



ID: 626491
Sample Name: 3j6e3XaMWM.dll
Cookbook: default.jbs
Time: 04:56:15
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 3j6e3XaMWM.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
E-Banking Fraud 5
Hooking and other Techniques for Hiding and Protection 5
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 11
Public IPs 11
Private 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 13
C:\ProgramData\Microsoft\Network\Downloader\qmgr.db 13
C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp 13
Static File Info 13
General 13
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 14
Rich Headers 15
Data Directories 16
Sections 16
Resources 16
Imports 16
Exports 16
Possible Origin 17
Network Behavior 17
TCP Packets 17
HTTP Request Dependency Graph 17
HTTPS Proxied Packets 17
Statistics 18
Behavior 18
System Behavior 18
Analysis Process: loaddll64.exePID: 7012, Parent PID: 2120 18
General 18

File Activities 18
Analysis Process: cmd.exePID: 7020, Parent PID: 7012 19
General 19
File Activities 19
Analysis Process: regsvr32.exePID: 7028, Parent PID: 7012 19
General 19
File Activities 19
File Deleted 19
Analysis Process: rundll32.exePID: 7040, Parent PID: 7020 20
General 20
File Activities 20
Analysis Process: rundll32.exePID: 7048, Parent PID: 7012 20
General 20
File Activities 20
Analysis Process: rundll32.exePID: 7104, Parent PID: 7012 20
General 21
File Activities 21
Analysis Process: regsvr32.exePID: 7160, Parent PID: 7028 21
General 21
Analysis Process: svchost.exePID: 5112, Parent PID: 604 21
General 21
File Activities 22
Analysis Process: svchost.exePID: 4856, Parent PID: 604 22
General 22
Analysis Process: svchost.exePID: 7060, Parent PID: 604 22
General 22
File Activities 22
Analysis Process: svchost.exePID: 6848, Parent PID: 604 22
General 22
File Activities 23
Analysis Process: svchost.exePID: 6664, Parent PID: 604 23
General 23
File Activities 23
Analysis Process: svchost.exePID: 2320, Parent PID: 604 23
General 23
File Activities 23
Registry Activities 23
Analysis Process: svchost.exePID: 6140, Parent PID: 604 24
General 24
File Activities 24
Analysis Process: svchost.exePID: 7040, Parent PID: 604 24
General 24
File Activities 24
Registry Activities 24
Disassembly 25

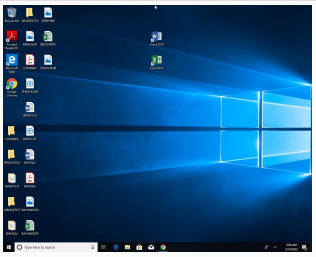
Windows Analysis Report

3j6e3XaMWM.dll

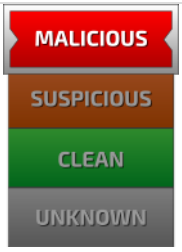
Overview

General Information

Sample Name:	3j6e3XaMWM.dll
Analysis ID:	626491
MD5:	fded8e79db5a44..
SHA1:	bec722ecd7d977..
SHA256:	1ddda2d0e1f888..
Tags:	exe trojan
Infos:	



Detection



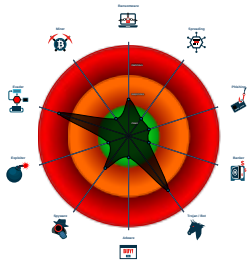
Emotet

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
- Query firmware table information (lik…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query local…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 7012 cmdline: loaddll64.exe "C:\Users\user\Desktop\3j6e3XaMWM.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 7020 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\3j6e3XaMWM.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 7040 cmdline: rundll32.exe "C:\Users\user\Desktop\3j6e3XaMWM.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 7028 cmdline: regsvr32.exe /s C:\Users\user\Desktop\3j6e3XaMWM.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 7160 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\OuJdDSrmhvdmo\XuUuFKSi.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 7048 cmdline: rundll32.exe C:\Users\user\Desktop\3j6e3XaMWM.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7104 cmdline: rundll32.exe C:\Users\user\Desktop\3j6e3XaMWM.dll,DllUnregisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 5112 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4856 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7060 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6848 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6664 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2320 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6140 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7040 cmdline: C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000004.00000002.369416171.0000015B32F70000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.369388046.000001EAD22B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.371341468.0000000001D50000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.752957792.0000000002750000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.371553108.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.regsvr32.exe.1d50000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.1d50000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.1ead22b0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.regsvr32.exe.2750000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.15b32f70000.1.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)

