

ID: 626490
Sample Name: wgJ5YjI2QO
Cookbook: default.jbs
Time: 04:43:15
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report wgJ5YjI2QO 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
E-Banking Fraud 5
Hooking and other Techniques for Hiding and Protection 5
HIPS / PFW / Operating System Protection Evasion 5
Stealing of Sensitive Information 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
Public IPs 10
Private 11
General Information 11
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\ProgramData\Microsoft\Network\Downloader\edb.chk 12
C:\ProgramData\Microsoft\Network\Downloader\edb.log 12
C:\ProgramData\Microsoft\Network\Downloader\qmgr.db 13
C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm 13
C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp 13
Static File Info 14
General 14
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 14
Rich Headers 16
Data Directories 16
Sections 16
Resources 16
Imports 17
Exports 17
Possible Origin 17
Network Behavior 17
TCP Packets 17
HTTP Request Dependency Graph 18
HTTPS Proxied Packets 18
Statistics 18
Behavior 18
System Behavior 18

Copyright Joe Security LLC 2022

Analysis Process: loaddll64.exePID: 6224, Parent PID: 3108 18
General 19
File Activities 19
Analysis Process: cmd.exePID: 3616, Parent PID: 6224 19
General 19
File Activities 19
Analysis Process: regsvr32.exePID: 4484, Parent PID: 6224 19
General 19
File Activities 20
File Deleted 20
Analysis Process: rundll32.exePID: 5152, Parent PID: 3616 20
General 20
File Activities 20
Analysis Process: rundll32.exePID: 3484, Parent PID: 6224 20
General 20
File Activities 21
Analysis Process: rundll32.exePID: 6088, Parent PID: 6224 21
General 21
File Activities 21
Analysis Process: regsvr32.exePID: 5780, Parent PID: 4484 21
General 21
Analysis Process: svchost.exePID: 4776, Parent PID: 580 22
General 22
File Activities 22
Analysis Process: svchost.exePID: 7008, Parent PID: 580 22
General 22
File Activities 22
Registry Activities 22
Analysis Process: svchost.exePID: 6756, Parent PID: 580 22
General 22
Analysis Process: svchost.exePID: 6936, Parent PID: 580 23
General 23
File Activities 23
Analysis Process: svchost.exePID: 3240, Parent PID: 580 23
General 23
File Activities 23
Disassembly 24

Copyright Joe Security LLC 2022

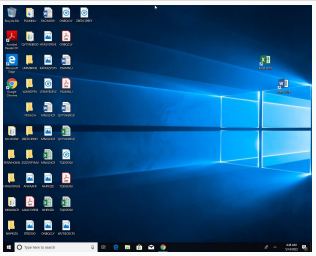
Windows Analysis Report

wgJ5YjI2QO

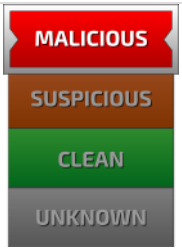
Overview

General Information

Sample Name:	wgJ5YjI2QO (renamed file extension from none to dll)
Analysis ID:	626490
MD5:	992ff50bf2c751a..
SHA1:	8749e61cf3e6a1..
SHA256:	9247ea9d5a188b.
Tags:	exe
Infos:	



Detection



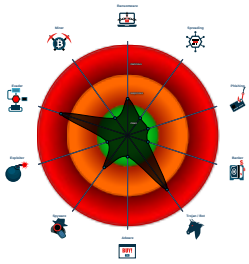
Emotet

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query local…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6224 cmdline: loaddll64.exe "C:\Users\user\Desktop\wgJ5YjI2QO.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 3616 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\wgJ5YjI2QO.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5152 cmdline: rundll32.exe "C:\Users\user\Desktop\wgJ5YjI2QO.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 4484 cmdline: regsvr32.exe /s C:\Users\user\Desktop\wgJ5YjI2QO.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 5780 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\OtCXm\kDbCLHDWWfGFPvP.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 3484 cmdline: rundll32.exe C:\Users\user\Desktop\wgJ5YjI2QO.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6088 cmdline: rundll32.exe C:\Users\user\Desktop\wgJ5YjI2QO.dll,DllUnregisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 4776 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7008 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6756 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6936 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3240 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.954962670.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000002.00000002.443887787.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.443280706.0000000000CD0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.954819708.00000000016F0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.440671277.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.20bbfb80000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.cd0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.20bbfb80000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.14421ca0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.cd0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Networking



