ID: 562433
Sample Name: GULPPYUMBy
Cookbook: default.jbs
Time: 21:36:06
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

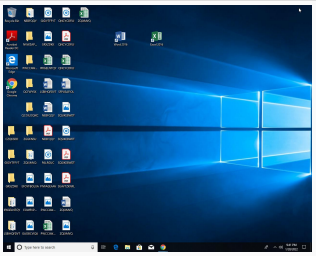
Windows Analysis Report

GULPPYUMBy

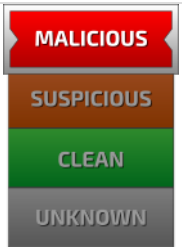
Overview

General Information

Sample Name:	GULPPYUMBy (renamed file extension from none to dll)
Analysis ID:	562433
MD5:	698e141f265911..
SHA1:	d802e890c313d4..
SHA256:	8f3b19090289f2c..
Tags:	32 dll exe trojan
Infos:	



Detection



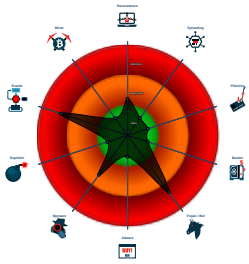
Emotet

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Emotet
- System process connects to networ…
- Machine Learning detection for sam…
- Sigma detected: Suspicious Call by…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query local…
- Deletes files inside the Windows fol…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6512 cmdline: loaddll32.exe "C:\Users\user\Desktop\GULPPYUMBy.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 1260 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\GULPPYUMBy.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5036 cmdline: rundll32.exe "C:\Users\user\Desktop\GULPPYUMBy.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6764 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GULPPYUMBy.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 4200 cmdline: regsvr32.exe /s C:\Users\user\Desktop\GULPPYUMBy.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - rundll32.exe (PID: 6748 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GULPPYUMBy.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6648 cmdline: rundll32.exe C:\Users\user\Desktop\GULPPYUMBy.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6272 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cpfkhipfqaawt\mtkslow.ijp",ARGENi MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 3840 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Cpfkhipfqaawt\mtkslow.ijp",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4128 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GULPPYUMBy.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 1088 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7108 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1260 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4176 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 588 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "74.207.230.120:8080",
    "139.196.72.155:8080",
    "37.44.244.177:8080",
    "37.59.209.141:8080",
    "116.124.128.206:8080",
    "217.182.143.207:443",
    "54.37.228.122:443",
    "203.153.216.46:443",
    "168.197.250.14:80",
    "207.148.81.119:8080",
    "195.154.146.35:443",
    "78.46.73.125:443",
    "191.252.103.16:80",
    "210.57.209.142:8080",
    "185.168.130.138:443",
    "142.4.219.173:8080",
    "118.98.72.86:443",
    "78.47.204.80:443",
    "159.69.237.188:443",
    "190.90.233.66:443",
    "104.131.62.48:8080",
    "62.171.178.147:8080",
    "185.148.168.15:8080",
    "54.38.242.185:443",
    "198.199.98.78:8080",
    "194.9.172.107:8080",
    "85.214.67.203:8080",
    "66.42.57.149:443",
    "185.148.168.220:8080",
    "103.41.204.169:8080",
    "128.199.192.135:8080",
    "195.77.239.39:8080",
    "59.148.253.194:443"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW"
  ]
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
GULPPYUMBy.dll	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.698154111.0000000004BD1000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.695678222.0000000004E61000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.697643809.0000000004800000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000B.00000002.1197600614.0000000005CF1000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000B.00000002.1196408950.00000000055F0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 58 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.rundll32.exe.5840000.12.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.4d30000.8.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.32f0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.rundll32.exe.4a10000.7.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
6.2.rundll32.exe.4b70000.9.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 86 entries				