Copyright Joe Security LLC 2022

Malware Analysis System Evasion



Query firmware table information (likely to detect VMs)

HIPS / PFW / Operating System Protection Evasion



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

Stealing of Sensitive Information



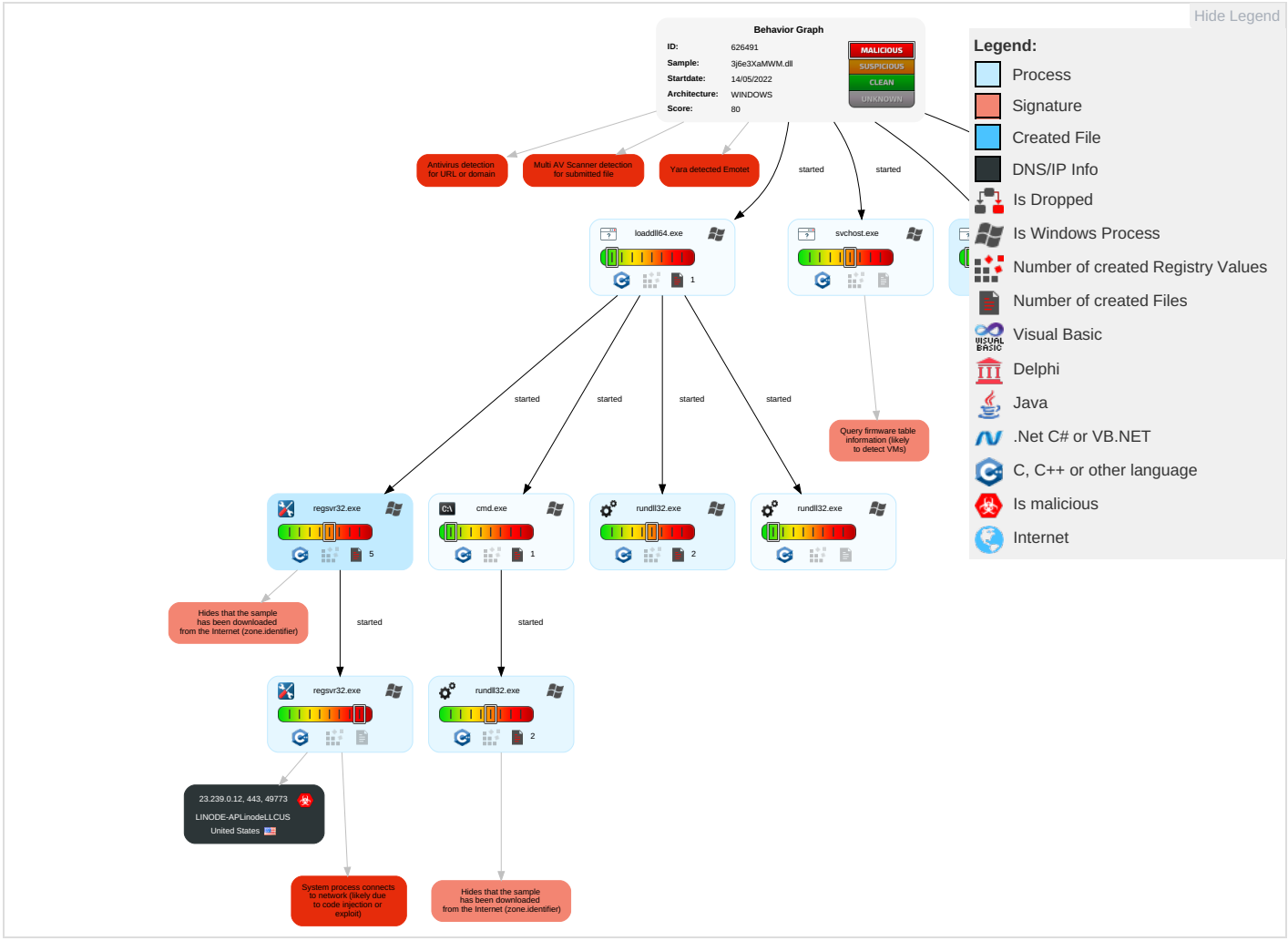
Yara detected Emotet

Mitre Att&ck Matrix

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

Behavior Graph

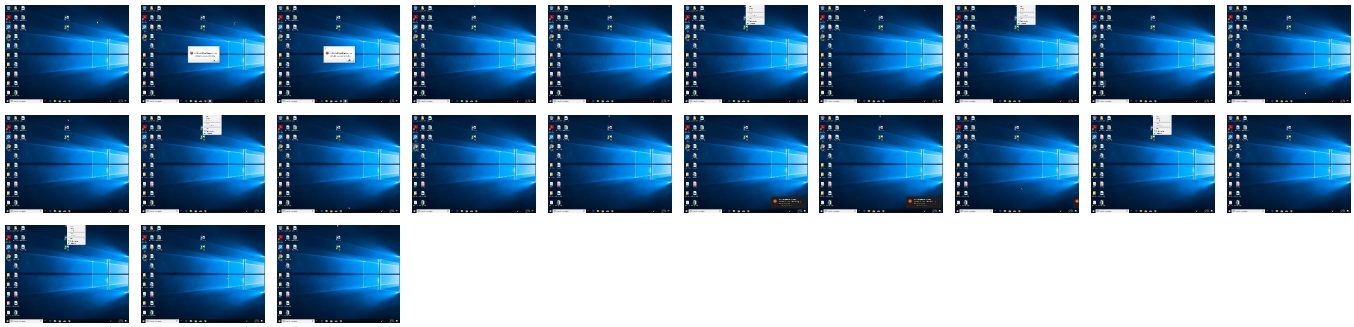
Copyright Joe Security LLC 2022



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
3j6e3XaMWM.dll	36%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.regsvr32.exe.2750000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
2.2.regsvr32.exe.1d50000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
4.2.rundll32.exe.15b32f70000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
3.2.rundll32.exe.1ead22b0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Domains

No Antivirus matches

Copyright Joe Security LLC 2022

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://23.239.0.12/c	100%	Avira URL Cloud	malware	
http://https://23.239.0.12/	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://23.239.0.12/k	100%	Avira URL Cloud	malware	
http://https://23.239.0.12/i	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

