



ID: 745008
Sample Name: zzkCldCoDt.exe
Cookbook: default.jbs
Time: 17:15:13
Date: 13/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report zzkCIdCoDt.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Emotet 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
E-Banking Fraud 6
Boot Survival 6
Hooking and other Techniques for Hiding and Protection 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 10
Public IPs 11
General Information 12
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 14
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 14
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 14
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log 14
Static File Info 15
General 15
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Rich Headers 17
Data Directories 17
Sections 17
Resources 18
Imports 18
Exports 18
Possible Origin 18
Network Behavior 19
Snort IDS Alerts 19
Network Port Distribution 19
TCP Packets 19
Statistics 20
Behavior 20
System Behavior 20

Copyright Joe Security LLC 2022

Analysis Process: loaddll64.exePID: 5224, Parent PID: 3452 20
General 20
File Activities 20
Analysis Process: conhost.exePID: 5236, Parent PID: 5224 21
General 21
Analysis Process: cmd.exePID: 2068, Parent PID: 5224 21
General 21
File Activities 21
Analysis Process: regsvr32.exePID: 5452, Parent PID: 5224 21
General 21
File Activities 22
Analysis Process: rundll32.exePID: 5456, Parent PID: 2068 22
General 22
File Activities 22
File Deleted 22
Analysis Process: rundll32.exePID: 5488, Parent PID: 5224 22
General 22
File Activities 23
Analysis Process: regsvr32.exePID: 5160, Parent PID: 5456 23
General 23
File Activities 23
Registry Activities 23
Key Value Created 23
Analysis Process: regsvr32.exePID: 5144, Parent PID: 5452 23
General 23
File Activities 24
Analysis Process: regsvr32.exePID: 3044, Parent PID: 5224 24
General 24
File Activities 24
Analysis Process: regsvr32.exePID: 736, Parent PID: 5488 24
General 24
File Activities 24
Analysis Process: regsvr32.exePID: 5144, Parent PID: 3452 25
General 25
File Activities 25
Analysis Process: regsvr32.exePID: 3796, Parent PID: 5144 25
General 25
File Activities 25
Analysis Process: MpCmdRun.exePID: 3968, Parent PID: 5452 25
General 25
File Activities 26
File Written 26
Analysis Process: conhost.exePID: 2072, Parent PID: 3968 27
General 27
Disassembly 27

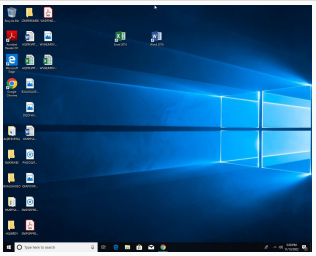
Windows Analysis Report

zzkCldCoDt.exe

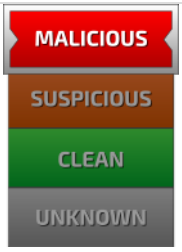
Overview

General Information

Sample Name:	zzkCldCoDt.exe (renamed file extension from exe to dll)
Analysis ID:	745008
MD5:	e383dda8987435.
SHA1:	8b3982937eddd4.
SHA256:	8c1db84c9f8667…
Tags:	dll exe
Infos:	