Sigma Overview

System Summary

Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

AV Detection

Found malware configuration

Machine Learning detection for sample

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

System Summary

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

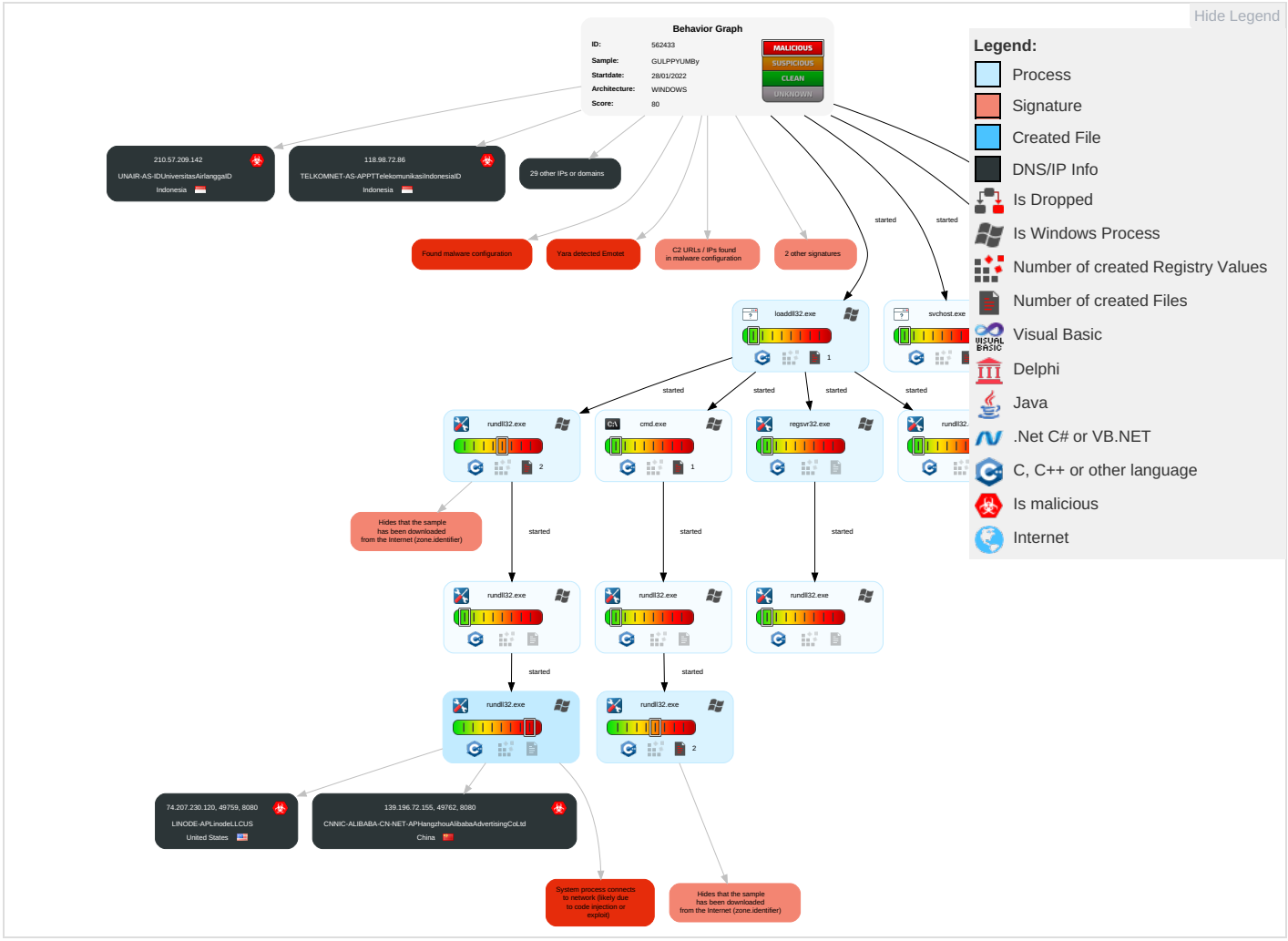
Yara detected Emotet

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	2 Input Capture	2 System Time Discovery	Remote Services	2 Input Capture	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	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Query Registry	Remote Desktop Protocol	1 Archive Collected Data	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)	1 1 1 Process Injection	Security Account Manager	2 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 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	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System 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	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	3 6 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

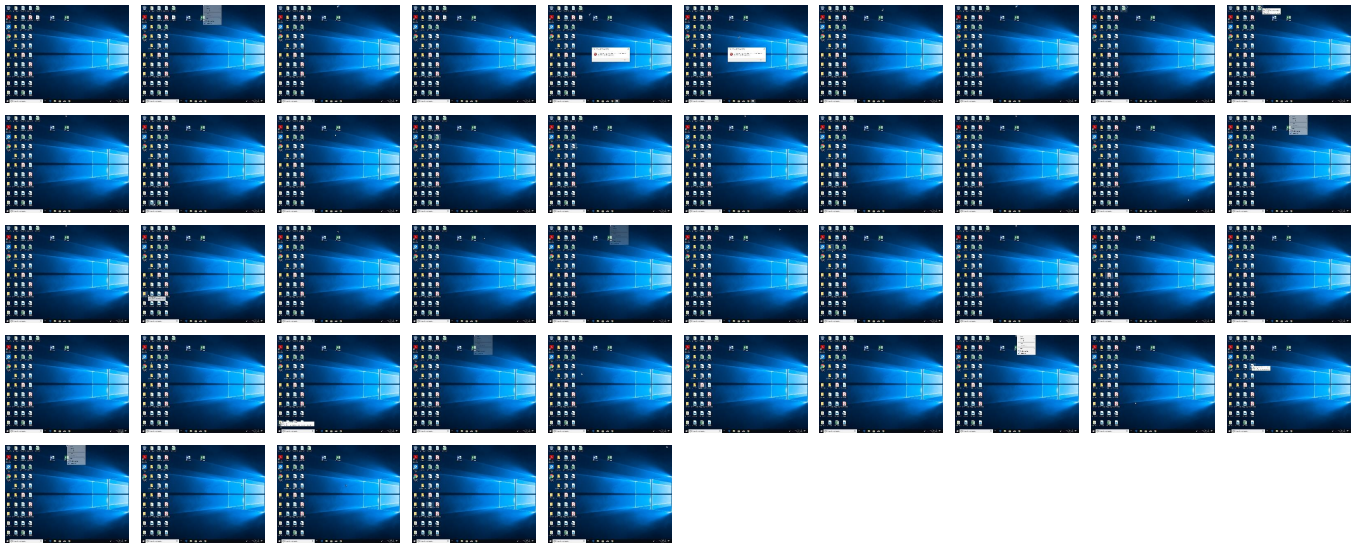
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
GULPPYUMBy.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.rundll32.exe.4ba0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.5840000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.4d30000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.4f90000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.5870000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.4b70000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.5620000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5780000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.51d0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.ca0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.32f0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.5650000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.4a10000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.bc0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.4d00000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5c40000.18.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.3360000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.regsvr32.exe.4960000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5a50000.16.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.55f0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.5a80000.17.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.regsvr32.exe.4790000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.5490000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.4d20000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.d60000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5960000.14.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.3100000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.4bd0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.3670000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.4800000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.49a0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.4830000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.4a40000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.d60000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.3620000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5cf0000.21.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.e20000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.750000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.4fc0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5c70000.19.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.4ba0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.35f0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.4cf0000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.2.loaddll32.exe.690000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.3130000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.4300000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5990000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.4cd0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.4e60000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.49e0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.54c0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.e30000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.890000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.5cc0000.20.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.rundll32.exe.4b70000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.rundll32.exe.42d0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		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://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://ctldl.windowsupdaZ	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

