ID: 829540
Sample Name: f_00321b
Cookbook: default.jbs
Time: 15:36:03
Date: 18/03/2023
Version: 37.0.0 Beryl

Table of Contents

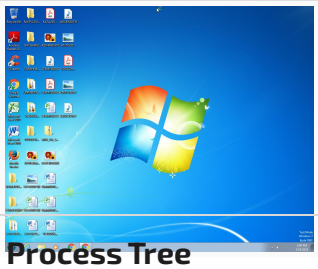
Windows Analysis Report

f_00321b.dll

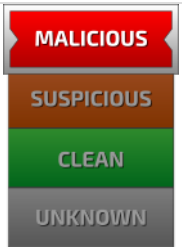
Overview

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:	829540
MD5:	bfc060937dc90..
SHA1:	c156c00c7e91…
SHA256:	2f39c2879989d..
Infos:	



Detection



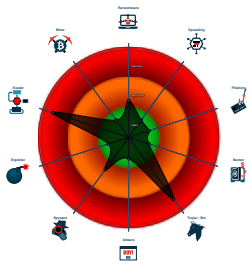
Emotet

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 w7x64**
- loaddll64.exe (PID: 1484 cmdline: loaddll64.exe "C:\Users\user\Desktop\f_00321b.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - cmd.exe (PID: 1624 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\f_00321b.dll",#1 MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - rundll32.exe (PID: 152 cmdline: rundll32.exe "C:\Users\user\Desktop\f_00321b.dll",#1 MD5: DD81D91FF3B0763C392422865C9AC12E)
      - regsvr32.exe (PID: 1748 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\CcdErbXwwqK\BMwTvRDPNYt.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 508 cmdline: regsvr32.exe /s C:\Users\user\Desktop\f_00321b.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1696 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\TMlQeVZkdztztmVcv\UUQGnKwW.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - rundll32.exe (PID: 500 cmdline: rundll32.exe C:\Users\user\Desktop\f_00321b.dll,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - regsvr32.exe (PID: 3068 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\PmXMgnVtL\uQQuLasS.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **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+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5SKNpb3sAAIg=",
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2QqNpb3sAAJA="
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.911933178.00000000001E1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.911793490.00000000001B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.911404298.00000000001C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.911845792.00000000001E1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000008.00000002.1424978614.0000000000150000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.regsvr32.exe.150000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.regsvr32.exe.150000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.rundll32.exe.1b0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.1b0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.regsvr32.exe.1c0000.0.raw.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 8 - Source IP: 192.168.2.22 - Destination IP: 187.63.160.88

Timestamp:	192.168.2.22187.63.160.8849176802404314 03/18/23-15:38:03.514864
SID:	2404314
Source Port:	49176
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 5 - Source IP: 192.168.2.22 - Destination IP: 164.90.222.65

Timestamp:	192.168.2.22164.90.222.65491804432404308 03/18/23-15:38:18.283118
SID:	2404308
Source Port:	49180
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 7 - Source IP: 192.168.2.22 - Destination IP: 182.162.143.56

Timestamp:	192.168.2.22182.162.143.56491744432404312 03/18/23-15:37:57.523500
SID:	2404312
Source Port:	49174
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 10 - Source IP: 192.168.2.22 - Destination IP: 206.189.28.199

Timestamp:	192.168.2.22206.189.28.1994919980802404318 03/18/23-15:39:57.037730
SID:	2404318
Source Port:	49199
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 23 - Source IP: 192.168.2.22 - Destination IP: 91.121.146.47

Timestamp:	192.168.2.2291.121.146.474917180802404344 03/18/23-15:37:36.144887
SID:	2404344
Source Port:	49171

Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 2 - Source IP: 192.168.2.22 - Destination IP: 104.168.155.143	
Timestamp:	192.168.2.22104.168.155.1434918180802404302 03/18/23-15:38:23.020494
SID:	2404302
Source Port:	49181
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 11 - Source IP: 192.168.2.22 - Destination IP: 213.239.212.5	
Timestamp:	192.168.2.22213.239.212.5492074432404320 03/18/23-15:40:50.591212
SID:	2404320
Source Port:	49207
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 16 - Source IP: 192.168.2.22 - Destination IP: 66.228.32.31	
Timestamp:	192.168.2.2266.228.32.314917370802404330 03/18/23-15:37:41.768531
SID:	2404330
Source Port:	49173
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 6 - Source IP: 192.168.2.22 - Destination IP: 167.172.199.165	
Timestamp:	192.168.2.22167.172.199.1654917880802404310 03/18/23-15:38:12.283319
SID:	2404310
Source Port:	49178
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 13 - Source IP: 192.168.2.22 - Destination IP: 45.235.8.30	
Timestamp:	192.168.2.2245.235.8.304920980802404324 03/18/23-15:40:56.034190
SID:	2404324
Source Port:	49209
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 3 - Source IP: 192.168.2.22 - Destination IP: 1.234.2.232	
Timestamp:	192.168.2.221.234.2.2324919580802404304 03/18/23-15:39:40.069060
SID:	2404304
Source Port:	49195
Destination Port:	8080
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

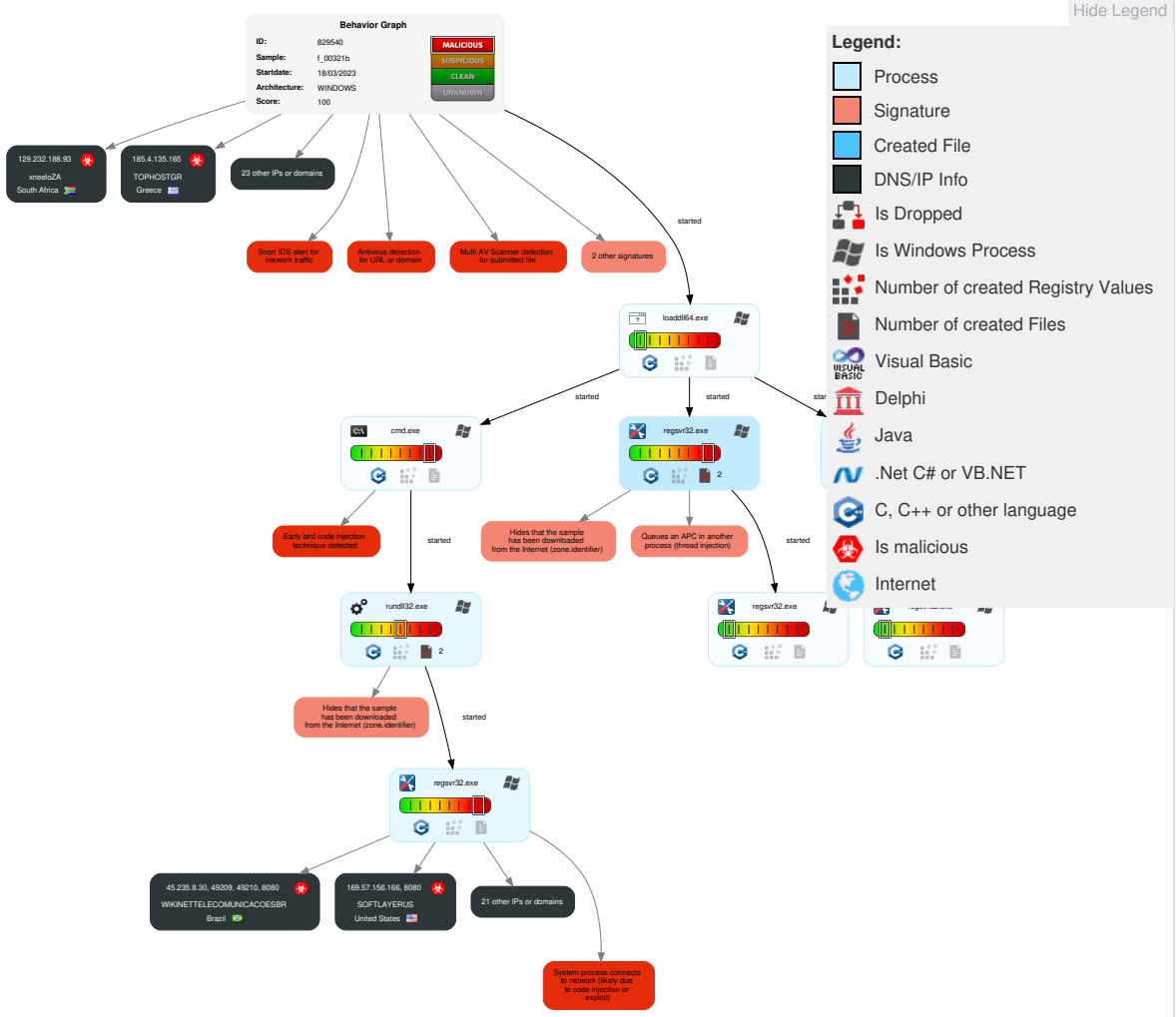
Mitre Att&ck Matrix

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	Path Interception	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	Boot or Logon Initialization Scripts	1 Modify Registry	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)	2 Virtualization/Sandbox Evasion	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)	3 1 1 Process Injection	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Obfuscated Files or Information	Cached Domain Credentials	2 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Regsvr32	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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 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 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

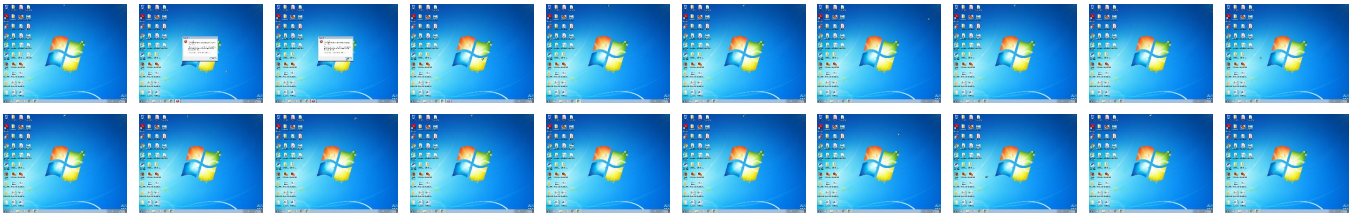
Hide Legend



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	79%	ReversingLabs	Win64.Trojan.Emotet	
f_00321b.dll	60%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.rundll32.exe.1b0000.0.unpack	100%	Avira	HEUR/AGEN.1215476		Download File
8.2.regsvr32.exe.150000.0.unpack	100%	Avira	HEUR/AGEN.1215476		Download File
6.2.rundll32.exe.1b0000.0.unpack	100%	Avira	HEUR/AGEN.1215476		Download File
4.2.regsvr32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1215476		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://164.90.222.65/wlqjqf/sqfqe/frrdsoxthmytiqq/rzfarh/	100%	Avira URL Cloud	malware	
http://https://45.235.8.30:8080/wlqjqf/sqfqe/frrdsoxthmytiqq/rzfarh/	100%	Avira URL Cloud	malware	
http://https://163.44.196.120:8080/wlqjqf/sqfqe/frrdsoxthmytiqq/rzfarh/$	100%	Avira URL Cloud	malware	
http://https://45.235.8.30:8080/wlqjqf/sqfqe/frrdsoxthmytiqq/rzfarh//A	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

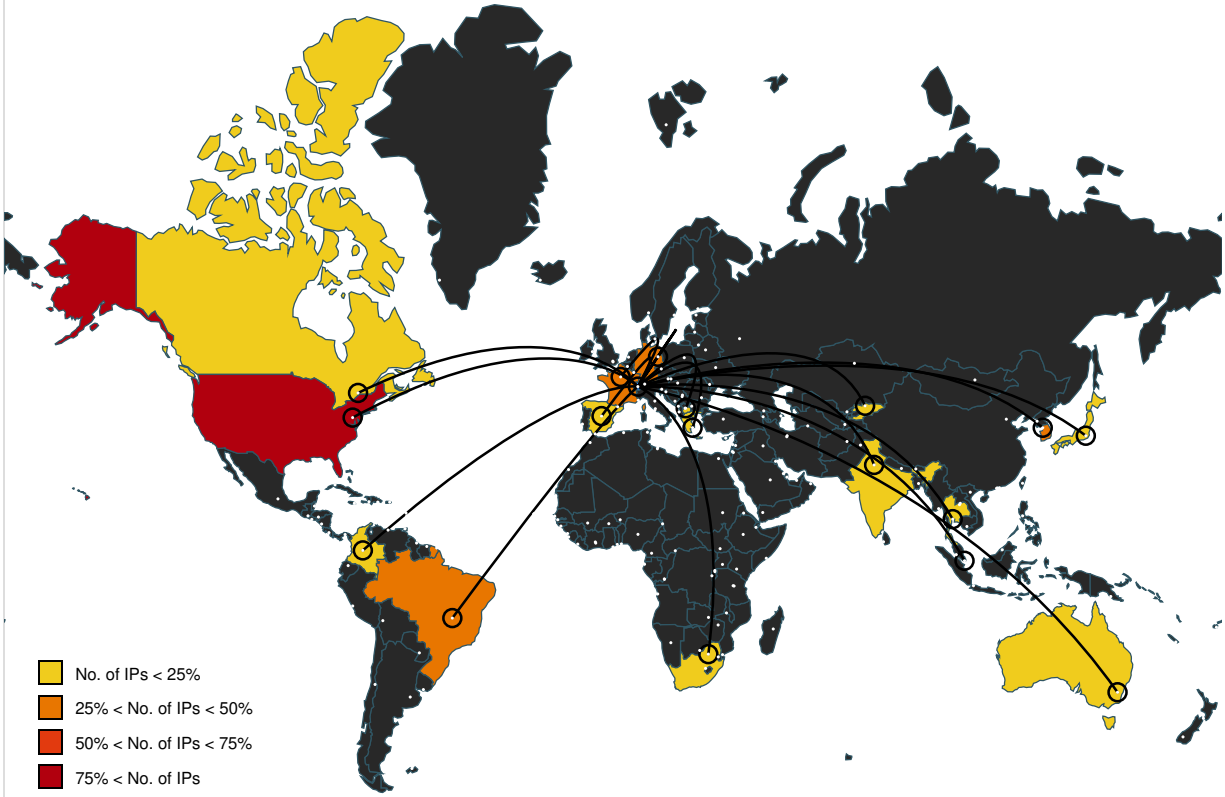
Name	Malicious	Antivirus Detection	Reputation
http://https://164.90.222.65/wlqjqf/sqfqe/frrdsoxthmytiqq/rzfarh/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000008.00000002.14250810 92.00000000003AB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0008.00000003.1079294071.00000000003AB00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000008.00000002.14250810 92.00000000003AB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0008.00000003.1079294071.00000000003AB00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000008.00000002.14250810 92.00000000003AB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0008.00000003.1079294071.00000000003AB00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://45.235.8.30:8080/wlqjqf/sqfqe/frrdsoxthmytiqq/rzfarh//A	regsvr32.exe, 00000008.00000002.14253405 70.0000000002C9F000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000008.00000002.14250810 92.00000000003AB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0008.00000003.1079294071.00000000003AB00 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://45.235.8.30:8080/wlqjqf/sqfqe/frrdsoxthmytiqq/rzfarh/	regsvr32.exe, 00000008.00000002.14250810 92.00000000003AB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0008.00000002.1425340570.0000000002C9F00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000008.00000002.14250810 92.00000000003AB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0008.00000003.1079294071.00000000003AB00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.entrust.net03	regsvr32.exe, 00000008.00000002.14250810 92.00000000003AB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0008.00000003.1079294071.00000000003AB00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000008.00000002.14250810 92.00000000003AB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0008.00000003.1079294071.00000000003AB00 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://163.44.196.120:8080/wlqjqf/sqfqe/frrdsoxthmytiqq/rzfarh/$	regsvr32.exe, 00000008.00000002.14250810 92.000000000039A000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000008.00000002.14250810 92.00000000003AB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0008.00000003.1079294071.00000000003AB00 0.00000004.00000020.00020000.00000000.sdmp	false		high

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
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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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:	829540
Start date and time:	2023-03-18 15:36:03 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)

Number of analysed new started processes analysed:	10
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@15/0@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: 89% • 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): dllhost.exe, conhost.exe
- TCP Packets have been reduced to 100
- 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 NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:36:21	API Interceptor	67x Sleep call for process: regsvr32.exe modified
15:36:21	API Interceptor	4x Sleep call for process: rundll32.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

No created / dropped files found

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:	3074e4d6ded4d0e4

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 00007FC93D23D377h
call 00007FC93D23D950h
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 00007FC93D23D204h
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 00007FC93D23D379h

Instruction
mov ecx, 00000002h
int 29h
dec eax
lea ecx, dword ptr [0002038Ah]
call 00007FC93D23D53Eh
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]
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
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	

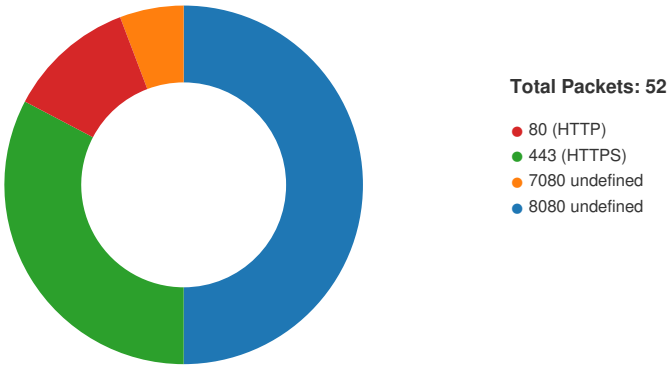
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.22187.63.160.88491768024043140 3/18/23-15:38:03.514864	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49176	80	192.168.2.22	187.63.160.88
192.168.2.22164.90.222.65491804432404308 03/18/23-15:38:18.283118	TCP	2404308	ET CNC Feodo Tracker Reported CnC Server TCP group 5	49180	443	192.168.2.22	164.90.222.65
192.168.2.22182.162.143.56491744432404312 03/18/23-15:37:57.523500	TCP	2404312	ET CNC Feodo Tracker Reported CnC Server TCP group 7	49174	443	192.168.2.22	182.162.143.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.22206.189.28.199491998080240431803/18/23-15:39:57.037730	TCP	2404318	ET CNC Feodo Tracker Reported CnC Server TCP group 10	49199	8080	192.168.2.22	206.189.28.199
192.168.2.2291.121.146.474917180802404344 03/18/23-15:37:36.144887	TCP	2404344	ET CNC Feodo Tracker Reported CnC Server TCP group 23	49171	8080	192.168.2.22	91.121.146.47
192.168.2.22104.168.155.1434918180802404302 03/18/23-15:38:23.020494	TCP	2404302	ET CNC Feodo Tracker Reported CnC Server TCP group 2	49181	8080	192.168.2.22	104.168.155.143
192.168.2.22213.239.212.5492074432404320 03/18/23-15:40:50.591212	TCP	2404320	ET CNC Feodo Tracker Reported CnC Server TCP group 11	49207	443	192.168.2.22	213.239.212.5
192.168.2.2266.228.32.314917370802404330 03/18/23-15:37:41.768531	TCP	2404330	ET CNC Feodo Tracker Reported CnC Server TCP group 16	49173	7080	192.168.2.22	66.228.32.31
192.168.2.22167.172.199.165491788080240431003/18/23-15:38:12.283319	TCP	2404310	ET CNC Feodo Tracker Reported CnC Server TCP group 6	49178	8080	192.168.2.22	167.172.199.165
192.168.2.2245.235.8.304920980802404324 03/18/23-15:40:56.034190	TCP	2404324	ET CNC Feodo Tracker Reported CnC Server TCP group 13	49209	8080	192.168.2.22	45.235.8.30
192.168.2.221.234.2.2324919580802404304 03/18/23-15:39:40.069060	TCP	2404304	ET CNC Feodo Tracker Reported CnC Server TCP group 3	49195	8080	192.168.2.22	1.234.2.232

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 15:37:36.144886971 CET	49171	8080	192.168.2.22	91.121.146.47
Mar 18, 2023 15:37:36.175470114 CET	8080	49171	91.121.146.47	192.168.2.22
Mar 18, 2023 15:37:36.175915003 CET	49171	8080	192.168.2.22	91.121.146.47
Mar 18, 2023 15:37:36.182074070 CET	49171	8080	192.168.2.22	91.121.146.47
Mar 18, 2023 15:37:36.212233067 CET	8080	49171	91.121.146.47	192.168.2.22
Mar 18, 2023 15:37:36.212558031 CET	8080	49171	91.121.146.47	192.168.2.22
Mar 18, 2023 15:37:36.212650061 CET	8080	49171	91.121.146.47	192.168.2.22
Mar 18, 2023 15:37:36.213042974 CET	49171	8080	192.168.2.22	91.121.146.47
Mar 18, 2023 15:37:36.217742920 CET	49171	8080	192.168.2.22	91.121.146.47
Mar 18, 2023 15:37:36.218523026 CET	49172	8080	192.168.2.22	91.121.146.47
Mar 18, 2023 15:37:36.248423100 CET	8080	49171	91.121.146.47	192.168.2.22
Mar 18, 2023 15:37:36.248658895 CET	8080	49172	91.121.146.47	192.168.2.22
Mar 18, 2023 15:37:36.248792887 CET	49172	8080	192.168.2.22	91.121.146.47

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 15:37:36.249490976 CET	49172	8080	192.168.2.22	91.121.146.47
Mar 18, 2023 15:37:36.279648066 CET	8080	49172	91.121.146.47	192.168.2.22
Mar 18, 2023 15:37:36.279700041 CET	8080	49172	91.121.146.47	192.168.2.22
Mar 18, 2023 15:37:36.279943943 CET	8080	49172	91.121.146.47	192.168.2.22
Mar 18, 2023 15:37:36.280045986 CET	49172	8080	192.168.2.22	91.121.146.47
Mar 18, 2023 15:37:36.280479908 CET	49172	8080	192.168.2.22	91.121.146.47
Mar 18, 2023 15:37:36.308737993 CET	8080	49172	91.121.146.47	192.168.2.22
Mar 18, 2023 15:37:41.768531084 CET	49173	7080	192.168.2.22	66.228.32.31
Mar 18, 2023 15:37:44.789923906 CET	49173	7080	192.168.2.22	66.228.32.31
Mar 18, 2023 15:37:50.797275066 CET	49173	7080	192.168.2.22	66.228.32.31
Mar 18, 2023 15:37:57.523499966 CET	49174	443	192.168.2.22	182.162.143.56
Mar 18, 2023 15:37:57.523564100 CET	443	49174	182.162.143.56	192.168.2.22
Mar 18, 2023 15:37:57.523648977 CET	49174	443	192.168.2.22	182.162.143.56
Mar 18, 2023 15:37:57.524748087 CET	49174	443	192.168.2.22	182.162.143.56
Mar 18, 2023 15:37:57.524776936 CET	443	49174	182.162.143.56	192.168.2.22
Mar 18, 2023 15:37:57.780865908 CET	443	49174	182.162.143.56	192.168.2.22
Mar 18, 2023 15:37:57.817265987 CET	49175	443	192.168.2.22	182.162.143.56
Mar 18, 2023 15:37:57.817320108 CET	443	49175	182.162.143.56	192.168.2.22
Mar 18, 2023 15:37:57.817373037 CET	49175	443	192.168.2.22	182.162.143.56
Mar 18, 2023 15:37:57.817914963 CET	49175	443	192.168.2.22	182.162.143.56
Mar 18, 2023 15:37:57.817941904 CET	443	49175	182.162.143.56	192.168.2.22
Mar 18, 2023 15:37:58.084074020 CET	443	49175	182.162.143.56	192.168.2.22
Mar 18, 2023 15:38:03.514863968 CET	49176	80	192.168.2.22	187.63.160.88
Mar 18, 2023 15:38:03.747106075 CET	80	49176	187.63.160.88	192.168.2.22
Mar 18, 2023 15:38:04.244808912 CET	49176	80	192.168.2.22	187.63.160.88
Mar 18, 2023 15:38:04.476881027 CET	80	49176	187.63.160.88	192.168.2.22
Mar 18, 2023 15:38:04.978034019 CET	49176	80	192.168.2.22	187.63.160.88
Mar 18, 2023 15:38:05.210088015 CET	80	49176	187.63.160.88	192.168.2.22
Mar 18, 2023 15:38:05.219971895 CET	49177	80	192.168.2.22	187.63.160.88
Mar 18, 2023 15:38:05.451931953 CET	80	49177	187.63.160.88	192.168.2.22
Mar 18, 2023 15:38:05.960834026 CET	49177	80	192.168.2.22	187.63.160.88
Mar 18, 2023 15:38:06.192723036 CET	80	49177	187.63.160.88	192.168.2.22
Mar 18, 2023 15:38:06.787751913 CET	49177	80	192.168.2.22	187.63.160.88
Mar 18, 2023 15:38:07.020184040 CET	80	49177	187.63.160.88	192.168.2.22
Mar 18, 2023 15:38:12.283318996 CET	49178	8080	192.168.2.22	167.172.199.165
Mar 18, 2023 15:38:12.453504086 CET	8080	49178	167.172.199.165	192.168.2.22
Mar 18, 2023 15:38:12.454113960 CET	49178	8080	192.168.2.22	167.172.199.165
Mar 18, 2023 15:38:12.454807997 CET	49178	8080	192.168.2.22	167.172.199.165
Mar 18, 2023 15:38:12.622737885 CET	8080	49178	167.172.199.165	192.168.2.22
Mar 18, 2023 15:38:12.622765064 CET	8080	49178	167.172.199.165	192.168.2.22
Mar 18, 2023 15:38:12.622783899 CET	8080	49178	167.172.199.165	192.168.2.22
Mar 18, 2023 15:38:12.623018980 CET	49178	8080	192.168.2.22	167.172.199.165
Mar 18, 2023 15:38:12.623205900 CET	49178	8080	192.168.2.22	167.172.199.165
Mar 18, 2023 15:38:12.623991013 CET	49179	8080	192.168.2.22	167.172.199.165
Mar 18, 2023 15:38:12.791045904 CET	8080	49178	167.172.199.165	192.168.2.22
Mar 18, 2023 15:38:12.792309999 CET	8080	49179	167.172.199.165	192.168.2.22
Mar 18, 2023 15:38:12.792481899 CET	49179	8080	192.168.2.22	167.172.199.165
Mar 18, 2023 15:38:12.793487072 CET	49179	8080	192.168.2.22	167.172.199.165
Mar 18, 2023 15:38:12.961529970 CET	8080	49179	167.172.199.165	192.168.2.22
Mar 18, 2023 15:38:12.961565018 CET	8080	49179	167.172.199.165	192.168.2.22
Mar 18, 2023 15:38:12.961589098 CET	8080	49179	167.172.199.165	192.168.2.22
Mar 18, 2023 15:38:12.961654902 CET	49179	8080	192.168.2.22	167.172.199.165
Mar 18, 2023 15:38:12.961990118 CET	49179	8080	192.168.2.22	167.172.199.165
Mar 18, 2023 15:38:13.130383015 CET	8080	49179	167.172.199.165	192.168.2.22
Mar 18, 2023 15:38:18.283118010 CET	49180	443	192.168.2.22	164.90.222.65
Mar 18, 2023 15:38:18.283179998 CET	443	49180	164.90.222.65	192.168.2.22
Mar 18, 2023 15:38:18.283273935 CET	49180	443	192.168.2.22	164.90.222.65
Mar 18, 2023 15:38:18.284213066 CET	49180	443	192.168.2.22	164.90.222.65
Mar 18, 2023 15:38:18.284236908 CET	443	49180	164.90.222.65	192.168.2.22

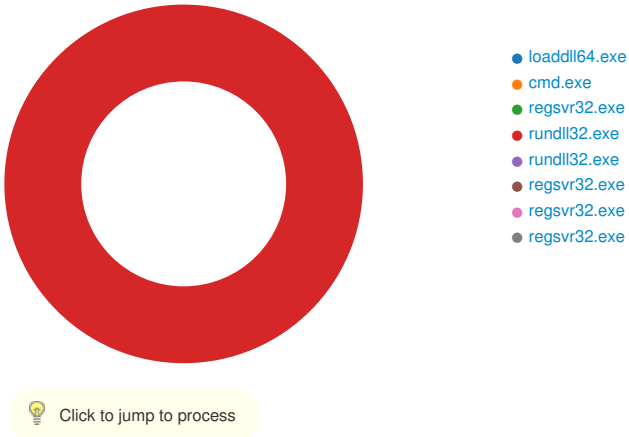
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 15:38:18.431541920 CET	443	49180	164.90.222.65	192.168.2.22
Mar 18, 2023 15:38:18.431782961 CET	49180	443	192.168.2.22	164.90.222.65
Mar 18, 2023 15:38:18.441814899 CET	49180	443	192.168.2.22	164.90.222.65
Mar 18, 2023 15:38:18.441848993 CET	443	49180	164.90.222.65	192.168.2.22
Mar 18, 2023 15:38:18.442712069 CET	443	49180	164.90.222.65	192.168.2.22
Mar 18, 2023 15:38:18.644869089 CET	49180	443	192.168.2.22	164.90.222.65
Mar 18, 2023 15:38:18.943536997 CET	49180	443	192.168.2.22	164.90.222.65
Mar 18, 2023 15:38:18.943609953 CET	443	49180	164.90.222.65	192.168.2.22
Mar 18, 2023 15:38:18.943661928 CET	49180	443	192.168.2.22	164.90.222.65
Mar 18, 2023 15:38:18.943677902 CET	443	49180	164.90.222.65	192.168.2.22
Mar 18, 2023 15:38:19.226474047 CET	443	49180	164.90.222.65	192.168.2.22
Mar 18, 2023 15:38:19.226640940 CET	443	49180	164.90.222.65	192.168.2.22
Mar 18, 2023 15:38:19.226731062 CET	49180	443	192.168.2.22	164.90.222.65
Mar 18, 2023 15:38:19.228950024 CET	49180	443	192.168.2.22	164.90.222.65
Mar 18, 2023 15:38:19.228950024 CET	49180	443	192.168.2.22	164.90.222.65
Mar 18, 2023 15:38:19.228988886 CET	443	49180	164.90.222.65	192.168.2.22
Mar 18, 2023 15:38:19.229007959 CET	443	49180	164.90.222.65	192.168.2.22
Mar 18, 2023 15:38:23.020493984 CET	49181	8080	192.168.2.22	104.168.155.143
Mar 18, 2023 15:38:23.184979916 CET	8080	49181	104.168.155.143	192.168.2.22
Mar 18, 2023 15:38:23.684108019 CET	49181	8080	192.168.2.22	104.168.155.143
Mar 18, 2023 15:38:23.847106934 CET	8080	49181	104.168.155.143	192.168.2.22
Mar 18, 2023 15:38:24.354909897 CET	49181	8080	192.168.2.22	104.168.155.143
Mar 18, 2023 15:38:24.517730951 CET	8080	49181	104.168.155.143	192.168.2.22
Mar 18, 2023 15:38:24.518639088 CET	49182	8080	192.168.2.22	104.168.155.143
Mar 18, 2023 15:38:24.680955887 CET	8080	49182	104.168.155.143	192.168.2.22
Mar 18, 2023 15:38:25.198741913 CET	49182	8080	192.168.2.22	104.168.155.143
Mar 18, 2023 15:38:25.361161947 CET	8080	49182	104.168.155.143	192.168.2.22
Mar 18, 2023 15:38:25.868345976 CET	49182	8080	192.168.2.22	104.168.155.143

HTTP Request Dependency Graph

- 164.90.222.65

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 1484, Parent PID: 1860

General

Target ID:	1
Start time:	15:36:18
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:	0x13f310000
File size:	139776 bytes
MD5 hash:	C676FC0263EDD17D4CE7D644B8F3FCD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 1624, Parent PID: 1484

General

Target ID:	3
Start time:	15:36:19
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:	0x4a7f0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 508, Parent PID: 1484

General

Target ID:	4
Start time:	15:36:19
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:	0xff750000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
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: 00000004.00000002.911404298.00000000001C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.911429954.00000000001F1000.00000020.00001000.00020000.00000000.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: rundll32.exe PID: **152**, Parent PID: **1624**

General

Target ID:	5
Start time:	15:36:19
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:	0xff1f0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
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: 00000005.00000002.911933178.00000000001E1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.911793490.00000000001B0000.00000040.00001000.00020000.00000000.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\CcdErbXwwqK\BMwTvRDPNYt.dll:Zone.Identifier	success or wait	1	1E289D	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: **500**, Parent PID: **1484**

General

Target ID:	6
Start time:	15:36:19
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:	0xff1f0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
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: 00000006.00000002.911845792.00000000001E1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.911734375.00000000001B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **1696**, Parent PID: **508**

General

Target ID:	7
Start time:	15:36:22
Start date:	18/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\TMlQeVZkdztztmVcv\UUQGnKwW.dll"
Imagebase:	0xff750000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **1748**, Parent PID: **152**

General

Target ID:	8
Start time:	15:36:22
Start date:	18/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\CcdErbXwwqK\BMwTvRDPNYt.dll"
Imagebase:	0xff750000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
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: 00000008.00000002.1424978614.0000000000150000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.1425013231.0000000000181000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: Yara detected Emotet, Source: 00000008.00000002.1425081092.000000000034A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **3068**, Parent PID: **500**

General

Target ID:	9
Start time:	15:36:22
Start date:	18/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\PmXMgnVtL\uQQuLasS.dll"
Imagebase:	0xff750000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
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

Disassembly

No disassembly