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

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



Copyright Joe Security LLC 2022

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

Stealing of Sensitive Information



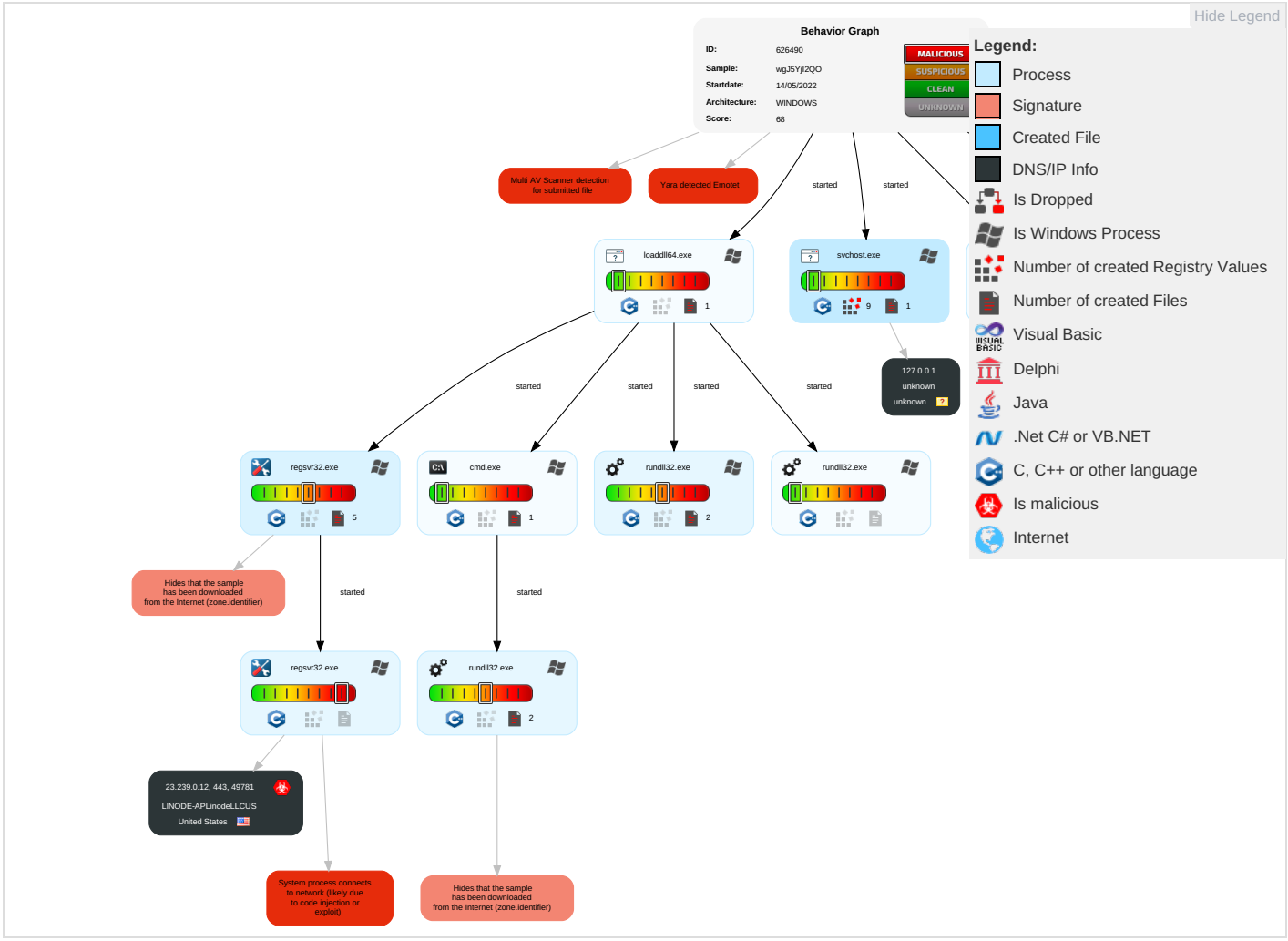
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Native API	1 DLL Side-Loading	1 1 1 Process Injection	2 Masqueradi ng	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communic ation	Remotely Track Device Without Authorizati on	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initializatio n Scripts	1 DLL Side-Loading	3 Virtualizatio n/Sandbox Evasion	LSASS Memory	3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati on	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 1 Process Injection	Security Account Manager	3 Virtualizatio n/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Hidden Files and Directories	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic ation		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.commo n	Rc.commo n	1 Regsvr32	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic ation	Jamming or Denial of Service		Abuse Accessibilit y Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Rundll32	DCSync	3 4 System Information Discovery	Windows Remote Manageme nt	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromis e	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passw d and /etc/shado w	System Network Connection s Discovery	Software Deploymen t Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph

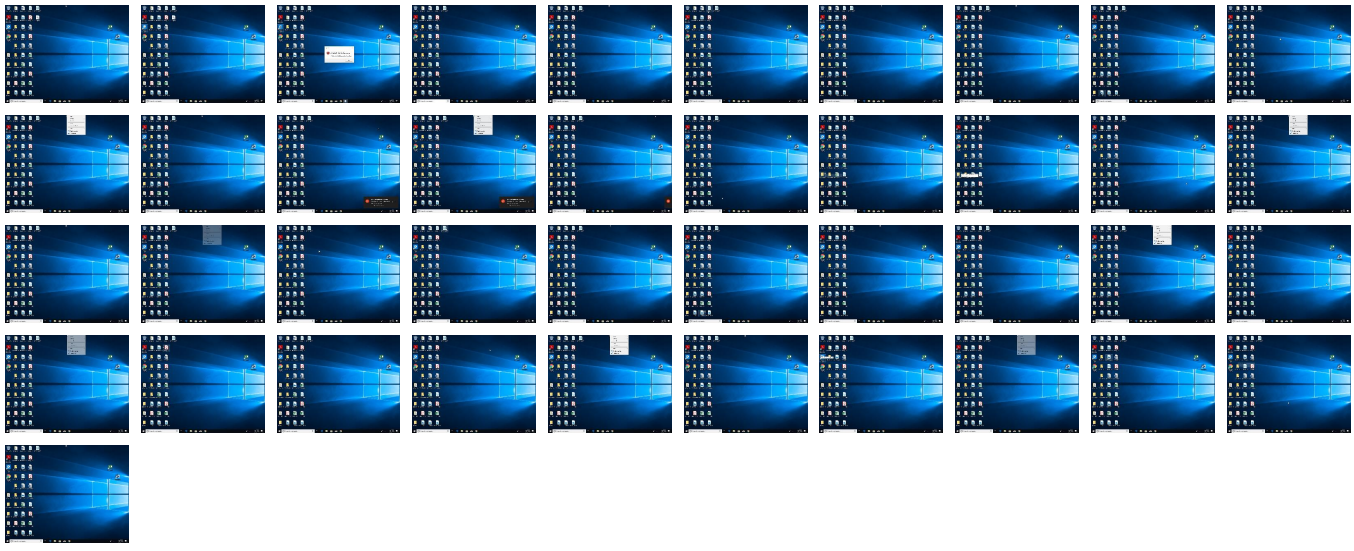
Copyright Joe Security LLC 2022



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
wgJ5YjI2QO.dll	33%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.regsvr32.exe.16f0000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
2.2.regsvr32.exe.cd0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
4.2.rundll32.exe.14421ca0000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
3.2.rundll32.exe.20bbfb80000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Domains

No Antivirus matches

Copyright Joe Security LLC 2022

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://23.239.0.12/	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://displaycatalog.mp.microsoft.c80	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

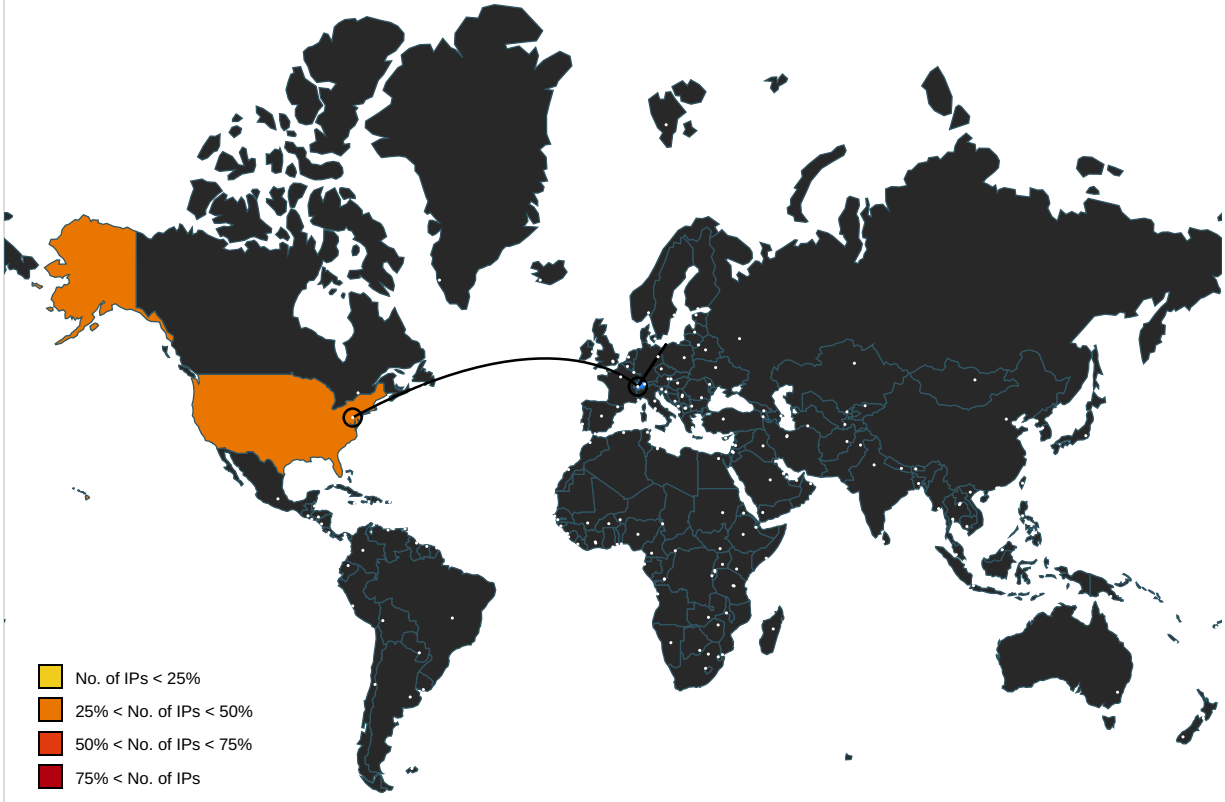
Name	Malicious	Antivirus Detection	Reputation
http://https://23.239.0.12/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000014.00000003.605344196.00000274D579C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000014.00000003.605344196.00000274D579C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/add	svchost.exe, 0000000C.00000002.838489492.000001D309AAB000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.837858257.000001D309AAB000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000014.00000003.601453935.00000274D5C03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.601437795.00000274D5C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.601485120.00000274D5797000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.601523433.00000274D5C19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.601499676.00000274D57A8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000014.00000003.601453935.00000274D5C03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.601437795.00000274D5C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.601485120.00000274D5797000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.601523433.00000274D5C19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.601499676.00000274D57A8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 00000014.00000003.605344196.00000274D579C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.ver)	svchost.exe, 0000000C.00000002.838642334.000001D30F200000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000002.631504398.00000274D5700000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://schemas.xmlsoap.org/ws/200	svchost.exe, 0000000C.00000002.838489492.000001D309AAB000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.837858257.000001D309AAB000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000014.00000003.609918954.00000274D579C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.609817579.00000274D57B2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.609976186.00000274D5C02000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://help.disneyplus.com.	svchost.exe, 00000014.00000003.605344196.00000274D579C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.hotspotshield.com/	svchost.exe, 00000014.00000003.601453935.00000274D5C03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.601437795.00000274D5C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.601485120.00000274D5797000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.601523433.00000274D5C19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.601499676.00000274D57A8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://displaycatalog.mp.microsoft.c80	svchost.exe, 00000014.00000003.615971807.00000274D5798000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000003.615953752.00000274D5796000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.239.0.12	unknown	United States		63949	LINODE-APLinodeLLCUS	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626490
Start date and time: 14/05/202204:43:15	2022-05-14 04:43:15 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wgJ5YjI2QO (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:	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:	mal68.troj.evad.winDLL@18/5@0/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 23.211.4.86, 20.223.24.244
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:44:57	API Interceptor	11x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\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):	0.24946962319269955
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4c:BJiRdwfu2SRU4c
MD5:	32EF2FF8D05346BB0D8D298C6644D0D9
SHA1:	E4BC04F4E139F376FF2C2F71BEADB23396010E23
SHA-256:	E347B9C55DAFFD58891C49772F0E19FBB33525C56B1C98FF4E77E887CC9ADE94
SHA-512:	F040CD4003EB9352EEBA25206F9616FD9E1C223B32553152D1915135EAC9FA7412738AD1EB78E3C86B1DB8A43DECA90C4987F979DB97A122D6B675B3E55FD46 A

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 0x5e833448, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2507041109602366
Encrypted:	false
SSDEEP:	384:MX9+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:MX+SB2nSB2RSjlK/+mLesOj1J2
MD5:	2F397D2DC895EDFA07D3CEE83A048EB6
SHA1:	2663B543480FD24500D6082A82BF577BF49FD0F3
SHA-256:	C19C1543E2305DF87BD75D70BC4997A26C44C0D78BC2F524E7A3738011FCF245
SHA-512:	31FB9847C2057309DF42E5D738C72E3E1DC1F3068999D508488E85BF85484606D87789CD7CF02D9B7B6DC4584D9D1BFA48E14F0059FFAE3859A2317D6280F60A
Malicious:	false
Preview:	^.4H... .....e.f.3...w.....).....0...z..9,...z..h.(.....0...z....).....3...w.....B.....@.....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07642731022417973
Encrypted:	false
SSDEEP:	3:xlD7vcJLuHlllGu0TCaUhI0fXlll/cL0MlllAll3VkttlmlnI:rrcFuNGu0TCaMX/lkwEA3
MD5:	DCE4A90E68BF0410805B9AEE469DBAA7
SHA1:	887CFBEC263EADB584A9A982FDCC0B12B15CD2E9
SHA-256:	C6B2803EB4806513E1EBF3F52E0F8D4879A7F4F04540670F96693D8C1129CF
SHA-512:	B26F61E8CD53AD7470A431356FC6693A3D51C9E7C6DADB7401D6F53696EDE0DB1DCA5D42C173FD0F534B0200F0C576A1794E5D472ECA8ACE11B762E3AFD4886
Malicious:	false
Preview:	.\.....3...w..9,...z...0...z.....0...z...0...z...D.i.0...z.g.....D8.0...z.....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.482093403616071
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	wgJ5YjI2QO.dll
File size:	545280
MD5:	992ff50bf2c751ac906a6868da38b4fb
SHA1:	8749e61cf3e6a151b15fdc6d0a01c1966d254dc4
SHA256:	9247ea9d5a188b6291f4093eb6fff8ac231c3ea72df8f21d4d227c3499d99c8c
SHA512:	86b368cfa1c46d169e189e967be0f5d717088d67a0e7748cc28c68f43fe7239026669c250de4c59ea5759128a90b3c44aa12e300b01e205da45d381b1030c055
SSDEEP:	12288:B4UJY9B+TenWsSEPHjMOUP9uXdt7JpfYNVr9RM54RutCTdJGqIoTCZ4eEsZDHxHy:B4UJY9BSenZSEPHjMOUP9Udt7JpfYNVj
TLSH:	B5C4CFA5435C08FCE762C3395C975BC5B1F7BDAE0664AF260BC18DA05E1BA90F53A381
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2.H.v.&.v.&.v.&.h...o.&.h...2.&.h.....&.Q6].s.&.v.'.9.&.h...w.&.h...w.&.h...w.&.h...w.&.Richv.&.....PE..d.....}b....."

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1800423a8
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627D8598 [Thu May 12 22:09:28 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	b268dbaa2e6eb6acd16e04d482356598

Entrypoint Preview

Instruction
dec eax
mov dword ptr [esp+08h], ebx
dec eax
mov dword ptr [esp+10h], esi
push edi
dec eax
sub esp, 20h
dec ecx
mov edi, eax
mov ebx, edx
dec eax

Instruction
mov esi, ecx
cmp edx, 01h
jne 00007F2E18A30277h
call 00007F2E18A32404h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007F2E18A30120h
int3
int3
int3
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 00000088h
dec eax
lea ecx, dword ptr [00014D05h]
call dword ptr [0000FC7Fh]
dec esp
mov ebx, dword ptr [00014DF0h]
dec esp
mov dword ptr [esp+58h], ebx
inc ebp
xor eax, eax
dec eax
lea edx, dword ptr [esp+60h]
dec eax
mov ecx, dword ptr [esp+58h]
call 00007F2E18A3EDFAh
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007F2E18A302B3h
dec eax
mov dword ptr [esp+38h], 00000000h
dec eax
lea eax, dword ptr [esp+48h]
dec eax
mov dword ptr [esp+30h], eax
dec eax
lea eax, dword ptr [esp+40h]
dec eax
mov dword ptr [esp+28h], eax
dec eax
lea eax, dword ptr [00014CB0h]
dec eax
mov dword ptr [esp+20h], eax
dec esp
mov ecx, dword ptr [esp+50h]

Instruction
dec esp
mov eax, dword ptr [esp+58h]
dec eax
mov edx, dword ptr [esp+60h]
xor ecx, ecx
call 00007F2E18A3EDA8h
jmp 00007F2E18A30294h
dec eax
mov eax, dword ptr [eax+eax+00000000h]

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x55cf0	0x6f	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5544c	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5a000	0x2dffc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x59000	0xe1c	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0x1d8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x52000	0x288	.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	0x504ca	0x50600	False	0.389081940124	zlib compressed data	5.26882252971	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x52000	0x3d5f	0x3e00	False	0.355342741935	data	5.39322725931	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x56000	0x20d8	0x1200	False	0.180772569444	data	2.18161586025	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x59000	0xe1c	0x1000	False	0.44580078125	data	4.98556265168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x5a000	0x2dffc	0x2e000	False	0.839408542799	data	7.73448363752	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0x6f8	0x800	False	0.1796875	data	1.81179169858	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x5a0a0	0x2de00	data	English	United States
RT_MANIFEST	0x87ea0	0x15a	ASCII text, with CRLF line terminators	English	United States

Name	RVA	Size	Type	Language	Country

Imports

DLL	Import
KERNEL32.dll	ExitProcess, VirtualAlloc, CompareStringW, CompareStringA, GetTimeZoneInformation, GetLocaleInfoW, GetCurrentThreadId, FlsSetValue, GetCommandLineA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RtlVirtualUnwind, RtlLookupFunctionEntry, RtlCaptureContext, EncodePointer, DecodePointer, TlsAlloc, FlsGetValue, FlsFree, SetLastError, GetLastError, GetCurrentThread, FlsAlloc, HeapFree, Sleep, GetModuleHandleW, GetProcAddress, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, HeapSetInformation, HeapCreate, HeapDestroy, RtlUnwindEx, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, LeaveCriticalSection, FatalAppExitA, EnterCriticalSection, HeapAlloc, HeapReAlloc, WriteFile, SetConsoleCtrlHandler, FreeLibrary, LoadLibraryA, InitializeCriticalSectionAndSpinCount, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetDateFormatA, GetTimeFormatA, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, HeapSize, SetEnvironmentVariableA
ole32.dll	CoTaskMemFree, CoLoadLibrary, CoTaskMemAlloc

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x180042050
DllUnregisterServer	2	0x180042080

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 04:45:02.566709042 CEST	49781	443	192.168.2.5	23.239.0.12
May 14, 2022 04:45:02.566776037 CEST	443	49781	23.239.0.12	192.168.2.5
May 14, 2022 04:45:02.566884041 CEST	49781	443	192.168.2.5	23.239.0.12
May 14, 2022 04:45:02.628936052 CEST	49781	443	192.168.2.5	23.239.0.12
May 14, 2022 04:45:02.628978968 CEST	443	49781	23.239.0.12	192.168.2.5
May 14, 2022 04:45:03.181308985 CEST	443	49781	23.239.0.12	192.168.2.5
May 14, 2022 04:45:03.181428909 CEST	49781	443	192.168.2.5	23.239.0.12
May 14, 2022 04:45:04.844511032 CEST	49781	443	192.168.2.5	23.239.0.12
May 14, 2022 04:45:04.844538927 CEST	443	49781	23.239.0.12	192.168.2.5
May 14, 2022 04:45:04.845127106 CEST	443	49781	23.239.0.12	192.168.2.5
May 14, 2022 04:45:04.845257998 CEST	49781	443	192.168.2.5	23.239.0.12
May 14, 2022 04:45:04.902632952 CEST	49781	443	192.168.2.5	23.239.0.12
May 14, 2022 04:45:04.944499969 CEST	443	49781	23.239.0.12	192.168.2.5
May 14, 2022 04:45:05.750308990 CEST	443	49781	23.239.0.12	192.168.2.5
May 14, 2022 04:45:05.750387907 CEST	443	49781	23.239.0.12	192.168.2.5
May 14, 2022 04:45:05.750457048 CEST	49781	443	192.168.2.5	23.239.0.12
May 14, 2022 04:45:05.750467062 CEST	49781	443	192.168.2.5	23.239.0.12
May 14, 2022 04:45:05.751250029 CEST	49781	443	192.168.2.5	23.239.0.12
May 14, 2022 04:45:05.751271963 CEST	443	49781	23.239.0.12	192.168.2.5

Copyright Joe Security LLC 2022

HTTP Request Dependency Graph

- 23.239.0.12

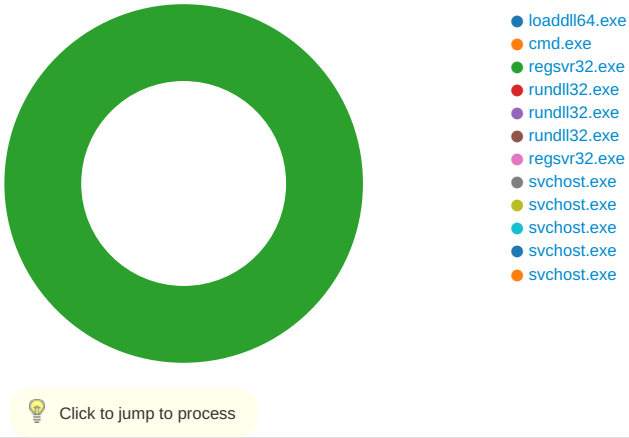
HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49781	23.239.0.12	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-14 02:45:04 UTC	0	OUT	GET / HTTP/1.1 Cookie: hqoLHvQpnIKdNGY=PI8Ba+HxAKZ/qXLx9rdDpMwdvd1nhNOE1SFzlXOV4/tvzdwRLHEf1ffDqNRnRPcaQ+/dPQgztq4zaPQwQMEKCr89yRo55tWlopOHIh4c1sWBFgHAJE59xl12hnl+45N8lUtiK+hQu9WrOpOVnd4QsFj0ablmTL/ka2lX4KtzuTFTG134Dsw221JVmRYDOjCewR9DI811niTKWrRZh17hYCeWgfxCDlUA8+Tb2t6jwKFVQYhPTAEHETiWzGU= Host: 23.239.0.12 Connection: Keep-Alive Cache-Control: no-cache
2022-05-14 02:45:05 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 14 May 2022 02:45:05 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2022-05-14 02:45:05 UTC	0	IN	Data Raw: 33 33 35 0d 0a 60 5b 05 c1 2b 34 44 6a 11 1d 48 2d 9b 19 e8 27 a5 1f d5 57 d9 3b db 21 eb 45 f5 0d e4 4e 0e 66 4b 76 8e a1 6d bf fb c4 3d 8b 6c 97 4f fa f5 db 2c 5c 61 9a 54 56 f1 52 a9 e0 be 38 fa 9a 05 42 58 bc f5 27 7e 95 88 52 18 44 97 5b 9a 1b bb d1 e6 c3 26 5c 41 b0 6f 0b 47 50 ad 98 02 e3 3e 5d f3 a9 1a 00 ee 4c 50 e9 82 50 2c 4a a0 1b 98 e5 39 a9 dd 15 81 8f d8 31 50 84 f3 9f f6 4f 15 4d b2 59 45 af 62 75 1e 82 15 19 27 ab f9 97 1e dc cd 60 24 22 79 e0 b2 10 ec ee 82 03 37 0e 49 c4 f1 86 60 dc de aa 89 cd e0 13 7d af cc 8f b5 a9 88 ed dc 4f 42 ae c2 6e 79 20 f1 f0 77 b4 19 aa 86 30 3f 99 55 3d eb 30 bf 77 f2 0e bf 11 0e 3a 74 f7 75 1d ab 39 e9 3e 8f a0 45 37 22 1e 8e d8 6d e0 a2 e9 8e 9e 49 7a 8e f3 4f f8 51 f6 4c 77 b3 84 06 a5 73 2e 0c dc 6a b8 Data Ascii: 335`[+4DjH-'W;!ENfKvm=lO,\aTVR8BX'~RD[&\AoGP>]LPP,J91POMYEbu`$"y7I`}OBny w0?U=0w:tu9>E7 "mIzOQLws.j

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **6224**, Parent PID: **3108**

Copyright Joe Security LLC 2022

General	
Target ID:	0
Start time:	04:44:28
Start date:	14/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\wgJ5YjI2QO.dll"
Imagebase:	0x7ff7bf0e0000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 3616, Parent PID: 6224

General	
Target ID:	1
Start time:	04:44:29
Start date:	14/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\wgJ5YjI2QO.dll",#1
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 4484, Parent PID: 6224

General	
Target ID:	2
Start time:	04:44:29
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\wgJ5YjI2QO.dll
Imagebase:	0x7ff6a18a0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.443887787.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.443280706.0000000000CD0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\OtCXm\kDbCLHDWWfGFPvP.dll:Zone.Identifier	success or wait	1	180009356	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: 5152, Parent PID: 3616

General

Target ID:	3
Start time:	04:44:29
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\wgJ5YjI2QO.dll",#1
Imagebase:	0x7ff69a820000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.440671277.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.441125052.0000020BBFB80000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3484, Parent PID: 6224

General

Target ID:	4
Start time:	04:44:29
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\wgJ5YjI2QO.dll,DllRegisterServer
Imagebase:	0x7ff69a820000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true

Copyright Joe Security LLC 2022

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.442354457.0000014421CA0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.440783829.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **6088**, Parent PID: **6224**

General

Target ID:	5
Start time:	04:44:33
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\wgJ5YjI2QO.dll,DllUnregisterServer
Imagebase:	0x7ff69a820000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **5780**, Parent PID: **4484**

General

Target ID:	6
Start time:	04:44:33
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\OtCXm\kDbCLHDWWfGFPvP.dll"
Imagebase:	0x7ff6a18a0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.954962670.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.954819708.00000000016F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: **4776**, Parent PID: **580**

General

Target ID:	10
Start time:	04:44:51
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **7008**, Parent PID: **580**

General

Target ID:	12
Start time:	04:44:57
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6756**, Parent PID: **580**

General

Target ID:	13

Start time:	04:45:06
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **6936**, Parent PID: **580**

General

Target ID:	14
Start time:	04:45:15
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **3240**, Parent PID: **580**

General

Target ID:	20
Start time:	04:45:33
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly

Copyright Joe Security LLC 2022