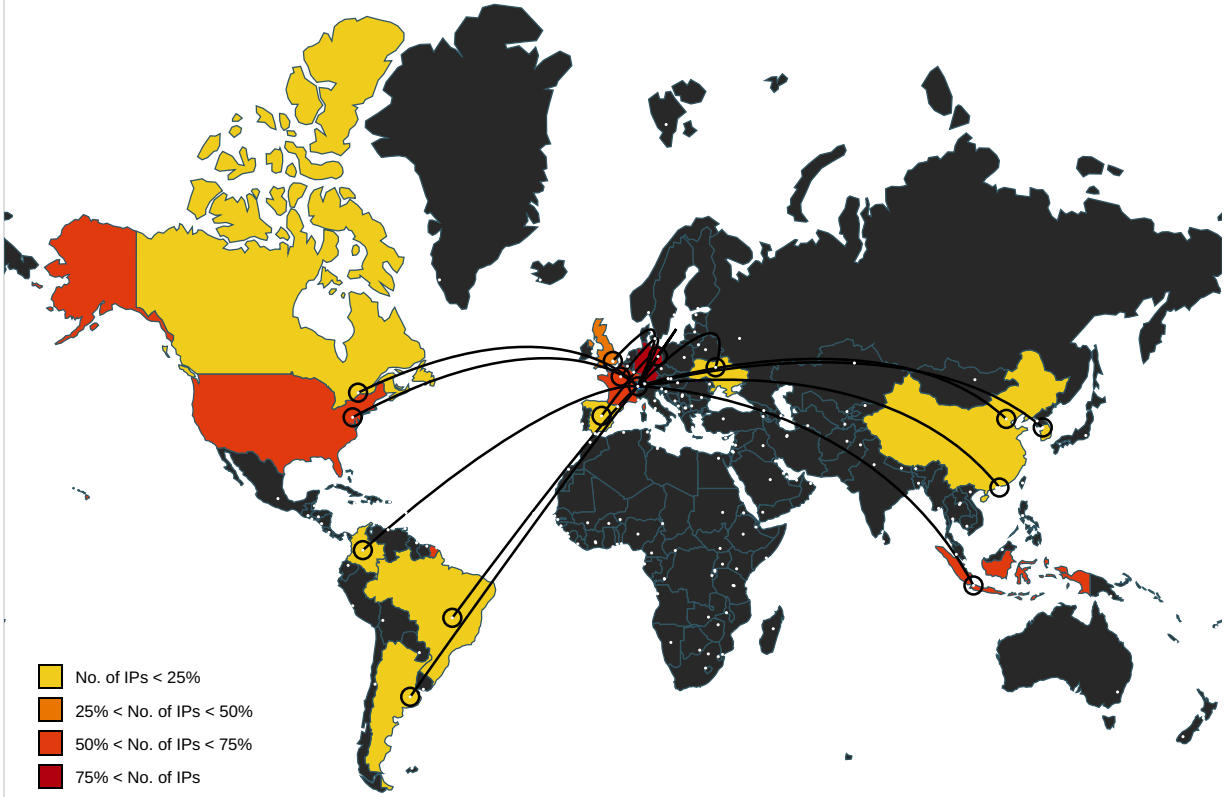
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000013.00000003.810079253.000001EE39558000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000013.00000003.810079253.000001EE39558000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.tiktok.com/legal/report	svchost.exe, 00000013.00000003.809882706.000001EE3957D000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000013.00000003.809882706.000001EE3957D000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.809743590.000001EE395A5000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.809816898.000001EE395A5000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ctldl.windowsupdaZ	rundll32.exe, 0000000B.00000003.757062289.0000000005B1F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://help.disneyplus.com.	svchost.exe, 00000013.00000003.810079253.000001EE39558000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 00000013.00000003.810079253.000001EE39558000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.148.81.119	unknown	United States		20473	AS-CHOOPAUS	true
104.131.62.48	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
198.199.98.78	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
194.9.172.107	unknown	unknown		207992	FEELBFR	true
59.148.253.194	unknown	Hong Kong		9269	HKBN-AS-APHongKongBroadbandNetworkLtdHK	true
74.207.230.120	unknown	United States		63949	LINODE-APLinodeLLCUS	true
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
191.252.103.16	unknown	Brazil		27715	LocawebServicosdeInternetSABR	true
168.197.250.14	unknown	Argentina		264776	OmarAnselmoRipollTDCNETAR	true
185.148.168.15	unknown	Germany		44780	EVERSCALE-ASDE	true
66.42.57.149	unknown	United States		20473	AS-CHOOPAUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
217.182.143.207	unknown	France		16276	OVHFR	true
203.153.216.46	unknown	Indonesia		45291	SURF-IDPTSurfindoNetworkID	true
159.69.237.188	unknown	Germany		24940	HETZNER-ASDE	true
116.124.128.206	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
37.59.209.141	unknown	France		16276	OVHFR	true
78.46.73.125	unknown	Germany		24940	HETZNER-ASDE	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
185.148.168.220	unknown	Germany		44780	EVERSCALE-ASDE	true
54.37.228.122	unknown	France		16276	OVHFR	true
185.168.130.138	unknown	Ukraine		49720	GIGACLOUD-ASUA	true
190.90.233.66	unknown	Colombia		18678	INTERNEXASAESPCO	true
142.4.219.173	unknown	Canada		16276	OVHFR	true
54.38.242.185	unknown	France		16276	OVHFR	true
195.154.146.35	unknown	France		12876	OnlineSASFR	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
118.98.72.86	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
128.199.192.135	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562433
Start date:	28.01.2022
Start time:	21:36:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	GULPPYUMBy (renamed file extension from none 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:	26
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:	mal80.troj.evad.winDLL@24/2@0/33
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 93.4%) • Quality average: 71.5% • Quality standard deviation: 26.4%

HCA Information:	• Successful, ratio: 100% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 2.20.157.220, 93.184.221.240, 8.238.85.126, 8.248.137.254, 8.248.131.254, 8.248.133.254, 8.248.119.254, 40.91.112.76, 20.54.104.15
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, displaycatalog-rp-uswest.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, wu-shim.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, ctldl.windowsupdate.com, consumerrp-displaycatalog-aks2aks-europe.md.mp.microsoft.com.akadns.net, wus2-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, arc.msn.com, wu.azureedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, consumer-displaycatalogrp-aks2aks-uswest.md.mp.microsoft.com.akadns.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, neu-consumerrp-displaycatalog-aks2aks-europe.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- 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.
- VT rate limit hit for: GULPPYUMBy.dll

Simulations

Behavior and APIs

Time	Type	Description
21:38:09	API Interceptor	7x 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:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	Microsoft Cabinet archive data, 61414 bytes, 1 file

Category:	dropped
Size (bytes):	61414
Entropy (8bit):	**7.995245868798237**
Encrypted:	**true**
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD89844761417C1D23ACC41F8AEBF3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090 0
Malicious:	false
Preview:	MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U....''<ke.....l.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.''.Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.''.g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....I..H.#...d.Qh..3..fCX....==#..M.l..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-...< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.........N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3..._ ..nN]..=..M.o.F.._..z....._...gY..!Z..?l....vp.l.:.d.Z..W.....~...N.._k...&.....$.....i.F.d.....D!e.....Y...,.E..m.;.1... $.F..O.F.o_}.uG....,.%.>,.Zx.....o....c../.;....g&.....

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

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.116057753988458
Encrypted:	false
SSDEEP:	6:kKWk8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:+9kPlE99SNxAhUeYlUSA/t
MD5:	D1FED154DF638910AC019AFA0CB83733
SHA1:	951BA120ACEBECC63FC248C40E87CF611A36C4E9
SHA-256:	7F6F686D8D41DC15FFF7FE2C5A78123408AADB2C260AC09CA3F5486E9FF39983
SHA-512:	930FD952EBA759F211B7F1AFF4A2B8A52526EE59B6952ECE36EBEDC191EB01E1FCD6B70E8C166954E9D1CD57E3FAFE98ED76E34EFF91C0776883FB47B22DD AC1
Malicious:	false
Preview:	p..... ....(..... ....q.\].....&.....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...''.0.7.1.e.1.5.c.5.d.c.4.d.7.1.:.0.''...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.004116662498383
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	GULPPYUMBy.dll
File size:	557056
MD5:	698e141f2659110386e428f6e1178dae
SHA1:	d802e890c313d4c8d898523e06574eb05bed7f06
SHA256:	8f3b19090289f2c0215353e2979abcd1c6ebf6217f144cebefba8a0572d5fdc4
SHA512:	9d99de6bcbae3bf2a283764a999d306d736646fee66283853b57ae50ac2234339e19042d4583ca7a150f97ceb4da96ffdee473fb9b0c3c9d18963ab6f44fadcd
SSDEEP:	6144:HUNF4UQXTkkAiBuGKDU5PSczbmOTT0DaTMGbUylbdTN1itwRClN6RfcjJxX4R0Zq:AeAa4DU5PSczbmmTzTnwyDx6BrWt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,..2...2&..2...27..2,..2...2...26..2...2...2...2...2...2-..2...2-..2 ...2-..2Rich,..2.....PE..L.....a...

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General	
Entrypoint:	0x10030d06
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x61F3FA91 [Fri Jan 28 14:15:45 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:	f4d2f65566a93075f8824e97bf321580

Entrypoint Preview
Instruction
cmp dword ptr [esp+08h], 01h
jne 00007F363CB2B347h
call 00007F363CB336A0h
push dword ptr [esp+04h]
mov ecx, dword ptr [esp+10h]
mov edx, dword ptr [esp+0Ch]
call 00007F363CB2B232h
pop ecx
retn 000Ch
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [100545D4h]
xor eax, ebp
push eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [100545D4h]
xor eax, ebp
push eax

Instruction
mov dword ptr [ebp-10h], esp
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [100545D4h]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x52d40	0x52	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x51034	0x104	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5a000	0x27650	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x82000	0x4e30	.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	0x4bd90	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x46000	0x594	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x50fac	0x40	.rdata
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	0x44539	0x45000	False	0.469910552536	data	6.61687356024	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x46000	0xcd92	0xd000	False	0.33779672476	data	5.22622411384	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x53000	0x6580	0x3000	False	0.2626953125	PGP symmetric key encrypted data -	4.05367526692	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x5a000	0x27650	0x28000	False	0.916259765625	data	7.8318744089	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x82000	0x9376	0xa000	False	0.346923828125	data	4.18220950375	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
DASHBOARD	0x5ab04	0x23600	data	Chinese	Taiwan
RT_CURSOR	0x7e104	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7e238	0xb4	data	Chinese	Taiwan
RT_CURSOR	0x7e2ec	0x134	AmigaOS bitmap font	Chinese	Taiwan
RT_CURSOR	0x7e420	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7e554	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7e688	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7e7bc	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7e8f0	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7ea24	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7eb58	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7ec8c	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7edc0	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7eef4	0x134	AmigaOS bitmap font	Chinese	Taiwan
RT_CURSOR	0x7f028	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7f15c	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7f290	0x134	data	Chinese	Taiwan
RT_BITMAP	0x7f3c4	0xb8	data	Chinese	Taiwan
RT_BITMAP	0x7f47c	0x144	data	Chinese	Taiwan
RT_DIALOG	0x7f5c0	0x148	data	Chinese	Taiwan
RT_DIALOG	0x7f708	0x26a	data	Chinese	Taiwan
RT_DIALOG	0x7f974	0xe8	data	Chinese	Taiwan
RT_DIALOG	0x7fa5c	0x34	data	Chinese	Taiwan
RT_STRING	0x7fa90	0x58	data	Chinese	Taiwan
RT_STRING	0x7fae8	0x82	data	Chinese	Taiwan
RT_STRING	0x7fb6c	0x2a	data	Chinese	Taiwan
RT_STRING	0x7fb98	0x192	data	Chinese	Taiwan
RT_STRING	0x7fd2c	0x4e2	data	Chinese	Taiwan
RT_STRING	0x80210	0x31a	data	Chinese	Taiwan
RT_STRING	0x8052c	0x2dc	data	Chinese	Taiwan
RT_STRING	0x80808	0x8a	data	Chinese	Taiwan
RT_STRING	0x80894	0xac	data	Chinese	Taiwan
RT_STRING	0x80940	0xde	data	Chinese	Taiwan
RT_STRING	0x80a20	0x4c4	data	Chinese	Taiwan
RT_STRING	0x80ee4	0x264	data	Chinese	Taiwan
RT_STRING	0x81148	0x2c	data	Chinese	Taiwan
RT_STRING	0x81174	0x42	data	Chinese	Taiwan
RT_GROUP_CURSOR	0x811b8	0x22	Lotus unknown worksheet or configuration, revision 0x2	Chinese	Taiwan
RT_GROUP_CURSOR	0x811dc	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x811f0	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x81204	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan

Name	RVA	Size	Type	Language	Country
RT_GROUP_CURSOR	0x81218	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x8122c	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x81240	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x81254	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x81268	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x8127c	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x81290	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x812a4	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x812b8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x812cc	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x812e0	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_VERSION	0x812f4	0x304	data	Chinese	Taiwan
RT_MANIFEST	0x815f8	0x56	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	FileTimeToSystemTime, FileTimeToLocalFileTime, GetFileAttributesA, GetFileTime, GetTickCount, RtlUnwind, GetSystemInfo, HeapReAlloc, GetCommandLineA, ExitProcess, ExitThread, CreateThread, RaiseException, HeapSize, TerminateProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, Sleep, HeapDestroy, HeapCreate, GetStdHandle, GetOEMCP, GetFileType, GetStartupInfoA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, QueryPerformanceCounter, GetSystemTimeAsFileTime, GetACP, GetStringTypeA, GetStringTypeW, GetTimeZoneInformation, GetConsoleCP, GetConsoleMode, LCMapStringA, LCMapStringW, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, SetEnvironmentVariableA, GetCPInfo, CreateFileA, GetFullPathNameA, GetVolumeInformationA, FindFirstFileA, FindClose, GetCurrentProcess, DuplicateHandle, GetThreadLocale, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, InterlockedIncrement, TlsFree, DeleteCriticalSection, LocalReAlloc, TlsSetValue, TlsAlloc, InitializeCriticalSection, GlobalHandle, GlobalReAlloc, EnterCriticalSection, TlsGetValue, LeaveCriticalSection, LocalAlloc, GlobalFlags, FormatMessageA, LocalFree, InterlockedDecrement, MulDiv, GlobalGetAtomNameA, GlobalFindAtomA, lstrcmpW, GetVersionExA, WritePrivateProfileStringA, GlobalUnlock, GlobalFree, FreeResource, GetCurrentProcessId, GlobalAddAtomA, CreateEventA, SuspendThread, SetEvent, WaitForSingleObject, ResumeThread, SetThreadPriority, CloseHandle, GetCurrentThread, GetCurrentThreadId, ConvertDefaultLocale, GetModuleFileNameA, EnumResourceLanguagesA, GetLocaleInfoA, GlobalLock, lstrcmpA, GlobalAlloc, GlobalDeleteAtom, GetModuleHandleA, GetLastError, lstrlenA, CompareStringA, CompareStringW, MultiByteToWideChar, InterlockedExchange, GetVersion, WideCharToMultiByte, LockResource, FindResourceA, FindResourceW, LoadResource, SizeofResource, HeapFree, GetNativeSystemInfo, GetProcessHeap, HeapAlloc, FreeLibrary, GetProcAddress, LoadLibraryA, IsBadReadPtr, VirtualProtect, SetLastError, VirtualAlloc, VirtualFree, SetHandleCount, VirtualQuery
USER32.dll	GetNextDlgGroupItem, MessageBeep, UnregisterClassA, RegisterClipboardFormatA, PostThreadMessageA, LoadCursorA, SetCapture, DestroyMenu, EndPaint, BeginPaint, GetWindowDC, ClientToScreen, GrayStringA, DrawTextExA, DrawTextA, TabbedTextOutA, ShowWindow, MoveWindow, SetWindowTextA, IsDialogMessageA, RegisterWindowMessageA, SendDlgItemMessageA, WinHelpA, GetCapture, GetClassLongA, GetClassNameA, SetPropA, GetPropA, RemovePropA, SetFocus, GetWindowTextLengthA, GetWindowTextA, GetForegroundWindow, InvalidateRgn, GetTopWindow, UnhookWindowsHookEx, GetMessageTime, GetMessagePos, MapWindowPoints, SetForegroundWindow, UpdateWindow, GetMenu, GetSubMenu, GetMenuItemID, GetMenuItemCount, CreateWindowExA, GetClassInfoExA, GetClassInfoA, RegisterClassA, GetSysColor, AdjustWindowRectEx, EqualRect, PtInRect, GetDlgCtrlID, DefWindowProcA, CallWindowProcA, OffsetRect, IntersectRect, SystemParametersInfoA, GetWindowPlacement, GetWindowRect, ReleaseDC, GetDC, CopyRect, SetWindowLongA, GetWindowLongA, GetSystemMetrics, DrawIcon, AppendMenuA, SendMessageA, GetWindow, SetWindowContextHelpId, MapDialogRect, SetWindowPos, GetDesktopWindow, SetActiveWindow, CreateDialogIndirectParamA, DestroyWindow, IsWindow, GetDlgItem, GetNextDlgTabItem, EndDialog, GetWindowThreadProcessId, InvalidateRect, SetRect, IsRectEmpty, CopyAcceleratorTableA, CharNextA, GetLastActivePopup, IsWindowEnabled, GetSysColorBrush, ReleaseCapture, GetSystemMenu, IsIconic, GetClientRect, EnableWindow, LoadIconA, CharUpperA, PostQuitMessage, PostMessageA, CheckMenuItem, EnableMenuItem, GetMenuState, ModifyMenuA, GetParent, GetFocus, LoadBitmapA, GetMenuCheckMarkDimensions, SetMenuItemBitmaps, ValidateRect, GetCursorPos, PeekMessageA, GetKeyState, IsWindowVisible, GetActiveWindow, DispatchMessageA, TranslateMessage, GetMessageA, CallNextHookEx, SetWindowsHookExA, SetCursor, MessageBoxA, IsChild
GDI32.dll	ExtSelectClipRgn, DeleteDC, GetStockObject, GetDeviceCaps, GetBkColor, GetTextColor, GetRgnBox, GetMapMode, ScaleWindowExtEx, SetWindowExtEx, ScaleViewportExtEx, SetViewportExtEx, OffsetViewportOrgEx, SetViewportOrgEx, SelectObject, Escape, ExtTextOutA, CreateBitmap, RectVisible, PtVisible, GetWindowExtEx, GetViewportExtEx, DeleteObject, SetMapMode, RestoreDC, SaveDC, GetObjectA, SetBkColor, SetTextColor, GetClipBox, CreateRectRgnIndirect, TextOutA
comdlg32.dll	GetFileTitleA
WINSPOOL.DRV	DocumentPropertiesA, OpenPrinterA, ClosePrinter

DLL	Import
ADVAPI32.dll	RegQueryValueA, RegSetValueExA, RegCreateKeyExA, RegCloseKey, RegOpenKeyA, RegEnumKeyA, RegDeleteKeyA, RegOpenKeyExA, RegQueryValueExA
COMCTL32.dll	InitCommonControlsEx
SHLWAPI.dll	PathFindFileNameA, PathStripToRootA, PathFindExtensionA, PathIsUNCA
WS2_32.dll	recv, connect, WSACleanup, socket, WSAStartup, htons, inet_addr, closesocket, send
oledlg.dll	
ole32.dll	StgOpenStorageOnILockBytes, CoGetClassObject, CoTaskMemAlloc, StgCreateDocfileOnILockBytes, CoTaskMemFree, CLSIDFromString, CLSIDFromProgID, CreateILockBytesOnHGlobal, CoRegisterMessageFilter, OleFlushClipboard, OleIsCurrentClipboard, CoRevokeClassObject, OleInitialize, CoFreeUnusedLibraries, OleUninitialize
OLEAUT32.dll	SysAllocStringLen, VariantClear, VariantChangeType, VariantInit, SysStringLen, SysAllocStringByteLen, OleCreateFontIndirect, VariantTimeToSystemTime, SystemTimeToVariantTime, SafeArrayDestroy, SysAllocString, VariantCopy, SysFreeString

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x10012860

Version Infos

Description	Data
LegalCopyright	Innoversal. All rights reserved.
InternalName	FinalChatSocketCli.exe
FileVersion	1.0.2.4
CompanyName	Innoversal
ProductName	Char room only
ProductVersion	1.0.2.4
FileDescription	Chat room
OriginalFilename	FinalChatSocketCli.exe
Translation	0x0404 0x03b6

Possible Origin

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

Network Behavior

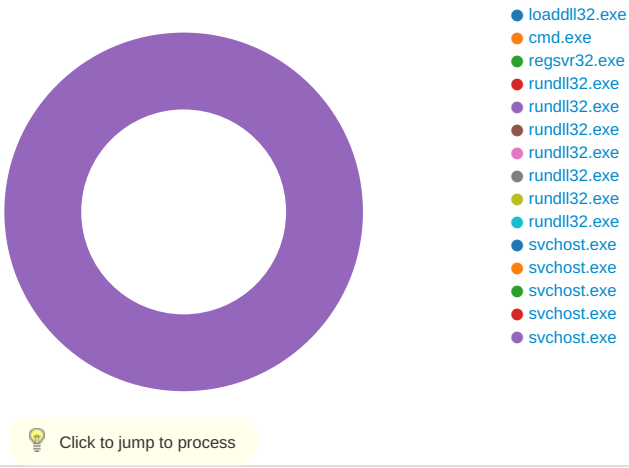
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:37:38.453679085 CET	49759	8080	192.168.2.4	74.207.230.120
Jan 28, 2022 21:37:38.602190018 CET	8080	49759	74.207.230.120	192.168.2.4
Jan 28, 2022 21:37:39.268378019 CET	49759	8080	192.168.2.4	74.207.230.120
Jan 28, 2022 21:37:39.417572975 CET	8080	49759	74.207.230.120	192.168.2.4
Jan 28, 2022 21:37:39.957154989 CET	49759	8080	192.168.2.4	74.207.230.120
Jan 28, 2022 21:37:40.106230021 CET	8080	49759	74.207.230.120	192.168.2.4
Jan 28, 2022 21:37:40.137888908 CET	49762	8080	192.168.2.4	139.196.72.155
Jan 28, 2022 21:37:40.375052929 CET	8080	49762	139.196.72.155	192.168.2.4
Jan 28, 2022 21:37:40.375256062 CET	49762	8080	192.168.2.4	139.196.72.155
Jan 28, 2022 21:37:41.012032986 CET	49762	8080	192.168.2.4	139.196.72.155
Jan 28, 2022 21:37:41.248980045 CET	8080	49762	139.196.72.155	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 21:37:41.262382984 CET	8080	49762	139.196.72.155	192.168.2.4
Jan 28, 2022 21:37:41.262408018 CET	8080	49762	139.196.72.155	192.168.2.4
Jan 28, 2022 21:37:41.262525082 CET	49762	8080	192.168.2.4	139.196.72.155
Jan 28, 2022 21:37:46.474993944 CET	49762	8080	192.168.2.4	139.196.72.155
Jan 28, 2022 21:37:46.712712049 CET	8080	49762	139.196.72.155	192.168.2.4
Jan 28, 2022 21:37:46.714340925 CET	49762	8080	192.168.2.4	139.196.72.155
Jan 28, 2022 21:37:46.718425035 CET	49762	8080	192.168.2.4	139.196.72.155
Jan 28, 2022 21:37:46.994680882 CET	8080	49762	139.196.72.155	192.168.2.4
Jan 28, 2022 21:37:47.825988054 CET	8080	49762	139.196.72.155	192.168.2.4
Jan 28, 2022 21:37:47.826212883 CET	49762	8080	192.168.2.4	139.196.72.155
Jan 28, 2022 21:37:50.824872971 CET	8080	49762	139.196.72.155	192.168.2.4
Jan 28, 2022 21:37:50.824945927 CET	8080	49762	139.196.72.155	192.168.2.4
Jan 28, 2022 21:37:50.825123072 CET	49762	8080	192.168.2.4	139.196.72.155
Jan 28, 2022 21:37:50.825158119 CET	49762	8080	192.168.2.4	139.196.72.155
Jan 28, 2022 21:39:29.431499958 CET	49762	8080	192.168.2.4	139.196.72.155
Jan 28, 2022 21:39:29.431545973 CET	49762	8080	192.168.2.4	139.196.72.155

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **6512**, Parent PID: **5216**

General

Target ID:	0
Start time:	21:37:06
Start date:	28/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\GULPPYUMBy.dll"
Imagebase:	0x1270000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
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: 00000000.00000002.686090984.0000000010001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.685943850.0000000000690000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.685979293.0000000000751000.00000020.00000800.00020000.00000000.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

Analysis Process: cmd.exe PID: 1260, Parent PID: 6512

General

Target ID:	1
Start time:	21:37:06
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\GULPPYUMBy.dll",#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: 4200, Parent PID: 6512

General

Target ID:	3
Start time:	21:37:06
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\GULPPYUMBy.dll
Imagebase:	0x8a0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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: 00000003.00000002.681695490.0000000004961000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.681496584.0000000004790000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.681720206.0000000010001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5036, Parent PID: 1260

General	
Target ID:	4
Start time:	21:37:07
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\GULPPYUMBy.dll",#1
Imagebase:	0xe60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000004.00000002.679578387.0000000003131000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.679544015.0000000003100000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.679681622.0000000010001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **6648**, Parent PID: **6512**

General	
Target ID:	5
Start time:	21:37:07
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\GULPPYUMBy.dll,DllRegisterServer
Imagebase:	0xe60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000005.00000002.695678222.0000000004E61000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.694796283.0000000000E30000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.695708473.0000000004F90000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.694598202.0000000000D61000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.695395247.0000000004B70000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.695172555.000000000049A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.695749630.0000000004FC1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.695641002.0000000004D30000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.695603326.0000000004D01000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.695422865.0000000004BA1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.695541961.0000000004CD0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.694543182.0000000000CA0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.695799200.0000000010001000.00000020.00000001.01000000.00000005.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\SysWOW64\Cpfkhipfqaawt\mtkslow.ijp:Zone.Identifier	success or wait	1	D6BB46	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: **6764**, Parent PID: **5036**

General

Target ID:	6
Start time:	21:37:08
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GULPPYUMBy.dll",DllRegisterServer
Imagebase:	0xe60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000006.00000002.698154111.0000000004BD1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.697643809.0000000004800000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.697928489.0000000004A11000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.698188921.0000000004CF0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.698237406.0000000004D21000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.697381734.0000000000D61000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.698024966.0000000004A40000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.698097030.0000000004B71000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.697679889.0000000004831000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.697883792.00000000049E0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.697578778.0000000004301000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.698123859.0000000004BA0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.697251813.0000000000890000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.697538665.00000000042D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.698300661.0000000010001000.00000020.00000001.01000000.00000005.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: **6748**, Parent PID: **4200**

General

Target ID:	7
Start time:	21:37:08

Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GULPPYUMBy.dll",DllRegisterServer
Imagebase:	0xe60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **4128**, Parent PID: **6512**

General

Target ID:	9
Start time:	21:37:11
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GULPPYUMBy.dll",DllRegisterServer
Imagebase:	0xe60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **6272**, Parent PID: **6648**

General

Target ID:	10
Start time:	21:37:14
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cpfkhipfqaawt\mtkslow.ijp",ARGENi
Imagebase:	0xe60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 0000000A.00000002.700428113.0000000000BC0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.700757747.0000000010001000.00000020.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.700559072.0000000000E21000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **3840**, Parent PID: **6272**

General

Target ID:	11
Start time:	21:37:18
Start date:	28/01/2022

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Cpfkhipfqaawt\mtkslow.ijp",DllRegisterServer
Imagebase:	0xe60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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.00000002.1197600614.0000000005CF1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196408950.000000000055F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1197748289.0000000010001000.00000020.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196837395.0000000005A81000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196803049.0000000005A50000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196180754.0000000003670000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1197083617.0000000005C40000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196131106.0000000003621000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196688032.0000000005960000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1195767818.0000000003361000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1197436981.0000000005CC0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196737137.0000000005991000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196460440.0000000005650000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1195681917.000000032F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1197274382.0000000005C71000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196435372.0000000005621000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196321416.0000000005490000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196503493.0000000005781000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196346409.000000054C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196572936.0000000005840000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196102968.000000035F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196608362.0000000005871000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1196239650.000000051D1000.00000020.00000800.00020000.00000000.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: svchost.exe PID: **1088**, Parent PID: **568**

General

Target ID:	13
Start time:	21:37:29
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000

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: 7108, Parent PID: 568

General

Target ID:	15
Start time:	21:37:37
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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: 1260, Parent PID: 568

General

Target ID:	16
Start time:	21:37:44
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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: 4176, Parent PID: 568

General

Target ID:	17
Start time:	21:37:55
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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: **588**, Parent PID: **568**

General

Target ID:	19
Start time:	21:38:07
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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