

JOeSandbox Cloud BASIC



ID: 531996

Sample Name:

spZRMihlrkFGqYq1f.dll

Cookbook: default.jbs

Time: 16:24:54

Date: 01/12/2021

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report spZRMihlrkFGqYq1f.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Emotet	4
Yara Overview	5
Memory Dumps	5
Unpacked PEs	5
Sigma Overview	5
System Summary:	5
Jbx Signature Overview	6
AV Detection:	6
Networking:	6
E-Banking Fraud:	6
System Summary:	6
Hooking and other Techniques for Hiding and Protection:	6
HIPS / PFW / Operating System Protection Evasion:	6
Stealing of Sensitive Information:	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	9
Contacted IPs	9
Public	9
General Information	10
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASN	11
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	13
Static File Info	13
General	13
File Icon	13
Static PE Info	13
General	13
Entrypoint Preview	13
Rich Headers	13
Data Directories	14
Sections	14
Resources	14
Imports	14
Exports	14
Possible Origin	14
Network Behavior	14
Snort IDS Alerts	14
Network Port Distribution	14
TCP Packets	14
HTTP Request Dependency Graph	14
HTTPS Proxied Packets	14
Code Manipulations	15
Statistics	15
Behavior	15
System Behavior	15
Analysis Process: loaddll32.exe PID: 6748 Parent PID: 2988	15
General	15

File Activities	15
Analysis Process: cmd.exe PID: 6740 Parent PID: 6748	15
General	16
File Activities	16
Analysis Process: rundll32.exe PID: 5572 Parent PID: 6748	16
General	16
File Activities	16
File Deleted	17
Analysis Process: rundll32.exe PID: 5376 Parent PID: 6740	17
General	17
Analysis Process: svchost.exe PID: 5144 Parent PID: 572	17
General	17
File Activities	17
Analysis Process: rundll32.exe PID: 5392 Parent PID: 5376	17
General	17
File Activities	18
Analysis Process: rundll32.exe PID: 4008 Parent PID: 5572	18
General	18
Analysis Process: rundll32.exe PID: 5348 Parent PID: 4008	18
General	18
Analysis Process: svchost.exe PID: 6668 Parent PID: 572	19
General	19
File Activities	19
Analysis Process: svchost.exe PID: 6712 Parent PID: 572	20
General	20
File Activities	20
Analysis Process: svchost.exe PID: 3928 Parent PID: 572	20
General	20
File Activities	20
Disassembly	20
Code Analysis	20

Windows Analysis Report spZRMihlrkFGqYq1f.dll

Overview

General Information

Sample Name:

spZRMihlrkFGqYq1f.dll

Analysis ID:

531996

MD5:

9f4fa905fd685d2...

SHA1:

e186e0869276d3..

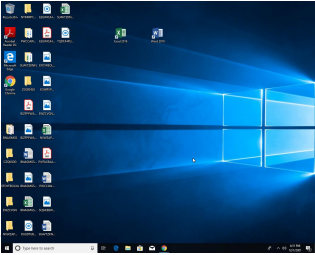
SHA256:

808e8247efd685b.

Infos:



Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Emotet

Score:

96

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Snort IDS alert for network traffic (e...

Multi AV Scanner detection for subm...

Yara detected Emotet

System process connects to networ...

Sigma detected: Emotet RunDLL32 ...

C2 URLs / IPs found in malware con...

Hides that the sample has been dow...

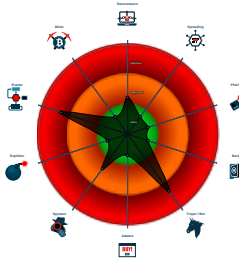
Uses 32bit PE files

Queries the volume information (nam...

Contains functionality to check if a d...

Contains functionality to query locale...