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

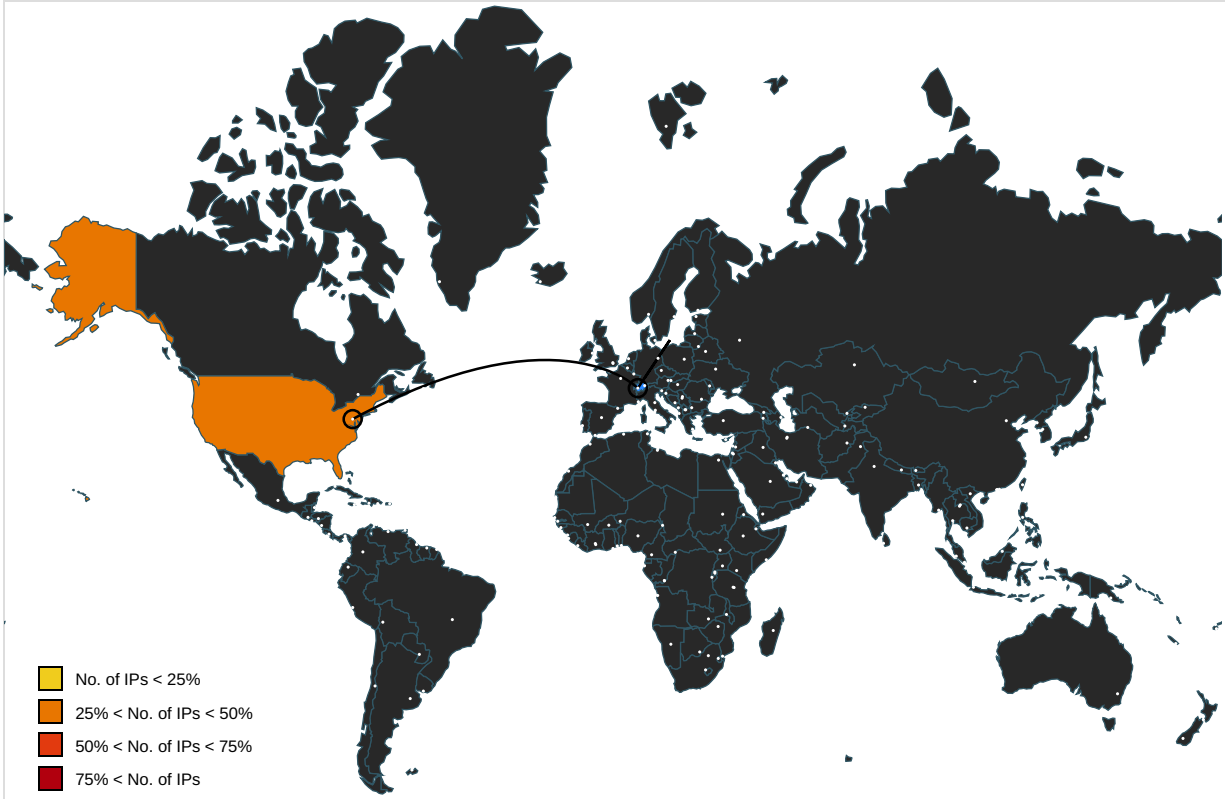
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000019.00000003.602688421.00000246C13B0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.602597594.00000246C138E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.602607367.00000246C139F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000019.00000003.602688421.00000246C13B0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.602597594.00000246C138E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.602607367.00000246C139F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000019.00000003.598795989.00000246C181A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598813964.00000246C181A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598683356.00000246C1388000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598698944.00000246C1399000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598831398.00000246C1802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598850481.00000246C1388000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598773872.00000246C13AA000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.pango.co/privacy	svchost.exe, 00000019.00000003.598795989.00000246C181A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598813964.00000246C181A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598683356.00000246C1388000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598698944.00000246C1399000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598831398.00000246C1802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598850481.00000246C1388000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598773872.00000246C13AA000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 00000019.00000003.602688421.00000246C13B0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.602597594.00000246C138E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.602607367.00000246C139F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ver)	svchost.exe, 00000018.00000002.752551637.0000019602229000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000002.629278465.00000246C08E6000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000002.752853803.0000022CC16D8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000019.00000003.609553277.00000246C1390000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.609738932.00000246C1802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.609646964.00000246C1818000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.609689190.00000246C1818000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.609674491.00000246C13B2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.609775203.00000246C1843000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://23.239.0.12/c	regsvr32.exe, 00000006.00000003.436820458.0000000000EA2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.752484263.0000000000EA2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://help.disneyplus.com.	svchost.exe, 00000019.00000003.602688421.00000246C13B0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.602597594.00000246C138E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.602607367.00000246C139F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.hotspotshield.com/	svchost.exe, 00000019.00000003.598795989.00000246C181A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598813964.00000246C181A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598683356.00000246C1388000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598698944.00000246C1399000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598831398.00000246C1802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598850481.00000246C1388000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.598773872.00000246C13AA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://23.239.0.12/k	regsvr32.exe, 00000006.00000003.436820458.0000000000EA2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.752484263.0000000000EA2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://23.239.0.12/i	regsvr32.exe, 00000006.00000003.43682045 8.0000000000EA2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.752484263.0000000000EA2000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

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

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626491
Start date and time: 14/05/202204:56:15	2022-05-14 04:56:15 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3j6e3XaMWM.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:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Copyright Joe Security LLC 2022

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@21/2@0/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• 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): MpCmdRun.exe, taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.4.86, 20.223.24.244, 23.205.181.161, 40.127.240.158, 20.49.150.241
- Excluded domains from analysis (whitelisted): fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, b-ring.msedge.net, arc.msn.com, e11290.dspg.akamaiedge.net, go.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, sls.update.microsoft.com, settings-prod-neu-1.northeurope.cloudapp.azure.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, atm-settingsfe-prod-geo.trafficmanager.net, fp-afd.azureedge.us, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.useroor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, settings-win.data.microsoft.com, ris.api.iris.microsoft.com, settings-prod-uks-2.uksouth.cloudapp.azure.com, store-images.s-microsoft.com, fp-vp.azureedge.net, go.microsoft.com.edgekey.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:59:09	API Interceptor	1x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x5444998a, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2507311729022606
Encrypted:	false
SSDEEP:	384:8+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:jSB2nSB2RSjlK/+mLesOj1J2
MD5:	A868B270B6FA8E00F43F8FFEE100A57D
SHA1:	CC97FF9BAE7F9C48ED82303323E38222A246A019
SHA-256:	5B66641FEA6421B479507B4160459141881AB8E7EC0E638AA58117BF58AA9B4C
SHA-512:	3C6BCAF6C1D423762382ACBE6F6EA8DBDE79F4D62C89EBE8C11B095E71C872E308F39A5232D07C597D1061B2130EDD819A626B559B1FA8A5BD113C75D966D 4F
Malicious:	false
Preview:	TD..... .....e.f.3...w.....&.....w...;...z..h.(.....3...w.....B.....@..... ....3...w..... .....8.;...z.....iZ..;...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:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA CA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.48207883239968
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:	3j6e3XaMWM.dll
File size:	545280
MD5:	fded8e79db5a443a816be9dde9f6b499
SHA1:	bec722ecd7d977f06914c629a345bad171a352e3
SHA256:	1ddda2d0e1f8885a26ddedce73bc64dd830bad2769ad1e4186b676e885dcf0ec
SHA512:	8bd1be01ae9feeb3f6439cc22396195e5713ad8cbc5574932947999dbeb5bccfca26684bb26dd7b1ba33ab9e692d10a9b50be984a7e1708d8e5a94db095c5496
SSDEEP:	12288:B4UJY9B+TenWsSEPHjMOUP9uXdt7JpfYNVr9RM54RutCTdJGqIoTCZ4eEsZoHxHy:B4UJY9BSenZSEPHjMOUP9Udt7JpfYNV0
TLSH:	A9C4CFA5435C08FCE762C3395C975BC5B1F7BDAE0664AF260BC18DA05E1BA90F53A381

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 00007F789CBEF9F7h
call 00007F789CBF1B84h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007F789CBEF8A0h

Copyright Joe Security LLC 2022

Instruction
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 00007F789CBFE57Ah
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007F789CBEFA33h
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 00007F789CBFE528h
jmp 00007F789CBEFA14h
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

Copyright Joe Security LLC 2022

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	0.355153729839	data	5.39183642982	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
ole32.dll	CoTaskMemFree, CoLoadLibrary, CoTaskMemAlloc

