

JoeSandbox Cloud BASIC



ID: 626507

Sample Name: S0Uj3iEhau.dll

Cookbook: default.jbs

Time: 05:24:37

Date: 14/05/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report S0Uj3iEhau.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

Behavior	21
System Behavior	21
Analysis Process: loadll64.exePID: 6276, Parent PID: 2380	21
General	21
File Activities	22
Analysis Process: cmd.exePID: 6284, Parent PID: 6276	22
General	22
File Activities	22
Analysis Process: regsvr32.exePID: 6292, Parent PID: 6276	22
General	22
File Activities	22
File Deleted	22
Analysis Process: rundll32.exePID: 6304, Parent PID: 6284	23
General	23
File Activities	23
Analysis Process: rundll32.exePID: 6324, Parent PID: 6276	23
General	23
File Activities	23
Analysis Process: regsvr32.exePID: 6416, Parent PID: 6292	24
General	24
Analysis Process: rundll32.exePID: 6424, Parent PID: 6276	24
General	24
File Activities	24
Analysis Process: svchost.exePID: 6860, Parent PID: 564	24
General	24
File Activities	25
Analysis Process: svchost.exePID: 6900, Parent PID: 564	25
General	25
Analysis Process: svchost.exePID: 6940, Parent PID: 564	25
General	25
File Activities	25
Registry Activities	25
Analysis Process: svchost.exePID: 7008, Parent PID: 564	26
General	26
Registry Activities	26
Analysis Process: svchost.exePID: 7080, Parent PID: 564	26
General	26
Analysis Process: SgrmBroker.exePID: 7152, Parent PID: 564	26
General	26
Analysis Process: svchost.exePID: 4496, Parent PID: 564	27
General	27
Registry Activities	27
Analysis Process: svchost.exePID: 2324, Parent PID: 564	27
General	27
File Activities	27
Analysis Process: svchost.exePID: 4220, Parent PID: 564	27
General	27
File Activities	28
Analysis Process: svchost.exePID: 3856, Parent PID: 564	28
General	28
File Activities	28
Registry Activities	28
Analysis Process: svchost.exePID: 5900, Parent PID: 564	28
General	28
File Activities	29
Analysis Process: svchost.exePID: 6788, Parent PID: 564	29
General	29
File Activities	29
Analysis Process: MpCmdRun.exePID: 5924, Parent PID: 4496	29
General	29
File Activities	29
File Written	29
Analysis Process: conhost.exePID: 5888, Parent PID: 5924	31
General	31
Disassembly	31

Windows Analysis Report

SOUj3iEhau.dll

Overview

General Information

Sample Name:

SOUj3iEhau.dll

Analysis ID:

626507

MD5:

bfc8c2c291a541...

SHA1:

0e2d22f72f957fd...

SHA256:

ecf2a07b01738c...

Tags:

exe trojan

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Emotet

Score:

80

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

Changes security center settings (n...

Hides that the sample has been dow...

Queries the volume information (nam...

Contains functionality to check if a d...

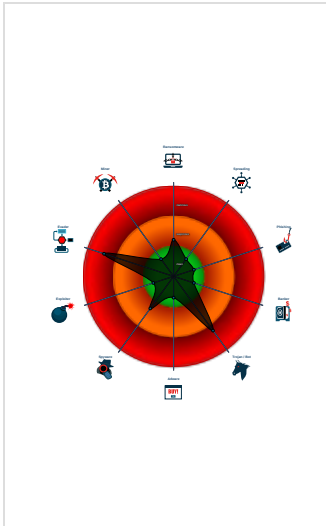
Contains functionality to query local...

Deletes files inside the Windows fol...

May sleep (evasive loops) to hinder...

Checks if Antivirus/Antispyware/Fire...

Classification



Process Tree

System is w10x64

loaddll64.exe (PID: 6276 cmdline: loaddll64.exe "C:\Users\user\Desktop\SOUj3iEhau.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)

cmd.exe (PID: 6284 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SOUj3iEhau.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)

rundll32.exe (PID: 6304 cmdline: rundll32.exe "C:\Users\user\Desktop\SOUj3iEhau.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)

regsvr32.exe (PID: 6292 cmdline: regsvr32.exe /s C:\Users\user\Desktop\SOUj3iEhau.dll MD5: D78B75FC68247E8A63ACBA846182740E)

regsvr32.exe (PID: 6416 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\IXqCbDaRwXzHyqHbxqD.dll" MD5: D78B75FC68247E8A63ACBA846182740E)

rundll32.exe (PID: 6324 cmdline: rundll32.exe C:\Users\user\Desktop\SOUj3iEhau.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)

rundll32.exe (PID: 6424 cmdline: rundll32.exe C:\Users\user\Desktop\SOUj3iEhau.dll,DllUnregisterServer MD5: 73C519F050C20580F8A62C849D49215A)

svchost.exe (PID: 6860 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 6900 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 6940 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 7008 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 7080 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

