ID: 666431
Sample Name:
PYCkUgesWB.com_15e2f984de986ecb59e38a1c3a4a2300
Cookbook: default.jbs
Time: 19:09:11
Date: 16/07/2022
Version: 35.0.0 Citrine

Table of Contents

Windows Analysis Report

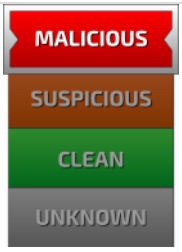
PYCkUgesWB.com_15e2f984de986ecb59e38a1c3a4a2300

Overview

General Information

Sample Name:	PYCkUgesWB.com_15e2f984de986ecb59e38a1c3a4a2300 (renamed file extension from com_15e2f984de986ecb59e38a1c3a4a2300 to dll)
Analysis ID:	666431
MD5:	15e2f984de986e..
SHA1:	795383a71c9030..
SHA256:	1e9a7692e74e98.
Tags:	dropped exe
Infos:	

Detection



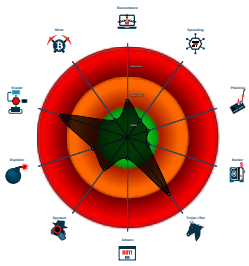
Emotet

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query local…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6924 cmdline: loaddll64.exe "C:\Users\user\Desktop\PYCkUgesWB.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6940 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\PYCkUgesWB.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6960 cmdline: rundll32.exe "C:\Users\user\Desktop\PYCkUgesWB.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 6948 cmdline: regsvr32.exe /s C:\Users\user\Desktop\PYCkUgesWB.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 5304 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XSYhmb\vuKI.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 6972 cmdline: rundll32.exe C:\Users\user\Desktop\PYCkUgesWB.dll,AjkRVrFNnyQmqXQdrComyaiwV MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7024 cmdline: rundll32.exe C:\Users\user\Desktop\PYCkUgesWB.dll,AkMhEGvNFpnSswjeCw MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7044 cmdline: rundll32.exe C:\Users\user\Desktop\PYCkUgesWB.dll,BMIWqtk MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 2820 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\AfzDfnhsGeYDyd\OsmuoIfhwEGDVL.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
- svchost.exe (PID: 2444 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6052 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5732 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4924 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4884 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6628 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5100 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "87.106.97.83:7080",
    "118.98.72.86:443",
    "93.104.209.107:8080",
    "157.230.99.206:8080",
    "104.244.79.94:443",
    "88.217.172.165:8080",
    "103.41.204.169:8080",
    "85.214.67.203:8080",
    "196.44.98.190:8080",
    "198.199.70.22:8080",
    "62.171.178.147:8080",
    "210.57.209.142:8080",
    "178.238.225.252:8080",
    "139.59.80.108:8080",
    "103.224.241.74:8080",
    "103.71.99.57:8080",
    "157.245.111.0:8080",
    "128.199.242.164:8080",
    "103.56.149.105:8080",
    "128.199.217.206:443",
    "85.25.120.45:8080",
    "190.145.8.4:443",
    "165.232.185.110:8080",
    "178.62.112.199:8080",
    "103.85.95.4:8080",
    "188.225.32.231:4143",
    "103.126.216.86:443",
    "37.44.244.177:8080",
    "64.227.55.231:8080",
    "190.107.19.179:443",
    "83.229.80.93:8080",
    "103.254.12.236:7080",
    "104.248.225.227:8080",
    "36.67.23.59:443",
    "43.129.209.178:443",
    "165.22.254.236:8080",
    "175.126.176.79:8080",
    "202.134.4.210:7080",
    "202.29.239.162:443",
    "46.101.98.60:8080",
    "54.37.228.122:443",
    "5.253.30.17:7080"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0yb8XUwABAI4=",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW6785UwAHAJM="
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.492629360.000001E200010000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.479464350.0000000001580000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000002.492455276.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.477702534.000001EC47BF0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000B.00000002.887240071.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 9 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.20500010000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.1b23e930000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.2.loaddll64.exe.1e200010000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
6.2.rundll32.exe.21dbea20000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
11.2.regsvr32.exe.2310000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 9 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 9 - Source IP: 192.168.2.7 - Destination IP: 174.138.33.49

Timestamp:	192.168.2.7174.138.33.494978670802404316 07/16/22-19:12:04.677504
SID:	2404316
Source Port:	49786
Destination Port:	7080
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