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x180042050

Copyright Joe Security LLC 2022

Name	Ordinal	Address
DllUnregisterServer	2	0x180042080

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 04:58:02.043716908 CEST	49773	443	192.168.2.7	23.239.0.12
May 14, 2022 04:58:02.043766975 CEST	443	49773	23.239.0.12	192.168.2.7
May 14, 2022 04:58:02.044025898 CEST	49773	443	192.168.2.7	23.239.0.12
May 14, 2022 04:58:03.504381895 CEST	49773	443	192.168.2.7	23.239.0.12
May 14, 2022 04:58:03.504421949 CEST	443	49773	23.239.0.12	192.168.2.7
May 14, 2022 04:58:04.053348064 CEST	443	49773	23.239.0.12	192.168.2.7
May 14, 2022 04:58:04.053636074 CEST	49773	443	192.168.2.7	23.239.0.12
May 14, 2022 04:58:06.004997015 CEST	49773	443	192.168.2.7	23.239.0.12
May 14, 2022 04:58:06.005028009 CEST	443	49773	23.239.0.12	192.168.2.7
May 14, 2022 04:58:06.005426884 CEST	443	49773	23.239.0.12	192.168.2.7
May 14, 2022 04:58:06.005505085 CEST	49773	443	192.168.2.7	23.239.0.12
May 14, 2022 04:58:06.038786888 CEST	49773	443	192.168.2.7	23.239.0.12
May 14, 2022 04:58:06.084496021 CEST	443	49773	23.239.0.12	192.168.2.7
May 14, 2022 04:58:06.880738974 CEST	443	49773	23.239.0.12	192.168.2.7
May 14, 2022 04:58:06.880834103 CEST	443	49773	23.239.0.12	192.168.2.7
May 14, 2022 04:58:06.880942106 CEST	49773	443	192.168.2.7	23.239.0.12
May 14, 2022 04:58:06.880970001 CEST	49773	443	192.168.2.7	23.239.0.12
May 14, 2022 04:58:06.884758949 CEST	49773	443	192.168.2.7	23.239.0.12
May 14, 2022 04:58:06.884794950 CEST	443	49773	23.239.0.12	192.168.2.7

HTTP Request Dependency Graph

- 23.239.0.12

HTTPS Proxied Packets

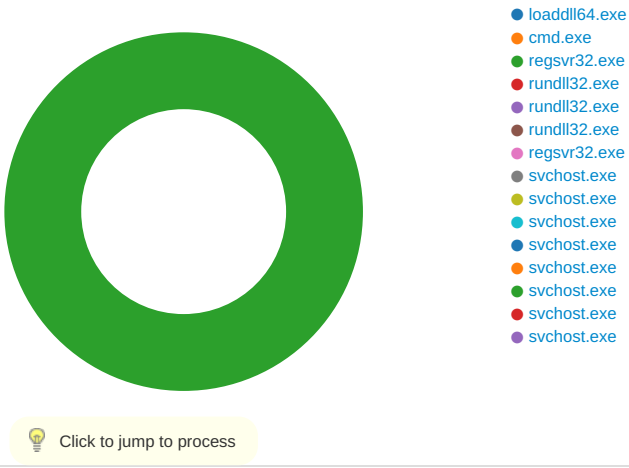
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49773	23.239.0.12	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-14 02:58:06 UTC	0	OUT	GET / HTTP/1.1 Cookie: vE=f6jIzQCjMejmy+jU5rWcrseqTzFWfvcFUwYG62ng7yO4vvVuz7f45Xr2DUwobbuPIqbGYmpR7Ny8q88 MYEUiANlvwaoqcB9h6m7aC/QxCOa6si2JvVNafzj8pIpAFekzWpzBZjWW+VLvS+zhCdnqH6/QjYiUTirAR4d9BQfIf 9wHcPd4xYG1NQkOm6TfsMxuV657oY95bY7ts2a9nLg4GAB0Ubt7gSml5330SJpd5uSpOL7vwGU2h5x8EDW+Zwr29P1 h9yS0wVcifJNpn2dBnJeSFoYfCrkzrfvCqALU Host: 23.239.0.12 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-14 02:58:06 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 14 May 2022 02:58:06 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2022-05-14 02:58:06 UTC	0	IN	Data Raw: 34 35 36 0d 0a 1e 29 fa 99 b7 8b f7 95 7a c2 e7 09 3a a8 ec b0 df a1 88 22 b8 68 74 52 c4 ac 0a 6f fd 30 5b 4a c1 58 4a 62 8c 25 26 b9 f3 36 ef 43 90 cb 1a 72 b1 ad 77 31 e8 3c be 5f e7 ac c7 49 10 09 ed 21 50 1c f2 f9 b9 9f ba cf 18 6b 17 b3 0d 3d ff ff 5f 12 ee e7 19 b4 b1 6e 83 4e a1 5e e5 3d 0a a6 6f 00 d5 45 6e 33 6d 4f 93 a0 57 4d e9 cd 8e 39 55 84 9b dd 43 1a 04 98 75 22 63 85 21 66 c4 7d 1f b1 af 0f bd 64 4c 70 cd 05 3c a7 81 08 2e f9 15 ee e9 f9 63 67 e9 1a f3 2b 63 4a 65 be 0e 7a ed c1 46 a6 bf a9 e6 d4 b9 fd c3 ed e1 d5 3b 83 f3 2e 8f 37 29 25 a4 79 5c 29 06 a1 86 97 b7 03 6b d2 f6 92 c1 b2 5a c3 d3 c0 6f e7 26 19 f0 23 5a bd dd de de fd b4 f2 68 02 4d 8c b0 6c 5b f6 cb 11 2a a7 26 92 91 63 1e f6 13 e7 c7 3c 7f 45 c2 27 31 90 46 c9 65 f1 a8 fd Data Ascii: 456)z:"htRo0[JXJb%&6Crw1<_l!Pk=_nN^=oEn3mOWM9UCu"c!f}dLp<.cg+cJezF;.7)%y\)kZo&#ZhMl[*&c E'1Fe

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **7012**, Parent PID: **2120**

General

Target ID:	0
Start time:	04:57:28
Start date:	14/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\3j6e3XaMWM.dll"
Imagebase:	0x7ff6c02d0000
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: 7020, Parent PID: 7012

General

Target ID:	1
Start time:	04:57:28
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\3j6e3XaMWM.dll",#1
Imagebase:	0x7ff6a6590000
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: 7028, Parent PID: 7012

General

Target ID:	2
Start time:	04:57:29
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\3j6e3XaMWM.dll
Imagebase:	0x7ff6b68e0000
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: 00000002.00000002.371341468.0000000001D50000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.371553108.0000000180001000.00000020.00001000.00020000.00000000.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\OuJdDSrmhvdmo\XuUuFKSi.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: **7040**, Parent PID: **7020**

General

Target ID:	3
Start time:	04:57:29
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\3j6e3XaMWM.dll",#1
Imagebase:	0x7ff7864c0000
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: 00000003.00000002.369388046.000001EAD22B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.368474960.0000000180001000.00000020.00001000.00020000.00000000.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: **7048**, Parent PID: **7012**

General

Target ID:	4
Start time:	04:57:29
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3j6e3XaMWM.dll,DllRegisterServer
Imagebase:	0x7ff7864c0000
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: 00000004.00000002.369416171.0000015B32F70000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.368812138.0000000180001000.00000020.00001000.00020000.00000000.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: **7104**, Parent PID: **7012**

General	
Target ID:	5
Start time:	04:57:33
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3j6e3XaMWM.dll,DllUnregisterServer
Imagebase:	0x7ff7864c0000
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: 7160, Parent PID: 7028

General	
Target ID:	6
Start time:	04:57:34
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\OuJdDSrmhvdmo\XuUuFKSi.dll"
Imagebase:	0x7ff6b68e0000
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: 00000006.00000002.752957792.0000000002750000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.753071239.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 5112, Parent PID: 604

General	
Target ID:	10
Start time:	04:57:56
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:	0x7ff7e8070000
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: **4856**, Parent PID: **604**

General

Target ID:	13
Start time:	04:58:06
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **7060**, Parent PID: **604**

General

Target ID:	15
Start time:	04:58:18
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7e8070000
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: **6848**, Parent PID: **604**

General

Target ID:	17
Start time:	04:58:28
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:	0x7ff7e8070000
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: **6664**, Parent PID: **604**

General

Target ID:	20
Start time:	04:58:51
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7e8070000
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: **2320**, Parent PID: **604**

General

Target ID:	24
Start time:	04:59:08
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:	0x7ff7e8070000
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.

Copyright Joe Security LLC 2022

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6140**, Parent PID: **604**

General

Target ID:	25
Start time:	04:59:08
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:	0x7ff7e8070000
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: svchost.exe PID: **7040**, Parent PID: **604**

General

Target ID:	29
Start time:	04:59:56
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
Imagebase:	0x7ff7e8070000
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	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	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly

Copyright Joe Security LLC 2022