SgrmBroker.exe (PID: 7152 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)

svchost.exe (PID: 4496 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)

MpCmdRun.exe (PID: 5924 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)

conhost.exe (PID: 5888 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

svchost.exe (PID: 2324 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 4220 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 3856 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 5900 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 6788 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

cleanup

Malware Configuration

No configs have been found

Copyright Joe Security LLC 2022

Page 4 of 31

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.245116750.0000000180001000.00000020.00001000.00020000.00000000.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.242723804.0000000180001000.00000020.00001000.00020000.00000000.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.242340810.0000000180001000.00000020.00001000.00020000.00000000.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.631796967.0000000180001000.00000020.00001000.00020000.00000000.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.244863789.00000000020F0000.00000040.00001000.00020000.00000000.sdump	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.115aee20000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.115aee20000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.230416a0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.20f0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.20f0000.0.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

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



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

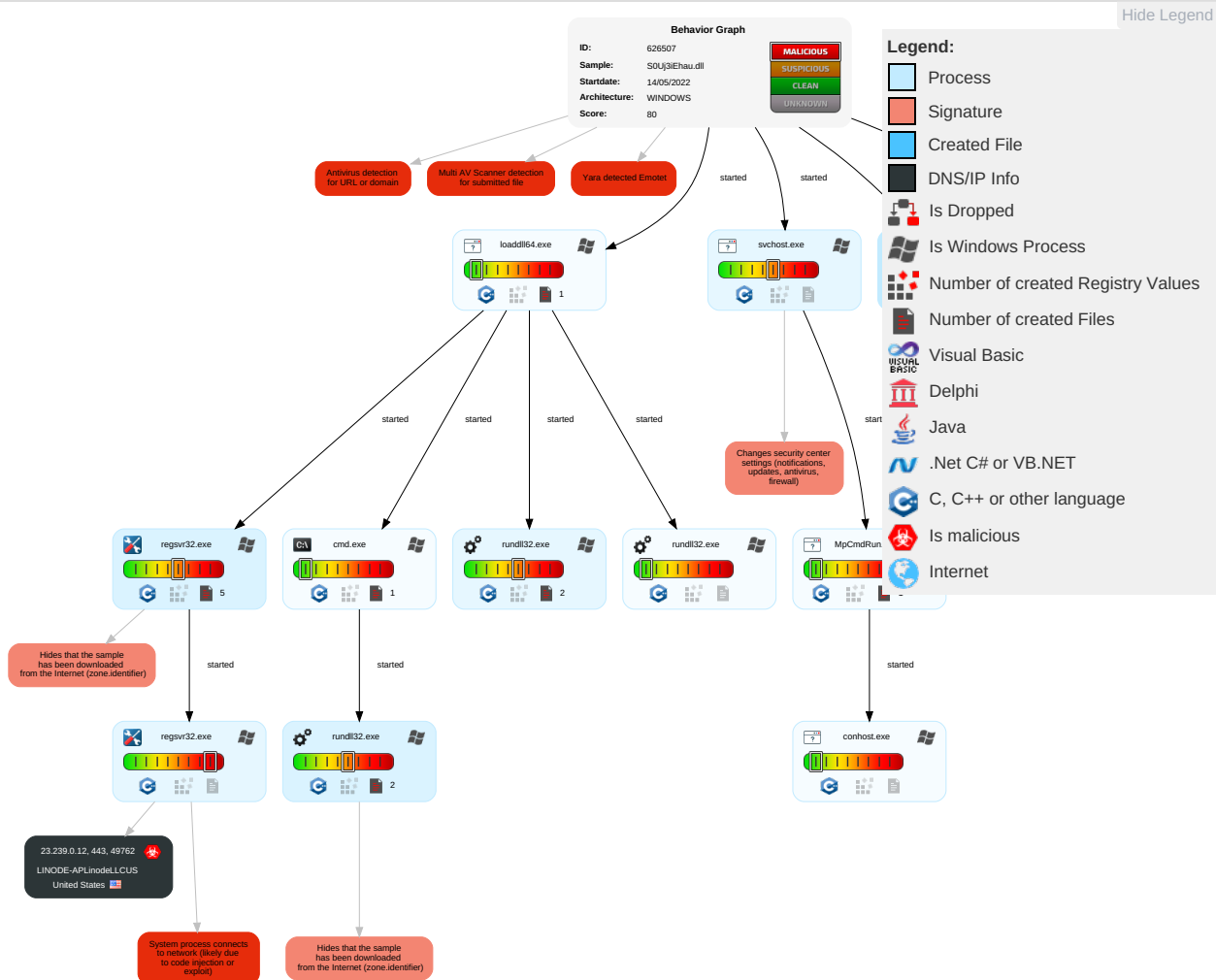


Yara detected Emotet

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

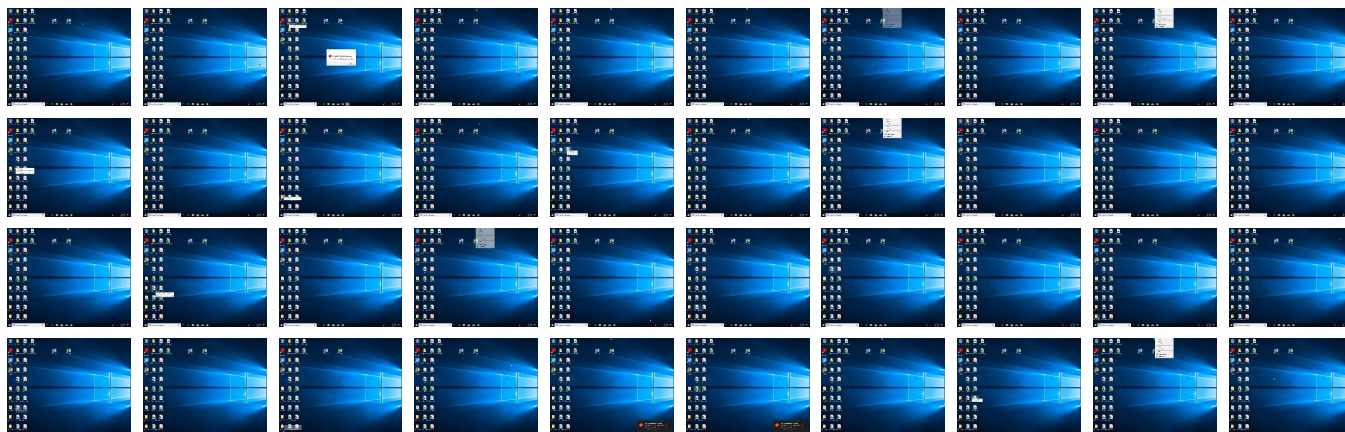
Behavior Graph



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
SOUj3iEhau.dll	30%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.regsrv32.exe.14e0000.1.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
3.2.rundll32.exe.230416a0000.0.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
4.2.rundll32.exe.115aee20000.1.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
2.2.regsrv32.exe.20f0000.0.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File

Domains

No Antivirus matches

URLs				
Source	Detection	Scanner	Label	Link
http://https://23.239.0.12/r	100%	Avira URL Cloud	malware	
http://https://23.239.0.12/s	100%	Avira URL Cloud	malware	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://www.bingmapsportal.comsv	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://23.239.0.12/7	100%	Avira URL Cloud	malware	
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://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://23.239.0.12/	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs
Contacted Domains
 No contacted domains info

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

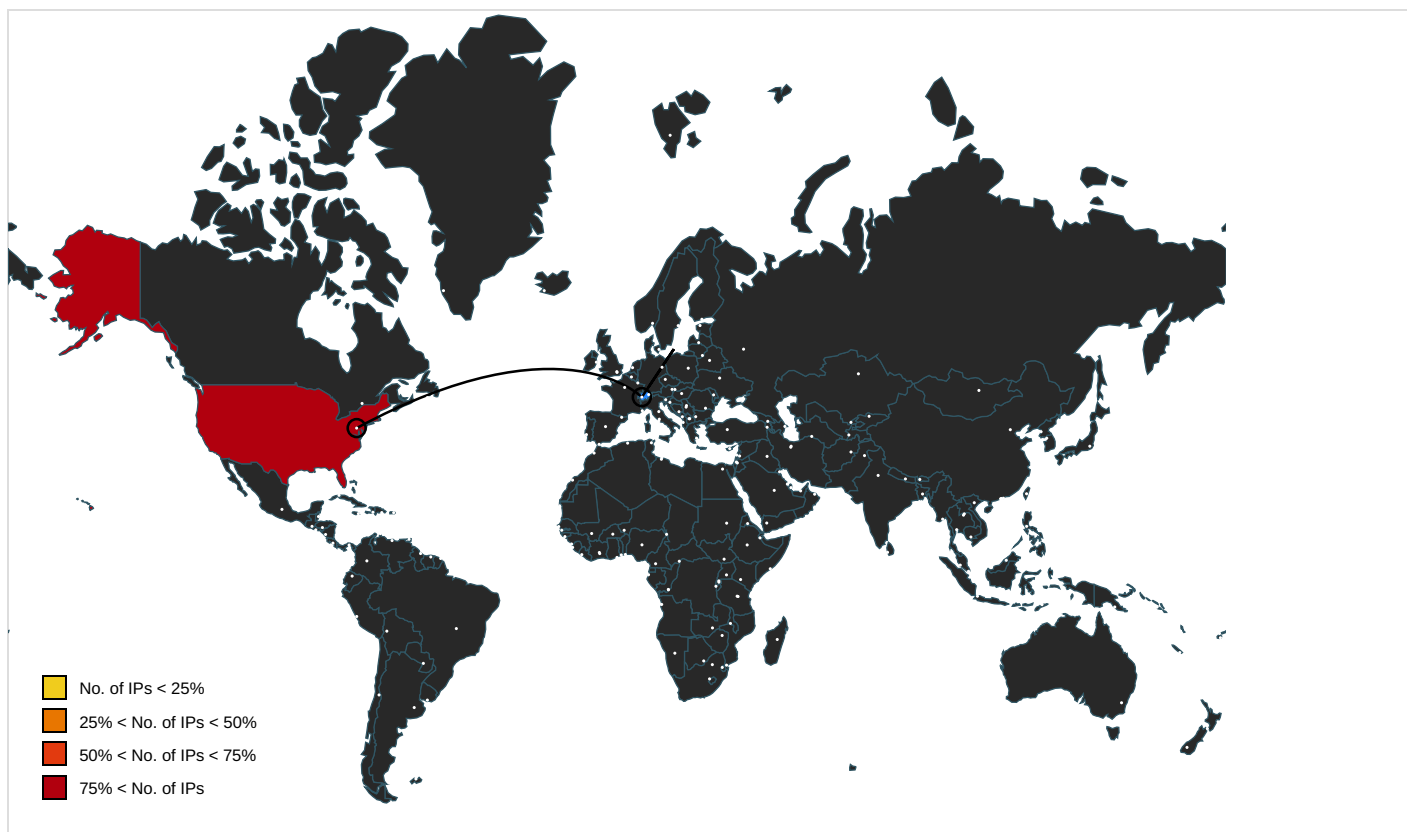
URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://23.239.0.12/r	regsvr32.exe, 00000005.00000002.63106541.3.0000000001341000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000005.00000003.308017457.0000000001341000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://23.239.0.12/s	regsvr32.exe, 00000005.00000002.63106541.3.0000000001341000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000005.00000003.308017457.0000000001341000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000E.00000002.313192030.00000297F963E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000E.00000003.312882378.00000297F9662000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000E.00000002.313192030.00000297F963E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000E.00000003.312898609.00000297F964A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.313201825.00000297F964C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000E.00000003.312889981.00000297F964F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.313210317.00000297F9650000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000E.00000003.312882378.00000297F9662000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000E.00000003.312911066.00000297F9641000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.312929225.00000297F9642000.0000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.313197331.00000297F9643000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000E.00000003.312882378.00000297F9662000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000E.00000003.312898609.00000297F964A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.313172579.00000297F9629000.0000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000E.00000003.291228066.00000297F9631000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000E.00000003.312911066.00000297F9641000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.312929225.00000297F9642000.0000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.313197331.00000297F9643000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000017.00000003.384563015.000001EF47DA2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.385055310.000001EF47DB8000.0000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.385198063.000001EF48202000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.384572697.000001EF47DD0000.0000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.384522095.000001EF47D98000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.385004148.000001EF47DD0000.0000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.384538301.000001EF47D86000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000017.00000003.384563015.000001EF47DA2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.385055310.000001EF47DB8000.0000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.385198063.000001EF48202000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.384572697.000001EF47DD0000.0000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.384522095.000001EF47D98000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.385004148.000001EF47DD0000.0000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.384538301.000001EF47D86000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/09/enumeration	svchost.exe, 00000014.00000003.596806522.000001C7D6CAA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000014.00000002.597263473.000001C7D6CAF000.0000004.00000020.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.comsv	svchost.exe, 0000000E.00000002.313155620.00000297F9613000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000E.00000002.313172579.00000297F9629000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000E.00000002.313192030.00000297F963E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000E.00000003.312882378.00000297F9662000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000017.00000003.392208829.000001EF47D8A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.392230018.000001EF47DA6000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000E.00000003.312911066.00000297F9641000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.312925803.00000297F9646000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://23.239.0.12/7	regsvr32.exe, 00000005.00000002.631065413.0000000001341000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.308017457.0000000001341000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 0000000E.00000002.313236676.00000297F966B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.312867648.00000297F9669000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000E.00000002.313192030.00000297F963E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 0000000E.00000002.313172579.00000297F9629000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000E.00000003.291228066.00000297F9631000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ver)	svchost.exe, 00000014.00000002.597449901.000001C7DC663000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000002.415365580.000001EF472EC000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000E.00000003.312911066.00000297F9641000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.312898609.00000297F964A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.313201825.00000297F964C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000017.00000003.395779444.000001EF47D8A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.395844246.000001EF47DD2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.395877090.000001EF48202000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000E.00000002.313155620.00000297F9613000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.313192030.00000297F963E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 0000000C.00000002.631321041.0000021D4A03E000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	low
