



ID: 626498
Sample Name: 1V4gPPcQvB.dll
Cookbook: default.jbs
Time: 05:13:08
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 1V4gPPcQvB.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 5
Memory Dumps 5
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 6
HIPS / PFW / Operating System Protection Evasion 6
Lowering of HIPS / PFW / Operating System Security Settings 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 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 12
Public IPs 13
Private 13
General Information 13
Warnings 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASNs 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
C:\ProgramData\Microsoft\Network\Downloader\edb.chk 14
C:\ProgramData\Microsoft\Network\Downloader\edb.log 15
C:\ProgramData\Microsoft\Network\Downloader\qmgr.db 15
C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm 15
C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp 16
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log 16
Static File Info 16
General 16
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Rich Headers 18
Data Directories 19
Sections 19
Resources 19
Imports 19
Exports 20
Possible Origin 20
Network Behavior 20
TCP Packets 20
HTTP Request Dependency Graph 20
HTTPS Proxied Packets 20
Statistics 21

Copyright Joe Security LLC 2022

Behavior 21
System Behavior 21
Analysis Process: loaddll64.exePID: 5896, Parent PID: 5844 21
General 21
File Activities 22
Analysis Process: cmd.exePID: 5904, Parent PID: 5896 22
General 22
File Activities 22
Analysis Process: regsvr32.exePID: 4572, Parent PID: 5896 22
General 22
File Activities 22
File Deleted 22
Analysis Process: rundll32.exePID: 3404, Parent PID: 5904 23
General 23
File Activities 23
Analysis Process: rundll32.exePID: 3748, Parent PID: 5896 23
General 23
File Activities 23
Analysis Process: rundll32.exePID: 2364, Parent PID: 5896 24
General 24
File Activities 24
Analysis Process: regsvr32.exePID: 6012, Parent PID: 4572 24
General 24
Analysis Process: svchost.exePID: 2224, Parent PID: 564 24
General 24
Analysis Process: svchost.exePID: 4572, Parent PID: 564 25
General 25
File Activities 25
Registry Activities 25
Analysis Process: svchost.exePID: 4732, Parent PID: 564 25
General 25
Registry Activities 25
Analysis Process: svchost.exePID: 4940, Parent PID: 564 26
General 26
Analysis Process: SgrmBroker.exePID: 1332, Parent PID: 564 26
General 26
Analysis Process: svchost.exePID: 1584, Parent PID: 564 26
General 26
Registry Activities 26
Analysis Process: svchost.exePID: 5076, Parent PID: 564 27
General 27
File Activities 27
Analysis Process: svchost.exePID: 6292, Parent PID: 564 27
General 27
File Activities 27
Analysis Process: svchost.exePID: 6332, Parent PID: 564 27
General 27
File Activities 28
Registry Activities 28
Analysis Process: svchost.exePID: 6832, Parent PID: 564 28
General 28
File Activities 28
Analysis Process: MpCmdRun.exePID: 3452, Parent PID: 1584 28
General 28
File Activities 29
File Written 29
Analysis Process: conhost.exePID: 3820, Parent PID: 3452 30
General 30
Analysis Process: svchost.exePID: 2740, Parent PID: 564 30
General 30
File Activities 31
Analysis Process: svchost.exePID: 6168, Parent PID: 564 31
General 31
File Activities 31
Disassembly 31

Copyright Joe Security LLC 2022

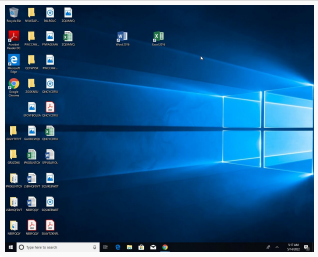
Windows Analysis Report

1V4gPPcQvB.dll

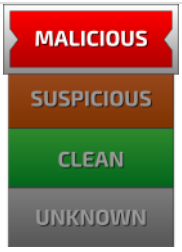
Overview

General Information

Sample Name:	1V4gPPcQvB.dll
Analysis ID:	626498
MD5:	571f80cb1a81ed..
SHA1:	9e12d3add08902.
SHA256:	c117963618d01c..
Tags:	exe trojan
Infos:	



Detection



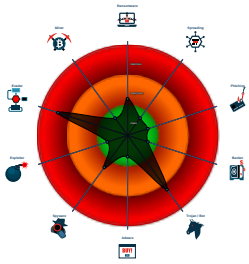
Emotet

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Changes security center settings (n…
- 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…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 5896 cmdline: loaddll64.exe "C:\Users\user\Desktop\1V4gPPcQvB.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 5904 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\1V4gPPcQvB.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 3404 cmdline: rundll32.exe "C:\Users\user\Desktop\1V4gPPcQvB.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 4572 cmdline: regsvr32.exe /s C:\Users\user\Desktop\1V4gPPcQvB.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 6012 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\TvcDyJjJQ\NcAvRfvDRbwLFn.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 3748 cmdline: rundll32.exe C:\Users\user\Desktop\1V4gPPcQvB.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2364 cmdline: rundll32.exe C:\Users\user\Desktop\1V4gPPcQvB.dll,DllUnregisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 2224 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4572 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4732 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4940 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1332 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 1584 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 3452 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 3820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 5076 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6292 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6332 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6832 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2740 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6168 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Copyright Joe Security LLC 2022

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.649155251.0000000000760000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.264793383.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.265168643.0000023396DC0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.649306435.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.264939318.0000020701410000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.20701410000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.22e0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.regsvr32.exe.760000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.22e0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.20701410000.0.raw.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

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Networking



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

E-Banking Fraud



Yara detected Emotet

Copyright Joe Security LLC 2022

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

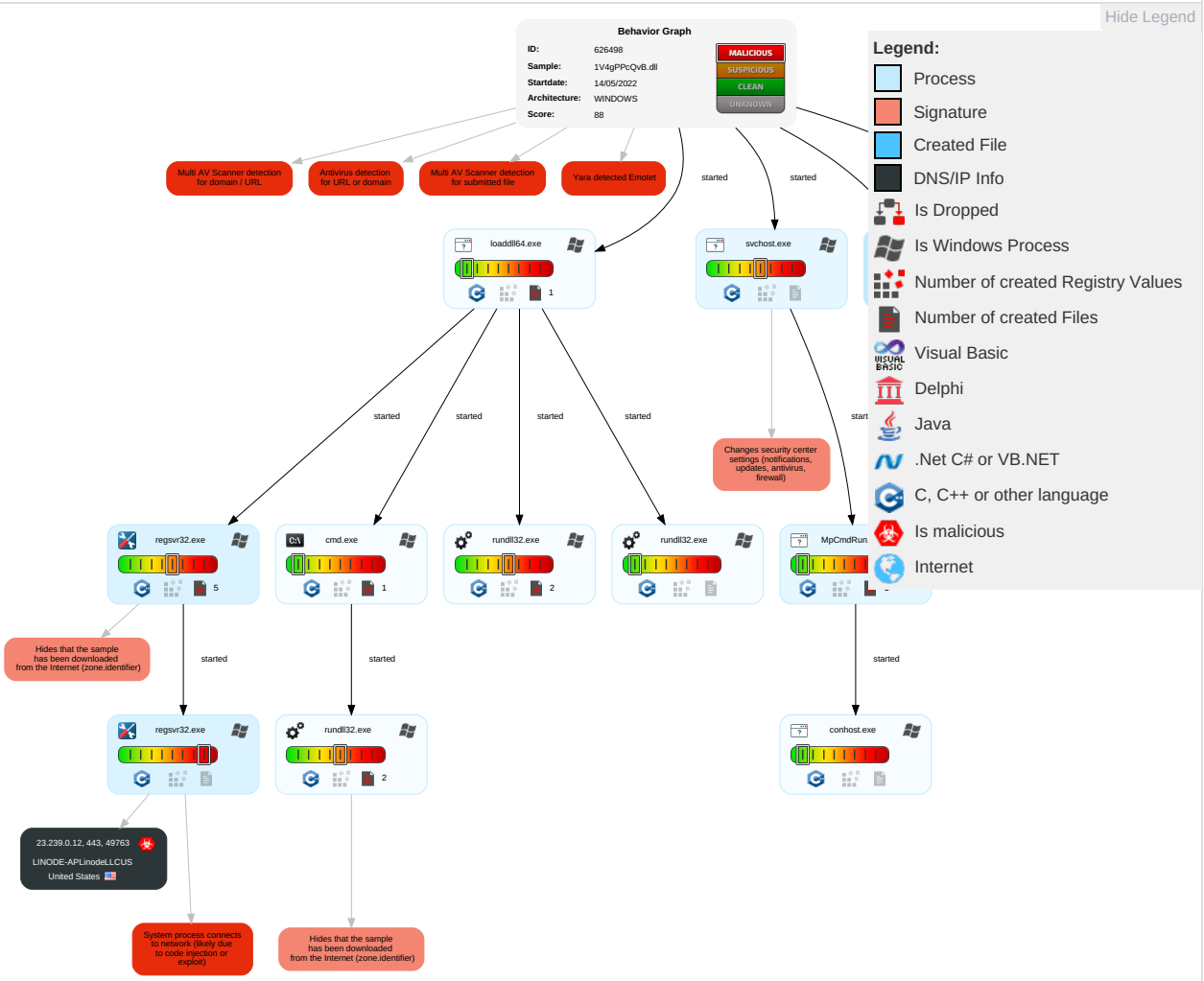


Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	2 1 Masquerading	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 Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	1 Query Registry	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 Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Virtualization/Sandbox Evasion	Security Account Manager	5 1 Security Software Discovery	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 1 1 Process Injection	NTDS	3 Virtualization/Sandbox Evasion	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 Hidden Files and Directories	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Regsvr32	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	3 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

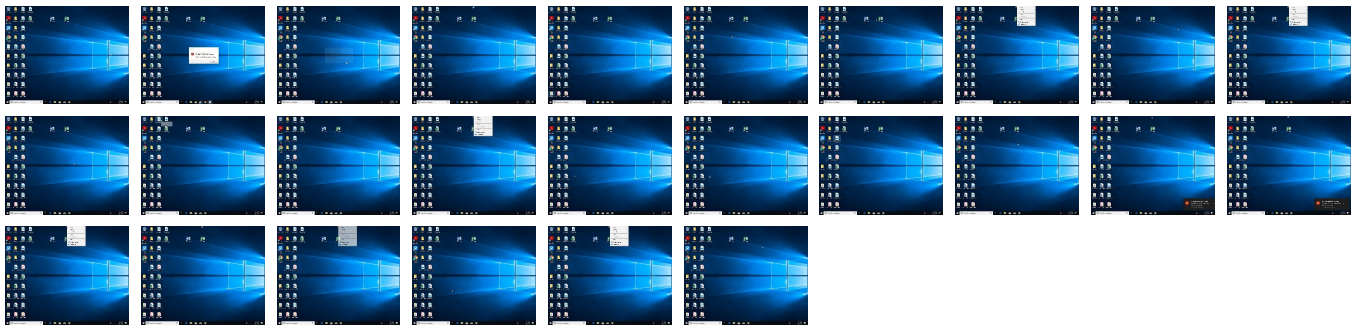
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
1V4gPPcQvB.dll	40%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.22e0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
3.2.rundll32.exe.23396dc0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
6.2.regsvr32.exe.760000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
4.2.rundll32.exe.20701410000.0.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://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	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://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report	0%	URL Reputation	safe	
http://https://23.239.0.12/	0%	URL Reputation	safe	
http://https://23.239.0.12/#mWwn	10%	Virustotal		Browse
http://https://23.239.0.12/#mWwn	100%	Avira URL Cloud	malware	
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://23.239.0.12/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

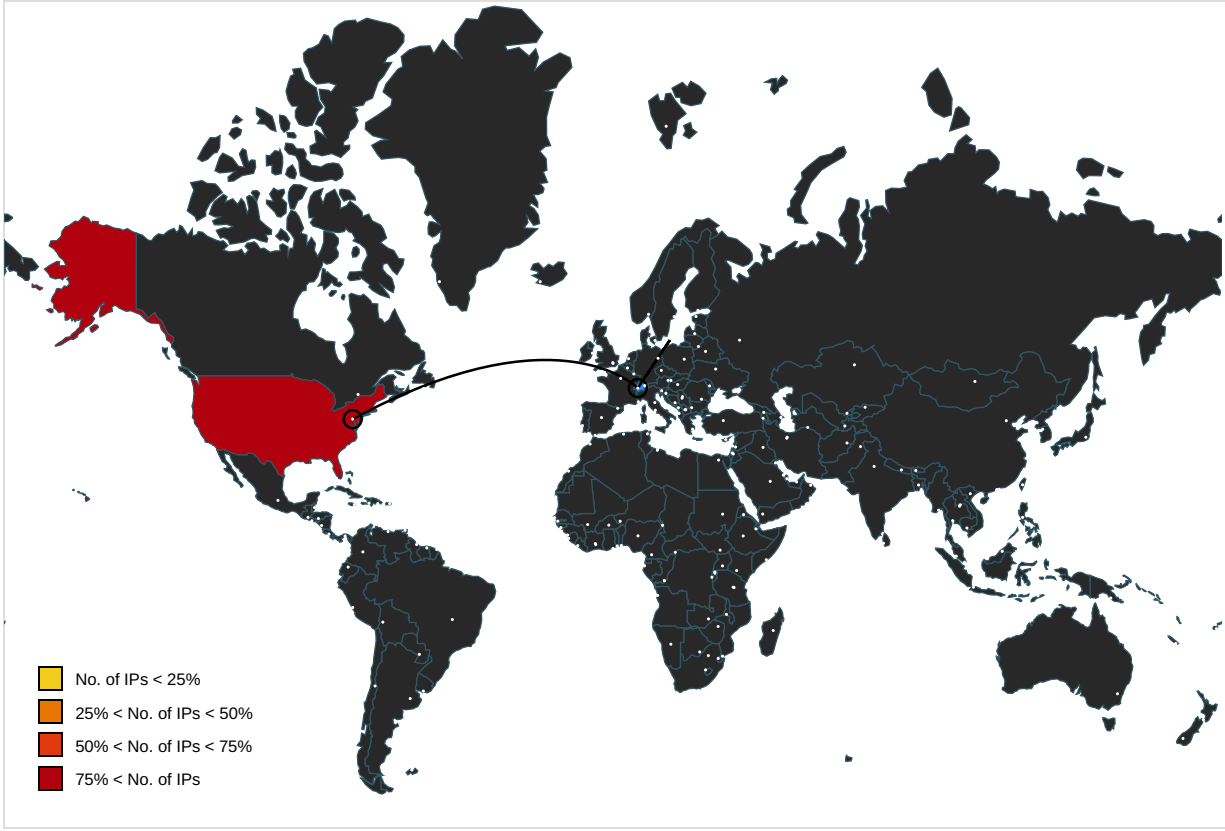
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000D.00000003.317075778.00000243CC461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000001C.00000003.513071382.000001F509775000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000D.00000003.317136899.00000243CC445000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317108861.00000243CC440000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000D.00000002.317469413.00000243CC43D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000D.00000003.317075778.00000243CC461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000D.00000002.317469413.00000243CC43D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000D.00000002.317537582.00000243CC45A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317096728.00000243CC459000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 0000000D.00000002.317551870.00000243CC46A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317069787.00000243CC467000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000D.00000003.317124705.00000243CC447000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.317526098.00000243CC44E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317108861.00000243CC440000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000D.00000002.317469413.00000243CC43D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000D.00000003.317136899.00000243CC445000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317108861.00000243CC440000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000D.00000003.317075778.00000243CC461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ver)	svchost.exe, 00000012.00000002.604912010.000001D2BDC15000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000D.00000002.317537582.00000243CC45A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317108861.00000243CC440000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317096728.00000243CC459000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 0000001C.00000003.516238842.000001F509C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.516180464.000001F5097B0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.516163337.000001F5097B0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.517705075.000001F509775000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.516211178.000001F50979A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000D.00000002.317469413.00000243CC43D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.317375524.00000243CC413000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000D.00000003.317108861.00000243CC440000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317141842.00000243CC441000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.317475430.00000243CC442000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 0000000B.00000002.649002780.000002577343D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000D.00000003.317124705.00000243CC447000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.317526098.00000243CC44E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317108861.00000243CC440000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000D.00000003.317075778.00000243CC461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000D.00000003.295407264.00000243CC432000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000D.00000003.317075778.00000243CC461000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.hotspotshield.com/	svchost.exe, 0000001C.00000003.507378636.000001F509C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.507537378.000001F509C19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.507451898.000001F509C03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.507505148.000001F50979F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.508895507.000001F509775000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.507491854.000001F50978E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000D.00000003.317075778.00000243CC461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000D.00000003.317086705.00000243CC45E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000D.00000003.317108861.00000243CC440000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000D.00000002.317537582.00000243CC45A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317096728.00000243CC459000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000001C.00000003.513071382.000001F509775000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000D.00000002.317537582.00000243CC45A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317096728.00000243CC459000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000D.00000003.317108861.00000243CC440000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317141842.00000243CC441000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.317475430.00000243CC442000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000D.00000002.317542755.00000243CC462000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000D.00000003.317075778.00000243CC461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 0000001C.00000003.507378636.000001F509C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.507537378.000001F509C19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.507451898.000001F509C03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.507505148.000001F50979F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.508895507.000001F509775000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.507491854.000001F50978E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 0000001C.00000003.507378636.000001F509C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.507537378.000001F509C19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.507451898.000001F509C03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.507505148.000001F50979F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.508895507.000001F509775000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.507491854.000001F50978E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://disneyplus.com/legal.	svchost.exe, 0000001C.00000003.513071382.000001F509775000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000D.00000002.317464357.00000243CC43B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.295407264.00000243CC432000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report	svchost.exe, 0000001C.00000003.517705075.000001F509775000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000D.00000002.317537582.00000243CC45A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317096728.00000243CC459000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://23.239.0.12/#mWwn	regsvr32.exe, 00000006.00000002.648685140.0000000000611000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.323873760.0000000000611000.00000004.00000020.00020000.00000000.sdmp	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://activity.windows.com	svchost.exe, 0000000B.00000002.649002780.000002577343D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000D.00000002.317375524.00000243CC413000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000D.00000003.317075778.00000243CC461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://help.disneyplus.com.	svchost.exe, 0000001C.00000003.513071382.000001F509775000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000D.00000002.317469413.00000243CC43D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000B.00000002.649002780.000002577343D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000D.00000002.317537582.00000243CC45A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.317096728.00000243CC459000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000D.00000003.317086705.00000243CC45E000.00000004.00000020.00020000.00000000.sdmp	false		high

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
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626498
Start date and time: 14/05/202205:13:08	2022-05-14 05:13:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1V4gPPcQvB.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:	32
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

Copyright Joe Security LLC 2022

Classification:	mal88.troj.evad.winDLL@28/6@0/2
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:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.4.86, 20.223.24.244
- Excluded domains from analysis (whitelisted): fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, 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, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.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
05:14:50	API Interceptor	1x Sleep call for process: svchost.exe modified
05:15:42	API Interceptor	1x Sleep call for process: MpCmdRun.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):	0.24941056697477726
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4l:BJiRdwfu2SRU4l
MD5:	488F924960085B7C2D0395E842A82D7D
SHA1:	8B4D074CE487424787C3195F60D2FF93A56F5FAE
SHA-256:	A9CAB5C9029C9B54A13A4633AFCCC47C517EA68C5B33844BB68C5EB0552F65A6
SHA-512:	F5AD8E50846F7F5BD8D953D4C91E1F8912ED85EE1A7D7177A32CF2DF3A5DF0FCDEABBD2EE77B1835F59DC2F4299FC1CD3CED5A30811A07AB91822D6A4717 213
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 0xf3be4723, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2505947281197957
Encrypted:	false
SSDEEP:	384:wHF+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:wH2SB2nSB2RSjlK/+mLesOj1J2
MD5:	401F9FDA82394D9257361D0648556E42
SHA1:	B5DE6AFB3A3607C6C595018AF19AE6E4ED9104B3
SHA-256:	57858C0A6694BBA1694B99A95FE3261F3FB482F08BDBE960F404010641B95544
SHA-512:	ACFB9CA25D66D17A8E1567BDFB8B3B3E9BC28E355C7FB68A57686F7E2CF04DC6FEA3EAFE20C884FDBAAAA59674849FC9C5458116EC49D0EFE06A0C3F2F937 1EB
Malicious:	false
Preview:	.G#... .....e.f.3...w.....).....z..2....z..h.(.....z....).....3...w.....B.....@..... ....z.....S..._....z..... .....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07627575078568044

Encrypted:	false
SSDEEP:	3:jAiR7vXyLfFljIllXDjll3Vkttlmlnl:1RrPLZ3
MD5:	AD46B3D923621A198E18F59602FA3B1B
SHA1:	1D2E0C2C0E697D4B13988E027952564187CDB04C
SHA-256:	3009B982A7C478943DEAC8FCEE47B58FB2E5019EC01AFB72AFD72E66AE63471C
SHA-512:	68EC29BB422D2448E68205E6DBBDA421C03BB5878AE3504AA8A63DBA73C053D3D6AE0DB174D5ABEAF4469209CED78DFE582DAFF8DEC8CD2A139F9BD172AE8A0F
Malicious:	false
Preview:	.;z.....3...w..2....z.....z.....z.....z..`%.....z.....S.._.....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"}

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
Category:	modified
Size (bytes):	10844
Entropy (8bit):	3.1623573157832574
Encrypted:	false
SSDEEP:	192:cY+38+DJM+i2Jt+iDQ+yw+f0+rU+0Jtk+EOtF+E7tC+Ewx+m:j+s+i+Z+z+B+c+Y+0g+J+j+1+m
MD5:	2DBAD0BEF1FA818AA001A84E8CBF9285
SHA1:	FF53E14E5BBC3CED407D6FF085B4A74E568A7E18
SHA-256:	269D4E02BB4FB866D1319CF883B6FA735BC4542ED64A446C466909942E01BAB8
SHA-512:	11828F5E49890637768BF83EF9E5B44E9EFC187CF319A48D24D3D0BBEF5A976688EDD1BE7EED5CFE63CB91AAD39AF48A63AA1C3E91F126529ECD4998B80670FE
Malicious:	false
Preview:	.....-.-.-.

MD5:	571f80cb1a81eddf1fb399a4cd96582c
SHA1:	9e12d3add0890234365af3ea43e94ec9b271aaa1
SHA256:	c117963618d01c8c1b37a8dbc31409318e343ae03493569bfa6d66e0ebdf8dbd
SHA512:	c17ffc3ab5c68a2371eb0b92063294756b0df3f235caa18bea538082feb6126202d9389cd2bd362b77ad8ec84b371f33e63879756d07fc2ea99ab80bc48ee4b5
SSDEEP:	12288:B4UJY9B+TenWsSEPHjMOUP9uXdt7JpfYNVr9RM54RutCTdJGqIoTCZ4eEsZTHxHy:B4UJY9BSenZSEPHjMOUP9Udt7JpfYNVH
TLSH:	47C4CFA5435C08FCE762C3395C975BC5B1F7BDAE0664AF260BC18DA05E1BA90F53A381
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
mov esi, ecx
cmp edx, 01h
jne 00007FF974D49EF7h
call 00007FF974D4C084h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]

Instruction
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007FF974D49DA0h
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 00007FF974D58A7Ah
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007FF974D49F33h
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]
dec esp
mov eax, dword ptr [esp+58h]
dec eax
mov edx, dword ptr [esp+60h]
xor ecx, ecx
call 00007FF974D58A28h
jmp 00007FF974D49F14h
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	0.355405745968	data	5.39218584631	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

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

Copyright Joe Security LLC 2022

DLL	Import
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 05:14:51.468854904 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 05:14:51.468904018 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 05:14:51.469100952 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 05:14:51.494986057 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 05:14:51.495014906 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 05:14:52.039237022 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 05:14:52.042095900 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 05:14:52.549948931 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 05:14:52.549968004 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 05:14:52.550399065 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 05:14:52.551075935 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 05:14:52.575092077 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 05:14:52.616496086 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 05:14:53.417742968 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 05:14:53.417864084 CEST	443	49763	23.239.0.12	192.168.2.4
May 14, 2022 05:14:53.417918921 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 05:14:53.417962074 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 05:14:53.455240965 CEST	49763	443	192.168.2.4	23.239.0.12
May 14, 2022 05:14:53.455270052 CEST	443	49763	23.239.0.12	192.168.2.4

HTTP Request Dependency Graph

- 23.239.0.12

HTTPS Proxied Packets

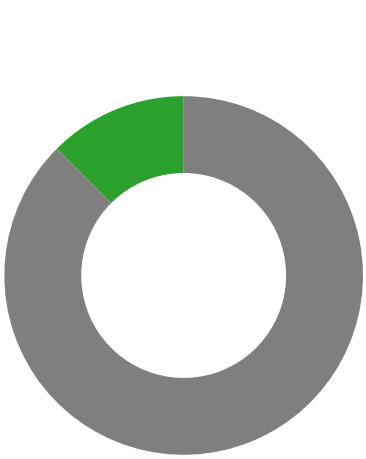
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49763	23.239.0.12	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-14 03:14:52 UTC	0	OUT	GET / HTTP/1.1 Cookie: hlRJjqHMHdV=nZwxi8WPWIMXNXTCUv3V5ewCiVaqak0UnFrOh9HPxFaBO28go/9+xWRpiaD+OvdLdpaS3K mMe0NROXF7P/v2uFUR2mdZcEYfCsU7esjRj8UoaBpR90xnOAMLNZb4Zf/GkJR+k0zKRYQ4snDyWIl1vlaP/fyz8s1x kPFTUva4UqN6kwBO8dE+yFUfheBRQWksHoH2WbfRu/bRMIQmJ6ipsT+oAAYPWV1JFEYVPpdNR6o= Host: 23.239.0.12 Connection: Keep-Alive Cache-Control: no-cache
2022-05-14 03:14:53 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 14 May 2022 03:14:53 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2022-05-14 03:14:53 UTC	0	IN	Data Raw: 32 61 32 0d 0a 3f 86 f2 80 c6 07 0e 5a d0 33 9d 9d bc bf fd da e8 a9 48 a3 cf 77 09 62 2c d1 08 d9 76 b8 11 af f2 34 8e 18 94 d0 87 a7 a3 20 42 30 a9 63 29 5a 4f 32 01 12 cc a0 e5 c1 b4 f6 ce 83 b3 80 54 a0 28 90 55 d6 ee 6a 84 35 15 bc f9 aa d1 54 c3 a8 bf 23 15 14 a9 d2 23 b9 49 58 e0 a8 f7 07 46 f9 4b 81 1b f8 2e 56 1f cc 24 6e 95 a8 a5 00 de 1b d7 06 50 1d 5e 94 0f d3 53 dd ce 28 97 22 7d 5c b6 0a c4 c5 ee 40 72 c6 62 4e 05 4a f3 68 7d f7 c7 3c 2d 10 30 aa 13 cc 5a 82 d3 56 15 b2 74 aa ed 8e c6 d8 c4 a8 bc fe 2c 2b cd 8a 67 4c 45 59 9c 4b 93 2b 96 24 f0 e5 c0 1d 86 70 0d 8f cb 6a 70 58 87 e5 22 ec 1d 0e 82 55 d3 66 c8 93 66 5e 83 0b f0 7b a1 30 05 bd 67 9e ea fc 86 9b 4f 9e 54 3c cc f3 41 a7 52 52 e9 6a 9c ce 02 c9 c1 8b 3c f7 0d 93 dc ae f8 a0 a0 35 Data Ascii: 2a2?Z3Hwb,v4 B0c)ZO2T(Uj5T##IXFK.V$nP^S("}\@rbNJh}<-0ZVt,+gLEYK+$pjpX"Uff^{0gOT<ARRj<5

Statistics

Behavior



- loaddll64.exe
- cmd.exe
- regsvr32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- regsvr32.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- SgrmBroker.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- MpCmdRun.exe
- conhost.exe
- svchost.exe
- svchost.exe

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: **5896**, Parent PID: **5844**

General

Target ID:	0
Start time:	05:14:19
Start date:	14/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\1V4gPPcQvB.dll"
Imagebase:	0x7ff6294d0000
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: **5904**, Parent PID: **5896**

General

Target ID:	1
Start time:	05:14:20
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\1V4gPPcQvB.dll",#1
Imagebase:	0x7ff7bb450000
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: **4572**, Parent PID: **5896**

General

Target ID:	2
Start time:	05:14:20
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\1V4gPPcQvB.dll
Imagebase:	0x7ff68d6a0000
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: 00000002.00000002.267070861.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.266871028.00000000022E0000.00000040.00001000.00020000.00000000.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\TvcDyJjJQ\NcAvRfvDRbwLFn.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: **3404**, Parent PID: **5904**

General

Target ID:	3
Start time:	05:14:20
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\1V4gPPcQvB.dll",#1
Imagebase:	0x7ff7bca70000
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: 00000003.00000002.265168643.0000023396DC0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.264935281.0000000180001000.00000020.00001000.00020000.00000000.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: **3748**, Parent PID: **5896**

General

Target ID:	4
Start time:	05:14:20
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\1V4gPPcQvB.dll,DllRegisterServer
Imagebase:	0x7ff7bca70000
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: 00000004.00000002.264793383.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.264939318.0000020701410000.00000040.00001000.00020000.00000000.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: **2364**, Parent PID: **5896**

General

Target ID:	5
Start time:	05:14:25
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\1V4gPPcQvB.dll,DllUnregisterServer
Imagebase:	0x7ff7bca70000
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: **6012**, Parent PID: **4572**

General

Target ID:	6
Start time:	05:14:25
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\TvcDyJjJQ\NcAvRfvDRbwLFn.dll"
Imagebase:	0x7ff68d6a0000
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: 00000006.00000002.649155251.0000000000760000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.649306435.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: **2224**, Parent PID: **564**

General

Target ID:	10
Start time:	05:14:35
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:	0x7ff7338d0000

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

Analysis Process: svchost.exe PID: **4572**, Parent PID: **564**

General

Target ID:	11
Start time:	05:14:37
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7338d0000
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

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

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	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **4732**, Parent PID: **564**

General

Target ID:	12
Start time:	05:14:38
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

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

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

Analysis Process: svchost.exe PID: **4940**, Parent PID: **564**

General	
Target ID:	13
Start time:	05:14:39
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7338d0000
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: **1332**, Parent PID: **564**

General	
Target ID:	14
Start time:	05:14:40
Start date:	14/05/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6d0590000
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: **1584**, Parent PID: **564**

General	
Target ID:	15
Start time:	05:14:40
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5076**, Parent PID: **564**

General

Target ID:	16
Start time:	05:14:41
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7338d0000
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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6292**, Parent PID: **564**

General

Target ID:	17
Start time:	05:14:49
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:	0x7ff7338d0000
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: **6332**, Parent PID: **564**

General

Target ID:	18
Start time:	05:14:49
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:	0x7ff7338d0000
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: **6832**, Parent PID: **564**

General

Target ID:	20
Start time:	05:15:28
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:	0x7ff7338d0000
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: MpCmdRun.exe PID: **3452**, Parent PID: **1584**

General

Target ID:	23
Start time:	05:15:41
Start date:	14/05/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff678970000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false

Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	9938	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10484	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10570	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 61 00 74 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 31 00 34 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 35 00 3a 00 31 00 35 00 3a 00 34 00 32 00 0d 00 0a 00	MpCmdRun: End Time: Sat May 14 2022 05:15:42	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10670	174	2d 00 2d 00 2d 00

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7338d0000
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: **6168**, Parent PID: **564**

General

Target ID:	28
Start time:	05:16:05
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:	0x7ff7338d0000
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