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

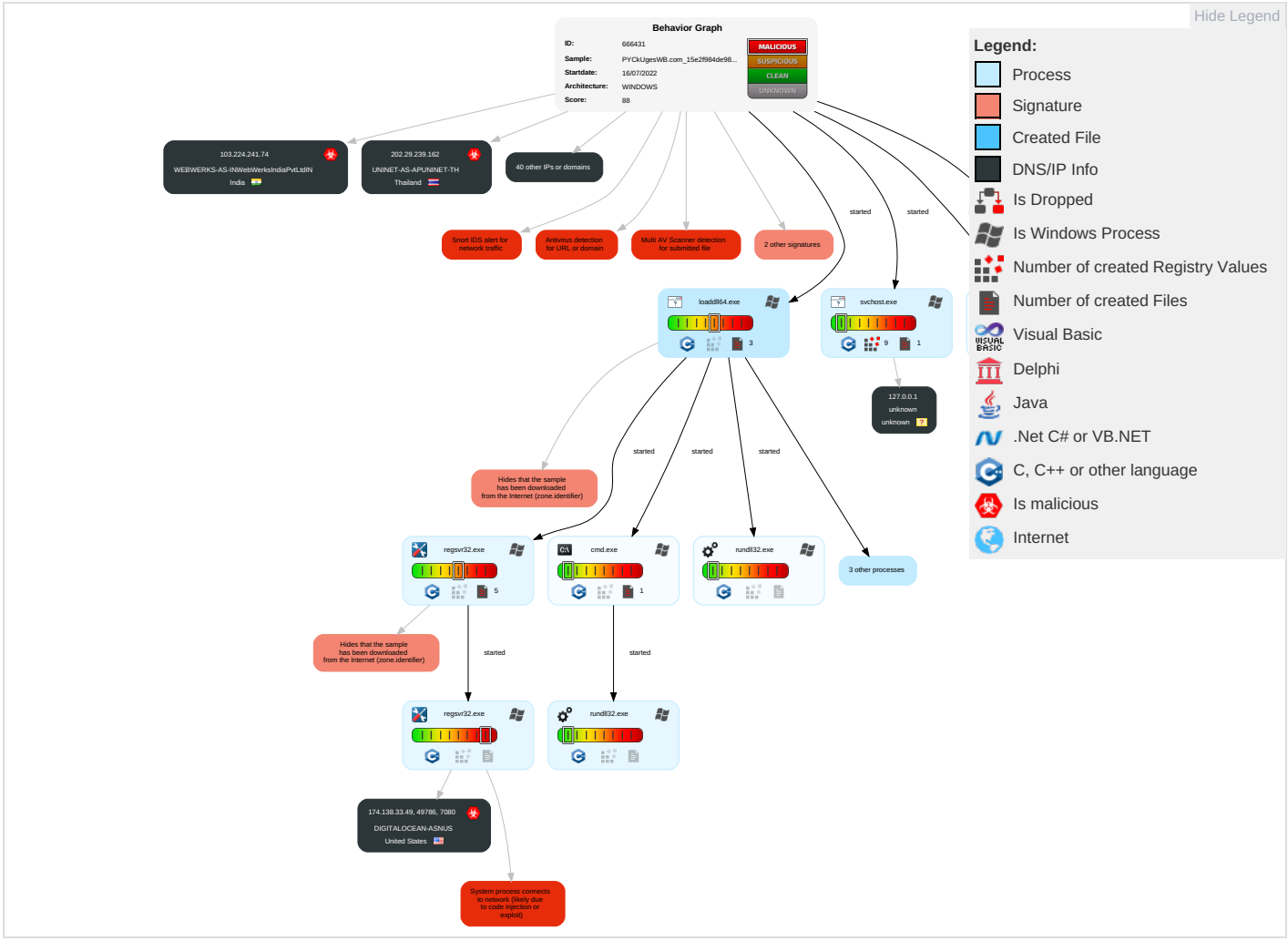
Stealing of Sensitive Information

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Native API	1 Windows Service	1 Windows Service	2 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 1 1 Process Injection	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)	1 DLL Side-Loading	1 1 1 Process Injection	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 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	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 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	3 5 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

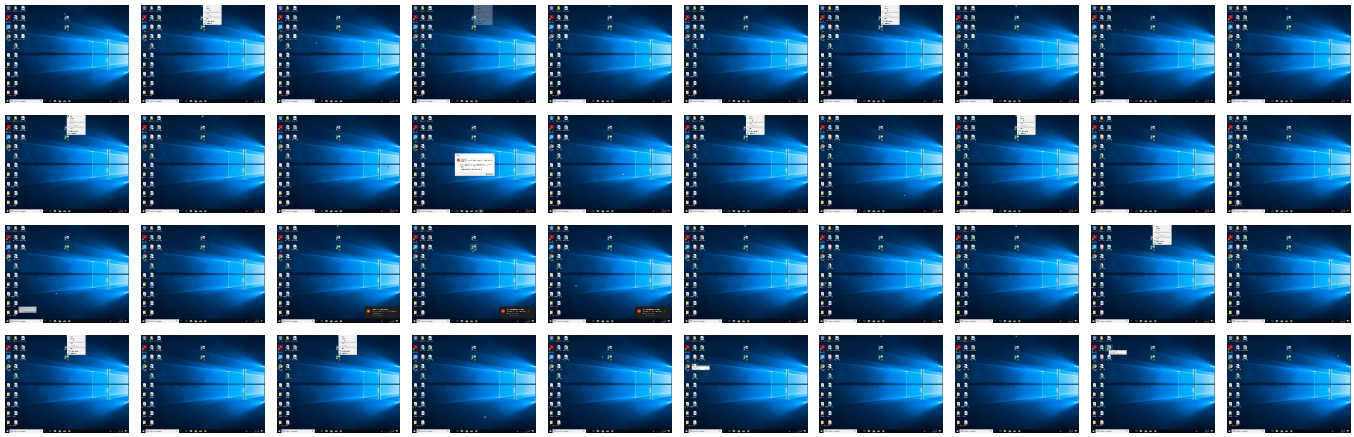
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PYCkUgesWB.dll	67%	Virustotal		Browse
PYCkUgesWB.dll	43%	Metadefender		Browse
PYCkUgesWB.dll	81%	ReversingLabs	Win64.Trojan.Emotet	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.1580000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.1b23e930000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
11.2.regsvr32.exe.2310000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.2.loaddll64.exe.1e200010000.1.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.rundll32.exe.1ec47bf0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.20500010000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
6.2.rundll32.exe.21dbea20000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://174.138.33.49:7080/a	100%	Avira URL Cloud	malware	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://174.138.33.49:7080/s64	100%	Avira URL Cloud	malware	
http://https://174.138.33.49:7080/	0%	URL Reputation	safe	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://174.138.33.49:7080/Num	100%	Avira URL Cloud	malware	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://174.138.33.49:7080/u	100%	Avira URL Cloud	malware	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://174.138.33.49/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