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000E.00000003.312882378.00000297F9662000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000E.00000003.291228066.00000297F9631000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000E.00000003.312882378.00000297F9662000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.hotspotshield.com/	svchost.exe, 00000017.00000003.384563015.000001EF47DA2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.385055310.000001EF47DB8000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.385198063.000001EF48202000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.384572697.000001EF47DD0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.384522095.000001EF47D98000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.385004148.000001EF47DD0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.384538301.000001EF47D86000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000E.00000003.312898609.00000297F964A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.313201825.00000297F964C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000017.00000003.392208829.000001EF47D8A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.392230018.000001EF47DA6000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000E.00000003.312898609.00000297F964A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.313201825.00000297F964C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000E.00000002.313210317.00000297F9650000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000E.00000003.312882378.00000297F9662000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://disneyplus.com/legal	svchost.exe, 00000017.00000003.392208829.000001EF47D8A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.392230018.000001EF47DA6000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000E.00000003.312937016.00000297F963B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.291228066.00000297F9631000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000E.00000002.313201825.00000297F964C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 0000000C.00000002.631321041.0000021D4A03E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000E.00000003.312882378.00000297F9662000.00000004.00000020.00020000.00000000.sdmp	false		high
http://help.disneyplus.com	svchost.exe, 00000017.00000003.392208829.000001EF47D8A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.392230018.000001EF47DA6000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000C.00000002.631321041.0000021D4A03E000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000E.00000003.312898609.00000297F964A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.313201825.00000297F964C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000E.00000003.312898609.00000297F964A000.00000004.00000020.00020000.00000000.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:	626507
Start date and time: 14/05/202205:24:37	2022-05-14 05:24:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	S0Uj3iEhau.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal80.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 were 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
05:26:19	API Interceptor	1x Sleep call for process: svchost.exe modified
05:27:09	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:ShaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF3180
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):	0.24946588560530503
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4K:BJiRdwfu2SRU4K
MD5:	D6BEFE60B765131F8E6B1F74D0007503
SHA1:	A1E68EFD0DB45763FBBBACCE0539B4C4E288908F
SHA-256:	E7D3FE966403EFEC42572B5870DB55E4BE5266F0E980A19D4F5CA98ACAC16CB5
SHA-512:	8E6082D6546E0638C225FEF19E914AB6A6ED21C7D5D7AAF580C326A9A236E7EF7CB366044F7BF578B4210342A46FB87D9AD89C00461A798ABBE40473288A7911
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 0x429db59e, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25071638117186734
Encrypted:	false
SSDEEP:	384:Rzu+W0StseCJ48EApW0StseCJ48E2rTsjlK/ebmLerYSRSY1J2:RzBSB2nSB2RSjlK/+mLesOj1J2
MD5:	C9D77FA1E985910DE98355A98EAF139E
SHA1:	020F88543A7336A42B59FA82B505596080109097
SHA-256:	92893C5AB8A6553DF7BE0C7188B153A390294120EF3C9BBF5D55BDC67A181C4B
SHA-512:	C593421AF7F83953BFA662E473B76BEED08BF0076EF6BE7511169476DABC5C4E726EDC14461618EAED1EF609CE4E5D1F97F046C64D604B859E32B9904430277
Malicious:	false
Preview:	B.....e.f.3...w.....).....z[.....z.h.(.....z[...]).....3...w.....B.....@.....l].9.....z[.....=.]......z[.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07660198235110685
Encrypted:	false

SSDEEP:	3:clZ7v2pf8Sp1lkaMnRk3ts5Pi3k1lol3Vktlmlnl:or2pf8w8tRk2MkQ3
MD5:	B5C629AD5C7F4D2D8F2C63014AF3BA0A
SHA1:	DF0EE0F1AE7495350145DB717ED6B0ACCE7F02F7
SHA-256:	484F33C6EB1324FDCF08E9EC3ACC090D46D978D41DEEC06A38F8EE01534B9824
SHA-512:	183667DF137CD9A9F0966DD1B2BC09545BF425BC248CC9BFDD6324E574590F8CF125C96C0088B4BD38C20CFADCA50183DD1F72D6D9C63C19945C856765B20A5
Malicious:	false
Preview:	.sKR.....3..w.....Z.....z[.....z.....z[R..l.....z.....=.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:YMRI83Xi2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA CA
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):	3.1620067482755942
Encrypted:	false
SSDEEP:	192:cY+38+DJM+itJt+iDQ+yw+f0+rU+0Jtk+E0tF+E7tC+EwB5+oT:j+s+i+Z+z+B+c+Y+0g+J+j+l5+oT
MD5:	726E92A914A80088ADA9C59B51E84C60
SHA1:	088178A50149E88CB387462F4AF8777C9E9D7C29
SHA-256:	BF7C6D5CF9C792BEFDBBA4DF41A3206B9208A8F7DECf4E4D6F92AECE8450EA3B
SHA-512:	2E26A555A98B4EC52E091233CE5210A65ECE84C1E6FA06934D0B56A159C98DDF3DBF136E1295CF2F08E53623C494175FF4690BDBDAD28167A5E5BB61D1BEA8 7F
Malicious:	false
Preview:	M.p.C.m.d.R.u.n.:.C.o.m.m.a.n.d. . Line.: "C:\P.r.o.g.r.a.m. .F.i.l.e.s.\W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\m.p.c.m.d.r.u.n...e.x.e". -w.d.e.n.a.b.l.e.....S.t.a.r.t. .T.i.m.e.:. .T.h.u. .J.u.n. .2.7...2.0.1.9. .0. 1.:2.9.:4.9.....M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:.h.r. =. .0.x.1....W.D.E.n.a.b.l.e.....E.R.R.O.R.:.M.p.W.D.E.n.a.b.l.e.(T.R.U.E). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:.E.n.d. .T.i.m.e.:. .T.h.u. .J.u.n. .2.7...2.0.1.9. .0.1.:2.9.:4.9.....

Static File Info	
General	
File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.482082028693859
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:	S0Uj3iEhau.dll
File size:	545280
MD5:	bfc8c2c291a541379642dcf219f78be4

SHA1:	0e2d22f72f957fda57c7d0c4498103ee52413127
SHA256:	ecf2a07b01738c05497f5ff5aef2a93622ec7bfc353a66357bad30a5898c1e21
SHA512:	c346ce4ef57f9a22cc30084310d77bc1e7cde958d75a3852ee2e660204a03018174a21662d49f856981b38897551ff5dfdda15fd4620b52526a1151005dbf0ce
SSDEEP:	12288:B4UJY9B+TenWsSEPHjMOUP9uXdt7JpfYNVrRM54RutCTdJGqloTCZ4eEsZOHxHy:B4UJY9BSenZSEPHjMOUP9Udt7JpfYNVm
TLSH:	32C4CFA5435C08FCE762C3395C975BC5B1F7BDAE0664AF260BC18DA05E1BA90F53A381
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 00007F64D0A43857h
call 00007F64D0A459E4h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax

Instruction
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007F64D0A43700h
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 00007F64D0A523DAh
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007F64D0A43893h
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 00007F64D0A52388h
jmp 00007F64D0A43874h
dec eax
mov eax, dword ptr [eax+eax+00000000h]

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	0.355279737903	data	5.39250228185	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.data	0x56000	0x20d8	0x1200	False	0.180772569444	data	2.18161586025	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x59000	0xe1c	0x1000	False	0.44580078125	data	4.98556265168	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x5a000	0x2dffc	0x2e000	False	0.839408542799	data	7.73448363752	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0x6f8	0x800	False	0.1796875	data	1.81179169858	IMAGE_SCN_CNT_INITIALIZE D_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

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 05:26:12.939707994 CEST	49762	443	192.168.2.4	23.239.0.12
May 14, 2022 05:26:12.939765930 CEST	443	49762	23.239.0.12	192.168.2.4
May 14, 2022 05:26:12.939850092 CEST	49762	443	192.168.2.4	23.239.0.12
May 14, 2022 05:26:12.956336021 CEST	49762	443	192.168.2.4	23.239.0.12
May 14, 2022 05:26:12.956371069 CEST	443	49762	23.239.0.12	192.168.2.4
May 14, 2022 05:26:13.501888037 CEST	443	49762	23.239.0.12	192.168.2.4
May 14, 2022 05:26:13.501976967 CEST	49762	443	192.168.2.4	23.239.0.12
May 14, 2022 05:26:14.327874899 CEST	49762	443	192.168.2.4	23.239.0.12
May 14, 2022 05:26:14.327923059 CEST	443	49762	23.239.0.12	192.168.2.4
May 14, 2022 05:26:14.328228951 CEST	443	49762	23.239.0.12	192.168.2.4
May 14, 2022 05:26:14.328310013 CEST	49762	443	192.168.2.4	23.239.0.12
May 14, 2022 05:26:14.333039045 CEST	49762	443	192.168.2.4	23.239.0.12
May 14, 2022 05:26:14.376506090 CEST	443	49762	23.239.0.12	192.168.2.4
May 14, 2022 05:26:15.178638935 CEST	443	49762	23.239.0.12	192.168.2.4
May 14, 2022 05:26:15.178755045 CEST	443	49762	23.239.0.12	192.168.2.4
May 14, 2022 05:26:15.178756952 CEST	49762	443	192.168.2.4	23.239.0.12
May 14, 2022 05:26:15.178833008 CEST	49762	443	192.168.2.4	23.239.0.12
May 14, 2022 05:26:15.364021063 CEST	49762	443	192.168.2.4	23.239.0.12
May 14, 2022 05:26:15.364051104 CEST	443	49762	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	49762	23.239.0.12	443	C:\Windows\System32\regsvr32.exe
Timestamp	kBytes transferred	Direction	Data		

Timestamp	kBytes transferred	Direction	Data
2022-05-14 03:26:14 UTC	0	OUT	GET / HTTP/1.1 Cookie: mNP!hrxnw=8Nvm/7974IMqSvseFzqKppsFkVLWCcqHvOH7W7OhCwTo9HKd975bkEdJWzmFrHJrYLbg2yViLYUvYww3+7Lq0mXKQ5YTFwEPfYvgUYyHYp4aMpd+/YnrYq6GPXBo/+LQNMBk1SN1iSNwaYknVeliUjs7kUwjxwk1r1FH6FqJ7eZY7WTacGmfr5ylQyvHKYagm3tVQV/Lj79YOG66+FRJkOjfs2BdhxEAD5ksfi5L2MpgVNYKHqM= Host: 23.239.0.12 Connection: Keep-Alive Cache-Control: no-cache
2022-05-14 03:26:15 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 14 May 2022 03:26:15 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2022-05-14 03:26:15 UTC	0	IN	Data Raw: 31 31 61 0d 0a 1d 88 4a 30 fc cf 98 21 5c f6 f2 1e bf 97 0f 24 9f 2d 12 01 b5 10 90 e6 3a 48 16 69 bf 44 1c 06 38 46 ea 2e b7 c9 d8 6f f9 8d b3 29 f1 80 70 9e 66 e6 85 23 f6 13 0c 60 4a aa a1 48 51 31 e1 ef 87 cc 87 33 86 cf 5b 1f 62 e5 83 19 21 86 55 8e af ae 5b 54 9a 9b a7 a3 77 da eb 14 97 ea f4 1d 80 e9 2f 33 00 6a fa ab a8 c6 12 ef d7 ac e0 7f 8e 60 1d 45 4c 1c 4d dd f4 73 9b be 5a 16 8d e7 e8 52 7c a3 db 35 f0 22 e3 34 75 86 b5 90 11 83 0b ee a4 c3 09 f7 87 9f 10 c6 7d 5d e4 3e 52 ef 1f 6f 03 99 6f 43 0d 64 95 c1 69 76 6e 27 2f a3 ad 04 05 6b 5f bc 1d 13 68 28 58 6c db 9d d7 42 77 f9 90 6e 99 e8 46 70 b7 c9 bc 3e 05 61 f7 64 04 a5 c3 08 23 0c 38 9e 07 37 d5 5c ef 01 b3 71 f2 42 77 a3 24 54 c4 5e d4 64 8b 50 13 34 1a cc 32 33 fa 51 e2 37 93 92 d4 bb Data Ascii: 11aJ0!\$-:HiD8F.o)p#'# JHQ13[b!U[Tw/3j'ELMsZRl5"4u]]>RooCdivn'/k_h(XlBwnFp>ad#87!qBw\$T^dP423Q7

Statistics

Behavior



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

 Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 6276, Parent PID: 2380

General

Target ID:	0
Start time:	05:25:39
Start date:	14/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\S0Uj3iEhau.dll"
Imagebase:	0x7ff682220000
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: 6284, Parent PID: 6276

General

Target ID:	1
Start time:	05:25:40
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\SOUj3iEhau.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: 6292, Parent PID: 6276

General

Target ID:	2
Start time:	05:25:40
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\SOUj3iEhau.dll
Imagebase:	0x7ff61f4a0000
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: 00000002.00000002.245116750.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.244863789.00000000020F0000.00000040.00001000.00020000.00000000.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\IXqCbDaRw\zHyqHbxqD.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: 6304, Parent PID: 6284

General

Target ID:	3
Start time:	05:25:40
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\S0Uj3iEhau.dll",#1
Imagebase:	0x7ff6eb5d0000
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: 00000003.00000002.242723804.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.243048238.00000230416A0000.00000040.00001000.00020000.00000000.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: 6324, Parent PID: 6276

General

Target ID:	4
Start time:	05:25:41
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\S0Uj3iEhau.dll,DllRegisterServer
Imagebase:	0x7ff6eb5d0000
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: 00000004.00000002.242340810.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.242462869.00000115AEE20000.00000040.00001000.00020000.00000000.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: regsvr32.exe PID: 6416, Parent PID: 6292

General

Target ID:	5
Start time:	05:25:44
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\lXqCbDaRw\lzHyqHbxqD.dll"
Imagebase:	0x7ff61f4a0000
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: 00000005.00000002.631796967.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.631602430.00000000014E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6424, Parent PID: 6276

General

Target ID:	6
Start time:	05:25:44
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\S0Uj3iEhau.dll,DllUnregisterServer
Imagebase:	0x7ff6eb5d0000
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: svchost.exe PID: 6860, Parent PID: 564

General

Target ID:	10
Start time:	05:26:02
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
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: svchost.exe PID: 6900, Parent PID: 564

General

Target ID:	11
Start time:	05:26:04
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: 6940, Parent PID: 564

General

Target ID:	12
Start time:	05:26:04
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: 7008, Parent PID: 564**General**

Target ID:	13
Start time:	05:26:05
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: 7080, Parent PID: 564**General**

Target ID:	14
Start time:	05:26:06
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: 7152, Parent PID: 564**General**

Target ID:	16
Start time:	05:26:07
Start date:	14/05/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff766120000
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: 4496, Parent PID: 564**General**

Target ID:	17
Start time:	05:26:07
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 wscsv
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: 2324, Parent PID: 564**General**

Target ID:	18
Start time:	05:26:08
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: 4220, Parent PID: 564**General**

Target ID:	19
Start time:	05:26:09
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: 3856, Parent PID: 564	
General	
Target ID:	20
Start time:	05:26:18
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: 5900, Parent PID: 564	
General	
Target ID:	21
Start time:	05:26:27
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: 6788, Parent PID: 564

General

Target ID:	23
Start time:	05:26:39
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
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: MpCmdRun.exe PID: 5924, Parent PID: 4496

General

Target ID:	28
Start time:	05:27:08
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
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

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 0d 00 0a 00	----- ----- -----	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10120	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 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 32 00 37 00 3a 00 30 00 39 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Sat May 14 2022 05:27 :09	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10378	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10464	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF67899BC96	WriteFile
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\ImpCmdRun.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 32 00 37 00 3a 00 30 00 39 00 0d 00 0a 00	MpCmdRun: End Time: Sat May 14 2022 05:27:09	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\ImpCmdRun.log	10670	174	2d 00 0d 00 0a 00	----- ----- -----	success or wait	1	7FF67899BC96	WriteFile

Analysis Process: conhost.exe PID: 5888, Parent PID: 5924

General

Target ID:	29
Start time:	05:27:08
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly