ID: 747450
Sample Name:
UC2DFXQIBiE2kQ.dll
Cookbook: default.jbs
Time: 11:58:13
Date: 16/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

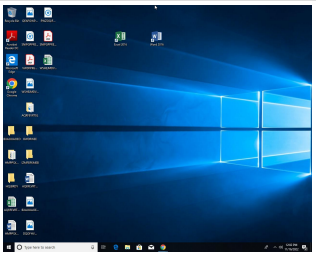
Windows Analysis Report

UC2DFXQIBiE2kQ.dll

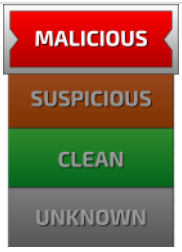
Overview

General Information

Sample Name:	UC2DFXQIBiE2kQ.dll
Analysis ID:	747450
MD5:	e2ec88ae31e147..
SHA1:	937a21ced7f266..
SHA256:	ae7e655db35a71..
Infos:	



Detection



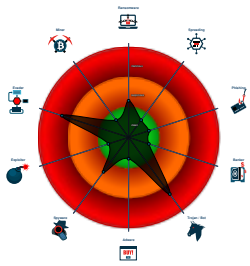
Emotet

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…
- Contains functionality to query local…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6056 cmdline: loaddll64.exe "C:\Users\user\Desktop\UC2DFXQIBiE2kQ.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 6100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6048 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\UC2DFXQIBiE2kQ.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6072 cmdline: rundll32.exe "C:\Users\user\Desktop\UC2DFXQIBiE2kQ.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 6076 cmdline: regsvr32.exe /s C:\Users\user\Desktop\UC2DFXQIBiE2kQ.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 5292 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\CqZilJuzKBQGfIL\PYmtZH.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 6052 cmdline: rundll32.exe C:\Users\user\Desktop\UC2DFXQIBiE2kQ.dll,ACeujVZMknFDjv MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5172 cmdline: rundll32.exe C:\Users\user\Desktop\UC2DFXQIBiE2kQ.dll,AHuDGMfIBfPryOEYjuTfbzJdEM MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5244 cmdline: rundll32.exe C:\Users\user\Desktop\UC2DFXQIBiE2kQ.dll,ATjQPkInxPUGuUu MD5: 73C519F050C20580F8A62C849D49215A)
- regsvr32.exe (PID: 5104 cmdline: C:\Windows\system32\regsvr32.exe" "C:\Windows\system32\CqZilJuzKBQGfIL\PYmtZH.dll MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 972 cmdline: C:\Windows\system32\regsvr32.exe "C:\Users\user\AppData\Local\OKCYiYOFwZjDclsn\OYsSIVLvWy.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"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.256991395.000001B505A51000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.261455242.0000000002D51000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.260696945.0000000001220000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.254973039.0000024188500000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000012.00000002.409592549.00000000013D0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.24188500000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.1220000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
7.2.regsvr32.exe.2080000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.regsvr32.exe.2080000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.1b505730000.0.raw.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: 192.168.2.5 - Destination IP: 115.178.55.22

Timestamp:	192.168.2.5115.178.55.2249702802404304 11/16/22-11:48:03.539047
SID:	2404304
Source Port:	49702
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

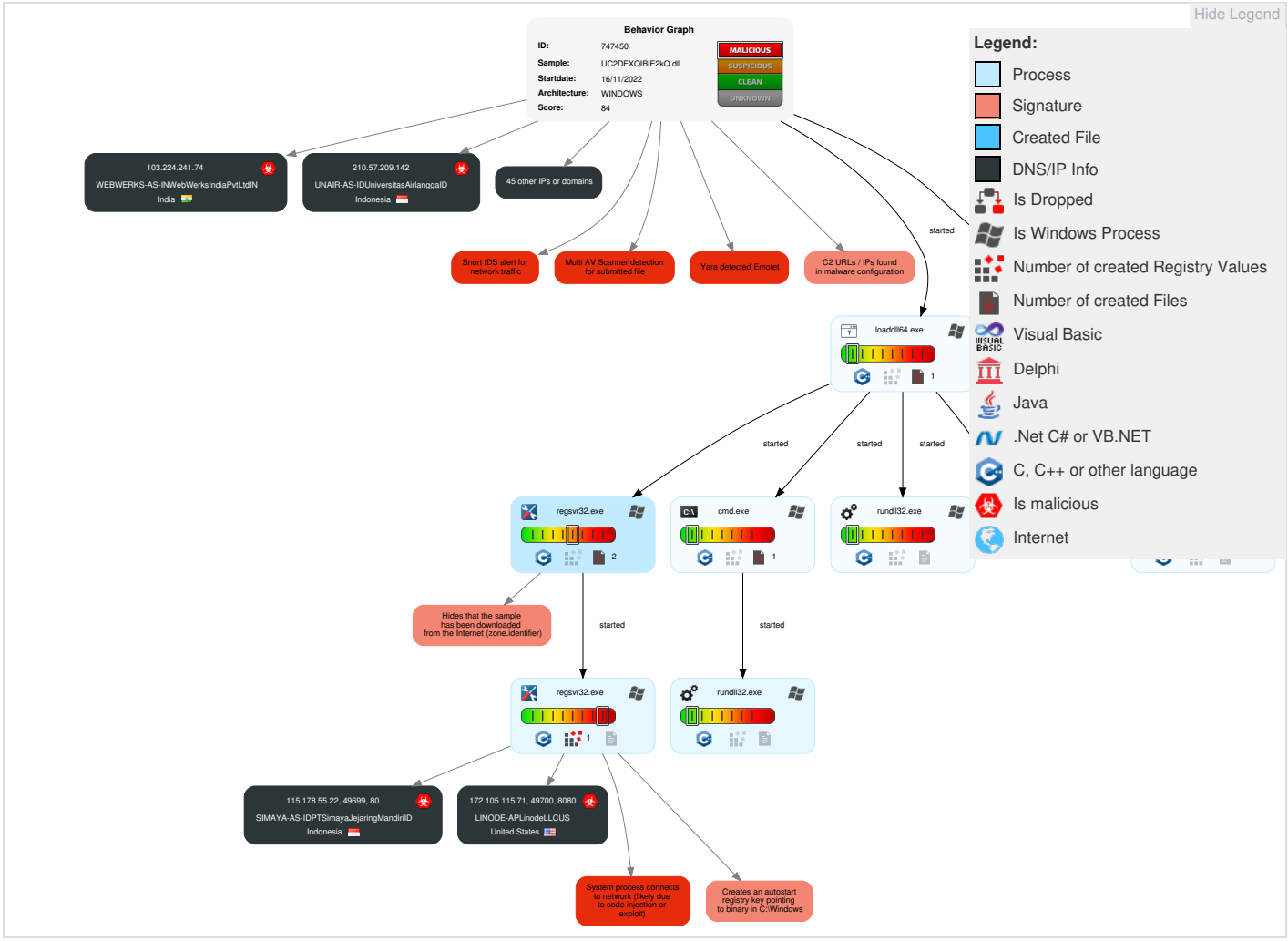
System process connects to network (likely due to code injection or exploit)

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 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	3 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 Deobfuscate/Decode Files or Information	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 Hidden Files and Directories	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	2 Obfuscated Files or Information	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 Regsvr32	DCSync	3 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 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

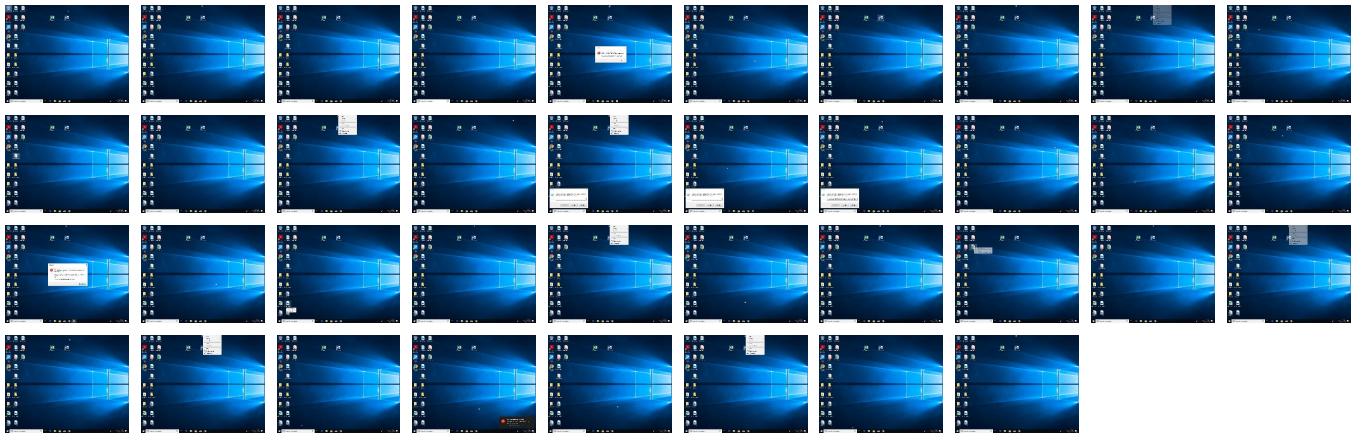
Behavior Graph



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
UC2DFXQIBiE2kQ.dll	81%	ReversingLabs	Win64.Trojan.Emotet	
UC2DFXQIBiE2kQ.dll	65%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.24188500000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.regsvr32.exe.1220000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.rundll32.exe.1b505730000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
18.2.regsvr32.exe.13d0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
6.2.rundll32.exe.1deaae80000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.regsvr32.exe.2080000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

Source	Detection	Scanner	Label	Link
windowsupdatebg.s.llnwi.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://172.105.115.71:8080/qfmakzntwajcoi/xgtrfra/	0%	Avira URL Cloud	safe	
http://https://172.105.115.71:8080/qfmakzntwajcoi/xgtrfra/O	0%	Avira URL Cloud	safe	
http://https://172.105.115.71:8080/s	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
windowsupdatebg.s.llnwi.net	95.140.236.0	true	false	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://172.105.115.71:8080/s	regsvr32.exe, 00000007.00000002.64420588 2.00000000007B9000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000003.377022283.00000000007AE000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.498731 511.00000000007AF000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00007.00000003.498831398.00000000007B800 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://172.105.115.71:8080/qfmakzntwajcoi/xgtrfra/O	regsvr32.exe, 00000007.00000003.37693849 0.00000000007D1000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000002.644320880.00000000007D5000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.376525 428.00000000007CE000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://172.105.115.71:8080/qfmakzntwajcoi/xgtrfra/	regsvr32.exe, 00000007.00000002.64386791 5.0000000000768000.00000004.00000020.000 20000.00000000.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

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:	747450
Start date and time:	2022-11-16 11:58:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	UC2DFXQIBiE2kQ.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	25
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:	mal84.troj.evad.winDLL@19/2@0/49
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 82% (good quality ratio 74.8%) • Quality average: 72.8% • Quality standard deviation: 32.3%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 95.140.236.0
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com, wu-bg-shim.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 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
12:00:08	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run PYmtZH.dll C:\Windows\system32\regsvr32.exe "C:\Windows\system32\CqZilJuzKBQGflL\PYmtZH.dll"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 62919 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	62919
Entropy (8bit):	**7.995280921994772**
Encrypted:	**true**
SSDEEP:	1536:d+OfVxHl7Wyf11lYom3xQcRVOtPHwQV4rP6Ji7:d+OxHxJlZcuPt4b6q
MD5:	3DCF580A93972319E82CAFBC047D34D5
SHA1:	8528D2A1363E5DE77DC3B1142850E51EAD0F4B6B
SHA-256:	40810E31F1B69075C727E6D557F9614D5880112895FF6F4DF1767E87AE5640D1
SHA-512:	98384BE7218340F95DAE88D1CB865F23A0B4E12855BEB6E74A3752274C9B4C601E493864DB777BCA677A370D0A9DBFFD68D94898A82014537F3A801CCE839C4
Malicious:	false
Preview:	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.l.....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#.....ld.w..B....s.8..(...dj....=L.)..s.d.]NxQX8 ....stV#.K.'7.tH..9u~.2..!..2./.....!..9C../...mP $..../y.....@p.6.}.`...5. 0r.w...@(.. .Q....)g.....m..z*.8rR..).].T9r<.L....0..`.....c.....;-.g..;.wk.).....i..c5.....{v.u...AS..=.....&.:... .....+..P.N..9..EAQ.V.$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...._.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	290
Entropy (8bit):	2.94999131157485
Encrypted:	false
SSDEEP:	6:kK3NzlNiN+SkQlPlEGYRMY9z+4KlDA3RUe/:FVkPlE99SNxAhUe/
MD5:	B68D3B9288C662D5D5C5AC656C356D98
SHA1:	99831C9C3EB93352282430B1F0D4A611545669A3
SHA-256:	91879FFA5FB7B6C7EC7C55618811C6FA5BE2B661EF8FD5D3072CEEB338264AC6
SHA-512:	45A3095424C3B31A65D69A925202518A8C2F80AAE5EB7D0140EFB0F6589478278CDAB22CB7E74144441DBFD912F73FD36B79E1ACFA747342862C664CABB39E8A
Malicious:	false
Preview:	p..... .....@r}.....(..... .....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...

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.82554843363977
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:	UC2DFXQlBiE2kQ.dll
File size:	636416
MD5:	e2ec88ae31e147d1976368c6a8988d3c
SHA1:	937a21ced7f2663c923c9c614cbe06d95def511a
SHA256:	ae7e655db35a71a3b2df96051d722d7995ec94feea3cbd59bec501042ab40847
SHA512:	ce9c95d721ee389dbbe3d7758d51bdde38f608675c7123d61fa6e0fde500e677651c043be3ef1d52d424b4a1d80d7191cb180887a8944059634ca55042bfa278
SSDEEP:	6144:S6/ptuaN+qWUILr1HRf/9Mu1vHLI7U9XWi9gQ30/bP/09Xls9HV6MExbnyDAzlsH:S6/ptu/qerXtU7U9XUZWYobyDAzl+
TLSH:	A7D4BE04B2AC40B5D5BBC17AC8A3592AE2B27C524764D7CB13A107BA1F2B7E11D3FB51
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\.....\.....\.r.....\.....Rich...

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180002e54
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:	0x636C09DF [Wed Nov 9 20:13:19 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:	bf309f28e2e75a572eb2f2244be62b26

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 00007FF968972187h
call 00007FF968972BDCh
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 00007FF968971FF0h
int3
int3
int3

Instruction
inc eax
push ebx
dec eax
sub esp, 20h
dec eax
mov ebx, ecx
xor ecx, ecx
call dword ptr [00049283h]
dec eax
mov ecx, ebx
call dword ptr [00049272h]
call dword ptr [0004927Ch]
dec eax
mov ecx, eax
mov edx, C0000409h
dec eax
add esp, 20h
pop ebx
dec eax
jmp dword ptr [00049270h]
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 38h
mov ecx, 00000017h
call dword ptr [00049264h]
test eax, eax
je 00007FF968972189h
mov ecx, 00000002h
int 29h
dec eax
lea ecx, dword ptr [00095FC2h]
call 00007FF96897245Eh
dec eax
mov eax, dword ptr [esp+38h]
dec eax
mov dword ptr [000960A9h], eax
dec eax
lea eax, dword ptr [esp+38h]
dec eax
add eax, 08h
dec eax
mov dword ptr [00096039h], eax
dec eax
mov eax, dword ptr [00096092h]
dec eax
mov dword ptr [00095F03h], eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x94ef0	0x1a30	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x96920	0x78	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa0000	0x268	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x9b000	0x3b34	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa1000	0x860	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x916a8	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x916d0	0x138	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x4c000	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	0x4a1e5	0x4a200	False	0.48174009274873525	data	6.479787977595784	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x4c000	0x4b592	0x4b600	False	0.611217998548922	data	6.281987992518068	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x98000	0x2a44	0xe00	False	0.18052455357142858	DOS executable (block device driver \322f\324\377\3772)	2.7637122521836313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x9b000	0x3b34	0x3c00	False	0.46953125	data	5.536843174034769	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
_RDATA	0x9f000	0xf4	0x200	False	0.30078125	data	1.982153456785509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xa0000	0x268	0x400	False	0.3173828125	data	3.200437559634333	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa1000	0x860	0xa00	False	0.46796875	data	5.031424688639632	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_STRING	0xa00a0	0x48	data	English	United States
RT_MANIFEST	0xa00e8	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
USER32.dll	MessageBoxA, InvalidateRect, GetMessageW, DefWindowProcW, DestroyWindow, CreateWindowExW, RegisterClassExW, LoadStringW, ShowWindow, DispatchMessageW, SetGestureConfig, GetGestureInfo, TranslateAcceleratorW, TranslateMessage, LoadCursorW, PostQuitMessage, UpdateWindow, BeginPaint, EndPaint, CloseGestureInfoHandle, ScreenToClient
GDI32.dll	Polyline, LineTo, CreatePen, MoveToEx, DeleteObject, SelectObject
ole32.dll	CoLoadLibrary
CRYPT32.dll	CryptStringToBinaryA
KERNEL32.dll	GetConsoleMode, GetConsoleCP, WriteFile, FlushFileBuffers, SetStdHandle, HeapReAlloc, GetFileSizeEx, WriteConsoleW, SetConsoleCtrlHandler, GetFileType, GetStdHandle, GetProcessHeap, EnumSystemLocalesW, SetFilePointerEx, ReadFile, ReadConsoleW, OutputDebugStringW, CreateFileW, HeapSize, CloseHandle, GetUserDefaultLCID, IsValidLocale, GetStringTypeW, DeleteCriticalSection, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, RtlUnwindEx, RtlPcToFileHeader, RaiseException, InterlockedPushEntrySList, InterlockedFlushSList, GetLastError, SetLastError, EncodePointer, EnterCriticalSection, LeaveCriticalSection, RtlUnwind, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, ExitProcess, GetModuleHandleExW, GetModuleFileNameW, GetCurrentThread, HeapFree, HeapAlloc, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, MultiByteToWideChar, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW

Exports

Name	Ordinal	Address
ACeujVZMknFDjv	1	0x180043600

Name	Ordinal	Address
AHuDGMflBfPryOEYjuTfbzJdEM	2	0x180043f30
ATjQPkInxPUGuUu	3	0x180043890
AmbryhtjKWGeCnsRXR	4	0x180043690
AukYzjkZpQjlyb	5	0x180043e80
BEHGKvjtYm	6	0x1800438c0
BRUFxz	7	0x180043b50
BUZBRSzPLxRhY	8	0x180043ba0
BZCzGXtURmWdlZoaE	9	0x180043a50
BZqjzJIejob	10	0x1800439a0
BmZYhYQxzCQQ	11	0x180043810
BubGPfVJvMw	12	0x180043420
CBkyPEXjXbRUHKXJo	13	0x180043330
CEsNfdgPgd	14	0x180044070
CVPqxJEtookkvK	15	0x180043e70
CaJBhuFKGDiSQoojdQF	16	0x180044120
CcKlmw	17	0x1800434f0
CfrkXlNpYveSkH	18	0x180043730
CtcUKaNM	19	0x180043d60
CtmIxtaSEWrJoeKFHYsQVRF	20	0x180043f20
DCcTBPjgUmKACiowmtURUFfgN	21	0x180043290
DRpUgpG	22	0x1800432d0
DYDsOtWxMUufQk	23	0x1800434c0
DacmPRKwn	24	0x180043ca0
DdBIgVVvJpDDYojhSveGWyVC	25	0x1800440d0
DllRegisterServer	26	0x180044a60
EDkUTFetsWTlyEplV	27	0x180043bd0
EZveIcVQbxXQvHAc	28	0x180043960
EetKwkljiiO	29	0x1800440e0
EiwSmYwuw	30	0x180043410
EjKZnNkyirwOPcLJfvNShOHV	31	0x180043250
ElumsVBNoiVQFecpcx	32	0x1800438f0
FVCmCSsewcOgpmVCPhNN	33	0x180043e90
FeniiccJDJZQOquCQEDZFbp	34	0x180043490
GhuZhUSaPqDNPQyLmKmMs	35	0x180043530
GidoxoYzkYTZBUKjTczrNz	36	0x180043240
GmOuZYJiGNspxqOxoBCu	37	0x180043af0
GoueteXAa	38	0x180043de0
HZyUwOgdhWiacaSFvYDsgUbdhh	39	0x180043370
HtmqUvH	40	0x1800437f0
HvKfMTiGc	41	0x180043ad0
HwiGZdXrkhPSBdQhcNF	42	0x180043d80
IOKBBQdlpeQCrqGhE	43	0x180043f80
IftUczqAOEEpksLc	44	0x1800440b0
IujIKjACwijLXf	45	0x180043a80
JPOlfklrHwimOYpdWU	46	0x180043980
JldHyQJYHPfgwSota	47	0x180043f70
KHRcAfeWiWXczrzetcsf	48	0x1800435c0
KSBSWsMPLKrvLpLuQEVBQaA	49	0x1800437b0
KXPHHrx	50	0x180043cc0
KqKYPtMNYPZwVVbFgnJskTDgXZ	51	0x180044080
KrLeibTbke	52	0x180043da0
KtNQbfYVcdlRzCxJLbItSH	53	0x180043fc0
KtZFnRWCN	54	0x180043c50
KyUDQzimOqrGaUdqnpHCadl	55	0x180043950
LNVXKJhSBOeqiQPpxZuBrf	56	0x180043770
LbOnTCPkjmOOEdhEeyEy	57	0x180043cf0
LlFlOHcteRaL	58	0x180043990
MAmiSwkyFlQMDaCByXR	59	0x1800438d0
MHyRvOCLFO	60	0x180043c00

Name	Ordinal	Address
MbZnIlsXkfnyOmtthLrL	61	0x180043640
MbsuSbHtpeltWArBKaXuf	62	0x180043eb0
MltZiwCXSxF	63	0x180043440
NFzpzSbcGrv	64	0x180043e20
NXasCwwz	65	0x180043310
NfwIIEvnLCKXIrpxWtDCbXx	66	0x180043bf0
NgkonMKeLNPfNxT	67	0x180043b30
NlplQAUkkIZ	68	0x1800437e0
OQruapyPUnukiDhEvANkgElZqh	69	0x180043700
ORBMTIE	70	0x180043e50
OdtvuFxrrpfsY	71	0x180043d00
OoZePWcMAAdh	72	0x1800432a0
PbgMOKpkqAeEgOBtpecKal	73	0x180043a90
PhHcvOzcWKVEzqGUAuH	74	0x180044020
PqcNviu	75	0x1800439b0
PxhniQgzegWvoSCaIPorRhqOEt	76	0x180043200
PzcLCLdBlldqBxBTbNiI	77	0x180043ab0
RFSoSJnzzPHjPzvZCOvWT	78	0x180043f90
RSrAlLsSbnJmicoYtpKsPYkwFn	79	0x180044040
ReujwDwTrVxLhVwaWvQS	80	0x180044100
RqzpZDiLuFMWsJ	81	0x180043630
SUemGjmeVuPs	82	0x180043a70
ScnrskpiicPdg	83	0x180043840
SeCKWgTgmmtDUvFC	84	0x180043be0
SjnxUxHKGlth	85	0x180043cd0
StNIEkqRHMtB	86	0x180043ae0
StepECvENJONrwlynYAOx	87	0x180043550
SyluAQQc	88	0x180043800
SyvpWCmyZbMrEFnfTmyrBRH	89	0x1800436d0
TLTUEROtrtYd	90	0x1800434d0
TdNJCbJiInjtCOpp	91	0x180043d20
TndRvx	92	0x180043fe0
TpEywJZSeYXzmbHgod	93	0x180043c70
TrziFVlHgMVVONOLNIfRem	94	0x180043d90
TzKueUFolaHBJPFhx	95	0x180043b40
UClTVsmfYtgzIL	96	0x1800437c0
URuQMqrUPMSAGVyWQTqN	97	0x180044010
UbLvGEZfkFcvnnw	98	0x180044170
VXfdoDKAoHiAA	99	0x180043390
VeRxloJdVvetDztDxLQT	100	0x180043dd0
VkIbTCoknzceJuPcnCXzzPj	101	0x180043e30
VqNxpzS	102	0x180043e00
WPumZrRRafooNh	103	0x1800435a0
WQIBBQj	104	0x1800431e0
WUVuwTliAyCBAOHuSOD	105	0x180043e40
WsADtJekvYjSfChaZ	106	0x1800434e0
XBRWcmDQWuUdmmFxx	107	0x180043570
XDLVzSefOKneeAsytcH	108	0x180043b60
XDecZDvu	109	0x180043ec0
XNmJlnrJjgZEjPQQeoOIT	110	0x180043860
XWdPewUOSEaHKCHnynymDhLttF	111	0x180044000
XmEMSisfXGvwdcnUI	112	0x180044130
XxYbsglQgKXTYWUmlX	113	0x1800433d0
YOqqPZdimbNEuvMaM	114	0x1800439d0
YXgNyXKelZfQK	115	0x180043220
YrlEvikMuwUvtjDbAASCV	116	0x180043b70
YrpQLSvKN	117	0x180043320
YtyiKWITImQlOTP	118	0x1800439f0
ZMAtbEQuVEpze	119	0x180043db0

Name	Ordinal	Address
ZOTjVFL	120	0x180043b20
ZXigMFrErZGCgnGQdpTo	121	0x180043790
ZcqfXQvmSIhHXuDEPmA	122	0x180043610
ZmNbZwqyJPRHpqmUZOmpJexK	123	0x1800436c0
aOxloUcrMaTBrKRkXkvrKaAy	124	0x180044050
aXDBQtKlOSCf	125	0x180043340
azZsnWvbQULjBuaCVG	126	0x180043650
bCHMpZKuNDwxXrs	127	0x180043f00
bFyNFHBUflbBAfRZV	128	0x180043560
bGaVPXQawxz	129	0x180043910
bVRtqQ	130	0x180043d40
bWXHfJrBjrdcVRLbuT	131	0x180043780
blakCcJabYayatiIl	132	0x180043c40
bsEGlgCVUNZeSRsr	133	0x1800431f0
btMHyPMu	134	0x180043380
bteqpXpGuaIzWJWPXQj	135	0x1800433e0
buvNCuoglefZoipISdUp	136	0x1800433a0
bvumZozkETqFchaDGgv	137	0x180044150
cKgbFcy	138	0x180043260
chPwzpRWTYf	139	0x180043400
cliUpMkAyvnx	140	0x180043460
cpEBzofbApJInexgeY	141	0x180043520
cpNZFVzZSKe	142	0x180043c20
cpmbLfWGBjxaaZNR	143	0x1800437a0
csebqY	144	0x1800433c0
czlJGyv	145	0x180043430
dOrUqBBEUz	146	0x1800440f0
disvxAJjTCcpofcItH	147	0x180043850
djhGwwWdNkNOGnSMVhO	148	0x180043f50
drTNkYg	149	0x1800435d0
elaOoLpqFiyIbnyvaU	150	0x180043500
fAKHjGkpTjHcAAfMvshh	151	0x180043bc0
fBFgQesCsDDEqolwHzSbbSIs	152	0x180043f40
fDZRRfyfwlYoeFo	153	0x180043b00
fLcYUVhVDDHHRUryudAO	154	0x180043720
fWkhxqQSpEMsqhItVlr	155	0x1800432b0
fZQaoqMpByybzlfgG	156	0x180043a20
fadaIHaPgvjpA	157	0x180044160
fodVsUcqiRZtLe	158	0x1800434b0
fwWFiWowsdju	159	0x180043a00
gQiEYElmfk	160	0x180043480
gexClfMSOkWBVEs	161	0x180044060
gnKyXNiVXhIQQVNkxutn	162	0x180043350
hHoSVYFgUoRXoGwPBdTY	163	0x1800436f0
hKiUTWNKTCBHARIejKtitX	164	0x180043970
hTcXrfT	165	0x180043b10
hdpzQLMeXdHLAXI	166	0x180043ef0
hqmMcxlMowrqdmwCD	167	0x1800432f0
huwZDnzyRrUuSv	168	0x180044110
hwwioGqcSiONSnnoqSgGGlYG	169	0x1800437d0
hwxiWyDPZ	170	0x180043300
iIMUBUcxlPgIoCou	171	0x180043ce0
iXVpeLZjxHYfZy	172	0x180043ed0
ickoyirauzuqSYooWRxIBKP	173	0x1800433b0
ixEhmcgYbORYTvwI	174	0x180043940
jXSCkxhrXSnIiziUsUkSa	175	0x1800438a0
jhMrQlkZnbNzE	176	0x1800435e0
jnmtHhyvcXOtUsFySuhzSRFwZ	177	0x180043c80
jqfPKICr	178	0x180043210

Name	Ordinal	Address
kFVNBreOaZSGgseVYXfZAQSt	179	0x180043e60
kLMzjQJrPZFPf	180	0x180043470
kONtiEAEi	181	0x180043510
kUNUwtZ	182	0x180043cb0
lIEZQCqZKko	183	0x180043ee0
lZiHnzEuXoXZIzRd	184	0x180043df0
larnkUFYFI	185	0x180043620
lfFBdv	186	0x180043e10
mJFTxuzjmKwZE	187	0x1800438e0
mJPUafqK	188	0x1800436b0
mRinbRZ	189	0x1800435b0
miGqUGeEk	190	0x180043f10
muHYTksHDRccMJtbMIVY	191	0x180043bb0
nEWvJUznqPuIORIkmbdcWjKd	192	0x180043fb0
nXCjDafayJLQ	193	0x180043fa0
nfPVFCecEC	194	0x180043fd0
ntSsSyvUegFeD	195	0x180043590
nttFqgw	196	0x180043f60
nuflNZYxVuFptSebTKUXxH	197	0x180043dc0
oFyUMrjmgKtGCEsn	198	0x180043d70
oJhfaaiLZFHiBCXJlPO	199	0x180043d30
oPpitKCbVriCZu	200	0x180043280
oTMlKNA	201	0x180043d10
pOQozXdpf	202	0x180043710
pqXsDgFAKqxqyeZwyCjZ	203	0x180043230
qhBjRUFjPgGnZCYf	204	0x180043a60
qnqswBvEbONoReovLIKnVYuSA	205	0x1800439c0
qpggbjTvfN	206	0x1800432c0
rGJIMlvpqBhxViL	207	0x180043880
rUmobKc	208	0x180043a10
rfqEeKHAx	209	0x180044140
rsgxCEvQpI	210	0x1800436e0
rstbQmhTSxcrhUlcaxRFhGIXK	211	0x180043c10
rxpoWUmUrHlSIHeznkyrivE	212	0x180043d50
rzgTPjoxRh	213	0x180044090
sFmMlSJDeOoy	214	0x180043a40
sGzvLqVdsbQ	215	0x180043930
sRyuPhAwDlOgUlGVplfduYySp	216	0x1800440a0
sTHzpfVYU	217	0x180043820
sUKvQla	218	0x180043680
sVMFsGCCfvDfoTh	219	0x180043450
sfAGqCcFJlYOMkqZahTjTiAX	220	0x1800439e0
stMogsRXrfH	221	0x180043c30
tBAtJGzOlooKPbZ	222	0x1800438b0
tTdsornziSGMnYRGtlv	223	0x180043870
taVJVqMCMlkFIDWVCcDLV	224	0x180043ea0
twRKUF	225	0x180043a30
uTtYPS	226	0x180043920
ujLBGDEExK	227	0x1800435f0
ujfIFiuxQFuoWpBYlfPja	228	0x1800436a0
unVwakRZhbHEVJWGGZDyCZP	229	0x1800434a0
utlgNYXohozxx	230	0x180043aa0
uvBxDGCDNqLbDaufFb	231	0x180043740
vycQUvI	232	0x180043830
vzdSRyxeERBiXlOkqVUB	233	0x180043ff0
wAHuFSGPWcgVtPzRzoUTnbwo	234	0x180043660
wiIXJqSWsUXvPbq	235	0x180043360
wjeHVSTrDxCzMVNUFEQoz	236	0x180043b90
xPjfyQjUovqeohLapv	237	0x1800440c0

Name	Ordinal	Address
xeyyJZUMQlYiCHikxXoEko	238	0x180043670
xmDlQKqSmhiJfARRXzslVED	239	0x1800433f0
xzJluXH	240	0x180043580
yAYxFjbdwTSooJJzoq	241	0x180043b80
yBpkXiNAKugdWlxIPQKL	242	0x180043540
yIApLIDSJNmmOc	243	0x180043270
yMokeHArDgIyDvmsuwd	244	0x180044030
yVLTygbNjHTxXaOuZBkHmpajxq	245	0x180043ac0
yhCymcBLApUWyPqapsEDJtfjMV	246	0x180043760
yjGXMXnz	247	0x180043c90
yprPVXLUkdnzWv	248	0x1800432e0
yzkENTmBV	249	0x180043750
zQnFkEsglvSmYtKlkFDTme	250	0x180043900
zdMhYw	251	0x180043c60

Possible Origin

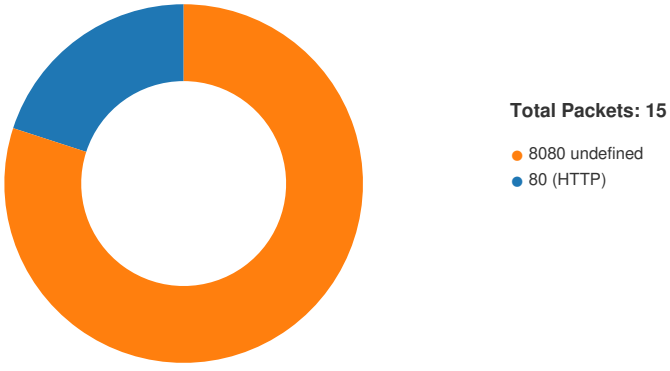
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5115.178.55.22 49702802404304 11/16/22-11:48:03.539047	TCP	2404304	ET CNC Feodo Tracker Reported CnC Server TCP group 3	49702	80	192.168.2.5	115.178.55.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 16, 2022 11:59:52.548481941 CET	49699	80	192.168.2.3	115.178.55.22
Nov 16, 2022 11:59:52.829572916 CET	80	49699	115.178.55.22	192.168.2.3
Nov 16, 2022 11:59:53.342060089 CET	49699	80	192.168.2.3	115.178.55.22
Nov 16, 2022 11:59:53.622711897 CET	80	49699	115.178.55.22	192.168.2.3

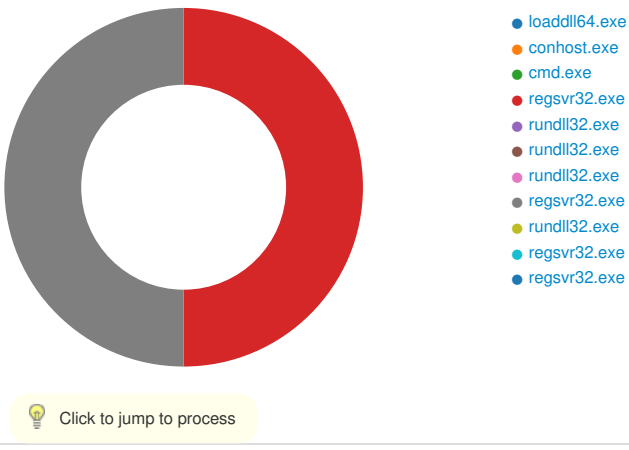
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 16, 2022 11:59:54.126924038 CET	49699	80	192.168.2.3	115.178.55.22
Nov 16, 2022 11:59:54.407995939 CET	80	49699	115.178.55.22	192.168.2.3
Nov 16, 2022 11:59:59.773596048 CET	49700	8080	192.168.2.3	172.105.115.71
Nov 16, 2022 11:59:59.937886000 CET	8080	49700	172.105.115.71	192.168.2.3
Nov 16, 2022 11:59:59.938010931 CET	49700	8080	192.168.2.3	172.105.115.71
Nov 16, 2022 11:59:59.942967892 CET	49700	8080	192.168.2.3	172.105.115.71
Nov 16, 2022 12:00:00.107225895 CET	8080	49700	172.105.115.71	192.168.2.3
Nov 16, 2022 12:00:00.124011993 CET	8080	49700	172.105.115.71	192.168.2.3
Nov 16, 2022 12:00:00.124042988 CET	8080	49700	172.105.115.71	192.168.2.3
Nov 16, 2022 12:00:00.124574900 CET	49700	8080	192.168.2.3	172.105.115.71
Nov 16, 2022 12:00:00.166908979 CET	49700	8080	192.168.2.3	172.105.115.71
Nov 16, 2022 12:00:00.331199884 CET	8080	49700	172.105.115.71	192.168.2.3
Nov 16, 2022 12:00:00.332292080 CET	8080	49700	172.105.115.71	192.168.2.3
Nov 16, 2022 12:00:00.386454105 CET	49700	8080	192.168.2.3	172.105.115.71
Nov 16, 2022 12:00:04.991183996 CET	49700	8080	192.168.2.3	172.105.115.71
Nov 16, 2022 12:00:04.991256952 CET	49700	8080	192.168.2.3	172.105.115.71
Nov 16, 2022 12:00:05.156111002 CET	8080	49700	172.105.115.71	192.168.2.3
Nov 16, 2022 12:00:05.156155109 CET	8080	49700	172.105.115.71	192.168.2.3
Nov 16, 2022 12:00:05.797419071 CET	8080	49700	172.105.115.71	192.168.2.3
Nov 16, 2022 12:00:05.933135033 CET	49700	8080	192.168.2.3	172.105.115.71
Nov 16, 2022 12:00:08.815905094 CET	8080	49700	172.105.115.71	192.168.2.3
Nov 16, 2022 12:00:08.815937042 CET	8080	49700	172.105.115.71	192.168.2.3
Nov 16, 2022 12:00:08.816031933 CET	49700	8080	192.168.2.3	172.105.115.71
Nov 16, 2022 12:00:08.816299915 CET	49700	8080	192.168.2.3	172.105.115.71
Nov 16, 2022 12:00:08.816466093 CET	49700	8080	192.168.2.3	172.105.115.71
Nov 16, 2022 12:00:08.980465889 CET	8080	49700	172.105.115.71	192.168.2.3
Nov 16, 2022 12:00:08.980499029 CET	8080	49700	172.105.115.71	192.168.2.3

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 16, 2022 12:00:04.010195971 CET	8.8.8.8	192.168.2.3	0x7baa	No error (0)	windowsupdatebg.s.llnwi.net		95.140.236.0	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **6056**, Parent PID: **3452**

General

Target ID:	0
Start time:	11:59:09
Start date:	16/11/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\UC2DFXQIBiE2kQ.dll"
Imagebase:	0x7ff7d8880000
File size:	139776 bytes
MD5 hash:	C676FC0263EDD17D4CE7D644B8F3FCD6
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: conhost.exe PID: **6100**, Parent PID: **6056**

General

Target ID:	1
Start time:	11:59:09
Start date:	16/11/2022
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: **6048**, Parent PID: **6056**

General

Target ID:	2
Start time:	11:59:09
Start date:	16/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\UC2DFXQIBiE2kQ.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: 6076, Parent PID: 6056

General

Target ID:	3
Start time:	11:59:09
Start date:	16/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\UC2DFXQIBiE2kQ.dll
Imagebase:	0x7ff708bd0000
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: 00000003.00000002.261455242.0000000002D51000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.260696945.0000000001220000.00000040.00001000.00020000.00000000.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\CqZilJuzKBQGflL\PYmtZH.dll:Zone.Identifier	success or wait	1	2D70786	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: 6072, Parent PID: 6048

General

Target ID:	4
Start time:	11:59:09
Start date:	16/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\UC2DFXQIBiE2kQ.dll",#1
Imagebase:	0x7ff648d10000
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: 00000004.00000002.254973039.0000024188500000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.255048336.0000024188541000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security

Reputation:	high

Analysis Process: rundll32.exe PID: **6052**, Parent PID: **6056**

General	
Target ID:	5
Start time:	11:59:09
Start date:	16/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\UC2DFXQIBiE2kQ.dll,ACeujVZMknFDjv
Imagebase:	0x7ff648d10000
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: 00000005.00000002.256991395.000001B505A51000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.256810706.000001B505730000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **5172**, Parent PID: **6056**

General	
Target ID:	6
Start time:	11:59:13
Start date:	16/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\UC2DFXQIBiE2kQ.dll,AHuDGMflBfPryOEYjuTfbzJdEM
Imagebase:	0x7ff648d10000
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: 00000006.00000002.261815497.000001DEAC681000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.261734338.000001DEAAE80000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: regsvr32.exe PID: **5292**, Parent PID: **6076**

General	
Target ID:	7
Start time:	11:59:14
Start date:	16/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\CqZilJuzKBQGfIL\PYmtZH.dll"
Imagebase:	0x7ff708bd0000
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: 00000007.00000002.645047092.00000000021E1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.644659709.0000000002080000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

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	PYmtZH.dll	unicode	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\CqZilJuzKBQGfIL\PYmtZH.dll"	success or wait	1	21E3442	RegSetValueExW

Analysis Process: rundll32.exe PID: **5244**, Parent PID: **6056**

General

Target ID:	8
Start time:	11:59:16
Start date:	16/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\UC2DFXQIBiE2kQ.dll,ATjQPkInxPUGuUu
Imagebase:	0x7ff648d10000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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: **5104**, Parent PID: **3452**

General

Target ID:	18
Start time:	12:00:16
Start date:	16/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe" "C:\Windows\system32\CqZilJuzKBQGfIL\PYmtZH.dll
Imagebase:	0x7ff708bd0000
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: 00000012.00000002.409592549.00000000013D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000012.00000002.409741112.0000000002CD1000.00000020.00001000.00020000.00000000.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: **972**, Parent PID: **5104**

General

Target ID:	19
Start time:	12:00:23
Start date:	16/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Users\user\AppData\Local\OKCYiYOFwZjDcIsn\OYsSlVLvWy.dll"
Imagebase:	0x7ff708bd0000
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

Disassembly

No disassembly