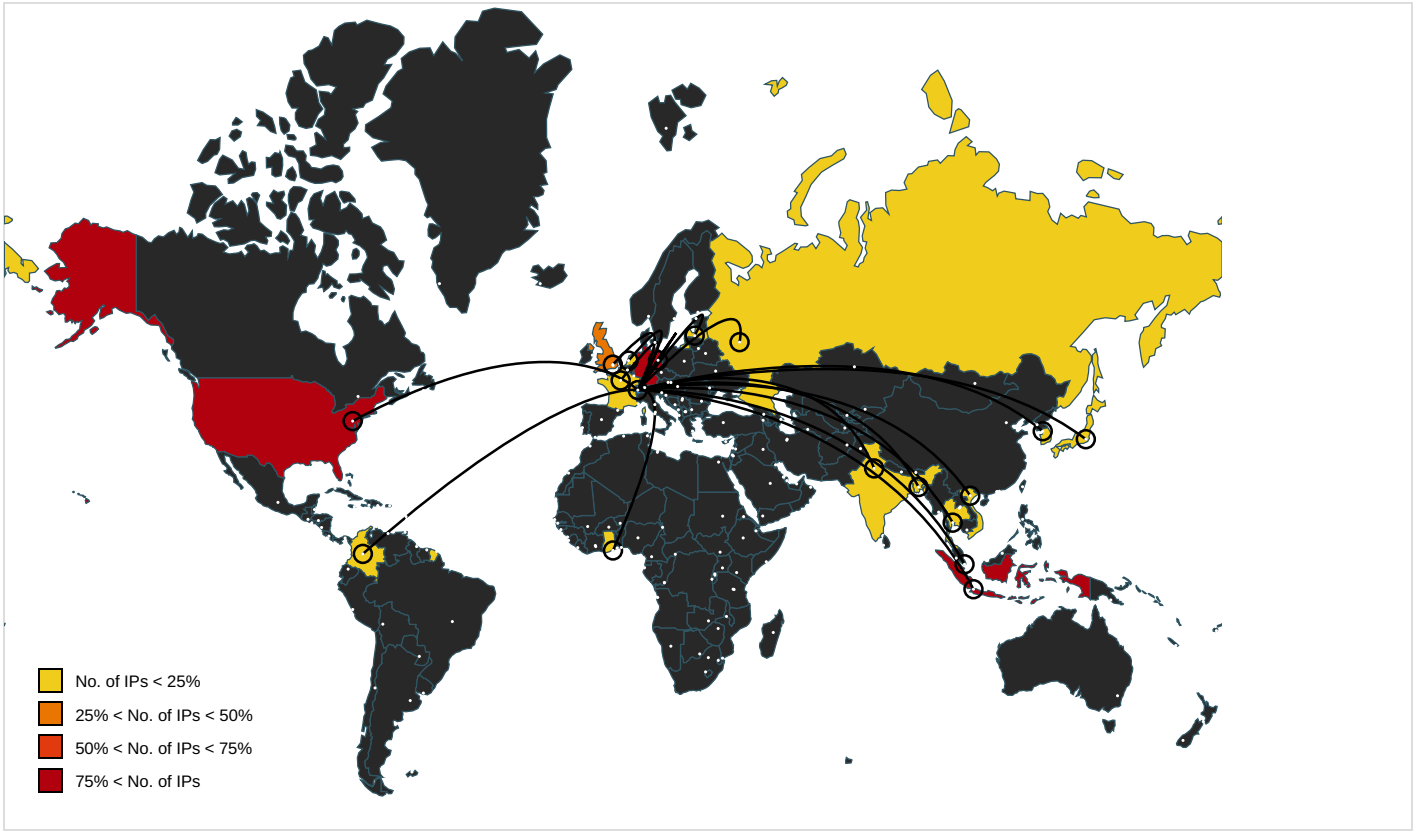
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addres	svchost.exe, 00000012.00000002.886351225.0000018974CAB000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000001B.00000003.776121457.00000170565B0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://174.138.33.49:7080/a	regsvr32.exe, 0000000B.00000002.885863277.00000000008CD000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000B.00000003.803078720.00000000008CD000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000001B.00000003.776121457.00000170565B0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://174.138.33.49:7080/s64	regsvr32.exe, 0000000B.00000002.885863277.00000000008CD000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000B.00000003.803078720.00000000008CD000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://174.138.33.49:7080/	regsvr32.exe, 0000000B.00000002.885863277.00000000008CD000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000B.00000003.803078720.00000000008CD000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.hotspotshield.com/terms/	svchost.exe, 0000001B.00000003.772609747.000001705658500.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.772596708.000001705658200.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771116472.00000170565B0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771585831.000001705657C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771543494.000001705657B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771348384.000001705659E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771440016.000001705657B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771293341.0000017056A1A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771489113.000001705657B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771257487.0000017056A1A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771315826.0000017056A02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771513285.000001705657C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771024338.000001705659E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771224165.00000170565BA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771633828.0000017056580000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 0000001B.00000003.772609747.000001705658500.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.772596708.000001705658200.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771116472.00000170565B0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771585831.000001705657C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771543494.000001705657B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771348384.000001705659E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771440016.000001705657B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771293341.0000017056A1A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771489113.000001705657B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771257487.0000017056A1A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771315826.0000017056A02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771513285.000001705657C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771024338.000001705659E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771224165.00000170565BA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771633828.0000017056580000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 0000001B.00000003.776121457.00000170565B0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ver)	svchost.exe, 0000001B.00000002.804530802.0000017055AEA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://174.138.33.49:7080/Num	regsvr32.exe, 0000000B.00000002.88586327 7.00000000008CD000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 00B.00000003.803078720.00000000008CD000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 0000001B.00000003.781191744 .000001705659E000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/0	svchost.exe, 00000012.00000002.886351225 .0000018974CAB000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://174.138.33.49:7080/u	regsvr32.exe, 0000000B.00000002.88586327 7.00000000008CD000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 00B.00000003.803078720.00000000008CD000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://help.disneyplus.com.	svchost.exe, 0000001B.00000003.776121457 .00000170565B0000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.hotspotshield.com/	svchost.exe, 0000001B.00000003.772609747 .0000017056585000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.772596708.0000017056582000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771116472 .00000170565B0000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.771585831.000001705657C000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771543494 .000001705657B000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.771348384.000001705659E000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771440016 .000001705657B000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.771293341.0000017056A1A000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771489113 .000001705657B000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.771257487.0000017056A1A000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771315826 .0000017056A02000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.771513285.000001705657C000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771024338 .000001705659E000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.771224165.00000170565BA000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.771633828 .0000017056580000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://174.138.33.49/	regsvr32.exe, 0000000B.00000003.80307872 0.00000000008CD000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.230.99.206	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
157.245.111.0	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
196.44.98.190	unknown	Ghana		327814	EcobandGH	true
202.29.239.162	unknown	Thailand		4621	UNINET-AS-APUNINET-TH	true
174.138.33.49	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
43.129.209.178	unknown	Japan		4249	LILLY-ASUS	true
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
36.67.23.59	unknown	Indonesia		17974	TELKOMNET-AS2-APPTTelekomunikasiIndonesiaID	true
5.253.30.17	unknown	Latvia		18978	ENZUINC-US	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
103.56.149.105	unknown	Indonesia		55688	BEON-AS-IDPTBeonIntermediaID	true
85.25.120.45	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
83.229.80.93	unknown	United Kingdom		8513	SKYVISIONGB	true
198.199.70.22	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
93.104.209.107	unknown	Germany		8767	MNET-ASGermanyDE	true
188.225.32.231	unknown	Russian Federation		9123	TIMEWEB-ASRU	true
175.126.176.79	unknown	Korea Republic of		9523	MOKWON-AS-KRMokwonUniversityKR	true
128.199.242.164	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
165.232.185.110	unknown	United States		22255	ALLEGHENYHEALTHNETWORKUS	true
103.126.216.86	unknown	Bangladesh		138482	SKYVIEW-AS-APSKYVIEWONLINELTDBD	true
104.248.225.227	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
178.238.225.252	unknown	Germany		51167	CONTABODE	true
128.199.217.206	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
190.145.8.4	unknown	Colombia		14080	TelmexColombiaSACO	true
46.101.98.60	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
103.224.241.74	unknown	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.71.99.57	unknown	India		135682	AWDHPL-AS-INAdvikaWebDevelopmentsHostingPvtLtdIN	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
190.107.19.179	unknown	Colombia		27951	MediaCommercePartnersSACO	true
87.106.97.83	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
103.254.12.236	unknown	Viet Nam		56151	DIGISTAR-VNDigiStarCompanyLimitedVN	true
103.85.95.4	unknown	Indonesia		136077	IDNIC-UNSRAT-AS-IDUniversitasIslamNegeriMataramID	true
54.37.228.122	unknown	France		16276	OVHFR	true
202.134.4.210	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
88.217.172.165	unknown	Germany		8767	MNET-ASGermanyDE	true
165.22.254.236	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
118.98.72.86	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
139.59.80.108	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
104.244.79.94	unknown	United States		53667	PONYNETUS	true
178.62.112.199	unknown	European Union		14061	DIGITALOCEAN-ASNUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
64.227.55.231	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	666431
Start date and time: 16/07/202219:09:11	2022-07-16 19:09:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PYCkUgesWB.com_15e2f984de986ecb59e38a1c3a4a2300 (renamed file extension from com_15e2f984de986ecb59e38a1c3a4a2300 to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.troj.evad.winDLL@24/4@0/44