Detection



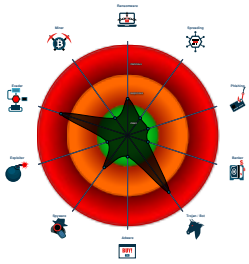
Emotet

Score:	84
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
- Creates an autostart registry key po…
- 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…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…
- Checks if Antivirus/Antispyware/Fire…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 5224 cmdline: loaddll64.exe "C:\Users\user\Desktop\zzkCldCoDt.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 5236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 2068 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\zzkCldCoDt.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5456 cmdline: rundll32.exe "C:\Users\user\Desktop\zzkCldCoDt.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - regsvr32.exe (PID: 5160 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\AmhzcKVtZLl\siQPBMdwCPAb.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 5452 cmdline: regsvr32.exe /s C:\Users\user\Desktop\zzkCldCoDt.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 5144 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\QxWCKZstQphkP\egknjpoziqlzVL.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 5144 cmdline: C:\Windows\system32\regsvr32.exe" "C:\Windows\system32\AmhzcKVtZLl\siQPBMdwCPAb.dll MD5: D78B75FC68247E8A63ACBA846182740E)
      - regsvr32.exe (PID: 3796 cmdline: C:\Windows\system32\regsvr32.exe "C:\Users\user\AppData\Local\UOEgTmwbpKANXEqN\KElhycJrzKCpLgeP.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
    - MpCmdRun.exe (PID: 3968 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
      - conhost.exe (PID: 2072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rundll32.exe (PID: 5488 cmdline: rundll32.exe C:\Users\user\Desktop\zzkCldCoDt.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
    - regsvr32.exe (PID: 736 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\BlngRITsHraAEaQWw\tRWuLwwWwn.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 3044 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\CXPSzClcOMY\wxJWjHQhm.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "172.105.115.71:8080",
    "218.38.121.17:443",
    "186.250.48.5:443",
    "103.71.99.57:8080",
    "85.214.67.203:8080",
    "85.25.120.45:8080",
    "139.196.72.155:8080",
    "103.85.95.4:8080",
    "198.199.70.22:8080",
    "209.239.112.82:8080",
    "78.47.204.80:443",
    "36.67.23.59:443",
    "104.244.79.94:443",
    "62.171.178.147:8080",
    "195.77.239.39:8080",
    "103.56.149.105:8080",
    "80.211.107.116:8080",
    "93.104.209.107:8080",
    "174.138.33.49:7080",
    "202.28.34.99:8080",
    "178.62.112.199:8080",
    "114.79.130.68:443",
    "118.98.72.86:443",
    "103.41.204.169:8080",
    "178.238.225.252:8080",
    "83.229.80.93:8080",
    "46.101.98.60:8080",
    "82.98.180.154:7080",
    "87.106.97.83:7080",
    "196.44.98.190:8080",
    "139.59.80.108:8080",
    "103.224.241.74:8080",
    "103.254.12.236:7080",
    "185.148.169.10:8080",
    "165.22.254.236:8080",
    "37.44.244.177:8080",
    "54.37.228.122:443",
    "51.75.33.122:443",
    "128.199.217.206:443",
    "188.165.79.151:443",
    "210.57.209.142:8080",
    "160.16.143.191:8080",
    "175.126.176.79:8080",
    "202.134.4.210:7080",
    "103.126.216.86:443",
    "190.145.8.4:443",
    "128.199.242.164:8080",
    "64.227.55.231:8080"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0UPxu9nIvAI4=",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCWof1h9lMsAJA="
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.268670128.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.773669828.000000000B00000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000013.00000002.417010229.000000000CF0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.270742537.000002AB001A0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.774717427.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 7 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.regsvr32.exe.2d00000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
6.2.regsvr32.exe.b00000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.2ab001a0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.13b3e6b0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
19.2.regsvr32.exe.cf0000.0.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 3 - Source IP: 192.168.2.3 - Destination IP: 115.178.55.22

Timestamp:	192.168.2.3115.178.55.2249700802404304 11/13/22-17:16:57.501080
SID:	2404304
Source Port:	49700
Destination Port:	80
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

Boot Survival

Creates an autostart registry key pointing to binary in C:\Windows

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

Copyright Joe Security LLC 2022

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

Stealing of Sensitive Information

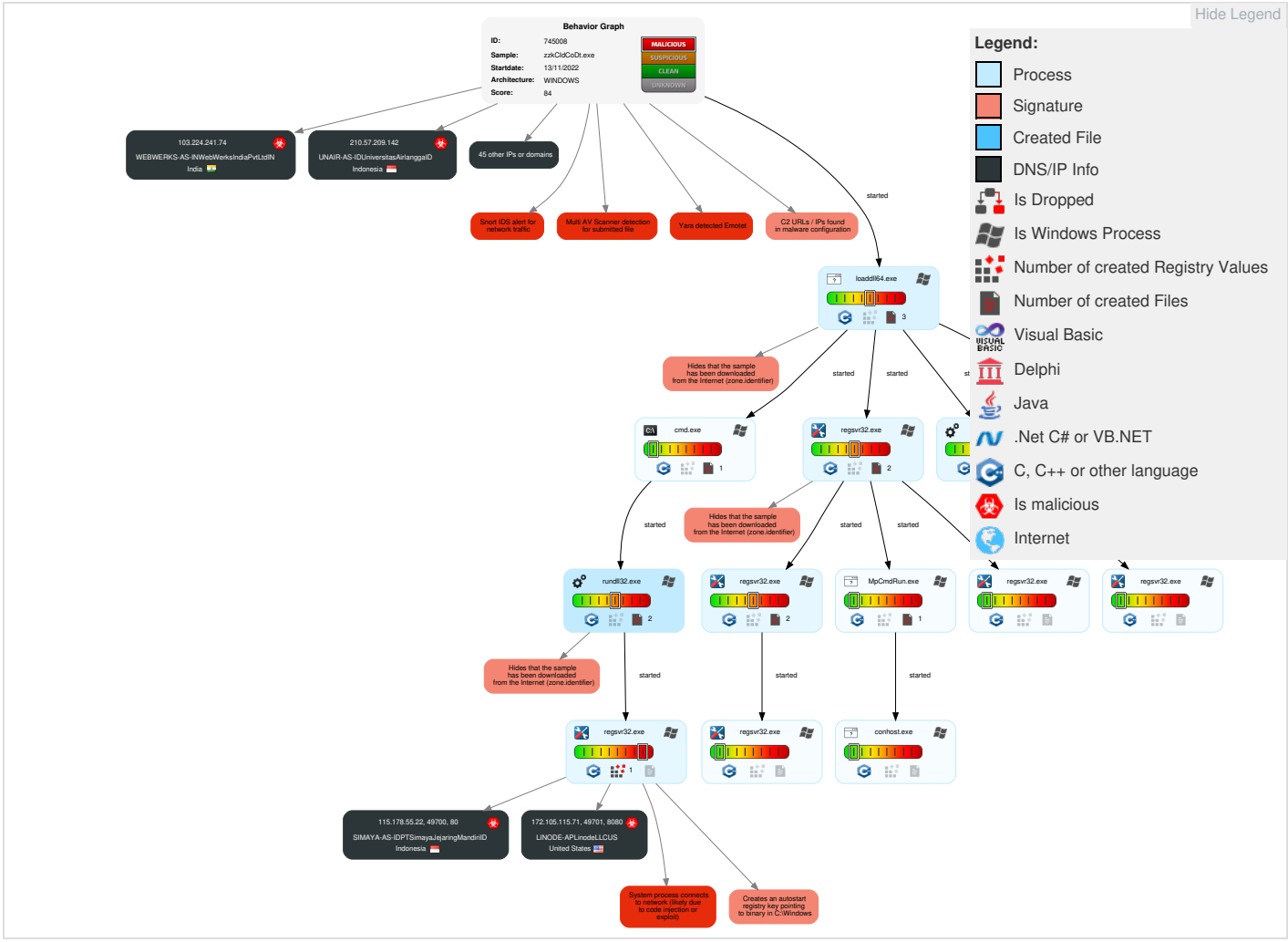


Yara detected Emotet

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	1 Windows Management Instrumentation	1 1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	2 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 1 Registry Run Keys / Startup Folder	2 Virtualization/Sandbox Evasion	LSASS Memory	4 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 1 1 Process Injection	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Hidden Files and Directories	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Regsvr32	Cached Domain Credentials	2 File and Directory 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 Rundll32	DCSync	2 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	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 File Deletion	/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

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
zzkCldCoDt.dll	44%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.regsvr32.exe.2d00000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.rundll32.exe.2ab001a0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
19.2.regsvr32.exe.cf0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
6.2.regsvr32.exe.b00000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.13b3e6b0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.2.loaddll64.exe.195a6500000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Copyright Joe Security LLC 2022

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://172.105.115.71:8080/xucipr/ysjolf/ncmjlqi/	0%	Avira URL Cloud	safe	
http://https://172.105.115.71:8080/z	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://https://172.105.115.71:8080/xucipr/ysjolf/ncmjlqi/	regsvr32.exe, 00000006.00000003.50597206 2.0000000000925000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.377253951.000000000091D000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.377685 702.0000000000920000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.505596792.000000000092500 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.772134880.0000 0000008B8000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000006.00 000002.772698476.0000000000925000.000000 04.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://172.105.115.71:8080/z	regsvr32.exe, 00000006.00000002.77257215 2.0000000000905000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.506108273.0000000000905000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.505525 715.00000000008FF000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.377753779.00000000008FE00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.105.115.71	unknown	United States		63949	LINODE-APLinodeLLCUS	true
188.165.79.151	unknown	France		16276	OVHFR	true
196.44.98.190	unknown	Ghana		327814	EcobandGH	true
174.138.33.49	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
36.67.23.59	unknown	Indonesia		17974	TELKOMNET-AS2-APPTTelekomunikasiIndonesiaID	true
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	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
186.250.48.5	unknown	Brazil		262807	RedfoxTelecomunicacoesLtdaBR	true
209.239.112.82	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	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
178.238.225.252	unknown	Germany		51167	CONTABODE	true
46.101.98.60	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
190.145.8.4	unknown	Colombia		14080	TelmexColombiaSACO	true
82.98.180.154	unknown	Spain		42612	DINAHOSTING-ASES	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

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
202.134.4.210	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	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
104.244.79.94	unknown	United States		53667	PONYNETUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
51.75.33.122	unknown	France		16276	OVHFR	true
160.16.143.191	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
103.56.149.105	unknown	Indonesia		55688	BEON-AS-IDPTBeonIntermediaID	true
85.25.120.45	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
115.178.55.22	unknown	Indonesia		38783	SIMAYA-AS-IDPTSimayaJejaringMandiriID	true
103.126.216.86	unknown	Bangladesh		138482	SKYVIEW-AS-APSKYVIEWONLINELTDBD	true
128.199.217.206	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
114.79.130.68	unknown	India		45769	DVOIS-IND-VoisBroadbandPvtLtdIN	true
103.224.241.74	unknown	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
202.28.34.99	unknown	Thailand		9562	MSU-TH-APMahasarakhamUniversityTH	true
80.211.107.116	unknown	Italy		31034	ARUBA-ASNIT	true
54.37.228.122	unknown	France		16276	OVHFR	true
218.38.121.17	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
185.148.169.10	unknown	Germany		44780	EVERSCALE-ASDE	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

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	745008
Start date and time:	2022-11-13 17:15:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zzkCIdCoDt.exe (renamed file extension from exe to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Copyright Joe Security LLC 2022

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:	mal84.troj.evad.winDLL@22/3@0/49
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 58.8% (good quality ratio 53.5%) • Quality average: 61.7% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 8.238.88.248, 8.238.191.126, 8.248.117.254, 8.238.85.126, 8.238.190.126
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:16:59	API Interceptor	2x Sleep call for process: regsvr32.exe modified
17:17:14	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run siQPBMdwCPAb.dll C:\Windows\system32\regsvr32.exe "C:\Windows\system32\AmhzcKVtZLl\siQPBMdwCPAb.dll"
17:17:30	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

<table>
<tr><th colspan="2">C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506</th></tr>
<tr><td>Process:</td><td>C:\Windows\System32\regsvr32.exe</td></tr>
<tr><td>File Type:</td><td>Microsoft Cabinet archive data, Windows 2000/XP setup, 62919 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>62919</td></tr>
<tr><td>Entropy (8bit):</td><td>7.995280921994772</td></tr>
<tr><td>Encrypted:</td><td>true</td></tr>
<tr><td>SSDEEP:</td><td>1536:d+OfVxHl7Wyf11lYom3xQcRVOtPHwQV4rP6Ji7:d+OxHxJlZcuPt4b6q</td></tr>
<tr><td>MD5:</td><td>3DCF580A93972319E82CAFBC047D34D5</td></tr>
<tr><td>SHA1:</td><td>8528D2A1363E5DE77DC3B1142850E51EAD0F4B6B</td></tr>
<tr><td>SHA-256:</td><td>40810E31F1B69075C727E6D557F9614D5880112895FF6F4DF1767E87AE5640D1</td></tr>
<tr><td>SHA-512:</td><td>98384BE7218340F95DAE88D1CB865F23A0B4E12855BEB6E74A3752274C9B4C601E493864DB777BCA677A370D0A9DBFFD68D94898A82014537F3A801CCE839C4</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>MSCF...........,...................I.......Q.........GU.\ .authroot.stl..O..5..CK..<Tk...c_.d....A.K...+.d.-;%.BJII!.QIR..$t)Kd.-QQ*...g......^..~|N=...y....{. .4{...W....b.i...j.I.......1:..b\.0....
.Ait.2t......w.%.&.",tL_...4.8L[G..;.57....AT.k.......V..K......(....mzS...G....r.".=H.?>.........x&...S%....X.M^..j...A..x.9`.9...A../.s..#.4#.....Id.w..B....s.8..(...dj....=L.)..s.d.]NxQX8<br>....stV#.K.'7.tH..9u~.2..!..2./.....!..9C../...mP $..../y.....@p.6.}.`...5. 0r.w...@(.. .Q....)g.........m..z*.8rR..).].T9r<.L....0..`.........c.....;-.g..;.wk.)......i..c5.....{v.u...AS..=.....&.:...<br>......+..P.N..9..EAQ.V.$s.......B.`.Mfe..8.......$...y-.q9J........W...2.Q8...O.......i..@\^.=X..dG$.M..#=....m.h..{9.'...-.v..Z...!....z.....N....i..^..,........d...%Xa~q.@D|0...Y.m........
...&d.4..A..{t=...../.t.3._.....?-.....uroP?.d.Z..S..{...$.i....X..$.O..4..N.)....U.Z..P....X,.... ...Lg..35..W..s.!c...Ap.].P..8..M..W.......U..,...m.u..|=.m1..~..!..b...._.</td></tr>
</table>

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.1108374798811247
Encrypted:	false
SSDEEP:	6:kK/VSaTN1HlNiN+SkQlPlEGYRMY9z+4KlDA3RUeKlTAlWRyf1:34aB/kPlE99SNxAhUexYo1
MD5:	43156C86A7520289C41B5FA58959ECAE
SHA1:	C79779653F313D6F972EE358013D5A3E344F9E3A
SHA-256:	5F60BF4848F60492318892444B27705228496879AC1E166F78917C1C1B620F1B
SHA-512:	B1B8399D9D0BEEB9DCCAD8E0A41D40BC28A9ADFA2EC742F7742D8A6B4D2D01ACADAF4AEE06746101829F4D599089AF4C5C1F3BB0702DA39EA83745B79675F E09
Malicious:	false
Preview:	p...... ....(... ....&..............h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c ./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.d.e.4.d.3.9.b.e.8.d.8.1.:.0."...

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	modified
Size (bytes):	10874
Entropy (8bit):	3.1666030657719118
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3z5+6I3+zJ8+3:j+s+v+b+P+m+0+Q+q+q+73+zu+3
MD5:	40867086CD88892047DB348A9F686336
SHA1:	2F8B90ABDEA0B274E574A7365D64C853A55AC941
SHA-256:	A096F8B4C7D36A3FEEB75B860BC71F12B2727778CD3C37B9A4D54BBFE9ADB577
SHA-512:	DA627DE66503A077607A37D3E28516FE8E556DBA0C0FA616BF9BE83879A32FA93CEF92737E6C5228BCBE4717C18FEB57F78DFF81ACD0776DD0496AA95EBC79 BA
Malicious:	false
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....- .-.............-.

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.6191658194371135
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:	zzkCldCoDt.dll
File size:	528896
MD5:	e383dda8987435a6a3950aa9a6909b2c
SHA1:	8b3982937eddd443b671161e04c80a2ed5e68818
SHA256:	8c1db84c9f86675e3487960e5275fdf2e690b53eff1879e2d72673463fe1055a
SHA512:	aa91286c79e99ca2d983b4ba397c2e02e0aa60b2e06b05cb185106f547731bb4ed31db9ab88ef99ce7e384421db9a68f1ad10f623c7a59e244e8584428d6f5b1
SSDEEP:	6144:mW1239bnTe+0Qv7NSEBj43USaI6Y/jOpxHRikSYI+QALgIJ1divndEXBn:mW1e9PeexPBjvKSpuvYI+TLgs1dcEXB
TLSH:	56B40829A59E76F0C951A1F5A0420B1595F33C88FEF68EAF03502F296F6F24425F768C
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....$...s...$.....$.....$.....`.....`.....e.h.....`.....Rich.....

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1800044e0
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, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x636D6724 [Thu Nov 10 21:03:32 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:	81146e0614ccc4eb7174ad2ad695dedb

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

Instruction
mov esi, ecx
cmp edx, 01h
jne 00007FC5B072B557h
call 00007FC5B072BAE8h
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
pop edi
jmp 00007FC5B072B3CCh
int3
int3
int3
inc eax
push ebx
dec eax
sub esp, 20h
dec eax
mov ebx, ecx
dec eax
mov eax, edx
dec eax
lea ecx, dword ptr [00033F0Dh]
dec eax
mov dword ptr [ebx], ecx
dec eax
lea edx, dword ptr [ebx+08h]
xor ecx, ecx
dec eax
mov dword ptr [edx], ecx
dec eax
mov dword ptr [edx+08h], ecx
dec eax
lea ecx, dword ptr [eax+08h]
call 00007FC5B072DD51h
dec eax
lea eax, dword ptr [00033F1Dh]
dec eax
mov dword ptr [ebx], eax
dec eax
mov eax, ebx
dec eax
add esp, 20h
pop ebx
ret
int3
xor eax, eax
dec eax
mov dword ptr [ecx+10h], eax
dec eax
lea eax, dword ptr [00033F13h]
dec eax

Instruction
mov dword ptr [ecx+08h], eax
dec eax
lea eax, dword ptr [00033EF8h]
dec eax
mov dword ptr [ecx], eax
dec eax
mov eax, ecx
ret
int3
inc eax
push ebx
dec eax
sub esp, 20h
dec eax
mov ebx, ecx
dec eax
mov eax, edx
dec eax
lea ecx, dword ptr [00033EADh]
dec eax
mov dword ptr [ebx], ecx
dec eax
lea edx, dword ptr [ebx+08h]
xor ecx, ecx
dec eax
mov dword ptr [edx], ecx
dec eax
mov dword ptr [edx+08h], ecx
dec eax
lea ecx, dword ptr [eax+08h]

Rich Headers

Programming Language:	• [EXP] VS2015 UPD3.1 build 24215 • [RES] VS2015 UPD3 build 24213 • [LNK] VS2015 UPD3.1 build 24215

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x7cda0	0x58	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7cdf8	0x78	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x87000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x82000	0x192c	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0x66c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x7a410	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	0x7a430	0x94	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x38000	0x370	.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

Copyright Joe Security LLC 2022

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x36fd5	0x37000	False	0.38967507102272725	data	5.930785005703424	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x38000	0x4597a	0x45a00	False	0.670528500897666	data	6.275564116113403	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x7e000	0x3394	0xc00	False	0.18294270833333334	DOS executable (block device driver \337-\231+])	2.573523630872546	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x82000	0x192c	0x1a00	False	0.4794170673076923	data	5.1711441720039435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gfids	0x84000	0xdc	0x200	False	0.244140625	Spectrum .TAP data "6 " - BASIC program	1.1531659578770692	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gxfg	0x85000	0x1000	0x1000	False	0.44091796875	data	5.088628746947821	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gehcont	0x86000	0xc	0x200	False	0.0390625	data	0.06116285224115448	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x87000	0x1e0	0x200	False	0.52734375	data	4.724728911998389	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0x66c	0x800	False	0.537109375	data	4.9054360857170005	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x87060	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetConsoleMode, GetConsoleOutputCP, WriteFile, FlushFileBuffers, SetStdHandle, HeapReAlloc, HeapSize, SetFilePointerEx, ExitProcess, GetStdHandle, GetProcessHeap, CreateFileW, CloseHandle, GetStringTypeW, LCMapStringW, GetFileType, VirtualAlloc, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, RtlPcToFileHeader, EncodePointer, RaiseException, RtlUnwindEx, InterlockedFlushSList, GetLastError, SetLastError, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, GetModuleHandleExW, GetModuleFileNameW, HeapFree, HeapAlloc, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, MultiByteToWideChar, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsW, FlsAlloc, FlsGetValue, FlsSetValue, FlsFree, WriteConsoleW
USER32.dll	EndPaint, BeginPaint, InvalidateRect, GetMessageW, DefWindowProcW, CloseTouchInputHandle, GetTouchInputInfo, DestroyWindow, MessageBoxW, CreateWindowExW, RegisterClassExW, LoadStringW, ShowWindow, DispatchMessageW, RegisterTouchWindow, MessageBoxA, UnregisterTouchWindow, TranslateAcceleratorW, TranslateMessage, LoadCursorW, PostQuitMessage, UpdateWindow
GDI32.dll	Polyline, LineTo, CreatePen, MoveToEx, DeleteObject, SelectObject
ole32.dll	CoUninitialize, CoCreateInstance, CoInitialize
CRYPT32.dll	CryptStringToBinaryA

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x180013f70

Possible Origin

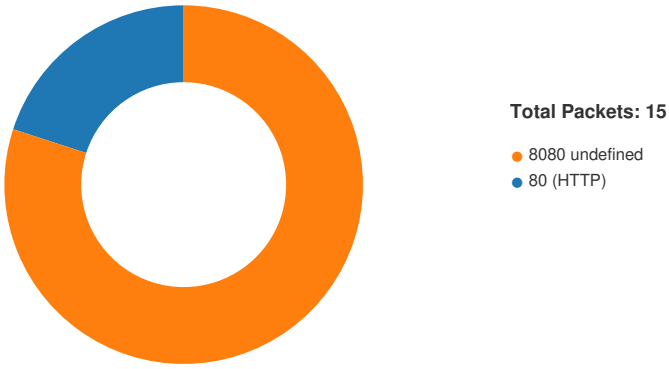
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3115.178.55.22 49700802404304 11/13/22-17:16:57.501080	TCP	2404304	ET CNC Feodo Tracker Reported CnC Server TCP group 3	49700	80	192.168.2.3	115.178.55.22

Network Port Distribution



TCP Packets

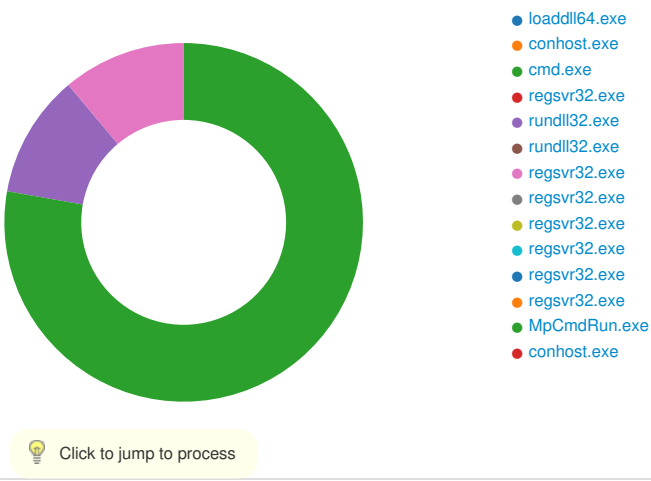
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 13, 2022 17:16:57.501080036 CET	49700	80	192.168.2.3	115.178.55.22
Nov 13, 2022 17:16:57.795387030 CET	80	49700	115.178.55.22	192.168.2.3
Nov 13, 2022 17:16:58.302907944 CET	49700	80	192.168.2.3	115.178.55.22
Nov 13, 2022 17:16:58.596817970 CET	80	49700	115.178.55.22	192.168.2.3
Nov 13, 2022 17:16:59.099888086 CET	49700	80	192.168.2.3	115.178.55.22
Nov 13, 2022 17:16:59.393485069 CET	80	49700	115.178.55.22	192.168.2.3
Nov 13, 2022 17:17:05.935923100 CET	49701	8080	192.168.2.3	172.105.115.71
Nov 13, 2022 17:17:06.101063967 CET	8080	49701	172.105.115.71	192.168.2.3
Nov 13, 2022 17:17:06.101551056 CET	49701	8080	192.168.2.3	172.105.115.71
Nov 13, 2022 17:17:06.106664896 CET	49701	8080	192.168.2.3	172.105.115.71
Nov 13, 2022 17:17:06.270914078 CET	8080	49701	172.105.115.71	192.168.2.3
Nov 13, 2022 17:17:06.287955999 CET	8080	49701	172.105.115.71	192.168.2.3
Nov 13, 2022 17:17:06.287991047 CET	8080	49701	172.105.115.71	192.168.2.3
Nov 13, 2022 17:17:06.288209915 CET	49701	8080	192.168.2.3	172.105.115.71
Nov 13, 2022 17:17:06.298588991 CET	49701	8080	192.168.2.3	172.105.115.71
Nov 13, 2022 17:17:06.462768078 CET	8080	49701	172.105.115.71	192.168.2.3
Nov 13, 2022 17:17:06.463995934 CET	8080	49701	172.105.115.71	192.168.2.3
Nov 13, 2022 17:17:06.603993893 CET	49701	8080	192.168.2.3	172.105.115.71
Nov 13, 2022 17:17:07.991117954 CET	49701	8080	192.168.2.3	172.105.115.71
Nov 13, 2022 17:17:07.991117954 CET	49701	8080	192.168.2.3	172.105.115.71
Nov 13, 2022 17:17:08.155518055 CET	8080	49701	172.105.115.71	192.168.2.3
Nov 13, 2022 17:17:08.155549049 CET	8080	49701	172.105.115.71	192.168.2.3
Nov 13, 2022 17:17:08.783451080 CET	8080	49701	172.105.115.71	192.168.2.3
Nov 13, 2022 17:17:08.835866928 CET	49701	8080	192.168.2.3	172.105.115.71
Nov 13, 2022 17:17:11.787537098 CET	8080	49701	172.105.115.71	192.168.2.3
Nov 13, 2022 17:17:11.787573099 CET	8080	49701	172.105.115.71	192.168.2.3
Nov 13, 2022 17:17:11.787766933 CET	49701	8080	192.168.2.3	172.105.115.71
Nov 13, 2022 17:17:11.788121939 CET	49701	8080	192.168.2.3	172.105.115.71

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 13, 2022 17:17:11.788218975 CET	49701	8080	192.168.2.3	172.105.115.71
Nov 13, 2022 17:17:11.952151060 CET	8080	49701	172.105.115.71	192.168.2.3
Nov 13, 2022 17:17:11.952179909 CET	8080	49701	172.105.115.71	192.168.2.3

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 5224, Parent PID: 3452

General

Target ID:	0
Start time:	17:16:08
Start date:	13/11/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\zzkCIdCoDt.dll"
Imagebase:	0x7ff76dba0000
File size:	139776 bytes
MD5 hash:	C676FC0263EDD17D4CE7D644B8F3FCD6
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: 00000000.00000002.267859077.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.268192562.00000195A6500000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2022

Analysis Process: conhost.exe PID: **5236**, Parent PID: **5224**

General	
Target ID:	1
Start time:	17:16:08
Start date:	13/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **2068**, Parent PID: **5224**

General	
Target ID:	2
Start time:	17:16:09
Start date:	13/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\zzkCIdCoDt.dll",#1
Imagebase:	0x7ff707bb0000
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: **5452**, Parent PID: **5224**

General	
Target ID:	3
Start time:	17:16:09
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\zzkCIdCoDt.dll
Imagebase:	0x7ff7453b0000
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: 00000003.00000002.270672400.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.269235056.0000000002D00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5456, Parent PID: 2068

General

Target ID:	4
Start time:	17:16:09
Start date:	13/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\zzkCIdCoDt.dll",#1
Imagebase:	0x7ff78b8b0000
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: 00000004.00000002.265684139.0000013B3E6B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.265510793.0000000180001000.00000020.00001000.00020000.00000000.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\AmhzcKVtZLl\siQPBMdwCPAb.dll:Zone.Identifier	success or wait	1	180020786	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: 5488, Parent PID: 5224

General

Target ID:	5
Start time:	17:16:09
Start date:	13/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\zzkCIdCoDt.dll,DllRegisterServer
Imagebase:	0x7ff78b8b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true

Copyright Joe Security LLC 2022

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.268670128.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.270742537.000002AB001A0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **5160**, Parent PID: **5456**

General

Target ID:	6
Start time:	17:16:16
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\AmhzcKVtZLI\siQPBMdwCPAb.dll"
Imagebase:	0x7ff7453b0000
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: 00000006.00000002.773669828.0000000000B00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.774717427.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	siQPBMdwCPAb.dll	unicode	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\AmhzcKVtZLI\siQPBMdwCPAb.dll"	success or wait	1	180003442	RegSetValueExW

Analysis Process: regsvr32.exe PID: **5144**, Parent PID: **5452**

General

Target ID:	7
Start time:	17:16:16
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\QxWCKZstQphkP\egknjpoziqlzVL.dll"
Imagebase:	0x7ff7453b0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **3044**, Parent PID: **5224**

General

Target ID:	8
Start time:	17:16:17
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\CXPSzCIcOMY\wxJWjHQhm.dll"
Imagebase:	0x7ff7453b0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **736**, Parent PID: **5488**

General

Target ID:	9
Start time:	17:16:17
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\BlngRITsHraAEaQWw\tRWuLwwWwn.dll"
Imagebase:	0x7ff7453b0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **5144**, Parent PID: **3452**

General

Target ID:	19
Start time:	17:17:22
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe" "C:\Windows\system32\AmhzcKVtZLl\siQPBMdwCPAb.dll
Imagebase:	0x7ff7453b0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.417010229.0000000000CF0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.417174444.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **3796**, Parent PID: **5144**

General

Target ID:	20
Start time:	17:17:27
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Users\user\AppData\Local\UOEgTmwbpKANXEqN\KElhycJrzKCpLgeP.dll"
Imagebase:	0x7ff7453b0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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: MpCmdRun.exe PID: **3968**, Parent PID: **5452**

General

Target ID:	21
Start time:	17:17:29
Start date:	13/11/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff68f300000

File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	9968	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF7757FBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10150	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 75 00 6e 00 20 00 0e 20 4e 00 6f 00 76 00 20 00 0e 20 31 00 33 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 31 00 37 00 3a 00 31 00 37 00 3a 00 32 00 39 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Sun Nov 13 2022 17:17:29	success or wait	1	7FF7757FBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10408	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF7757FBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10494	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF7757FBC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10514	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF7757FBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10600	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 75 00 6e 00 20 00 0e 20 4e 00 6f 00 76 00 20 00 0e 20 31 00 33 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 31 00 37 00 3a 00 31 00 37 00 3a 00 33 00 30 00 0d 00 0a 00	MpCmdRun: End Time: Sun Nov 13 2022 17:17:30	success or wait	1	7FF7757FBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10700	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF7757FBC96	WriteFile

Analysis Process: conhost.exe PID: **2072**, Parent PID: **3968**

General

Target ID:	22
Start time:	17:17:29
Start date:	13/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly