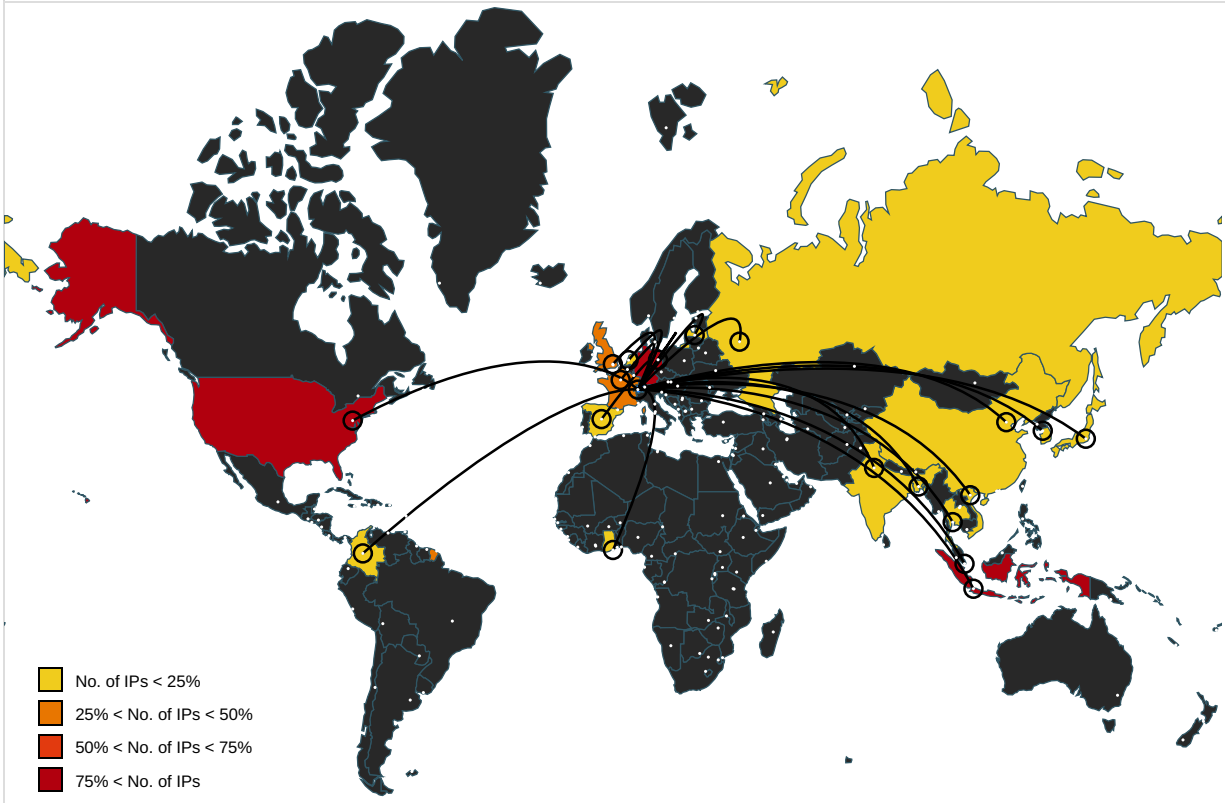
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://188.165.79.151/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://188.165.79.151/6S#	regsvr32.exe, 00000007.00000002.78390566 5.0000000000EE8000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.v	regsvr32.exe, 00000007.00000002.78420619 1.0000000000F84000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000003.475529987.0000000000F84000. 00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://188.165.79.151/~r	regsvr32.exe, 00000007.00000003.47579276 5.0000000000F33000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000002.784016944.0000000000F33000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.475615 056.0000000000F33000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.230.99.206	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
188.165.79.151	unknown	France		16276	OVHFR	true
196.44.98.190	unknown	Ghana		327814	EcobandGH	true
43.129.209.178	unknown	Japan		4249	LILLY-ASUS	true
36.67.23.59	unknown	Indonesia		17974	TELKOMNET-AS2-APPTTelekomunikasiIndonesiaID	true
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
5.253.30.17	unknown	Latvia		18978	ENZUINC-US	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
83.229.80.93	unknown	United Kingdom		8513	SKYVISIONGB	true
198.199.70.22	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
93.104.209.107	unknown	Germany		8767	MNET-ASGermanyDE	true
188.225.32.231	unknown	Russian Federation		9123	TIMEWEB-ASRU	true
175.126.176.79	unknown	Korea Republic of		9523	MOKWON-AS-KRMokwonUniversityKR	true
128.199.242.164	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
104.248.225.227	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
46.101.98.60	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
190.145.8.4	unknown	Colombia		14080	TelmexColombiaSACO	true
103.71.99.57	unknown	India		135682	AWDHPL-AS-INAdvikaWebDevelopmentsHostingPvtLtdIN	true
87.106.97.83	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
103.254.12.236	unknown	Viet Nam		56151	DIGISTAR-VNDigiStarCompanyLimitedVN	true
103.85.95.4	unknown	Indonesia		136077	IDNIC-UNSRAT-AS-IDUniversitasIslamNegeriMataramID	true
202.134.4.210	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
88.217.172.165	unknown	Germany		8767	MNET-ASGermanyDE	true
165.22.254.236	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
118.98.72.86	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
139.59.80.108	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
104.244.79.94	unknown	United States		53667	PONYNETUS	true
157.245.111.0	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
54.37.106.167	unknown	France		16276	OVHFR	true
202.29.239.162	unknown	Thailand		4621	UNINET-AS-APUNINET-TH	true
103.56.149.105	unknown	Indonesia		55688	BEON-AS-IDPTBeonIntermediaID	true
85.25.120.45	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
37.187.114.15	unknown	France		16276	OVHFR	true
46.101.234.246	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
165.232.185.110	unknown	United States		22255	ALLEGHENYHEALTHNETWORKUS	true
103.126.216.86	unknown	Bangladesh		138482	SKYVIEW-AS-APSKYVIEWONLINELTDBD	true
128.199.217.206	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
116.124.128.206	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
103.224.241.74	unknown	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
190.107.19.179	unknown	Colombia		27951	MediaCommercePartnersSACO	true
202.28.34.99	unknown	Thailand		9562	MSU-TH-APMahasarakhamUniversityTH	true
54.37.228.122	unknown	France		16276	OVHFR	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
178.62.112.199	unknown	European Union		14061	DIGITALOCEAN-ASNUS	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
64.227.55.231	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	671666
Start date and time: 22/07/202213:26:18	2022-07-22 13:26:18 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5CUFfVMSaQ.dll
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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	21
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.troj.evad.winDLL@19/0@0/51
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 88.8% (good quality ratio 83.1%) • Quality average: 75.3% • Quality standard deviation: 30.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Sleeps bigger than 300000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- Excluded IPs from analysis (whitelisted): 20.54.89.106
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.

- 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 NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.931234965672042
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	5CUFfVMSaQ.dll
File size:	691200
MD5:	5d4728494832d03bbfb75367836fef4e
SHA1:	abcbd283801a05390995862f59dcb5310f3d3d88
SHA256:	caa60b9025dfba07efac6cae5438a8e20d9b7c210a721a4cf1f9d7b6df4d7d90
SHA512:	89f38029d8cc4718af304e325a290294a000e68fea0d036fbe118cc04bd3ae5a676cab2dbc6ea4d1c53eeac804cd23756c01dce378a317cb683200365ad5079a

SSDEEP:	12288:pBBKShhc/bQisqkxf3CJS+HQ58B6loNJYlvw9zaaxRHdAsxuvt3a1gYao3ovJK6S:bBHlvw9GanHrot3hoW
TLSH:	45E4BE56ABE404B1E1B7D235C9128E81FAB3FC544724AB8B03E095B62F233AC557F716
File Content Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d.....b....." .....d?.....0..... .....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180003f64
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, NX_COMPAT
Time Stamp:	0x62BAE9E7 [Tue Jun 28 11:45:43 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	6cc0be0d01417a15b61c3b6a580e87ed

Entrypoint Preview

Instruction
dec eax
mov dword ptr [esp+08h], ebx
dec eax
mov dword ptr [esp+10h], esi
push edi
dec eax
sub esp, 20h
dec ecx
mov edi, eax
mov ebx, edx
dec eax
mov esi, ecx
cmp edx, 01h
jne 00007F6430A07C37h
call 00007F6430A07C54h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h

Instruction
pop edi
jmp 00007F6430A07AC4h
int3
int3
int3
dec eax
mov dword ptr [esp+20h], ebx
push ebp
dec eax
mov ebp, esp
dec eax
sub esp, 20h
dec eax
mov eax, dword ptr [0006E0C0h]
dec eax
mov ebx, 2DDFA232h
cdq
sub eax, dword ptr [eax]
add byte ptr [eax+3Bh], cl
ret
jne 00007F6430A07CA6h
dec eax
and dword ptr [ebp+18h], 00000000h
dec eax
lea ecx, dword ptr [ebp+18h]
call dword ptr [0006741Ah]
dec eax
mov eax, dword ptr [ebp+18h]
dec eax
mov dword ptr [ebp+10h], eax
call dword ptr [0006738Ch]
mov eax, eax
dec eax
xor dword ptr [ebp+10h], eax
call dword ptr [00067370h]
mov eax, eax
dec eax
lea ecx, dword ptr [ebp+20h]
dec eax
xor dword ptr [ebp+10h], eax
call dword ptr [00067490h]
mov eax, dword ptr [ebp+20h]
dec eax
lea ecx, dword ptr [ebp+10h]
dec eax
shl eax, 20h
dec eax
xor eax, dword ptr [ebp+20h]
dec eax
xor eax, dword ptr [ebp+10h]
dec eax
xor eax, ecx
dec eax
mov ecx, FFFFFFFFh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x69f18	0xe9d	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6adb5	0x50	.rdata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x89000	0x28080	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x75000	0x4620	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb2000	0x808	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x5ed80	0x138	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x6b1b8	0x3b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
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	0x5c966	0x5ca00	False	0.4055093412618084	data	6.495336903226537	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x5e000	0x13174	0x13200	False	0.41204554738562094	data	5.399737438631881	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x72000	0x2894	0xe00	False	0.15625	data	2.3008281540935718	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x75000	0x4620	0x4800	False	0.4896918402777778	data	5.7263789636668765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.00cfg	0x7a000	0x28	0x200	False	0.05859375	data	0.37171553503035126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gehcont	0x7b000	0x50	0x200	False	0.130859375	PGP\011Secret Sub-key -	0.5546627733147627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gxfg	0x7c000	0x9eb0	0xa000	False	0.336083984375	data	5.261757688277708	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.retplne	0x86000	0x5c	0x200	False	0.087890625	data	0.8458487823546629	
.voltbl	0x87000	0x54	0x200	False	0.18359375	data	1.322754253639915	
_RDATA	0x88000	0xf4	0x200	False	0.314453125	data	1.9917660782863578	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x89000	0x28080	0x28200	False	0.8353168808411215	data	7.725336511078031	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb2000	0x808	0xa00	False	0.454296875	data	4.922299312910362	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_STRING	0xb1038	0x48	data	English	United States
RT_HTML	0x89238	0x27e00	data	English	United States
RT_MANIFEST	0x890f0	0x143	XML 1.0 document, ASCII text	English	United States

Imports

DLL	Import
GDI32.dll	CreatePen, DeleteObject, LineTo, MoveToEx, Polyline, SelectObject
USER32.dll	BeginPaint, CloseGestureInfoHandle, CreateWindowExW, DefWindowProcW, DestroyWindow, DispatchMessageW, EndPaint, GetGestureInfo, GetMessageW, InvalidateRect, LoadCursorW, LoadStringW, PostQuitMessage, RegisterClassExW, ScreenToClient, SetGestureConfig, ShowWindow, TranslateAcceleratorW, TranslateMessage, UpdateWindow

DLL	Import
KERNEL32.dll	CloseHandle, CompareStringW, CreateFileW, DeleteCriticalSection, EncodePointer, EnterCriticalSection, EnumSystemLocalesW, ExitProcess, FindClose, FindFirstFileExW, FindNextFileW, FlsAlloc, FlsFree, FlsGetValue, FlsSetValue, FlushFileBuffers, FreeEnvironmentStringsW, FreeLibrary, GetACP, GetCPInfo, GetCommandLineA, GetCommandLineW, GetConsoleMode, GetConsoleOutputCP, GetCurrentProcess, GetCurrentProcessId, GetCurrentThread, GetCurrentThreadId, GetDateFormatW, GetEnvironmentStringsW, GetFileSizeEx, GetFileType, GetLastError, GetLocaleInfoW, GetModuleFileNameW, GetModuleHandleExW, GetModuleHandleW, GetOEMCP, GetProcAddress, GetProcessHeap, GetStartupInfoW, GetStdHandle, GetStringTypeW, GetSystemTimeAsFileTime, GetTimeFormatW, GetUserDefaultLCID, HeapAlloc, HeapFree, HeapReAlloc, HeapSize, InitializeCriticalSectionAndSpinCount, InitializeSListHead, InterlockedFlushSList, InterlockedPushEntrySList, IsDebuggerPresent, IsProcessorFeaturePresent, IsValidCodePage, IsValidLocale, LCMapStringW, LeaveCriticalSection, LoadLibraryExW, MultiByteToWideChar, OutputDebugStringW, QueryPerformanceCounter, RaiseException, ReadConsoleW, ReadFile, RtlCaptureContext, RtlLookupFunctionEntry, RtlPcToFileHeader, RtlUnwind, RtlUnwindEx, RtlVirtualUnwind, SetConsoleCtrlHandler, SetEnvironmentVariableW, SetFilePointerEx, SetLastError, SetStdHandle, SetUnhandledExceptionFilter, TerminateProcess, TlsAlloc, TlsFree, TlsGetValue, TlsSetValue, UnhandledExceptionFilter, VirtualAlloc, WideCharToMultiByte, WriteConsoleW, WriteFile

Exports

Name	Ordinal	Address
ABeFtrnwmgAedx	1	0x1800029d0
AEjATalExpQg	2	0x180002890
AbfBlUFQKbpevAFdaCpElBdscB	3	0x180002200
AhCiOqhwyUiZbbsGncKmyLU	4	0x1800026f0
AppWcUGsNPSALiojxbzmIncLqw	5	0x1800028f0
BuDIuWLYHzeYLi	6	0x180002260
BzspXLkN	7	0x1800024f0
CAJbrnGzThPxKInHYeNbeiD	8	0x180002980
CAizYoExRRpdPoWVbPYKFDwgiU	9	0x180002800
DllRegisterServer	10	0x180002170
DsznQlJtSEfpoaC	11	0x1800022b0
DwKmpHIDu	12	0x180002930
ECDzEWMCYJeoRkryuQOsYJpmq	13	0x1800022e0
FAcdRHAWz	14	0x180002610
FFgOwmblMRuJiEZKeYTYiuzs	15	0x1800023f0
FGcNCKAlddUwyHBYG	16	0x180002860
FrsmtxAdhb	17	0x180002590
FycDPRFayBivcQtViJFBB	18	0x180002320
GGGPAvQKBPbfXZZaHVp	19	0x180002920
GKgyyDJNJDeNTLdDtczKsL	20	0x180002340
GMWWgDWCipXIlkjHwoUVUkcYR	21	0x1800026e0
GXJpVyiTrLHOne	22	0x1800023d0
HJTFoxcPliQgvLgH	23	0x180002820
HLCABIQMByMWBQl	24	0x180002720
HSSmJwdyKCypI	25	0x180002650
HuenqNYbiVIeAyMGFYkiYBPFpc	26	0x180002770
IxremlDMjrvkDxgZfhGQZrk	27	0x180002700
IxvOJTyBGbJYNRuYaPxjyAUmf	28	0x180002380
JQPbXc	29	0x180002270
JcMTbvPHZlumePpXUBhRJWcp	30	0x180002350
JnZLIBBbkn	31	0x1800025e0
JohOupoqASpLhYFLsyWn	32	0x180002950
JwPmjlqZQXgHaQjgtKwKH	33	0x180002940
LsCgTlMZDLwMutNSvzYIEdEhwL	34	0x180002330
MPWJOPLDpgeYBymjBqgQIjmNoZ	35	0x180002360
MXztYxhtX	36	0x1800021f0
McniJoPJlmcEHlRCsaUz	37	0x180002550
MhvpJKCzeAS	38	0x180002620
MmBOoLzloNcLojEtz	39	0x1800027a0
MoxtcCOHATssMTmiLf	40	0x1800029e0
MpzzLNccslEpsqsI	41	0x180002540
NqTxbmWhjf	42	0x1800027e0
NsnrjJneCojFavepwQt	43	0x180002430
OFTAEmNeIKkEpTykdZkNKIzp	44	0x180002520
OguNFmV	45	0x1800025f0

Name	Ordinal	Address
PXDdTdN	46	0x1800026d0
PvWkibWuSiAacbZGzrkJUt	47	0x1800021b0
QFGNloHdiwsP	48	0x180002450
QOFKcQtiQXM	49	0x180002830
QmukeRFviFO	50	0x1800021a0
QupOoHScTGifO	51	0x1800026a0
QyvetqDJywCLrVJLzofDOegxwP	52	0x180002710
RmPpiUfGU	53	0x180002750
SIkquaNCflVmESatNcndpdTlpe	54	0x1800028d0
SflHxYaArvTuFNrMVIbyX	55	0x180002470
UWpelES	56	0x180002880
UkLettFcomFXma	57	0x180002990
VLdhIHLdMhyW	58	0x1800025b0
VcULfipZVLXGKZRfrueex	59	0x180002500
VqpcWzxeRjlVhQwQzv	60	0x180002410
WBpPkPKcWeqGwAzzvNIH	61	0x180002790
WEDyKrcivTPPlSwCwT	62	0x180002370
WoptoKqfVNqOqwssFKVZfo	63	0x180002670
XnGdCqyiMLdhVnMShSkq	64	0x180002630
YMyyyHvdBObwWJjXdFk	65	0x180002250
YihCWA	66	0x180002530
YweLMeZukpQkvnZnYHkhCM	67	0x180002780
ZLVzkIypQXUkzx	68	0x180002900
ZSoNGzxKLdyqDghj	69	0x180002640
ZkiQhRLkrjLkJNX	70	0x180002730
ZmqtKkySX	71	0x180002210
aPfqQAbMTzuJNp	72	0x180002390
aehnZNNrhIsF	73	0x1800029a0
amxdxgjfMZcXaFUifsfcvLXi	74	0x1800022a0
bPfPnNT	75	0x1800023a0
bubLuYEWIvIWsBNJTUOnl	76	0x1800023e0
cTcqyCZyBDJvEFnsvQYDCOLAoT	77	0x1800022f0
cYubuRW	78	0x1800027f0
clFUgmrVuPSljrxXorVz	79	0x180002230
dbMiEkrHbNnvIlaysX	80	0x180002600
dgAUOlElUrm	81	0x1800021d0
dxEatgtTYroSUkMiQaL	82	0x180002220
eCkbiLnmCybWxEn	83	0x180002440
efVluiugFvmsD	84	0x1800029b0
exoEcLTZltlKDhXcTPLBLvM	85	0x1800026b0
fAgLiyKNqrsT	86	0x180002660
fEeZsQFKbuLaABrhuAbOhNj	87	0x180002420
gYiNJrEBUixiSygWCLlsEf	88	0x180002680
gpObsYCSb	89	0x1800023c0
gtbMrIHBEjSZnmBWPb	90	0x180002840
hCcvyzzlUZCYlRNZCTK	91	0x1800027b0
hPDZNFuvABEgQeoD	92	0x180002850
hsEYnjr	93	0x180002460
iLEOjsJklFUGkNI	94	0x1800025c0
iLjGFeOafkDi	95	0x1800024d0
jcCPKYwgGqRpySHQKBnfldayWD	96	0x1800022c0
jjTWNPlegZljgiNVCWFLUDkFH	97	0x180002280
kffHAP	98	0x180002560
lUlTXKofnHgBxwxJLPdDPpCz	99	0x1800028c0
lYaeKiHDZBLcjXyoPcEOBUc	100	0x1800024c0
lpGoEIn	101	0x1800023b0
mAtENYctTeMWWmtQ	102	0x180002760
mEiZkvnenxFVSgbXocseslt	103	0x1800028a0
mSkIHCWnxYjPAvLhkizRM	104	0x180002480

Name	Ordinal	Address
nciUfwCE	105	0x1800025a0
nfBvdBN	106	0x180002310
ngwzyo	107	0x180002960
njQxmJYMOWniVlJCxlqYaGwyco	108	0x180002290
pikxaDuNdKkEyUKlBLtRo	109	0x1800024b0
qYcNCgPzHhoixH	110	0x180002400
qbLCbNjvgZccfXANyoilYHLz	111	0x1800024a0
rIgvWBvLm	112	0x180002810
rMHLHjlymAUoTHNFdsfNPiQH	113	0x1800028b0
riiAnEEXhiFVUIdp	114	0x180002870
sCXUQoygEhYAvHSLAtQPOlI	115	0x180002910
sNgDDxTXeDBSWJVL	116	0x1800021c0
sjmfaFHjAYLiTOs	117	0x180002970
uFvBoQlDuBHPbcggfbqTz	118	0x180002240
uKxBgklrkubs	119	0x180002300
ueGFocoIB	120	0x180002690
ueINzYdzNpuGfNAPnf	121	0x1800029c0
vAVSflnhL	122	0x1800022d0
vJROvhiSqVeOiIsH	123	0x1800021e0
vfDcFWpsvSWqEKgMwpzmloZ	124	0x1800027c0
vzyObHl	125	0x1800027d0
wAavZUBVHJ	126	0x180002740
wCHWOvC	127	0x1800026c0
wQlVOK	128	0x1800028e0
wZFewnVovChWmNJWJDqUTvJm	129	0x180002580
wkraMphf	130	0x1800025d0
xkQCLrMtQvyCjJhPSdk	131	0x1800024e0
yYodwLnmm	132	0x180002510
ysdKlUzdVU	133	0x180002570
zFCiVYrpvmmXdRHTSKMcojyZb	134	0x180002490

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5188.165.79.151497724432404320 07/22/22-13:16:45.923727	TCP	2404320	ET CNC Feodo Tracker Reported CnC Server TCP group 11	49772	443	192.168.2.5	188.165.79.151

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 22, 2022 13:28:19.643986940 CEST	49750	443	192.168.2.6	188.165.79.151
Jul 22, 2022 13:28:19.644041061 CEST	443	49750	188.165.79.151	192.168.2.6
Jul 22, 2022 13:28:19.644174099 CEST	49750	443	192.168.2.6	188.165.79.151
Jul 22, 2022 13:28:19.676512957 CEST	49750	443	192.168.2.6	188.165.79.151
Jul 22, 2022 13:28:19.676542997 CEST	443	49750	188.165.79.151	192.168.2.6
Jul 22, 2022 13:28:19.796740055 CEST	443	49750	188.165.79.151	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 22, 2022 13:28:19.797034025 CEST	49750	443	192.168.2.6	188.165.79.151
Jul 22, 2022 13:28:20.188575983 CEST	49750	443	192.168.2.6	188.165.79.151
Jul 22, 2022 13:28:20.188611031 CEST	443	49750	188.165.79.151	192.168.2.6
Jul 22, 2022 13:28:20.188957930 CEST	443	49750	188.165.79.151	192.168.2.6
Jul 22, 2022 13:28:20.189049959 CEST	49750	443	192.168.2.6	188.165.79.151
Jul 22, 2022 13:28:20.193274975 CEST	49750	443	192.168.2.6	188.165.79.151
Jul 22, 2022 13:28:20.236506939 CEST	443	49750	188.165.79.151	192.168.2.6
Jul 22, 2022 13:28:20.432982922 CEST	443	49750	188.165.79.151	192.168.2.6
Jul 22, 2022 13:28:20.433113098 CEST	49750	443	192.168.2.6	188.165.79.151
Jul 22, 2022 13:28:20.433130026 CEST	443	49750	188.165.79.151	192.168.2.6
Jul 22, 2022 13:28:20.433193922 CEST	49750	443	192.168.2.6	188.165.79.151
Jul 22, 2022 13:28:20.441657066 CEST	49750	443	192.168.2.6	188.165.79.151
Jul 22, 2022 13:28:20.441689968 CEST	443	49750	188.165.79.151	192.168.2.6

HTTP Request Dependency Graph

- 188.165.79.151

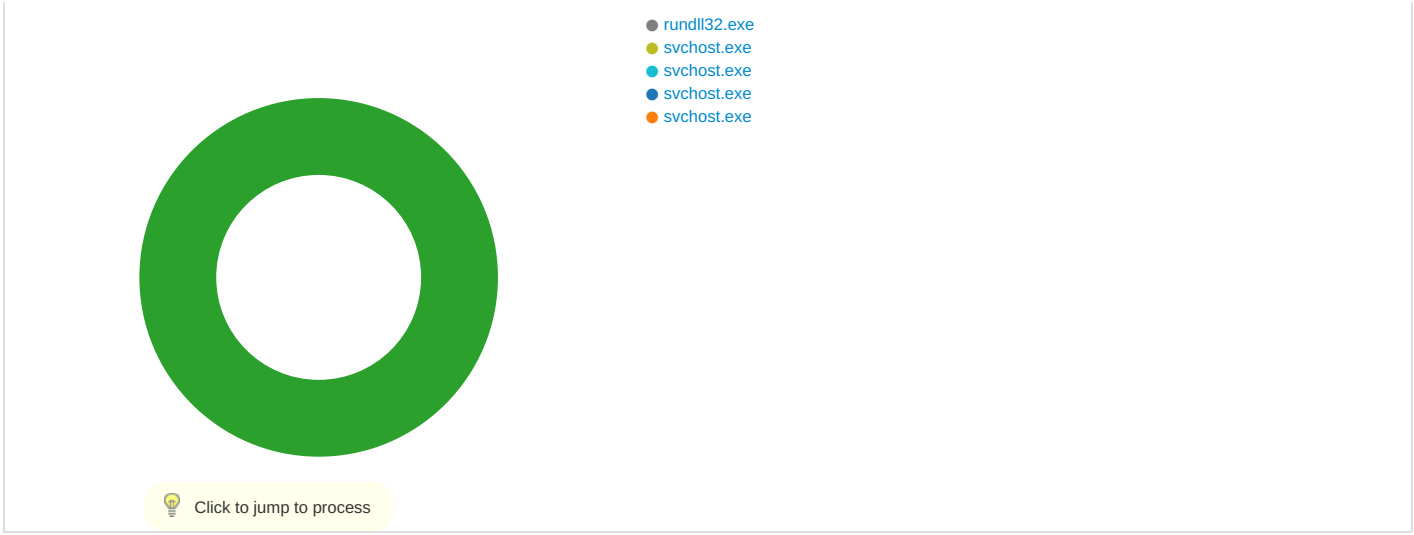
HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49750	188.165.79.151	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-22 11:28:20 UTC	0	OUT	GET / HTTP/1.1 Cookie: CQHd=zROF5f0ZV1ZxZOeiJnhhFnLT/eIdAOEXkS+UqWmvXeeUa5HALooquXLstVuCCdmOVXvsMahuGIil7Z/r6qOuFjhQfDI8A2ofEM43G9ttUICAE9uNx6Fhx1n2lrRsMMMTx3azM7U+3k65+iRIhu5mKmMzhsnLsyfOfT+iQxewJc6NKVR9NE+e3qcP1Y3CnYPdyxgLKnYwwKKfunxCRdsXDWoB+OQyPwn+AGHfjdB6T5vGh5leD3pSUO5Ugv+Zrf4TmbS68/7svPcIMrtO2sDXc6RbVzCzf0fXaatnTZT1WjG8ZjSZDVfUeqe5k106rGD3Tg== Host: 188.165.79.151 Connection: Keep-Alive Cache-Control: no-cache
2022-07-22 11:28:20 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 22 Jul 2022 11:28:20 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2022-07-22 11:28:20 UTC	0	IN	Data Raw: 32 65 66 0d 0a 40 3b 9e 82 cd 97 13 b8 f6 6d 02 bc 58 e4 e8 bd d4 4a 34 40 fc fc 38 09 84 4a ee a8 8c dc a9 ab 02 e8 65 7a 0d 0c 69 d0 d7 1c 6d 1d 9f 6a a9 5c 7a b1 ea 09 00 34 54 f7 21 03 d5 76 bb 1a 09 fc 3c ef 2f af 60 dc 80 7c 56 0f e7 1d a8 48 fc 26 f0 73 39 86 8d c7 cd 7e 1d 22 f6 75 a6 bd 7d 3d b2 d3 12 67 cd 61 85 74 00 51 75 cf 60 60 0c 13 50 0f 45 2b 68 ad b1 d4 fd 2e 4b de f3 45 9f 9b 5b b3 2e fa bb 03 53 ef 34 41 04 c4 c5 0d 1d 6f 90 2a 8c da f9 59 31 59 28 85 89 d9 45 f1 73 f0 12 b8 e8 2f 20 f5 56 ad d4 05 e6 ee b3 23 ce 7f ab 28 0f 4e 5c 6a 07 0e d1 6a ad 42 fe 1c 91 0b cc 31 d5 67 38 34 0c 16 e7 62 e6 07 52 38 fe 07 fa 57 6a 73 2c 1f 34 02 f2 05 a5 95 b3 7e 09 94 68 47 9c 98 1a ed 5e 61 99 57 b4 5f b3 a0 01 7f a8 7a 32 70 b9 08 88 a5 17 63 Data Ascii: 2ef@;mXJ4@8Jezimj\z4T!v</`|VH&s9~"u}=gatQu``PE+h.KE[.S4Ao*Y1Y(Es/ V#(N\jjB1g84bR8Wjs,4~h G^aW_z2pc

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **6804**, Parent PID: **3028**

General	
Target ID:	0
Start time:	13:27:38
Start date:	22/07/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\5CUFfVMSaQ.dll"
Imagebase:	0x7ff641d20000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6812**, Parent PID: **6804**

General	
Target ID:	1
Start time:	13:27:38
Start date:	22/07/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\5CUFfVMSaQ.dll",#1
Imagebase:	0x7ff6edbd0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 6844, Parent PID: 6804

General

Target ID:	3
Start time:	13:27:39
Start date:	22/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\5CUFfVMSaQ.dll
Imagebase:	0x7ff608e30000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.404900294.0000000002681000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_2, Description: Yara detected Emotet, Source: 00000003.00000002.406068538.0000000180001000.00000020.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.404818681.0000000002650000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\ZJPGATOTIe\uLEHsZT.dll:Zone.Identifier	success or wait	1	2692226	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6856, Parent PID: 6812

General

Target ID:	4
Start time:	13:27:39
Start date:	22/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\5CUFfVMSaQ.dll",#1
Imagebase:	0x7ff6eb6e0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.398318822.000001ED72500000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.398411719.000001ED72641000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6880, Parent PID: 6804

General

Target ID:	5
Start time:	13:27:39
Start date:	22/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\5CUFfVMSaQ.dll,ABeFtrnwmgAedx
Imagebase:	0x7ff6eb6e0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.399047583.000001766C2B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.399210556.000001766C3F1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6924, Parent PID: 6804

General

Target ID:	6
Start time:	13:27:43
Start date:	22/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\5CUFfVMSaQ.dll,AEjATaIExpQg
Imagebase:	0x7ff6eb6e0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.404253356.0000026BAB700000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.404280554.0000026BAB731000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: regsvr32.exe PID: 6964, Parent PID: 6844

General

Target ID:	7
Start time:	13:27:45
Start date:	22/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZJPGATOTIe\uLEHsZT.dll"
Imagebase:	0x7ff608e30000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_3, Description: , Source: 00000007.00000002.783905665.0000000000EE8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_2, Description: Yara detected Emotet, Source: 00000007.00000002.784489149.0000000180001000.00000020.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.783816835.0000000000E81000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.783761119.0000000000E50000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **6980**, Parent PID: **6804**

General

Target ID:	8
Start time:	13:27:47
Start date:	22/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\5CUFfVMSaQ.dll,AbfBlUFQKbpevAFdaCpElBdscB
Imagebase:	0x7ff6eb6e0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **4376**, Parent PID: **588**

General

Target ID:	12
Start time:	13:28:17
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **6864**, Parent PID: **588**

General

Target ID:	16
Start time:	13:29:51
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 4724, Parent PID: 588

General

Target ID:	19
Start time:	13:30:29
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5144, Parent PID: 588

General

Target ID:	20
Start time:	13:30:37
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly