ID: 829552
Sample Name: f_00321b
Cookbook: default.jbs
Time: 15:56:02
Date: 18/03/2023
Version: 37.0.0 Beryl

Table of Contents

Windows Analysis Report

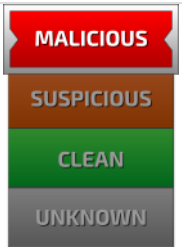
f_00321b.dll

Overview

General Information

Sample Name:	f_00321b.dll (renamed file extension from none to dll, renamed because original name is a hash value)
Original Sample Name:	f_00321b
Analysis ID:	829552
MD5:	bfc060937dc90..
SHA1:	c156c00c7e91…
SHA256:	2f39c2879989d..
Infos:	

Detection



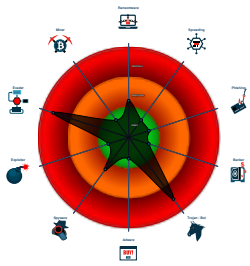
Emotet

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

Signatures

- Early bird code injection technique d…
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Queues an APC in another process …
- 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…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 4224 cmdline: loaddll64.exe "C:\Users\user\Desktop\f_00321b.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 2516 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 3216 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\f_00321b.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 1264 cmdline: rundll32.exe "C:\Users\user\Desktop\f_00321b.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - regsvr32.exe (PID: 5968 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\RymKYMmySRfU\EAqrfXJOpHznppsf.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 4888 cmdline: regsvr32.exe /s C:\Users\user\Desktop\f_00321b.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 1312 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZbmMPnDvLqwXll\QyzgcRWJYZS.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 1240 cmdline: rundll32.exe C:\Users\user\Desktop\f_00321b.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
    - regsvr32.exe (PID: 4768 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\IzuSuDitBV\QmEREbzuu.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
    - conhost.exe (PID: 5432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Emotet	While Emotet historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content delivery. For example, since mid 2018 it is used by Trickbot for installs, which may also lead to ransomware attacks using Ryuk, a combination observed several times against high-profile targets.It is always stealing information from victims but what the criminal gang behind it did, was to open up another business channel by selling their infrastructure delivering additional malicious software. From malware analysts it has been classified into epochs depending on command and control, payloads, and delivery solutions which change over time.Emotet had been taken down by authorities in January 2021, though it appears to have sprung back to life in November 2021.	• GOLD CABIN • MUMMY SPIDER • Mealybug	http://blog.fortinet.com/2017/05/03/deep-analysis-of-new-emotet-variant-part-1http://blog.trendmicro.com/trendlabs-security-intelligence/emotet-returns-starts-spreading-via-spam-botnet/http://ropgadget.com/posts/defensive_pcres.htmlhttps://adalogics.com/blog/the-state-of-advanced-code-injectionshttps://asec.ahnlab.com/en/33600/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet

Malware Configuration

Threatname: Emotet


```
{
  "C2 list": [
    "91.121.146.47:8080",
    "66.228.32.31:7080",
    "182.162.143.56:443",
    "187.63.160.88:80",
    "167.172.199.165:8080",
    "164.90.222.65:443",
    "104.168.155.143:8080",
    "163.44.196.120:8080",
    "160.16.142.56:8080",
    "159.89.202.34:443",
    "159.65.88.10:8080",
    "186.194.240.217:443",
    "149.56.131.28:8080",
    "72.15.201.15:8080",
    "1.234.2.232:8080",
    "82.223.21.224:8080",
    "206.189.28.199:8080",
    "169.57.156.166:8080",
    "107.170.39.149:8080",
    "103.43.75.120:443",
    "91.207.28.33:8080",
    "213.239.212.5:443",
    "45.235.8.30:8080",
    "119.59.103.152:8080",
    "164.68.99.3:8080",
    "95.217.221.146:8080",
    "153.126.146.25:7080",
    "197.242.150.244:8080",
    "202.129.205.3:8080",
    "103.132.242.26:8080",
    "139.59.126.41:443",
    "110.232.117.186:8080",
    "183.111.227.137:8080",
    "5.135.159.50:443",
    "201.94.166.162:443",
    "103.75.201.2:443",
    "79.137.35.198:8080",
    "172.105.226.75:8080",
    "94.23.45.86:4143",
    "115.68.227.76:8080",
    "153.92.5.27:8080",
    "167.172.253.162:8080",
    "188.44.20.25:443",
    "147.139.166.154:8080",
    "129.232.188.93:443",
    "173.212.193.249:8080",
    "185.4.135.165:8080",
    "45.176.232.124:443"
  ],
  "Public Key": [
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj50W/ClAAOAIo=",
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKTS88RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr10vZ2Pz+AQWzRMggQmAtO6rPH7nyx2xW++lAAKAJA="
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.320583141.0000024067ED1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.839406801.0000000002031000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.839010466.000000000072B000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Emotet_3	Yara detected Emotet	Joe Security	
00000006.00000002.839356776.0000000001FE0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.319594851.0000000002301000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.rundll32.exe.1caef360000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.24067ea0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.24067ea0000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.22d0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.22d0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 3 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 11 - Source IP: 192.168.2.4 - Destination IP: 213.239.212.5

Timestamp:	192.168.2.4213.239.212.5497294432404320 03/18/23-16:00:53.457464
SID:	2404320
Source Port:	49729
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 2 - Source IP: 192.168.2.4 - Destination IP: 104.168.155.143

Timestamp:	192.168.2.4104.168.155.1434970580802404302 03/18/23-15:58:29.445426
SID:	2404302
Source Port:	49705
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 13 - Source IP: 192.168.2.4 - Destination IP: 45.235.8.30

Timestamp:	192.168.2.445.235.8.304973380802404324 03/18/23-16:00:58.958124
SID:	2404324
Source Port:	49733
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 6 - Source IP: 192.168.2.4 - Destination IP: 167.172.199.165

Timestamp:	192.168.2.4167.172.199.1654970380802404310 03/18/23-15:58:19.699415
SID:	2404310
Source Port:	49703
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 5 - Source IP: 192.168.2.4 - Destination IP: 164.90.222.65

Timestamp:	192.168.2.4164.90.222.65497044432404308 03/18/23-15:58:24.948314
SID:	2404308
Source Port:	49704

Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 8 - Source IP: 192.168.2.4 - Destination IP: 187.63.160.88	
Timestamp:	192.168.2.4187.63.160.8849702802404314 03/18/23-15:58:11.945439
SID:	2404314
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 3 - Source IP: 192.168.2.4 - Destination IP: 1.234.2.232	
Timestamp:	192.168.2.41.234.2.2324971980802404304 03/18/23-15:59:46.453351
SID:	2404304
Source Port:	49719
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 23 - Source IP: 192.168.2.4 - Destination IP: 91.121.146.47	
Timestamp:	192.168.2.491.121.146.474969580802404344 03/18/23-15:57:43.982133
SID:	2404344
Source Port:	49695
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 10 - Source IP: 192.168.2.4 - Destination IP: 206.189.28.199	
Timestamp:	192.168.2.4206.189.28.1994972180802404318 03/18/23-16:00:02.963968
SID:	2404318
Source Port:	49721
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 16 - Source IP: 192.168.2.4 - Destination IP: 66.228.32.31	
Timestamp:	192.168.2.466.228.32.314969770802404330 03/18/23-15:57:49.653644
SID:	2404330
Source Port:	49697
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 7 - Source IP: 192.168.2.4 - Destination IP: 182.162.143.56	
Timestamp:	192.168.2.4182.162.143.56496984432404312 03/18/23-15:58:05.445458
SID:	2404312
Source Port:	49698
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

Early bird code injection technique detected

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

Queues an APC in another process (thread injection)

Stealing of Sensitive Information

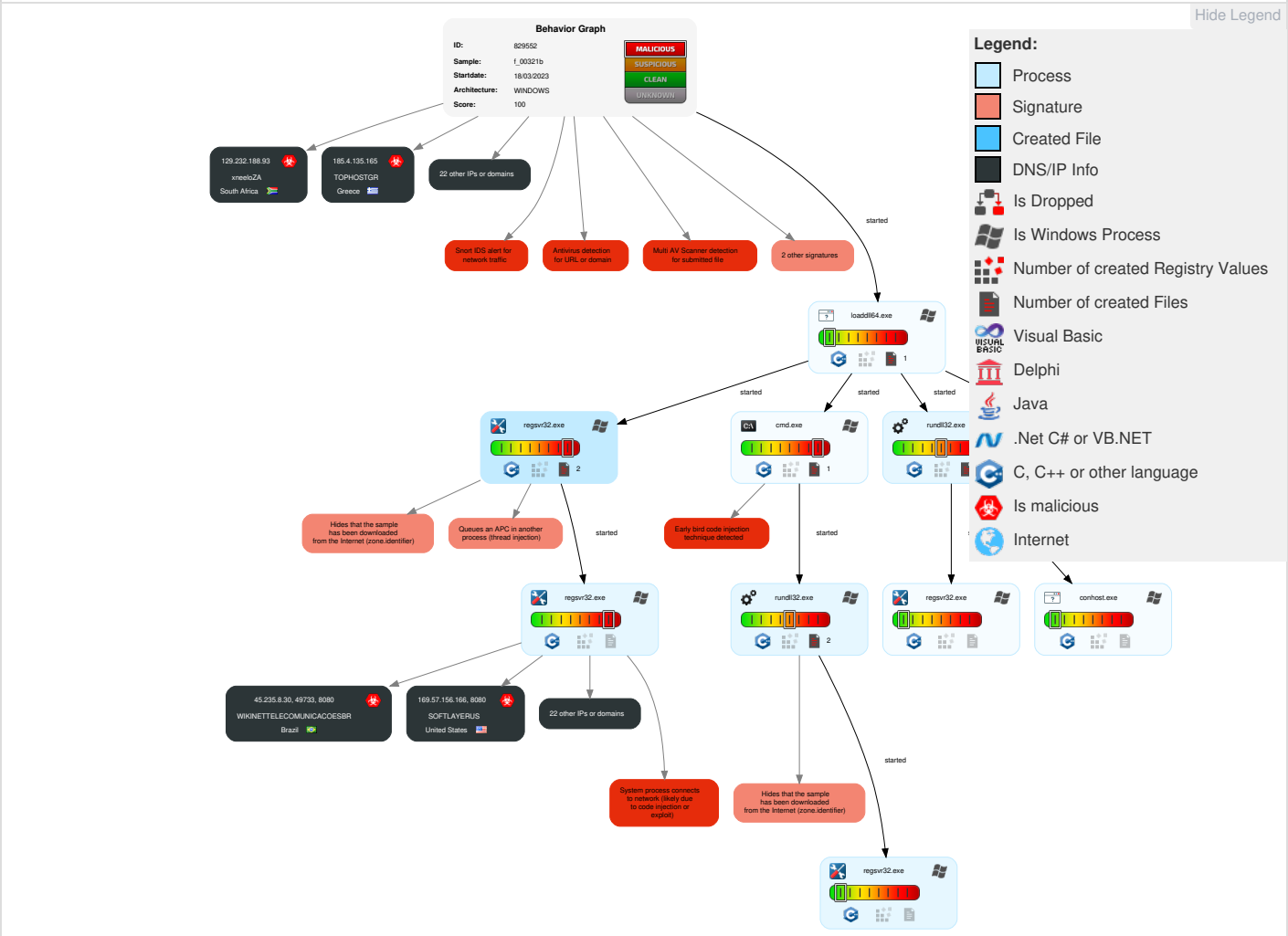
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	3 1 1 Process Injection	2 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	2 Virtualization/Sandbox Evasion	LSASS Memory	3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 1 Process Injection	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Hidden Files and Directories	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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
f_00321b.dll	60%	Virustotal		Browse
f_00321b.dll	79%	ReversingLabs	Win64.Trojan.Emotet	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Source	Detection	Scanner	Label	Link	Download
5.2.rundll32.exe.1caef360000.1.unpack	100%	Avira	HEUR/AGEN.1215476		Download File
4.2.rundll32.exe.24067ea0000.1.unpack	100%	Avira	HEUR/AGEN.1215476		Download File
3.2.regsvr32.exe.22d0000.0.unpack	100%	Avira	HEUR/AGEN.1215476		Download File
6.2.regsvr32.exe.1fe0000.0.unpack	100%	Avira	HEUR/AGEN.1215476		Download File

Domains

Source	Detection	Scanner	Label	Link
c-0001.c-msedge.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://164.90.222.65/	0%	URL Reputation	safe	
http://https://45.235.8.30:8080/nnukk/upfurpftd/ltwomnfleb/0u	100%	Avira URL Cloud	malware	
http://https://45.235.8.30:8080/nnukk/upfurpftd/ltwomnfleb//	100%	Avira URL Cloud	malware	
http://https://213.239.212.5/~	100%	Avira URL Cloud	malware	
http://https://45.235.8.30:8080/nnukk/upfurpftd/ltwomnfleb/	100%	Avira URL Cloud	malware	
http://https://21.235.8.30:8080/	0%	Avira URL Cloud	safe	
http://https://213.239.212.5/nnukk/upfurpftd/ltwomnfleb/	100%	Avira URL Cloud	malware	
http://https://119.59.103.152:8080/nnukk/upfurpftd/ltwomnfleb/	100%	Avira URL Cloud	malware	
http://https://82.223.21.224:8080/nnukk/upfurpftd/ltwomnfleb/	100%	Avira URL Cloud	malware	
http://https://107.170.39.149:8080/	100%	Avira URL Cloud	malware	
http://https://167.172.199.165:8080/Y	100%	Avira URL Cloud	malware	
http://https://82.223.21.224:8080/	100%	Avira URL Cloud	malware	
http://https://91.207.28.33:8080/-	100%	Avira URL Cloud	malware	
http://https://159.65.88.10:8080/nnukk/upfurpftd/ltwomnfleb/	100%	Avira URL Cloud	malware	
http://https://104.168.155.143:8080/nnukk/upfurpftd/ltwomnfleb/	100%	Avira URL Cloud	malware	
http://https://119.59.103.152:8080/nnukk/upfurpftd/ltwomnfleb/?	100%	Avira URL Cloud	malware	
http://https://164.90.222.65/nnukk/upfurpftd/ltwomnfleb//K	100%	Avira URL Cloud	malware	
http://https://164.90.222.65:443/nnukk/upfurpftd/ltwomnfleb/b/X	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/nnukk/upfurpftd/ltwomnfleb/	100%	Avira URL Cloud	malware	
http://https://189.56.131.28:8080/	0%	Avira URL Cloud	safe	
http://https://107.170.39.149:8080/nnukk/upfurpftd/ltwomnfleb/	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/	100%	Avira URL Cloud	malware	
http://https://119.59.103.152:8080/	100%	Avira URL Cloud	malware	
http://https://119.59.103.152:8080/l/z	100%	Avira URL Cloud	malware	
http://https://187.172.199.165:8080/	0%	Avira URL Cloud	safe	
http://https://167.172.199.165:8080/nnukk/upfurpftd/ltwomnfleb/	100%	Avira URL Cloud	malware	
http://https://187.63.160.88:80/nnukk/upfurpftd/ltwomnfleb/	100%	Avira URL Cloud	malware	
http://https://45.235.8.30:8080/	100%	Avira URL Cloud	malware	
http://https://167.172.199.165:8080/o	100%	Avira URL Cloud	malware	
http://https://66.228.32.31:7080/	100%	Avira URL Cloud	malware	
http://https://167.172.199.165:8080/	100%	Avira URL Cloud	malware	
http://https://164.90.222.65/nnukk/upfurpftd/ltwomnfleb/w	100%	Avira URL Cloud	malware	
http://https://164.90.222.65/nnukk/upfurpftd/ltwomnfleb/	100%	Avira URL Cloud	malware	
http://https://103.44.196.120:8080/	0%	Avira URL Cloud	safe	
http://https://119.59.103.152:8080/nnukk/upfurpftd/ltwomnfleb/%	100%	Avira URL Cloud	malware	
http://https://164.90.222.65/wn	100%	Avira URL Cloud	malware	
http://https://45.235.8.30:8080/nnukk/upfurpftd/ltwomnfleb/Y	100%	Avira URL Cloud	malware	
http://https://213.239.212.5:443/nnukk/upfurpftd/ltwomnfleb/N	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
c-0001.c-msedge.net	13.107.4.50	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://164.90.222.65/nnukk/upfurpftd/ltwomnfleb/	true	• Avira URL Cloud: malware	unknown

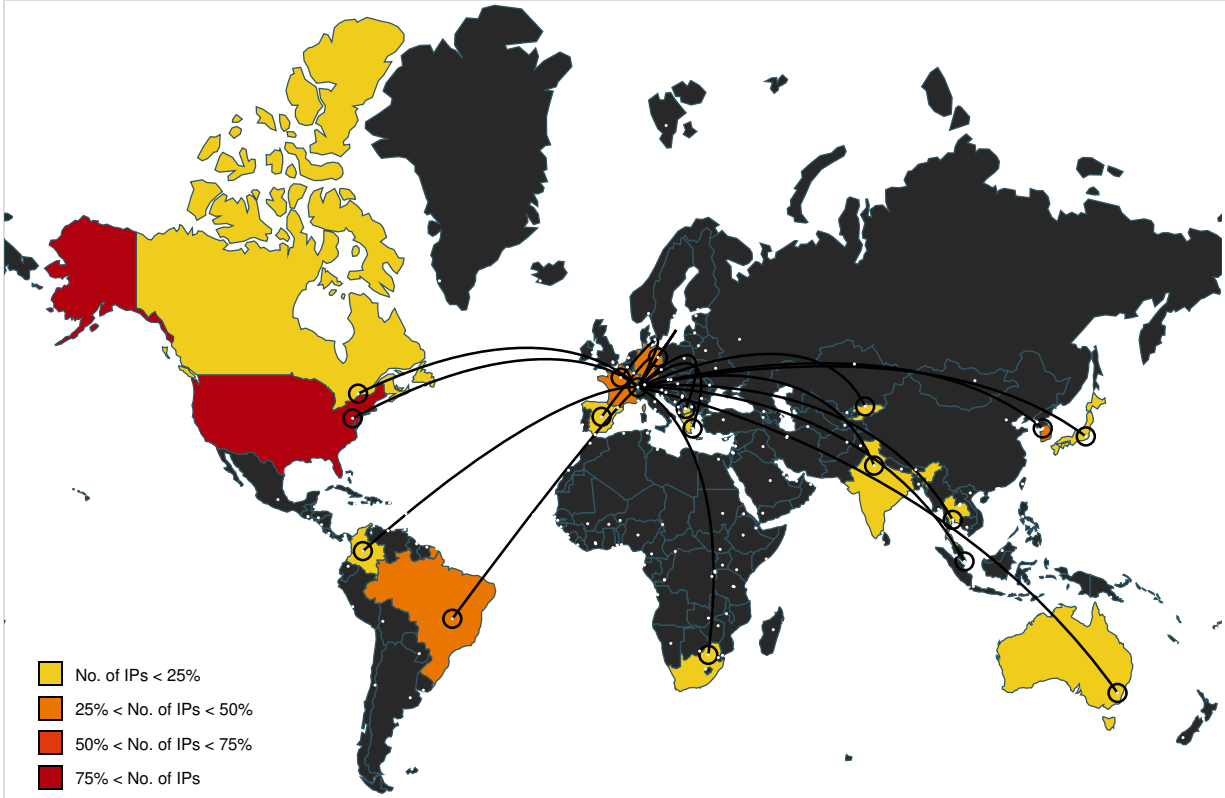
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://45.235.8.30:8080/nnukk/upfurpftd/ltwomnfleb//	regsvr32.exe, 00000006.00000002.83948329 3.000000000285E000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://45.235.8.30:8080/nnukk/upfurpftd/ltwomnfleb/0u	regsvr32.exe, 00000006.00000002.83916142 2.00000000007DE000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://167.172.199.165:8080/Y	regsvr32.exe, 00000006.00000003.48963697 0.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://213.239.212.5/~	regsvr32.exe, 00000006.00000002.83930534 8.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://45.235.8.30:8080/nnukk/upfurpftd/ltwomnfleb/	regsvr32.exe, 00000006.00000002.83916142 2.0000000000797000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.839305348.00000000007F4000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://119.59.103.152:8080/nnukk/upfurpftd/ltwomnfleb/	regsvr32.exe, 00000006.00000002.83916142 2.00000000007DE000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://21.235.8.30:8080/	regsvr32.exe, 00000006.00000002.83948329 3.00000000027F0000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://164.90.222.65/	regsvr32.exe, 00000006.00000003.49027376 7.0000000000797000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.490542704.0000000000755000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.839161 422.0000000000797000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.490454644.000000000079700 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.490651926.0000 0000007A2000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000006.00 000003.489636970.0000000000797000.000000 04.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://213.239.212.5/nnukk/upfurpftd/ltwomnfleb/	regsvr32.exe, 00000006.00000002.83930534 8.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://82.223.21.224:8080/	regsvr32.exe, 00000006.00000002.83930534 8.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://107.170.39.149:8080/	regsvr32.exe, 00000006.00000002.83930534 8.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://82.223.21.224:8080/nnukk/upfurpftd/ltwomnfleb/	regsvr32.exe, 00000006.00000002.83916142 2.00000000007DE000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://91.207.28.33:8080/-	regsvr32.exe, 00000006.00000002.83930534 8.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://159.65.88.10:8080/nnukk/upfurpftd/ltwomnfleb/	regsvr32.exe, 00000006.00000002.83948329 3.000000000285E000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://164.90.222.65/nnukk/upfurpftd/ltwomnfleb//K	regsvr32.exe, 00000006.00000003.49027376 7.0000000000797000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.490454644.0000000000797000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.490651 926.00000000007A2000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.489636970.000000000079700 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://104.168.155.143:8080/nnukk/upfurpftd/ltwomnfleb/	regsvr32.exe, 00000006.00000002.83948329 3.000000000285E000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://119.59.103.152:8080/nnukk/upfurpftd/ltwomnfleb/?	regsvr32.exe, 00000006.00000002.83916142 2.0000000000797000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://164.90.222.65:443/nnukk/upfurpftd/ltwomnfleb/b/X	regsvr32.exe, 00000006.00000003.48947725 6.000000000285E000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://91.121.146.47:8080/nnukk/upfurpftd/ltwomnfleb/	regsvr32.exe, 00000006.00000002.83901046 6.000000000072B000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.839083307.0000000000783000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.490273 767.0000000000783000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.404883022.000000000078300 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://189.56.131.28:8080/	regsvr32.exe, 00000006.00000002.83948329 3.00000000027F0000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://107.170.39.149:8080/nnukk/upfurpftd/ltwomnfleb/	regsvr32.exe, 00000006.00000002.83948329 3.000000000285E000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://119.59.103.152:8080/	regsvr32.exe, 00000006.00000002.83930534 8.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.839483293.00000000027F0000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://119.59.103.152:8080/l/z	regsvr32.exe, 00000006.00000002.83930534 8.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://91.121.146.47:8080/	regsvr32.exe, 00000006.00000002.83901046 6.000000000072B000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://187.172.199.165:8080/	regsvr32.exe, 00000006.00000003.49054270 4.000000000075A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://167.172.199.165:8080/nnukk/upfurpftd/ltwomnfleb/	regsvr32.exe, 00000006.00000003.48963697 0.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://187.63.160.88:80/nnukk/upfurpftd/ltwomnfleb/	regsvr32.exe, 00000006.00000003.48963697 0.0000000000797000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.489477256.000000000285E000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://45.235.8.30:8080/	regsvr32.exe, 00000006.00000002.83930534 8.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://167.172.199.165:8080/o	regsvr32.exe, 00000006.00000003.48963697 0.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://66.228.32.31:7080/	regsvr32.exe, 00000006.00000003.48963697 0.0000000000797000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://167.172.199.165:8080/	regsvr32.exe, 00000006.00000003.48963697 0.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://119.59.103.152:8080/nnukk/upfurpftd/ltwomnfleb/%	regsvr32.exe, 00000006.00000002.83930534 8.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://164.90.222.65/nnukk/upfurpftd/ltwomnfleb/w	regsvr32.exe, 00000006.00000003.49027376 7.0000000000797000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.839161422.0000000000797000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.490454 644.0000000000797000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.490651926.00000000007A200 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.489636970.0000 000000797000.00000004.00000020.00020000. 00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://164.90.222.65/wn	regsvr32.exe, 00000006.00000003.48963697 0.0000000000797000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://103.44.196.120:8080/	regsvr32.exe, 00000006.00000002.83930534 8.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://45.235.8.30:8080/nnukk/upfurpftd/ltwomnfleb/Y	regsvr32.exe, 00000006.00000002.83930534 8.00000000007F4000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://213.239.212.5:443/nnukk/upfurpftd/ltwomnfleb/N	regsvr32.exe, 00000006.00000002.83948329 3.000000000285E000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
159.65.88.10	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
172.105.226.75	unknown	United States		63949	LINODE-APLinodeLLCUS	true
164.90.222.65	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
110.232.117.186	unknown	Australia		56038	RACKCORP-APRackCorpAU	true
213.239.212.5	unknown	Germany		24940	HETZNER-ASDE	true
5.135.159.50	unknown	France		16276	OVHFR	true
186.194.240.217	unknown	Brazil		262733	NetceteraTelecomunicacoesLtdaBR	true
103.132.242.26	unknown	India		45117	INPL-IN-APIshansNetworkIN	true
104.168.155.143	unknown	United States		54290	HOSTWINDSUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
119.59.103.152	unknown	Thailand		56067	METRABYTE-TH453LadplacoutJorakhaebuaTH	true
79.137.35.198	unknown	France		16276	OVHFR	true
159.89.202.34	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
91.121.146.47	unknown	France		16276	OVHFR	true
160.16.142.56	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
201.94.166.162	unknown	Brazil		28573	CLAROSABR	true
91.207.28.33	unknown	Kyrgyzstan		39819	PROHOSTKG	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
103.43.75.120	unknown	Japan		20473	AS-CHOOPAUS	true
115.68.227.76	unknown	Korea Republic of		38700	SMILESERV-AS-KRSMILESERVKR	true
188.44.20.25	unknown	Macedonia		57374	GIV-ASMK	true
45.235.8.30	unknown	Brazil		267405	WIKINETTELECOMUNICACOESBR	true
153.126.146.25	unknown	Japan		7684	SAKURA-ASAKURAInternetIncJP	true
72.15.201.15	unknown	United States		13649	ASN-VINSUS	true
163.44.196.120	unknown	Singapore		135161	GMO-Z-COM-THGMO-ZcomNetDesignHoldingsCoLtdSG	true
206.189.28.199	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
107.170.39.149	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
66.228.32.31	unknown	United States		63949	LINODE-APLinodeLLCUS	true
187.63.160.88	unknown	Brazil		28169	BITCOMPROVEDORDESERVICOSDEINTERNETLTDABR	true
82.223.21.224	unknown	Spain		8560	ONEANDONE-ASBrauerstrasse48DE	true
197.242.150.244	unknown	South Africa		37611	AfrihostZA	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
185.4.135.165	unknown	Greece		199246	TOPHOSTGR	true
183.111.227.137	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
45.176.232.124	unknown	Colombia		267869	CABLEYTELECOMUNICACIONESDECOLOMBIASASCABLETELCOC	true
95.217.221.146	unknown	Germany		24940	HETZNER-ASDE	true
149.56.131.28	unknown	Canada		16276	OVHFR	true
169.57.156.166	unknown	United States		36351	SOFTLAYERUS	true
164.68.99.3	unknown	Germany		51167	CONTABODE	true
182.162.143.56	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
139.59.126.41	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
1.234.2.232	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
167.172.253.162	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
129.232.188.93	unknown	South Africa		37153	xneeloZA	true
167.172.199.165	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
202.129.205.3	unknown	Thailand		45328	NIPA-AS-THNIPATECHNOLOGYCOLTDTH	true
147.139.166.154	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true
153.92.5.27	unknown	Germany		47583	AS-HOSTINGERLT	true
94.23.45.86	unknown	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	37.0.0 Beryl

Analysis ID:	829552
Start date and time:	2023-03-18 15:56:02 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	14
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
Sample file name:	f_00321b.dll (renamed file extension from none to dll, renamed because original name is a hash value)
Original Sample Name:	f_00321b
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@17/2@0/48
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 50.2% (good quality ratio 42.4%) • Quality average: 60.5% • Quality standard deviation: 35.6%
HCA Information:	• Successful, ratio: 84% • 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): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.4.50
- Excluded domains from analysis (whitelisted): 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
15:57:44	API Interceptor	23x Sleep call for process: regsvr32.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

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, 62582 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	62582
Entropy (8bit):	**7.996063107774368**
Encrypted:	**true**
SSDEEP:	1536:Jk3XPi43VgGp0gB2itudTSRAn/TWTdWftu:CHa43V5p022iZ4CgA
MD5:	E71C8443AE0BC2E282C73FAEAD0A6DD3
SHA1:	0C110C1B01E68EDFACAEAE64781A37B1995FA94B
SHA-256:	95B0A5ACC5BF70D3ABDFD091D0C9F9063AA4FDE65BD34DBF16786082E1992E72
SHA-512:	B38458C7FA2825AFB72794F374827403D5946B1132E136A0CE075DFD351277CF7D957C88DC8A1E4ADC3BCAE1FA8010DAE3831E268E910D517691DE24326391A
Malicious:	false
Preview:	MSCF....v.....,.....I.....BVrl .authroot.stl....oJ5..CK..8U....a..3.1.P. J.".t..2F2e.dHH.....$E.KB.2D..-SJE....^..'..y.}...{m.....\...]4.G.....h....148...e.gr.....48:.L. ..g.....Xef.x:..t...J...6-....kW6Z>....&.....ye.U.Q&z:.vZ..._....a...]..T.E.....B.h.,...[....V.O.3..EW.x.?.Q..$.@.W..=.B.f..8a.Y.JK..g./%p..C.4CD.s..Jd.u..@.g=...a.. .h%..'.xjy7.E ..\.....A..':.4TdW?Ko3$.Hg.z.d~...../q..C.....`...A[ W(.....9...GZ.;....I&?.....F...p?... .p.....{S.L4..v.+...7.T?.....p..`..&..9.....f...0+.L.....1.2b)..vX5L'.~....2vz.,E.Ni.{#...o..w.?.#.3 ..h.v<.S%.].tD@!Le.w.q.7.8....QW.FT.....hE.....Y...../.%Q...k...*.Y.n..v.A..../...>B..5\..-Ko.....O<.b.K.{.O.b...._.7...4.;%9N..K.X>.....kg-9..r.c.g.G|.*[.-...HT...",?.q...ad. ...7RE.....!f..#../....?.-.^.K.c^...+{.g.....]<..$.=.O....ii7.wJ+S..Z..d.....>..J*...T..Q7..`.r,<$....\d:K`..T.n....N.....C..j.;.1SX..j....1...R....+....Yg....]....3..9..S..D..`.

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):	3.123641537625697
Encrypted:	false
SSDEEP:	6:kKOry/7UN+SkQlPlEGYRMY9z+4KlDA3RUecZUt:mCvkPlE99SNxAhUext
MD5:	1D721B64039DC653E2772556CCB02D45
SHA1:	804188A5F346A929ADFE4618FBE24CDF9BB0C38F
SHA-256:	10F85BCAB9F99A4D5BF26EA9A275348685020D302B71C4CAF4ABB46EA66940B4
SHA-512:	BAC9FCC93AD14D431147EDBB4C1986839274A47B1E53BF0C9085F445AD6B8B654F51DAC40E21ADD3F44F66FA891C1C6C7471B75159D7BF3A3AAF68866BE25C B8
Malicious:	false
Preview:	p..... .....9....Y..(..... .....).K.....&.....v...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.d.2.f.9.2.9.a.7.4.b.d.9.1.:.0."...

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	7.337848702590508

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:	f_00321b.dll
File size:	316928
MD5:	bfc060937dc90b273eccb6825145f298
SHA1:	c156c00c7e918f0cb7363614fb1f177c90d8108a
SHA256:	2f39c2879989ddd7f9ecf52b6232598e5595f8bf367846ff188c9dfbf1251253
SHA512:	cc1fee19314b0a0f9e292fa84f6e98f087033d77db937848dda1da0c88f49997866cba5465df04bf929b810b42fdb81481341064c4565c9b6272fa7f3b473ac5
SSDEEP:	6144:cwNQMQTlfdUPABVy559hhR3iP7TfPYbrF1EFVw0todxKROsCt:rNbadDBkZ6rPeEFizdxxsCt
TLSH:	2C649D47E2A601E7FC62763DA0734708A766B0524314EB5F02B04F5B2F637A3FD5AA25
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L`.=...n...n...nCy.o...nCy.o...nCy.o...n.z.o(..n.z.o...n.z.o...nCy.o...n...nq..n.z.o...n.z.o...n.zsn...n...n...n.z.o...nRich...

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x18000179c
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:	0x640B360F [Fri Mar 10 13:52:15 2023 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:	abb9300283e542fb453de5c4c87cd55d

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 00007FDE20B6DC67h
call 00007FDE20B6E240h
dec esp
mov eax, edi

Instruction
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 00007FDE20B6DAF4h
int3
int3
int3
inc eax
push ebx
dec eax
sub esp, 20h
dec eax
mov ebx, ecx
xor ecx, ecx
call dword ptr [00014903h]
dec eax
mov ecx, ebx
call dword ptr [000148F2h]
call dword ptr [000148FCh]
dec eax
mov ecx, eax
mov edx, C0000409h
dec eax
add esp, 20h
pop ebx
dec eax
jmp dword ptr [000148F0h]
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 38h
mov ecx, 00000017h
call dword ptr [000148E4h]
test eax, eax
je 00007FDE20B6DC69h
mov ecx, 00000002h
int 29h
dec eax
lea ecx, dword ptr [0002038Ah]
call 00007FDE20B6DE2Eh
dec eax
mov eax, dword ptr [esp+38h]
dec eax
mov dword ptr [00020471h], eax
dec eax
lea eax, dword ptr [esp+38h]
dec eax
add eax, 08h
dec eax
mov dword ptr [00020401h], eax
dec eax
mov eax, dword ptr [0002045Ah]

Instruction
dec eax
mov dword ptr [000202CBh], eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1f910	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1f964	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26000	0x2bd28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x23000	0x11a0	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x52000	0x684	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1e1b0	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x1e070	0x140	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x16000	0x360	.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	0x14415	0x14600	False	0.5082438650306749	data	6.388870950832575	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x16000	0xa4b4	0xa600	False	0.4210749246987952	data	4.746360898517369	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x21000	0x1ea4	0xc00	False	0.1513671875	DOS executable (block device driver \322f\324\377\3772)	2.0951973339816368	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x23000	0x11a0	0x1200	False	0.4715711805555556	data	4.892908366942992	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
_RDATA	0x25000	0x15c	0x200	False	0.408203125	data	2.8023223995708944	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x26000	0x2bd28	0x2be00	False	0.8690349002849003	data	7.841437382818367	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x52000	0x684	0x800	False	0.51708984375	data	4.920748452777265	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
LXGUM	0x26130	0xa2c	data	English	United States
LXGUM	0x26b60	0x2b000	data	English	United States
RT_STRING	0x51b60	0x48	data	English	United States
RT_MANIFEST	0x51ba8	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import

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

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x180010a70

Possible Origin

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

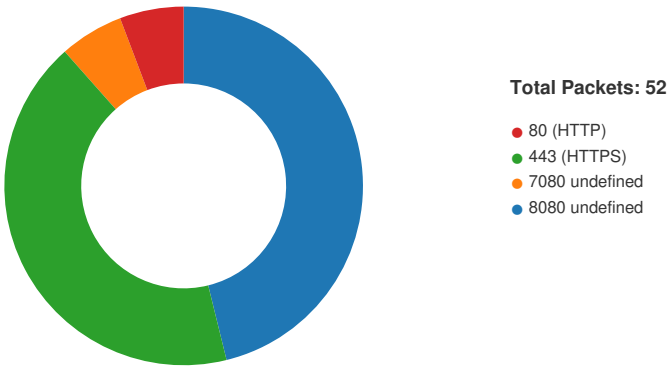
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4213.239.212.5 49729 4432404320 03/18/23-16:00:53.457464	TCP	2404320	ET CNC Feodo Tracker Reported CnC Server TCP group 11	49729	443	192.168.2.4	213.239.212.5
192.168.2.4104.168.155.1 434970580802404302 03/18/23-15:58:29.445426	TCP	2404302	ET CNC Feodo Tracker Reported CnC Server TCP group 2	49705	8080	192.168.2.4	104.168.155.143
192.168.2.445.235.8.3049 73380802404324 03/18/23-16:00:58.958124	TCP	2404324	ET CNC Feodo Tracker Reported CnC Server TCP group 13	49733	8080	192.168.2.4	45.235.8.30
192.168.2.4167.172.199.1 654970380802404310 03/18/23-15:58:19.699415	TCP	2404310	ET CNC Feodo Tracker Reported CnC Server TCP group 6	49703	8080	192.168.2.4	167.172.199.165
192.168.2.4164.90.222.65 497044432404308 03/18/23-15:58:24.948314	TCP	2404308	ET CNC Feodo Tracker Reported CnC Server TCP group 5	49704	443	192.168.2.4	164.90.222.65
192.168.2.4187.63.160.88 49702802404314 03/18/23-15:58:11.945439	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49702	80	192.168.2.4	187.63.160.88
192.168.2.41.234.2.23249 71980802404304 03/18/23-15:59:46.453351	TCP	2404304	ET CNC Feodo Tracker Reported CnC Server TCP group 3	49719	8080	192.168.2.4	1.234.2.232

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.491.121.146.47 4969580802404344 03/18/23-15:57:43.982133	TCP	2404344	ET CNC Feodo Tracker Reported CnC Server TCP group 23	49695	8080	192.168.2.4	91.121.146.47
192.168.2.4206.189.28.19 94972180802404318 03/18/23-16:00:02.963968	TCP	2404318	ET CNC Feodo Tracker Reported CnC Server TCP group 10	49721	8080	192.168.2.4	206.189.28.199
192.168.2.466.228.32.314 969770802404330 03/18/23-15:57:49.653644	TCP	2404330	ET CNC Feodo Tracker Reported CnC Server TCP group 16	49697	7080	192.168.2.4	66.228.32.31
192.168.2.4182.162.143.5 6496984432404312 03/18/23-15:58:05.445458	TCP	2404312	ET CNC Feodo Tracker Reported CnC Server TCP group 7	49698	443	192.168.2.4	182.162.143.56

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 15:57:43.982132912 CET	49695	8080	192.168.2.4	91.121.146.47
Mar 18, 2023 15:57:44.010421038 CET	8080	49695	91.121.146.47	192.168.2.4
Mar 18, 2023 15:57:44.010539055 CET	49695	8080	192.168.2.4	91.121.146.47
Mar 18, 2023 15:57:44.013843060 CET	49695	8080	192.168.2.4	91.121.146.47
Mar 18, 2023 15:57:44.041975975 CET	8080	49695	91.121.146.47	192.168.2.4
Mar 18, 2023 15:57:44.064595938 CET	8080	49695	91.121.146.47	192.168.2.4
Mar 18, 2023 15:57:44.064632893 CET	8080	49695	91.121.146.47	192.168.2.4
Mar 18, 2023 15:57:44.064770937 CET	49695	8080	192.168.2.4	91.121.146.47
Mar 18, 2023 15:57:44.077897072 CET	49695	8080	192.168.2.4	91.121.146.47
Mar 18, 2023 15:57:44.107184887 CET	8080	49695	91.121.146.47	192.168.2.4
Mar 18, 2023 15:57:44.155500889 CET	49695	8080	192.168.2.4	91.121.146.47
Mar 18, 2023 15:57:45.521246910 CET	49695	8080	192.168.2.4	91.121.146.47
Mar 18, 2023 15:57:45.521328926 CET	49695	8080	192.168.2.4	91.121.146.47
Mar 18, 2023 15:57:45.553070068 CET	8080	49695	91.121.146.47	192.168.2.4
Mar 18, 2023 15:57:45.563245058 CET	8080	49695	91.121.146.47	192.168.2.4
Mar 18, 2023 15:57:45.608760118 CET	49695	8080	192.168.2.4	91.121.146.47
Mar 18, 2023 15:57:48.559087038 CET	8080	49695	91.121.146.47	192.168.2.4
Mar 18, 2023 15:57:48.559130907 CET	8080	49695	91.121.146.47	192.168.2.4
Mar 18, 2023 15:57:48.559294939 CET	49695	8080	192.168.2.4	91.121.146.47
Mar 18, 2023 15:57:48.559461117 CET	49695	8080	192.168.2.4	91.121.146.47
Mar 18, 2023 15:57:48.559514999 CET	49695	8080	192.168.2.4	91.121.146.47
Mar 18, 2023 15:57:48.587496996 CET	8080	49695	91.121.146.47	192.168.2.4
Mar 18, 2023 15:57:48.587532997 CET	8080	49695	91.121.146.47	192.168.2.4
Mar 18, 2023 15:57:49.653644085 CET	49697	7080	192.168.2.4	66.228.32.31
Mar 18, 2023 15:57:52.656811953 CET	49697	7080	192.168.2.4	66.228.32.31

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 15:57:58.703701019 CET	49697	7080	192.168.2.4	66.228.32.31
Mar 18, 2023 15:58:05.445457935 CET	49698	443	192.168.2.4	182.162.143.56
Mar 18, 2023 15:58:05.445525885 CET	443	49698	182.162.143.56	192.168.2.4
Mar 18, 2023 15:58:05.445621014 CET	49698	443	192.168.2.4	182.162.143.56
Mar 18, 2023 15:58:05.446594000 CET	49698	443	192.168.2.4	182.162.143.56
Mar 18, 2023 15:58:05.446608067 CET	443	49698	182.162.143.56	192.168.2.4
Mar 18, 2023 15:58:05.713150024 CET	443	49698	182.162.143.56	192.168.2.4
Mar 18, 2023 15:58:05.713974953 CET	49699	443	192.168.2.4	182.162.143.56
Mar 18, 2023 15:58:05.714050055 CET	443	49699	182.162.143.56	192.168.2.4
Mar 18, 2023 15:58:05.714160919 CET	49699	443	192.168.2.4	182.162.143.56
Mar 18, 2023 15:58:05.715395927 CET	49699	443	192.168.2.4	182.162.143.56
Mar 18, 2023 15:58:05.715436935 CET	443	49699	182.162.143.56	192.168.2.4
Mar 18, 2023 15:58:05.987780094 CET	443	49699	182.162.143.56	192.168.2.4
Mar 18, 2023 15:58:05.989764929 CET	49700	443	192.168.2.4	182.162.143.56
Mar 18, 2023 15:58:05.989820957 CET	443	49700	182.162.143.56	192.168.2.4
Mar 18, 2023 15:58:05.990039110 CET	49700	443	192.168.2.4	182.162.143.56
Mar 18, 2023 15:58:05.991280079 CET	49700	443	192.168.2.4	182.162.143.56
Mar 18, 2023 15:58:05.991303921 CET	443	49700	182.162.143.56	192.168.2.4
Mar 18, 2023 15:58:06.239960909 CET	443	49700	182.162.143.56	192.168.2.4
Mar 18, 2023 15:58:06.241710901 CET	49701	443	192.168.2.4	182.162.143.56
Mar 18, 2023 15:58:06.241755962 CET	443	49701	182.162.143.56	192.168.2.4
Mar 18, 2023 15:58:06.241857052 CET	49701	443	192.168.2.4	182.162.143.56
Mar 18, 2023 15:58:06.242470980 CET	49701	443	192.168.2.4	182.162.143.56
Mar 18, 2023 15:58:06.242486954 CET	443	49701	182.162.143.56	192.168.2.4
Mar 18, 2023 15:58:06.501095057 CET	443	49701	182.162.143.56	192.168.2.4
Mar 18, 2023 15:58:11.945439100 CET	49702	80	192.168.2.4	187.63.160.88
Mar 18, 2023 15:58:12.179195881 CET	80	49702	187.63.160.88	192.168.2.4
Mar 18, 2023 15:58:12.689225912 CET	49702	80	192.168.2.4	187.63.160.88
Mar 18, 2023 15:58:12.922725916 CET	80	49702	187.63.160.88	192.168.2.4
Mar 18, 2023 15:58:13.423608065 CET	49702	80	192.168.2.4	187.63.160.88
Mar 18, 2023 15:58:13.661552906 CET	80	49702	187.63.160.88	192.168.2.4
Mar 18, 2023 15:58:19.699414968 CET	49703	8080	192.168.2.4	167.172.199.165
Mar 18, 2023 15:58:19.867234945 CET	8080	49703	167.172.199.165	192.168.2.4
Mar 18, 2023 15:58:19.867444038 CET	49703	8080	192.168.2.4	167.172.199.165
Mar 18, 2023 15:58:19.868233919 CET	49703	8080	192.168.2.4	167.172.199.165
Mar 18, 2023 15:58:20.035275936 CET	8080	49703	167.172.199.165	192.168.2.4
Mar 18, 2023 15:58:20.045103073 CET	8080	49703	167.172.199.165	192.168.2.4
Mar 18, 2023 15:58:20.045140028 CET	8080	49703	167.172.199.165	192.168.2.4
Mar 18, 2023 15:58:20.045212030 CET	49703	8080	192.168.2.4	167.172.199.165
Mar 18, 2023 15:58:20.051392078 CET	49703	8080	192.168.2.4	167.172.199.165
Mar 18, 2023 15:58:20.219124079 CET	8080	49703	167.172.199.165	192.168.2.4
Mar 18, 2023 15:58:20.220163107 CET	49703	8080	192.168.2.4	167.172.199.165
Mar 18, 2023 15:58:20.428314924 CET	8080	49703	167.172.199.165	192.168.2.4
Mar 18, 2023 15:58:21.038682938 CET	8080	49703	167.172.199.165	192.168.2.4
Mar 18, 2023 15:58:21.080550909 CET	49703	8080	192.168.2.4	167.172.199.165
Mar 18, 2023 15:58:24.038556099 CET	8080	49703	167.172.199.165	192.168.2.4
Mar 18, 2023 15:58:24.038588047 CET	8080	49703	167.172.199.165	192.168.2.4
Mar 18, 2023 15:58:24.038654089 CET	49703	8080	192.168.2.4	167.172.199.165
Mar 18, 2023 15:58:24.039973974 CET	49703	8080	192.168.2.4	167.172.199.165
Mar 18, 2023 15:58:24.040021896 CET	49703	8080	192.168.2.4	167.172.199.165
Mar 18, 2023 15:58:24.207125902 CET	8080	49703	167.172.199.165	192.168.2.4
Mar 18, 2023 15:58:24.207159042 CET	8080	49703	167.172.199.165	192.168.2.4
Mar 18, 2023 15:58:24.948313951 CET	49704	443	192.168.2.4	164.90.222.65
Mar 18, 2023 15:58:24.948385954 CET	443	49704	164.90.222.65	192.168.2.4
Mar 18, 2023 15:58:24.948482990 CET	49704	443	192.168.2.4	164.90.222.65
Mar 18, 2023 15:58:24.949033022 CET	49704	443	192.168.2.4	164.90.222.65
Mar 18, 2023 15:58:24.949058056 CET	443	49704	164.90.222.65	192.168.2.4
Mar 18, 2023 15:58:25.070983887 CET	443	49704	164.90.222.65	192.168.2.4
Mar 18, 2023 15:58:25.071180105 CET	49704	443	192.168.2.4	164.90.222.65

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 15:58:25.075246096 CET	49704	443	192.168.2.4	164.90.222.65
Mar 18, 2023 15:58:25.075273991 CET	443	49704	164.90.222.65	192.168.2.4
Mar 18, 2023 15:58:25.075628996 CET	443	49704	164.90.222.65	192.168.2.4
Mar 18, 2023 15:58:25.127825975 CET	49704	443	192.168.2.4	164.90.222.65
Mar 18, 2023 15:58:25.402632952 CET	49704	443	192.168.2.4	164.90.222.65
Mar 18, 2023 15:58:25.402668953 CET	443	49704	164.90.222.65	192.168.2.4
Mar 18, 2023 15:58:25.615834951 CET	443	49704	164.90.222.65	192.168.2.4
Mar 18, 2023 15:58:25.615917921 CET	443	49704	164.90.222.65	192.168.2.4
Mar 18, 2023 15:58:25.616075039 CET	49704	443	192.168.2.4	164.90.222.65
Mar 18, 2023 15:58:25.616332054 CET	49704	443	192.168.2.4	164.90.222.65
Mar 18, 2023 15:58:25.616355896 CET	443	49704	164.90.222.65	192.168.2.4
Mar 18, 2023 15:58:25.616396904 CET	49704	443	192.168.2.4	164.90.222.65
Mar 18, 2023 15:58:25.616406918 CET	443	49704	164.90.222.65	192.168.2.4
Mar 18, 2023 15:58:29.445425987 CET	49705	8080	192.168.2.4	104.168.155.143
Mar 18, 2023 15:58:29.608290911 CET	8080	49705	104.168.155.143	192.168.2.4
Mar 18, 2023 15:58:30.112575054 CET	49705	8080	192.168.2.4	104.168.155.143

DNS Answers

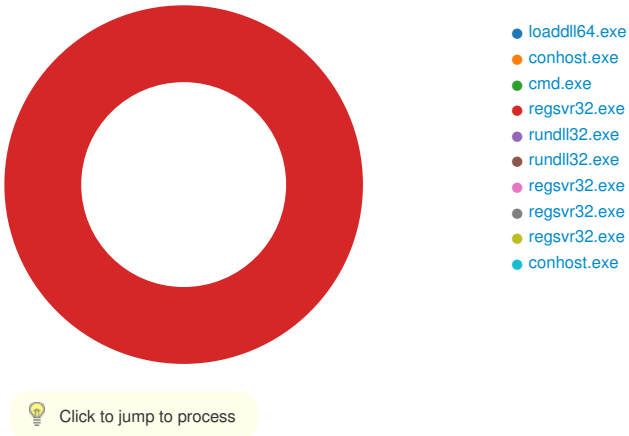
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 18, 2023 15:57:44.642750978 CET	8.8.8.8	192.168.2.4	0x901a	No error (0)	au.c-0001.c-msedge.net	c-0001.c-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 18, 2023 15:57:44.642750978 CET	8.8.8.8	192.168.2.4	0x901a	No error (0)	c-0001.c-msedge.net		13.107.4.50	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 164.90.222.65

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **4224**, Parent PID: **3528**

General	
Target ID:	0
Start time:	15:57:02
Start date:	18/03/2023
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\f_00321b.dll"
Imagebase:	0x7ff73c1f0000
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: **2516**, Parent PID: **4224**

General	
Target ID:	1
Start time:	15:57:02
Start date:	18/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: **3216**, Parent PID: **4224**

General	
Target ID:	2
Start time:	15:57:02
Start date:	18/03/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\f_00321b.dll",#1
Imagebase:	0x7ff632260000
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: **4888**, Parent PID: **4224**

General

Target ID:	3
Start time:	15:57:02
Start date:	18/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\f_00321b.dll
Imagebase:	0x7ff6746f0000
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: 00000003.00000002.319594851.0000000002301000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.319426857.00000000022D0000.00000040.00001000.00020000.00000000.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\ZbmMPnDvLqwXll\QyzgcRWJYZS.dll:Zone.Identifier	success or wait	1	230289D	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: **1264**, Parent PID: **3216**

General

Target ID:	4
Start time:	15:57:02
Start date:	18/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\f_00321b.dll",#1
Imagebase:	0x7ff669490000
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: 00000004.00000002.320583141.0000024067ED1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.320487184.0000024067EA0000.00000040.00001000.00020000.00000000.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: **1240**, Parent PID: **4224**

General

Target ID:	5
Start time:	15:57:02
Start date:	18/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\f_00321b.dll,DllRegisterServer
Imagebase:	0x7ff669490000
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: 00000005.00000002.320938696.000001CAEF360000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.320983303.000001CAEF391000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **1312**, Parent PID: **4888**

General

Target ID:	6
Start time:	15:57:04
Start date:	18/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZbmMPnDvLqwXll\QyzgcRWJYZS.dll"
Imagebase:	0x7ff6746f0000
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: 00000006.00000002.839406801.0000000002031000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: Yara detected Emotet, Source: 00000006.00000002.839010466.000000000072B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.839356776.0000000001FE0000.00000040.00001000.00020000.00000000.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

Analysis Process: regsvr32.exe PID: **5968**, Parent PID: **1264**

General

Target ID:	7
Start time:	15:57:05
Start date:	18/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\RymKYMmySRfU\EAqrfXJOpHznppsf.dll"
Imagebase:	0x7ff6746f0000
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: **4768**, Parent PID: **1240**

General

Target ID:	8
Start time:	15:57:05
Start date:	18/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\IzuSuDitBV\QmEREbzuu.dll"
Imagebase:	0x7ff6746f0000
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: conhost.exe PID: **5432**, Parent PID: **1240**

General

Target ID:	10
Start time:	15:57:50
Start date:	18/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000

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