Classification



Process Tree

System is w10x64

 loaddll32.exe (PID: 6748 cmdline: loaddll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)

 cmd.exe (PID: 6740 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

 rundll32.exe (PID: 5376 cmdline: rundll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

 rundll32.exe (PID: 5392 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

 rundll32.exe (PID: 5572 cmdline: rundll32.exe C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

 rundll32.exe (PID: 4008 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Thkptzp\bxlyirts.twn",wJPKT MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

 rundll32.exe (PID: 5348 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Thkptzp\bxlyirts.twn",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

 svchost.exe (PID: 5144 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

 svchost.exe (PID: 6668 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

 svchost.exe (PID: 6712 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

 svchost.exe (PID: 3928 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

cleanup

Malware Configuration

Threatname: Emotet

Copyright Joe Security LLC 2021

Page 4 of 20

```
{
  "C2 list": [
    "51.178.61.60:443",
    "168.197.250.14:80",
    "45.79.33.48:8080",
    "196.44.98.190:8080",
    "177.72.80.14:7080",
    "51.210.242.234:8080",
    "185.148.169.10:8080",
    "142.4.219.173:8080",
    "78.47.204.80:443",
    "78.46.73.125:443",
    "37.44.244.177:8080",
    "37.59.209.141:8080",
    "191.252.103.16:80",
    "54.38.242.185:443",
    "85.214.67.203:8080",
    "54.37.228.122:443",
    "207.148.81.119:8080",
    "195.77.239.39:8080",
    "66.42.57.149:443",
    "195.154.146.35:443"
  ],
  "Public Key": [
    "RUNTMSAAAADBLxqDnHonUYwk8sqo7IWuU1LRdUiUBnACc6ronsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeLZU0",
    "RUNLMSAAAADYNZPXy4tQxd/N4WnS5TYAnStU0xY2oL1ELrI4MNHhNni640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.294421724.0000000002CA 0000.00000040.00000001.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.299095986.000000002B50000.00000 040.00000001.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.295708086.0000000004470000.00000 040.00000001.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.687143531.00000000048A0000.00000 040.00000001.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.686773719.0000000002E80000.00000 040.00000010.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 29 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.rundll32.exe.5270000.10.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.5590000.16.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.50b0000.6.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.rundll32.exe.4d50000.6.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.5390000.13.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 46 entries

Sigma Overview

System Summary:



Sigma detected: Emotet RunDLL32 Process Creation

Jbx Signature Overview

 Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Networking:



Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:



Yara detected Emotet

System Summary:



Hooking and other Techniques for Hiding and Protection:



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

HIPS / PFW / Operating System Protection Evasion:



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

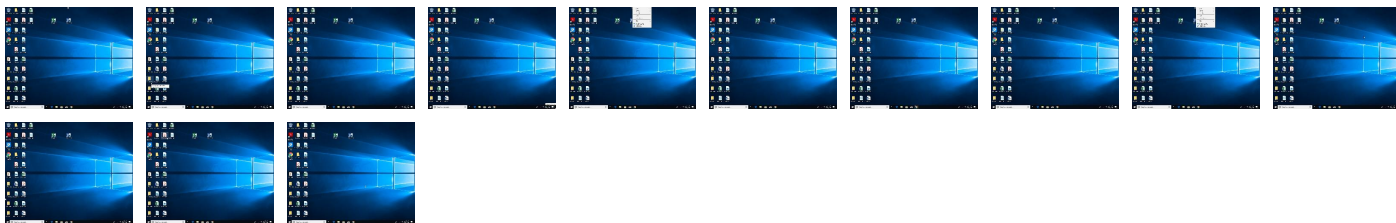
Stealing of Sensitive Information:



Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 2	Path Interception	Process Injection 1 1 2	Masquerading 2	Input Capture 1	System Time Discovery 2	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS7 to Redirect Phishing Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
spZRMihlrkFGqYq1f.dll	70%	VirusTotal		Browse
spZRMihlrkFGqYq1f.dll	43%	Metadefender		Browse
spZRMihlrkFGqYq1f.dll	57%	ReversingLabs	Win32.Trojan.Mansabo	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.4f40000.11.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.44a0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.44a0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.49d0000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.2d60000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.4de0000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.50e0000.7.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.5390000.13.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.5240000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.5000000.5.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.52a0000.11.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.4d80000.7.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.55c0000.17.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.4b00000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.4be0000.5.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.2eb0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.54b0000.15.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://51.178.61.60/IJkHjHYuxCdTZukielYhLRnUuQlzcYbcaXcjoFrijtLCdYogUVaLxnRUqnklmC	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://help.disneyplus.com .	0%	URL Reputation	safe	
http://https://disneyplus.com/legal .	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://51.178.61.60/IJkHjHYuxCdTZukielYhLRnUuQlzcYbcaXcjoFrijtLCdYogUVaLxnRUqnklmC	true	Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.148.81.119	unknown	United States		20473	AS-CHOOPAUS	true
196.44.98.190	unknown	Ghana		327814	EcobandGH	true
78.46.73.125	unknown	Germany		24940	HETZNER-ASDE	true
37.59.209.141	unknown	France		16276	OVHFR	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
191.252.103.16	unknown	Brazil		27715	LocawebServicosdeInternet SABR	true
45.79.33.48	unknown	United States		63949	LINODE-APLinodeLLCUS	true
54.37.228.122	unknown	France		16276	OVHFR	true
185.148.169.10	unknown	Germany		44780	EVERSCALE-ASDE	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.4.219.173	unknown	Canada		16276	OVHFR	true
54.38.242.185	unknown	France		16276	OVHFR	true
195.154.146.35	unknown	France		12876	OnlineSASFR	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
168.197.250.14	unknown	Argentina		264776	OmarAnselmoRipollTDCNET AR	true
51.178.61.60	unknown	France		16276	OVHFR	true
177.72.80.14	unknown	Brazil		262543	NewLifeFibraBR	true
66.42.57.149	unknown	United States		20473	AS-CHOOPAUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
51.210.242.234	unknown	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	531996
Start date:	01.12.2021
Start time:	16:24:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	spZRMihlrkFGqYq1f.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	23
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@17/0@0/20
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 99.3% (good quality ratio 90.9%) • Quality average: 75.3% • Quality standard deviation: 29.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
207.148.81.119	gvtdsqavfej.dll	Get hash	malicious	Browse	
	mhOX6jll6x.dll	Get hash	malicious	Browse	
	dguQYT8p8j.dll	Get hash	malicious	Browse	
	jSxlzXfwc7.dll	Get hash	malicious	Browse	
	mhOX6jll6x.dll	Get hash	malicious	Browse	
	X2XCewl2Yy.dll	Get hash	malicious	Browse	
	dguQYT8p8j.dll	Get hash	malicious	Browse	
	HMvjzUYq2h.dll	Get hash	malicious	Browse	
	s9BZBDWmi4.dll	Get hash	malicious	Browse	
	bFx5bZRC6P.dll	Get hash	malicious	Browse	
	c7IUEh66u6.dll	Get hash	malicious	Browse	
	HMvjzUYq2h.dll	Get hash	malicious	Browse	
	s9BZBDWmi4.dll	Get hash	malicious	Browse	
	bFx5bZRC6P.dll	Get hash	malicious	Browse	
	WfCt2B042X.dll	Get hash	malicious	Browse	
	ZKVYER7XcT.dll	Get hash	malicious	Browse	
	2cq85E4EeM.dll	Get hash	malicious	Browse	
	WfCt2B042X.dll	Get hash	malicious	Browse	
	ZKVYER7XcT.dll	Get hash	malicious	Browse	
196.44.98.190	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	
	gvtdsqavfej.dll	Get hash	malicious	Browse	
	mhOX6jll6x.dll	Get hash	malicious	Browse	
	dguQYT8p8j.dll	Get hash	malicious	Browse	
	jSxlzXfwc7.dll	Get hash	malicious	Browse	
	mhOX6jll6x.dll	Get hash	malicious	Browse	
	X2XCewl2Yy.dll	Get hash	malicious	Browse	
	dguQYT8p8j.dll	Get hash	malicious	Browse	
	HMvjzUYq2h.dll	Get hash	malicious	Browse	
	s9BZBDWmi4.dll	Get hash	malicious	Browse	
	bFx5bZRC6P.dll	Get hash	malicious	Browse	
	c7IUEh66u6.dll	Get hash	malicious	Browse	
	HMvjzUYq2h.dll	Get hash	malicious	Browse	
	s9BZBDWmi4.dll	Get hash	malicious	Browse	
	bFx5bZRC6P.dll	Get hash	malicious	Browse	
	WfCt2B042X.dll	Get hash	malicious	Browse	
	ZKVYER7XcT.dll	Get hash	malicious	Browse	
	2cq85E4EeM.dll	Get hash	malicious	Browse	
	WfCt2B042X.dll	Get hash	malicious	Browse	
	ZKVYER7XcT.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	66.42.57.149
	iU17wh2uUd.exe	Get hash	malicious	Browse	149.28.253.196
	iU17wh2uUd.exe	Get hash	malicious	Browse	149.28.253.196
	Sz4lxTmH7r.exe	Get hash	malicious	Browse	149.28.253.196
	7AF33E5528AB8A8F45EE7B8C4DD24B4014FEAA6E1D310.exe	Get hash	malicious	Browse	149.28.253.196
	RFIISRQKzj.exe	Get hash	malicious	Browse	45.32.115.235
	setup_x86_x64_install.exe	Get hash	malicious	Browse	149.28.253.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	991D4DC612FF80AB2506510DBA31531DB995FE3F64318.exe	Get hash	malicious	Browse	149.28.253.196
	MMUc2aeWxZ.exe	Get hash	malicious	Browse	149.28.253.196
	0pvsj0MF1D.exe	Get hash	malicious	Browse	149.28.253.196
	Linux_amd64	Get hash	malicious	Browse	45.32.162.141
	nkXzJnW7AH.exe	Get hash	malicious	Browse	149.28.253.196
	67MPsax8fd.exe	Get hash	malicious	Browse	136.244.117.138
	Linux_x86	Get hash	malicious	Browse	45.77.44.252
	ul6mJo4TJQ.exe	Get hash	malicious	Browse	149.28.253.196
	ul6mJo4TJQ.exe	Get hash	malicious	Browse	149.28.253.196
	M2jG6lMe7Y.exe	Get hash	malicious	Browse	202.182.120.6
	7LPqKHiPCL.exe	Get hash	malicious	Browse	139.180.133.9
	wvYbWkOPqJ.exe	Get hash	malicious	Browse	149.28.253.196
	wvYbWkOPqJ.exe	Get hash	malicious	Browse	149.28.253.196
EcobandGH	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	196.44.98.190
	gvtdsqavfej.dll	Get hash	malicious	Browse	196.44.98.190
	mhOX6jll6x.dll	Get hash	malicious	Browse	196.44.98.190
	dguQYT8p8j.dll	Get hash	malicious	Browse	196.44.98.190
	jSxlzXfwc7.dll	Get hash	malicious	Browse	196.44.98.190
	mhOX6jll6x.dll	Get hash	malicious	Browse	196.44.98.190
	X2XCewl2Yy.dll	Get hash	malicious	Browse	196.44.98.190
	dguQYT8p8j.dll	Get hash	malicious	Browse	196.44.98.190
	HMvjzUYq2h.dll	Get hash	malicious	Browse	196.44.98.190
	s9BZBDWmi4.dll	Get hash	malicious	Browse	196.44.98.190
	bFx5bZRC6P.dll	Get hash	malicious	Browse	196.44.98.190
	c7IUeh66u6.dll	Get hash	malicious	Browse	196.44.98.190
	HMvjzUYq2h.dll	Get hash	malicious	Browse	196.44.98.190
	s9BZBDWmi4.dll	Get hash	malicious	Browse	196.44.98.190
	bFx5bZRC6P.dll	Get hash	malicious	Browse	196.44.98.190
	WfCt2B042X.dll	Get hash	malicious	Browse	196.44.98.190
	ZKVYER7XcT.dll	Get hash	malicious	Browse	196.44.98.190
	2cq85E4EeM.dll	Get hash	malicious	Browse	196.44.98.190
	WfCt2B042X.dll	Get hash	malicious	Browse	196.44.98.190
	ZKVYER7XcT.dll	Get hash	malicious	Browse	196.44.98.190

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	51.178.61.60
	fehivK2JSx.dll	Get hash	malicious	Browse	51.178.61.60
	kQ9HU0gKVH.exe	Get hash	malicious	Browse	51.178.61.60
	gvtdsqavfej.dll	Get hash	malicious	Browse	51.178.61.60
	mhOX6jll6x.dll	Get hash	malicious	Browse	51.178.61.60
	dguQYT8p8j.dll	Get hash	malicious	Browse	51.178.61.60
	jSxlzXfwc7.dll	Get hash	malicious	Browse	51.178.61.60
	mhOX6jll6x.dll	Get hash	malicious	Browse	51.178.61.60
	X2XCewl2Yy.dll	Get hash	malicious	Browse	51.178.61.60
	dguQYT8p8j.dll	Get hash	malicious	Browse	51.178.61.60
	date1%3fBNLv65=pAAS.dll	Get hash	malicious	Browse	51.178.61.60
	HMvjzUYq2h.dll	Get hash	malicious	Browse	51.178.61.60
	s9BZBDWmi4.dll	Get hash	malicious	Browse	51.178.61.60
	bFx5bZRC6P.dll	Get hash	malicious	Browse	51.178.61.60
	c7IUeh66u6.dll	Get hash	malicious	Browse	51.178.61.60
	HMvjzUYq2h.dll	Get hash	malicious	Browse	51.178.61.60
	s9BZBDWmi4.dll	Get hash	malicious	Browse	51.178.61.60
	bFx5bZRC6P.dll	Get hash	malicious	Browse	51.178.61.60
	WfCt2B042X.dll	Get hash	malicious	Browse	51.178.61.60
	ZKVYER7XcT.dll	Get hash	malicious	Browse	51.178.61.60

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.7859159976425
TrID:	- Win32 Dynamic Link Library (generic) (1002004/3) 95.51% - InstallShield setup (43055/19) 4.10% - Generic Win/DOS Executable (2004/3) 0.19% - DOS Executable Generic (2002/1) 0.19% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	spZRMihlrkFGqYq1f.dll
File size:	712704
MD5:	9f4fa905fd685d28c4ff28f24ad224a1
SHA1:	e186e0869276d3af6465d7c754b22527c7ac2ced
SHA256:	808e8247efd685bdbae3ea0e55de1e8ed8aecdd1359a213b0c6291b73f007fdaf
SHA512:	d8c33eb38fe54e40d463f20b6091c88863f0fadc70382ad826d7c33e61d696af614e9ba8c73f84d4e13fb141289d5bd978451a5565f61e869a054a837fdef5e0
SSDEEP:	12288:WKEUkuAOLka1miSmuYr1V7nAobS3qTHPR101D:TEQLka1nBVDAoS3WvR
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$......Y.V.8... 8...8..I7...8..I7...8...8.....8.....48.....8.....8..... 8.....8..Rich.8.....PE..L...(.a...

File Icon

	
Icon Hash:	be71f1aca0b8c0c4

Static PE Info

General	
Entrypoint:	0x1003d301
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x61A0C528 [Fri Nov 26 11:29:44 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	d8c52655a835ecb2c6fea489c7c7674b

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x566b7	0x57000	False	0.574984846444	data	6.6363911364	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x58000	0x188de	0x19000	False	0.30236328125	data	4.88012998463	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x71000	0x2a254	0x27000	False	0.931434044471	data	7.84888321435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x9c000	0x9af8	0xa000	False	0.241723632813	data	3.85640321845	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa6000	0xbd48	0xc000	False	0.347106933594	data	4.87718770475	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-16:12:03.931139	TCP	2404336	ET CNC Feodo Tracker Reported CnC Server TCP group 19	49775	443	192.168.2.4	51.178.61.60

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 51.178.61.60

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49750	51.178.61.60	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-01 15:28:27 UTC	0	OUT	GET /lJkHjHYuxCdTZukielYhLRnUuQlzcYbcaXcjoFrjtLCdYogUVaLxnRUqnklmC HTTP/1.1 Cookie: PAQTVIsSYfud=hHS8zfpj4oGmf1BJz19EG4wtDXynDl0rFeTsdmFttAYml0/MBamrj2Ji1+m2lK4MZXHf5 PYTXhyurxVEhCtf5E7CksirazP0eBUw+b8Gls8/rWhl4ppyDek9yadBnYnu/OP7jMcO7nFENCnAGjQgt+FpnxDYohm 38NGKWKj6N/ZfzNCIL0fOql6yiXb5Neq5AZNKM6b8yrT50ZGNxEJw32EAn5oFjwpC2CybO6ZMM4S0eF/K8HS28PVDh odiRcpBkFM= Host: 51.178.61.60 Connection: Keep-Alive Cache-Control: no-cache
2021-12-01 15:28:27 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 01 Dec 2021 15:28:27 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2021-12-01 15:28:27 UTC	0	IN	Data Raw: 33 36 39 0d 0a 2b 2b 07 97 7b 00 e6 e2 9e fa d5 16 b4 e8 42 19 69 9c 55 49 1e 25 02 b8 95 be b2 02 17 d4 62 16 09 8c f1 e3 7d 31 b7 50 fd 58 c3 60 ed 15 b2 c6 93 dc 68 3a 0c b9 ce 3f 7a 50 3c 34 52 1d eb 28 dd 4a 64 36 e8 92 17 ae 01 ff bc 5e 30 24 dc 50 19 15 83 94 72 df 92 ad ac 4e 97 25 08 47 75 1f 69 fe 1e 69 70 75 52 00 8d 9d 1e d5 5e 61 4d 97 69 cb 4a 5c bb 54 d8 04 e3 26 37 d2 38 32 03 a4 11 21 ea e6 fd 47 f3 de 40 87 81 fe 5e 5e 8f 74 7e c9 04 e5 20 55 38 9e 5b 84 2b a1 03 ae 84 c2 ca 9b dc 2e 70 03 80 a2 e5 40 84 3e 09 68 95 e7 fe 44 7c 60 ff 84 1c d1 9f 49 f5 e7 7a 4c c2 c3 68 a0 be c7 91 5c 40 d9 3e 43 06 33 bd 0f fa 2d 76 61 a0 68 60 23 cf 33 75 e9 da 9a 83 8f bd cf 35 e8 8d 02 74 a9 eb eb c5 b1 9a 93 ab 92 ae 0a 8f 63 98 e5 73 13 92 26 56 5f Data Ascii: 369++{BiUI%b}1PX`h:?zP<4R(Jd6^0\$PrN%GuiipuR^aMiJlT&782!G@^t~ U8[+.p@>hDl'IzLh\@>C3-vah` #3u5tcs&V_

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6748 Parent PID: 2988

General

Start time:	16:28:14
Start date:	01/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1df.dll"
Imagebase:	0x300000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6740 Parent PID: 6748

General

Start time:	16:28:15
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll",#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3DBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

[Show Windows behavior](#)

Analysis Process: rundll32.exe PID: 5572 Parent PID: 6748

General

Start time:	16:28:15
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll,Control_RunDLL
Imagebase:	0x840000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.295708086.0000000004470000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.296174836.0000000004BE1000.00000020.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.296473938.0000000004F10000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.296324799.0000000004D81000.00000020.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.296432898.0000000004DE1000.00000020.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.296540541.0000000004F41000.00000020.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.296066491.0000000004B01000.00000020.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.296034357.0000000004AD0000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.295759130.00000000044A1000.00000020.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.296271084.0000000004D50000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.296143062.0000000004BB0000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.296388886.0000000004DB0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

[Show Windows behavior](#)

Analysis Process: rundll32.exe PID: 5376 Parent PID: 6740

General

Start time:	16:28:15
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll",#1
Imagebase:	0x840000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.294421724.0000000002CA0000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.294515907.0000000002D61000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 5144 Parent PID: 572

General

Start time:	16:28:15
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
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

Show Windows behavior

Analysis Process: rundll32.exe PID: 5392 Parent PID: 5376

General

Start time:	16:28:16
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\spZRMihlrkFGqYq1f.dll",Control_RunDLL
Imagebase:	0x840000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 4008 Parent PID: 5572

General

Start time:	16:28:16
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Thkptzplbxyirts.twn",wJPKT
Imagebase:	0x840000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.299095986.0000000002B50000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.299196346.00000000044A1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5348 Parent PID: 4008

General

Start time:	16:28:17
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Thkptzplbxyirts.twn",Control_RunDLL
Imagebase:	0x840000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:

- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.687143531.00000000048A0000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.686773719.0000000002E80000.00000040.00000010.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.688356150.0000000005391000.00000020.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.686844140.0000000002EB1000.00000020.00000010.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.687491386.0000000004FD0000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.688282448.0000000005360000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.688116591.00000000052A1000.00000020.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.687565744.0000000005001000.00000020.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.687927978.0000000005210000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.688520704.0000000005480000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.687727344.00000000050B0000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.689006243.00000000055C1000.00000020.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.687967360.0000000005241000.00000020.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.687815211.00000000050E1000.00000020.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.687213898.00000000049D1000.00000020.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.688892944.0000000005590000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.688613212.00000000054B1000.00000020.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.688043473.0000000005270000.00000040.00000001.sdmp, Author: Joe Security

Reputation:

high

Analysis Process: svchost.exe PID: 6668 Parent PID: 572

General

Start time:	16:28:36
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
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

Show Windows behavior

Analysis Process: svchost.exe PID: 6712 Parent PID: 572

General

Start time:	16:28:54
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

[Show Windows behavior](#)

Analysis Process: svchost.exe PID: 3928 Parent PID: 572

General

Start time:	16:29:05
Start date:	01/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

[Show Windows behavior](#)

Disassembly

Code Analysis