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 45.4% (good quality ratio 40.8%) • Quality average: 78.1% • Quality standard deviation: 33.1%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 67.26.75.254, 8.248.145.254, 8.253.207.120, 8.248.135.254, 8.253.207.121, 8.248.133.254, 67.26.81.254, 67.26.73.254, 8.248.149.254, 67.26.139.254, 23.211.4.86, 80.67.82.235, 80.67.82.211, 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.useroor.bigcatalog.commerce.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu-bg-shim.trafficmanager.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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
19:12:06	API Interceptor	10x Sleep call for process: svchost.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:\ProgramData\Microsoft\Network\Downloader\qmgr.db

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x4dfe4fb8, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2505933374184895
Encrypted:	false
SSDEEP:	384:k+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:bSB2nSB2RSjlK/+mLesOj1J2
MD5:	EB961E7113E3D08479E5A7A470B28163
SHA1:	97161FC542A63DB96B7287C22D11D1E19C706A19
SHA-256:	2E4145142F92749B4EC51BF620D2BE8883371813557B449FE39A9BFE1DD20024
SHA-512:	F2CE12E33979D5093DFAA3ABBD0318D5BD2E7A88DE76CEEB5563375B8302A215DE86C34E923BDC77F2A33A25D6409C4F09EB6788F8AA9C1E9560DBA0EA34B3FF
Malicious:	false
Preview:	M.O.... .....e.f.3...w.....&.....w.....zo.h.(.....3...w.....B.....@..... ....3...w..... .....1H.v.....zo.....gC.....zo..... .....

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

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B
Malicious:	false
Preview:	MSCF.....,.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C.....`h!0.I.(C..1Q*L.p..".s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<.....3....s.T...._'...%{v...s.....KgV.0..X=.A.9w9.Ea.x.....\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....ul.....}.....d....M.....6q.Q~.0.\.'U^)`.u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.l.E.6..a8.6..nq..x.r4..1t.....,.u.O..O.L...Uf...X.u.F .(.(....."..q...n{%U.-u....l6!....Z....~o0.}Q'.s.i....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

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

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.1358915940078615
Encrypted:	false
SSDEEP:	6:kK79ku+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:zGuNkPlE99SNxAhUeE1
MD5:	CB006CC6314BF3DEB2C82425738A567F
SHA1:	91210AC0A73CDB5A354D2F1346B707377751F76E
SHA-256:	5255C7343D802A3FE510DCC6B5E9DCA3DC3FB2BB8F891695F57354FA1812E6EA
SHA-512:	EC31D35FB61206C20020B20AFAD8EAFFE8AFA30B8751F8585F9EF66C4276E6DF3A9D078C060E2B2C670C18944F8002193F63618B1AA1D07E58283FE1ED70EC82
Malicious:	false
Preview:	p..... .....(..... ....L.....$.....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...".0.9.f.4.c.9.6.9.8.b.d.8.1.:.0."...

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false

SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	7.4523768271907125
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:	PYCkUgesWB.dll
File size:	284672
MD5:	15e2f984de986ecb59e38a1c3a4a2300
SHA1:	795383a71c9030a2c52624795a1e539bfedbf84c
SHA256:	1e9a7692e74e98ac5d21a4d3bfb3696d69d8306e4e42d53bcb4604b3dff420bb
SHA512:	ae2e7f175844ac5d106e36474f3c2f86d27948b2c967ab01a10e8b8dc836a2349bc1dfc26119cbc4f41a96526dca5a79f315d7d7971683fb7db4fba41edef172
SSDEEP:	6144:H8aVTnVgcpYT4Xf+WXv8cMkjdF4r6UrjCxGNh3XlwfjR96:H8wTV7UwHXvJMmdCrvrjZA3
TLSH:	A954D001A99DD0A5C57E5939A4B78F03D3A1BC10977A93EF9B3109349A333E56D3D3A0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N...N...N...i...F...i...l...i.....8R..C...N...9...i...M...i...O...i...O...i...O...RichN.....PE..d...c..b....."

File Icon

Icon Hash:	66f2d2d2d2d2c4ca

Static PE Info

General

Entrypoint:	0x100018a0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	
Time Stamp:	0x62C6D463 [Thu Jul 7 12:41:07 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	63eff8a065c6d44859c3b54eb482a5d6

Entrypoint Preview

Instruction
dec eax
sub esp, 28h
cmp edx, 01h
dec eax
mov dword ptr [esp+38h], ebx
dec eax
mov dword ptr [esp+40h], esi
dec eax
mov dword ptr [esp+48h], edi
mov ebx, edx
dec eax
mov esi, ecx
dec ecx
mov edi, eax
jne 00007FDA70D2C397h
call 00007FDA70D2ED70h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov edi, dword ptr [esp+48h]
dec eax
mov esi, dword ptr [esp+40h]
dec eax
mov ebx, dword ptr [esp+38h]
dec eax
add esp, 28h
jmp 00007FDA70D2C210h
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 00000088h
dec eax
lea ecx, dword ptr [0001593Dh]
call dword ptr [0000F86Fh]
dec eax
mov eax, dword ptr [00015A28h]
dec eax
mov dword ptr [esp+58h], eax
inc ebp
xor eax, eax
dec eax
lea edx, dword ptr [esp+60h]
dec eax
mov ecx, dword ptr [esp+58h]
call 00007FDA70D32B90h

Instruction
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007FDA70D2C3D3h
dec eax
mov dword ptr [esp+38h], 00000000h
dec eax
lea eax, dword ptr [esp+48h]
dec eax
mov dword ptr [esp+30h], eax
dec eax
lea eax, dword ptr [esp+40h]
dec eax
mov dword ptr [esp+28h], eax
dec eax
lea eax, dword ptr [000158E8h]
dec eax
mov dword ptr [esp+20h], eax
dec esp
mov ecx, dword ptr [esp+50h]
dec esp
mov eax, dword ptr [esp+58h]

Rich Headers

Programming Language:	• [ASM] VS2005 build 50727 • [C++] VS2005 build 50727 • [C] VS2005 build 50727 • [EXP] VS2005 build 50727 • [RES] VS2005 build 50727 • [LNK] VS2005 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x14a10	0x13a4	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x13ec4	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1a000	0x2e480	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x19000	0x99c	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x49000	0x1e4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x11000	0x368	.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	0xfd4a	0xfe00	False	0.4856206938976378	data	5.920035349065038	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x11000	0x4db4	0x4e00	False	0.47571113782051283	data	5.5301844227687305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x16000	0x2878	0x1200	False	0.2055121527777778	data	2.203174750959508	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x19000	0x99c	0xa00	False	0.488671875	data	4.691904567122826	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x1a000	0x2e480	0x2e600	False	0.8459452914420486	data	7.832588443776017	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x49000	0x5b0	0x600	False	0.23372395833333334	data	2.3778281936909145	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1a340	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x1a468	0x2e8	data	English	United States
RT_MENU	0x1a750	0x4a	data	English	United States
RT_DIALOG	0x1a79c	0xac	data	English	United States
RT_DIALOG	0x1a848	0xfe	data	English	United States
RT_DIALOG	0x1a948	0x12a	data	English	United States
RT_STRING	0x1aa74	0x10c	data	English	United States
RT_STRING	0x1ab80	0x12a	data	English	United States
RT_STRING	0x1acac	0x38	data	English	United States
RT_ACCELERATOR	0x1ace4	0x10	data	English	United States
RT_GROUP_ICON	0x1acf4	0x22	data	English	United States
RT_HTML	0x1ad18	0x2d600	data	English	United States
RT_MANIFEST	0x48318	0x168	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	VirtualAlloc, FormatMessageW, LocalFree, GetStringTypeW, GetStringTypeA, LCMapStringW, GetLastError, GetLocaleInfoA, MultiByteToWideChar, HeapReAlloc, HeapSize, GetOEMCP, GetACP, GetCPInfo, InitializeCriticalSection, LoadLibraryA, EnterCriticalSection, LeaveCriticalSection, GetSystemTimeAsFileTime, LCMapStringA, GetFullPathNameW, GetCurrentProcessId, GetTickCount, QueryPerformanceCounter, RtlUnwindEx, GetEnvironmentStringsW, WideCharToMultiByte, FreeEnvironmentStringsW, GetEnvironmentStrings, FreeEnvironmentStringsA, DeleteCriticalSection, HeapAlloc, HeapFree, GetCurrentThreadId, FlsSetValue, GetCommandLineA, GetVersionExA, GetProcessHeap, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RtlVirtualUnwind, RtlLookupFunctionEntry, RtlCaptureContext, GetProcAddress, GetModuleHandleA, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, HeapSetInformation, HeapCreate, HeapDestroy, RaiseException, RtlPcToFileHeader, FlsGetValue, TlsFree, FlsFree, SetLastError, TlsSetValue, FlsAlloc, Sleep, SetHandleCount, GetFileType, GetStartupInfoA
USER32.dll	MessageBoxW, LoadStringW, LoadAcceleratorsW, GetMessageW, IsDialogMessageW, TranslateAcceleratorW, PostMessageW, EndPaint, BeginPaint, DefWindowProcW, PostQuitMessage, GetDlgItem, GetWindowRect, SetWindowPos, CreateDialogParamW, TranslateMessage, SendMessageW, SetWindowTextW, GetWindowTextW, DestroyWindow, UpdateWindow, ShowWindow, CreateWindowExW, RegisterClassExW, LoadCursorW, LoadIconW, MessageBoxA, DispatchMessageW
GDI32.dll	CreateSolidBrush
comdlg32.dll	GetOpenFileNameW
ole32.dll	CoInitializeEx, CoUninitialize, CoCreateInstance, CoInitialize
OLEAUT32.dll	SysFreeString, SysAllocString

Exports

Name	Ordinal	Address
AjkRVrFNnyQmqXQdrComyaiwV	1	0x100085a0
AkMhEGvNFpnSswjeCw	2	0x10008690
BMIWqtk	3	0x10008520
BpsBUyIiAmXYU	4	0x10008ab0
BxBybURSqJfOwVmXj	5	0x100083e0
CCSLGUsdVtcCbfF	6	0x10008d00
CWBdqFubMR	7	0x10008500
CbEceKaoQvfuhhIK	8	0x100089c0
CcBDyidVYuvtjWfG	9	0x10008460

Name	Ordinal	Address
CeOVtVdkUnRPoUvswsvkEf	10	0x10008710
CvxIGiXAzAG	11	0x10008c30
DPsWXvFrrwOLZwoq	12	0x10008b70
DllRegisterServer	13	0x10009510
ENtihcf	14	0x10008c80
EVYoaysfyVmedMKzqOkd	15	0x10008dd0
FSgLIbzCJsGhKrdTRUhBnjq	16	0x10008c70
FXswjNvwqEmJHSzKXfB	17	0x10008450
FmRrLoGPniSXxeHYAaRXrsSIt	18	0x100087d0
FzYYWlRKDQMfKaJAUq	19	0x10008610
GEQqgSeWrJkaNSdjOw	20	0x100083d0
GLvPFjzv	21	0x10008cc0
GTfYoyhXUmiOrfM	22	0x10008630
GVTerofsGHUASHLhWfIFX	23	0x100088b0
GlLOHKioWJZCQPS	24	0x10008c20
GpqOdmj	25	0x10008970
GtaEQGQNcgERZqWo	26	0x10008930
GzdHPyIXWoMGb	27	0x10008680
HKgdkPfboZzjQODFfSu	28	0x100084a0
HmXZBMEhrWvTg	29	0x10008f00
HvFWvy	30	0x100084e0
ICrKqnEJHHrxYaH	31	0x10008bd0
IDENrF	32	0x10008af0
ISuniIBoqjzfv	33	0x10008800
IcEiBSQQHwaxZGs	34	0x10008a00
JCFScdjDVMLKVa	35	0x100085f0
JGwGKVHFHwfxsyCIp	36	0x10008eb0
JnkFkZthy	37	0x10008e30
LSRvMYckceDUkCMxwUAq	38	0x10008b10
LhZoEaJRggyJr	39	0x10008490
MknuTlXosJJdvczIkg	40	0x10008410
MrhDZxAutnSSobTVt	41	0x10008c10
NRfTvw	42	0x10008a50
NZDMYgNWoHhCVPBFWyuTBSesQ	43	0x100083b0
NmBmwe	44	0x10008440
NzYPpUvQ	45	0x10008df0
OThzaIZTEfYKTCCRQlcnW	46	0x100088a0
OWMilsbkgGVyJL	47	0x10008540
OguxguFiYSHz	48	0x100089b0
PHzWjRI	49	0x100083f0
PNJeVrAcZDAW	50	0x10008ad0
PSDYwlgmLiVzYESIaUYrbKg	51	0x10008b00
PiJSThSmMmzNNC	52	0x10008b40
PnelJqdSVVerltCm	53	0x10008cd0
PpsLezsCiHiCVkHmZP	54	0x10008e60
PuoUVwFKYxjCqT	55	0x10008b20
PwNlKX	56	0x10008a70
QRkaVvgiLqTCjGKy	57	0x10008c90
RJAcdfSthTv	58	0x10008550
RYkwsDq	59	0x10008890
RZtKxjO	60	0x10008b50
RcnQoaySRBXJxsiZQlHxe	61	0x10008c60
RdnXeofUSzEDgzxXeW	62	0x100086b0
RfsPQSmuvBYXfIScfOT	63	0x100086c0
RkfakVk	64	0x10008720
RmhqixPgftgQ	65	0x10008ef0
SInCoGYrouPZGmYYJGKIR	66	0x10008420
SRXSueHCT	67	0x10008430
SVlQsYSAXEyhEvVkdWdX	68	0x10008860

Name	Ordinal	Address
SnLgFTA	69	0x10008de0
SxfQZPkEOIcG	70	0x10008dc0
TJZCJgp	71	0x10008590
TSNqZL	72	0x10008820
TfpEQJjWUDp	73	0x10008ba0
TvUVDsEcInyvKdGRA	74	0x10008d70
TvtXyQtNShHDYCMvH	75	0x10008a10
UGXSNpc	76	0x10008e10
ULOMXGiV	77	0x10008940
UVzHIeChKCEwTMG	78	0x100084b0
UagSsmENTltTUKpktiEuRJfE	79	0x10008b90
UbjFSQJG	80	0x10008780
UjDfVglhgynLAuMpwrtpXkH	81	0x10008a80
UrxprELRNWbXXBuOJlJ	82	0x10008bf0
VXDuMBzruSCyfbAMzIrvV	83	0x10008a90
VcrtEzpxSRmZr	84	0x10008760
VkRjra	85	0x10008750
WMxfpgNLwoiQTZjkM	86	0x10008920
WjtCBeYwDkRZvKLfJD	87	0x10008a20
XoMiJXhdBRBldnkLkgMM	88	0x10008a40
XsBeDFcmOsaqRihqMytJ	89	0x100088c0
YGPQhuvjFbQXSoJfVilOnVw	90	0x100084d0
YvzKAJK	91	0x10008830
ZAppiYnp	92	0x10008c50
ZXZEfUeKC	93	0x10008910
ZoyjBLvuBnIxXaWxFC	94	0x10008660
aZwlVZLRtClfDmaYbAXR	95	0x10008e40
bdnAzUNoMZJXxzHG	96	0x100086f0
btmsIKQVm	97	0x100084f0
cFminOM	98	0x100088e0
cKjOEfqQYYQ	99	0x10008730
czIvuAZ	100	0x100085d0
dMEJcsHSUiODu	101	0x10008810
dPYgmMRi	102	0x10008880
dStUmppUwHfwVxtCgCewXt	103	0x10008ca0
deMXieymThIxfyWzHCMb	104	0x10008e80
dgCMMkwNpUNZ	105	0x10008cb0
eDtAbxMTlNFwGjIRymBKxBFTe	106	0x10008da0
ePfrWQkHuKqOV	107	0x10008480
eQnPJdIEwUrOjHyYKajVY	108	0x10008770
eWqtOcNgKbDEwKynrCTAaqRd	109	0x10008ac0
eiRJXgFAjkyObQxtC	110	0x10008740
fLsjxmtTmthGKPw	111	0x10008700
fqsAeZLb	112	0x10008e00
frkkGhhTKCPBzCLoveBHn	113	0x10008640
fxmvSQNzSiXj	114	0x100087a0
gATjvjWkzNfdmAJbeFMKFtUmoI	115	0x10008ce0
gCFmNdxvaAq	116	0x10008e50
gfeRIwKkCZUnQQ	117	0x10008f10
gjZENXkR	118	0x10008400
gzzlrzxMlshrI	119	0x10008d30
hClTxV	120	0x100087b0
hDdSABujeGhBdM	121	0x10008c00
hJbRrovBnfzadHBLOAaX	122	0x100085b0
hLNWWET	123	0x10008d10
ilJmtODVuCFQPMFae	124	0x10008600
iltzzFKWzIZojfOFqJG	125	0x10008b80
ibqesePIQXoUwnfgkLvfcuMFHK	126	0x100086a0
ieuLWaTjVeuBYegSaGXuly	127	0x100088f0

Name	Ordinal	Address
igFffrhNCQcHQStroQFS	128	0x10008f20
irtTnxRuuXAWDuDRGCivHz	129	0x100086d0
jVNpFjHcSQ	130	0x100084c0
jotleypmamgIHEUfZPLSmMtq	131	0x10008db0
jrkFXlWfdhOn	132	0x100085c0
kOcvjMhVkKI	133	0x10008580
kPsHiOxOlxeVBpHYooACxIXHB	134	0x10008560
kUHyuFSDHjRQgcFnZIHgvahta	135	0x100089e0
kXMermOELWqc	136	0x10008790
kkWRnVCjitIbHTy	137	0x100087c0
kpoFTDgQJFpD	138	0x10008be0
kvCgXPvHuWWWdAHGy	139	0x10008aa0
lFcjChjFWgKWuOuaAxn	140	0x10008b30
lKFTvqNg	141	0x100089a0
lcbnVGCdYXcKZTYevsVX	142	0x10008900
lefIOOsVMhliLLj	143	0x10008390
mKrNVAlauoRSIht	144	0x10008c40
nRVfeUAoalGiEviupjuyTviKt	145	0x10008ea0
nWkMZMN	146	0x100087e0
naKLRCkO	147	0x10008510
njUWLbQgRBGSd	148	0x10008d20
nlBfCJTJQhnnPxbkQkUAwWpmaA	149	0x10008b60
nmBYnmjGCq	150	0x10008cf0
oIAdOUfQaetEfqMDSL	151	0x10008ec0
osSAAvHx	152	0x10008620
ovwgmHjsMpOQyjNpuqeLd	153	0x100085e0
ozpFyAlRWIHNYPuJbOLpoZosmO	154	0x10008650
pAbWNQjHuawouRBUprBVrXw	155	0x10008670
pCYRinZyYkFOxayPFyJDEDxKzO	156	0x10008870
pQvYHQSqPMdqFOFub	157	0x10008ae0
pbzbgZeZipMwitVYJJbYTdyYQ	158	0x100089f0
pnbxRJnSdfpDADRIEWZXepR	159	0x100087f0
qAirVWefWGdomxGs	160	0x100086e0
qbgUwwXPUNM	161	0x10008850
rJVMJaiBojiOWxURyzmLWnxH	162	0x10008bb0
rOlGGoosrOYjYnwqSX	163	0x10008d60
rSHUNkevMkknNwSlqR	164	0x10008950
rmrMOmqIIM	165	0x10008e70
sBcaPzIWckINwkFTBxmdkiKID	166	0x10008960
sJXDLm	167	0x10008d50
sNQjkxnpfL	168	0x10008530
sPKnvGEKVGRHsXgbRRJFS	169	0x10008ee0
snoSMpnSAlGCDUoadZDE	170	0x10008a60
tGDiqYCDbgMaBXHmxqrJv	171	0x10008e90
tGdwKquShaUWskzgERPqeG	172	0x100083c0
tXncljehbaR	173	0x10008bc0
taNCAYWnFedga	174	0x10008d80
uFBMgXMRHfYmHKtd	175	0x10008e20
uQadijPTgYiRGTkxDpqTOeI	176	0x10008380
vlEZdJoJilVuJxGaLFCzX	177	0x10008990
vlPATCQWfWfv	178	0x10008570
vnMwerzIvV	179	0x10008d90
wDtWqzCTVUWdqo	180	0x10008ed0
weKcSTEtgvLwNKGEWr	181	0x10008980
wyslQDXAh	182	0x10008840
xRklmHvgNdkXc	183	0x10008470
xbTTVacjLMTUBskAADEzpolBV	184	0x100083a0
xbcfQIhiMJswKveISUtGpEWTr	185	0x10008d40
ytgHNsgBKfkMoZjHI	186	0x100089d0

Name	Ordinal	Address
zLypEkbxfdampkTf	187	0x10008a30
ziTLFIzOnbzURBefGdA	188	0x100088d0

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
192.168.2.7174.138.33.49 4978670802404316 07/16/22-19:12:04.677504	TCP	2404316	ET CNC Feodo Tracker Reported CnC Server TCP group 9	49786	7080	192.168.2.7	174.138.33.49

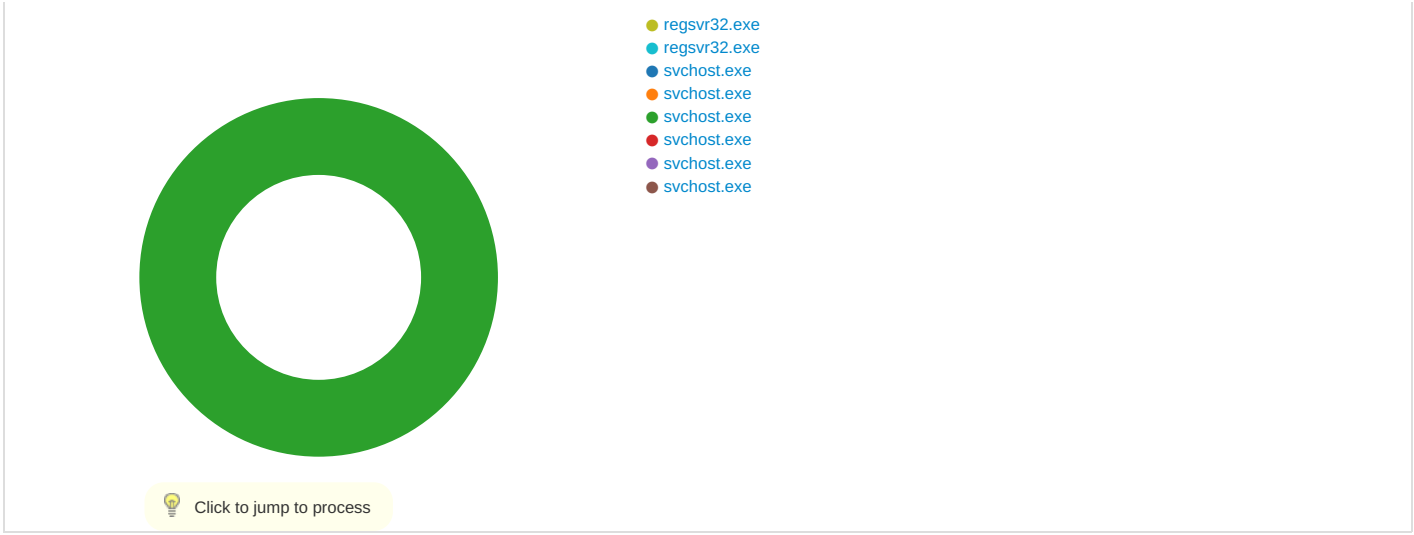
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 16, 2022 19:12:04.677504063 CEST	49786	7080	192.168.2.7	174.138.33.49
Jul 16, 2022 19:12:04.782668114 CEST	7080	49786	174.138.33.49	192.168.2.7
Jul 16, 2022 19:12:04.782854080 CEST	49786	7080	192.168.2.7	174.138.33.49
Jul 16, 2022 19:12:04.846545935 CEST	49786	7080	192.168.2.7	174.138.33.49
Jul 16, 2022 19:12:04.949121952 CEST	7080	49786	174.138.33.49	192.168.2.7
Jul 16, 2022 19:12:04.969825983 CEST	7080	49786	174.138.33.49	192.168.2.7
Jul 16, 2022 19:12:04.969861984 CEST	7080	49786	174.138.33.49	192.168.2.7
Jul 16, 2022 19:12:04.974636078 CEST	49786	7080	192.168.2.7	174.138.33.49
Jul 16, 2022 19:12:09.163804054 CEST	49786	7080	192.168.2.7	174.138.33.49
Jul 16, 2022 19:12:09.266911983 CEST	7080	49786	174.138.33.49	192.168.2.7
Jul 16, 2022 19:12:09.267055035 CEST	49786	7080	192.168.2.7	174.138.33.49
Jul 16, 2022 19:12:09.271817923 CEST	49786	7080	192.168.2.7	174.138.33.49
Jul 16, 2022 19:12:09.414453983 CEST	7080	49786	174.138.33.49	192.168.2.7
Jul 16, 2022 19:12:09.797220945 CEST	7080	49786	174.138.33.49	192.168.2.7
Jul 16, 2022 19:12:09.797314882 CEST	49786	7080	192.168.2.7	174.138.33.49
Jul 16, 2022 19:12:12.801305056 CEST	7080	49786	174.138.33.49	192.168.2.7
Jul 16, 2022 19:12:12.801331997 CEST	7080	49786	174.138.33.49	192.168.2.7
Jul 16, 2022 19:12:12.801448107 CEST	49786	7080	192.168.2.7	174.138.33.49
Jul 16, 2022 19:13:54.821356058 CEST	49786	7080	192.168.2.7	174.138.33.49
Jul 16, 2022 19:13:54.821396112 CEST	49786	7080	192.168.2.7	174.138.33.49

Statistics

Behavior

- loaddll64.exe
- cmd.exe
- regsvr32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- svchost.exe



System Behavior

Analysis Process: loaddll64.exe PID: 6924, Parent PID: 2852

General

Target ID:	0
Start time:	19:10:27
Start date:	16/07/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\PYCkUgesWB.dll"
Imagebase:	0x7ff770350000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.492629360.000001E200010000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.492455276.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6940, Parent PID: 6924

General

Target ID:	1
Start time:	19:10:28
Start date:	16/07/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\PYCkUgesWB.dll",#1
Imagebase:	0x7ff6a6590000
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: **6948**, Parent PID: **6924**

General

Target ID:	2
Start time:	19:10:28
Start date:	16/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\PYCkUgesWB.dll
Imagebase:	0x7ff6047c0000
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: 00000002.00000002.479464350.0000000001580000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.479882020.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\XSYhmb\vuKI.dll:Zone.Identifier	success or wait	1	18001ED93	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: **6960**, Parent PID: **6940**

General

Target ID:	3
Start time:	19:10:28
Start date:	16/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\PYCkUgesWB.dll",#1
Imagebase:	0x7ff7efde0000
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: 00000003.00000002.466579273.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.466935474.0000020500010000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **6972**, Parent PID: **6924**

General

Target ID:	4
Start time:	19:10:29
Start date:	16/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\PYCkUgesWB.dll,AjkRVrFNnyQmqXQdrComyaiwV
Imagebase:	0x7ff7efde0000
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: 00000004.00000002.466000340.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.466138189.000001B23E930000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **7024**, Parent PID: **6924**

General

Target ID:	5
Start time:	19:10:33
Start date:	16/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\PYCkUgesWB.dll,AkMhEGvNFpnSswjeCw
Imagebase:	0x7ff7efde0000
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: 00000005.00000002.477702534.000001EC47BF0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.477040143.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **7044**, Parent PID: **6924**

General

Target ID:	6
Start time:	19:10:38
Start date:	16/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\PYCkUgesWB.dll,BMIWqtk
Imagebase:	0x7ff7efde0000

File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.485258322.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.487464916.0000021DBEA20000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: **2444**, Parent PID: **604**

General

Target ID:	10
Start time:	19:11:09
Start date:	16/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: **5304**, Parent PID: **6948**

General

Target ID:	11
Start time:	19:11:21
Start date:	16/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XSYhmb\vuKI.dll"
Imagebase:	0x7ff6047c0000
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: 0000000B.00000002.887240071.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.886485279.0000000002310000.00000040.00001000.00020000.00000000.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: **2820**, Parent PID: **6924**

General

Target ID:	12
Start time:	19:11:28
Start date:	16/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\AfzDfnhsGeYDyd\OsmuofIfhwEGDVL.dll"
Imagebase:	0x7ff6047c0000
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: svchost.exe PID: 6052, Parent PID: 604

General

Target ID:	17
Start time:	19:12:01
Start date:	16/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5732, Parent PID: 604

General

Target ID:	18
Start time:	19:12:05
Start date:	16/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **4924**, Parent PID: **604**

General

Target ID:	20
Start time:	19:12:31
Start date:	16/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **4884**, Parent PID: **604**

General

Target ID:	21
Start time:	19:12:41
Start date:	16/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x210000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6628**, Parent PID: **604**

General

Target ID:	24
Start time:	19:13:08
Start date:	16/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5100**, Parent PID: **604**

General

Target ID:	27
Start time:	19:13:25
Start date:	16/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly