ID: 626482
Sample Name: yj81rxDZIp
Cookbook: default.jbs
Time: 04:32:13
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

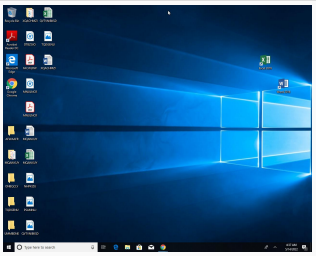
Windows Analysis Report

yj81rxDZIp

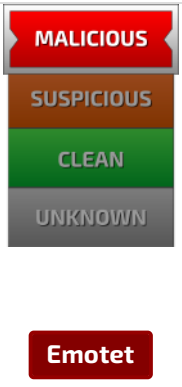
Overview

General Information

Sample Name:	yj81rxDZIp (renamed file extension from none to dll)
Analysis ID:	626482
MD5:	4f1cdae4390ecb…
SHA1:	082de69d519913.
SHA256:	c4e2c26fd37189…
Tags:	exe trojan
Infos:	



Detection



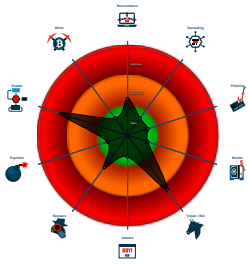
Emotet

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Hides that the sample has been dow…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query local…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 7068 cmdline: loaddll64.exe "C:\Users\user\Desktop\yj81rxDZIp.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 7080 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\yj81rxDZIp.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 7104 cmdline: rundll32.exe "C:\Users\user\Desktop\yj81rxDZIp.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - regsvr32.exe (PID: 2532 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\KZsiDdn\sdxQuTDjzsbvXJ.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 7092 cmdline: regsvr32.exe /s C:\Users\user\Desktop\yj81rxDZIp.dll MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 7112 cmdline: rundll32.exe C:\Users\user\Desktop\yj81rxDZIp.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3384 cmdline: rundll32.exe C:\Users\user\Desktop\yj81rxDZIp.dll,DllUnregisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 1300 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5756 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6356 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7160 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6696 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1592 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.436780201.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.434955422.000001A2C05E0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.434632880.0000000000CE0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.944705463.0000000000B80000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.437553196.0000012A08A10000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.12a08a10000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.regsvr32.exe.b80000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.regsvr32.exe.b80000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.ce0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.1a2c05e0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

Sigma Signatures

⊘ **No Sigma rule has matched**

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 7 - Source IP: 192.168.2.5 - Destination IP: 150.95.66.124 −

Timestamp:	192.168.2.5150.95.66.1244977580802404312 05/14/22-04:33:59.725234
SID:	2404312
Source Port:	49775
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Networking

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

Snort IDS alert for network traffic

E-Banking Fraud

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)

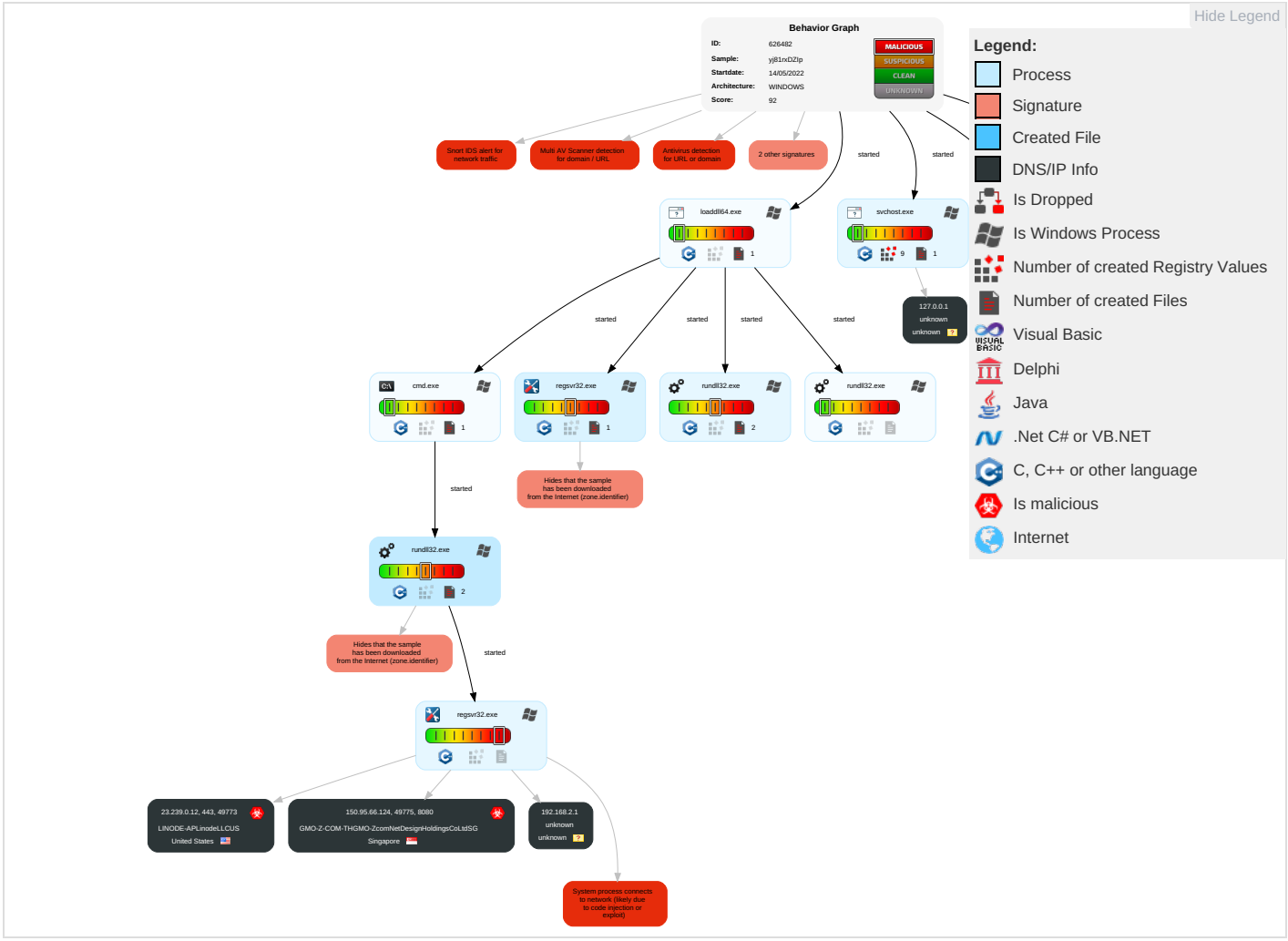
Stealing of Sensitive Information

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 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	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	3 Virtualization/Sandbox Evasion	LSASS Memory	3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 1 Process Injection	Security Account Manager	3 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Ingress Tool Transfer	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	1 Non-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	2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Regsvr32	Cached Domain Credentials	2 File and Directory 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 Rundll32	DCSync	3 4 System Information 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 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/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

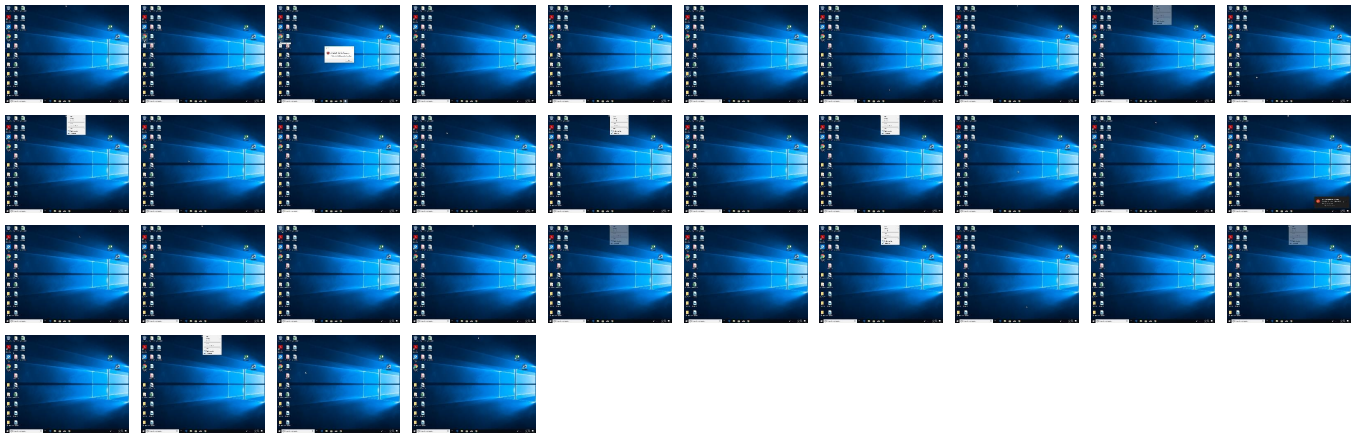
Behavior Graph



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
yj81rxDZIp.dll	35%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.ce0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
4.2.rundll32.exe.1a2c05e0000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
6.2.regsvr32.exe.b80000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
3.2.rundll32.exe.12a08a10000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Domains

No Antivirus matches

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://150.95.66.124:8080/	7%	Virustotal		Browse
http://https://150.95.66.124:8080/	0%	Avira URL Cloud	safe	
http://https://150.95.66.124/	0%	Avira URL Cloud	safe	
http://https://23.239.0.12/x	100%	Avira URL Cloud	malware	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://23.239.0.12/?	100%	Avira URL Cloud	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://23.239.0.12/=	100%	Avira URL Cloud	malware	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://23.239.0.12/	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	

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

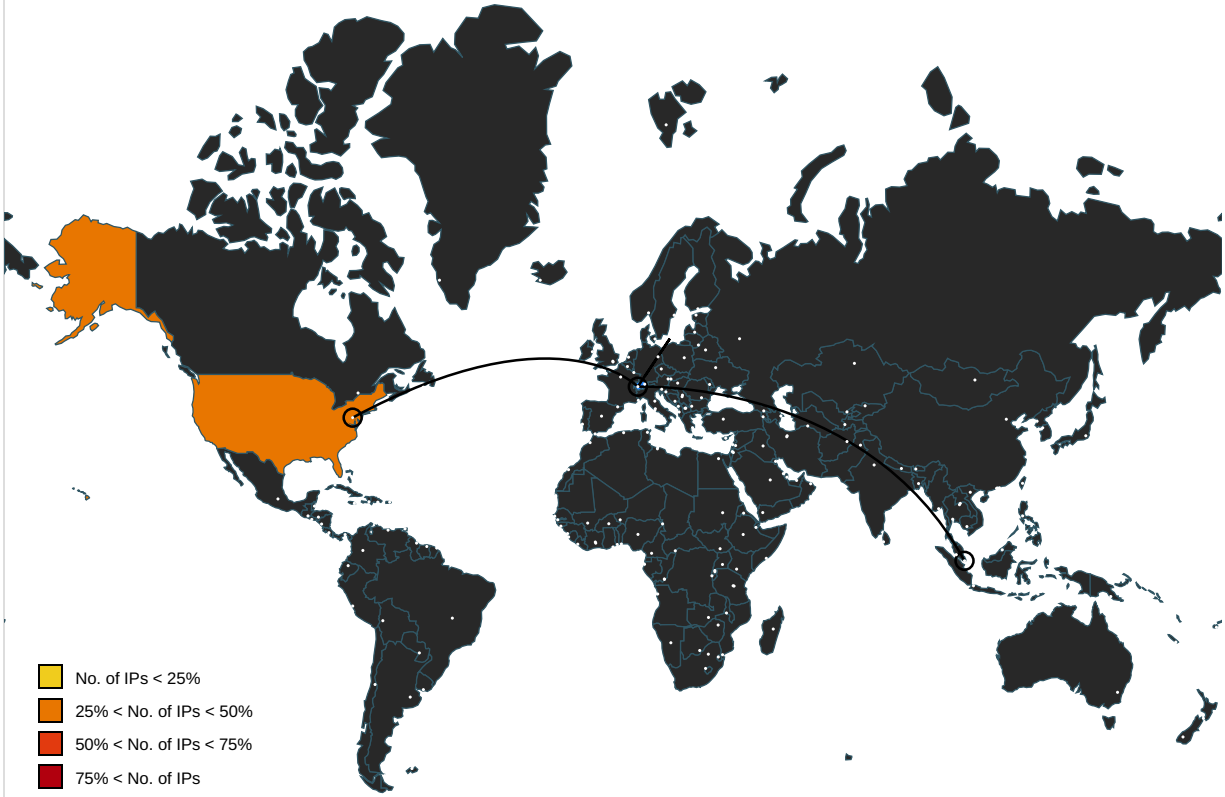
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000016.00000003.589933112.0000023559D9F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.590112698.0000023559D82000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000016.00000003.589933112.0000023559D9F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.590112698.0000023559D82000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://150.95.66.124:8080/	regsvr32.exe, 00000006.00000003.504672087.0000000000A41000.00000004.00000020.00020000.00000000.sdmp	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://150.95.66.124/	regsvr32.exe, 00000006.00000003.504573320.00000000009F2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.944559132.00000000009F2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000016.00000003.585431569.0000023559DBC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.585412811.0000023559DD4000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.585397505.0000023559DD4000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.585362996.0000023559D9B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.585448090.000002355A202000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.586829312.0000023559D82000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://23.239.0.12/x	regsvr32.exe, 00000006.00000003.50457332 0.00000000009F2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.499268137.00000000009F2000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.944559 132.00000000009F2000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.pango.co/privacy	svchost.exe, 00000016.00000003.585431569 .0000023559DBC000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 6.00000003.585412811.0000023559DD4000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.585397505 .0000023559DD4000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 6.00000003.585362996.0000023559D9B000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.585448090 .000002355A202000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 6.00000003.586829312.0000023559D82000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 00000016.00000003.589933112 .0000023559D9F000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 6.00000003.590112698.0000023559D82000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://23.239.0.12/?	regsvr32.exe, 00000006.00000003.50458568 5.0000000000A07000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.504659041.0000000000A21000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.499295 870.0000000000A07000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.499409533.0000000000A2100 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.944590898.0000 000000A22000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.ver)	svchost.exe, 00000016.00000002.616786064 .00000235594EB000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://23.239.0.12/=	regsvr32.exe, 00000006.00000003.50458568 5.0000000000A07000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.504659041.0000000000A21000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.499295 870.0000000000A07000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.499409533.0000000000A2100 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.944590898.0000 000000A22000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000016.00000003.594720633 .000002355A218000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 6.00000003.594881074.0000023559DA1000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.594813489 .000002355A218000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 6.00000003.594855999.0000023559D82000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.594837634 .000002355A202000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://help.disneyplus.com.	svchost.exe, 00000016.00000003.589933112 .0000023559D9F000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 6.00000003.590112698.0000023559D82000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.hotspotshield.com/	svchost.exe, 00000016.00000003.585431569.0000023559DBC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.585412811.0000023559DD4000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.585397505.0000023559DD4000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.585362996.0000023559D9B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.585448090.000002355A202000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.586829312.0000023559D82000.00000004.00000020.00020000.00000000.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
150.95.66.124	unknown	Singapore		135161	GMO-Z-COM-THGMO-ZcomNetDesignHoldingsCoLtdSG	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626482
Start date and time: 14/05/202204:32:13	2022-05-14 04:32:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 35s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yj81rxDZIp (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
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:	mal92.troj.evad.winDLL@19/5@0/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.49.150.241, 23.205.181.161, 40.127.240.158, 23.211.4.86, 20.223.24.244
- Excluded domains from analysis (whitelisted): fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.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, atm-settingsfe-prod-geo.trafficmanager.net, prod.fs.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, settings-prod-uks-2.uksouth.cloudapp.azure.com, store-images.s-microsoft.com, 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
04:33:55	API Interceptor	11x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk

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

C:\ProgramData\Microsoft\Network\Downloader\edb.log

Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24941011137019306
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4Y:BJiRdwfu2SRU4Y
MD5:	0A50BC0D8944C740545889B492DD729E
SHA1:	09C2138770C17485809429A5588CCE24EB529AC5
SHA-256:	EC34BBB5C1C72A00395DC9091C87DFD3C931AE939B5655476F6E8CA22567B97C
SHA-512:	2311FCD429210E56378B47BC08EEDD8E9288CDEB14406097FAC6F02BF55ACB53D0D77F4F26CD462ADC0BC09ADA6853512943A8986F7409B10D85E1AA0FA434 A
Malicious:	false
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x48378a27, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25070166097977487
Encrypted:	false

SSDEEP:	384:Rnm+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:RnJSB2nSB2RSjlK/+mLesOj1J2
MD5:	928624A83F9D798FF803E65377721137
SHA1:	11C16385024ACA104734770654E915BDEA55196A
SHA-256:	E8711ACA4D7AB3DD0C82E9B59BCE3CA2DE255D78D544741EF7E9D6B901FD780C
SHA-512:	B1C108C99AA6443226F7D118A4F249018C710E364A22263067F84D265F2C9FB43983CF59EE294A35EADA58B5C8FA143E0CC97F825CA003BEDC6D13BD64FEEB B
Malicious:	false
Preview:	H7.'... .....e.f.3...w.....)....%...z..9!...z..h.(.....%...z....).....3...w.....B.....@... ....%...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):	0.07727315315325223
Encrypted:	false
SSDEEP:	3:Er7vcEkBjApfm1/+mmgkcICA//FjApfm1/All3VkttlmlnI:ErrcEk6oYDzWoA3
MD5:	4146FB090B15A32AA759FB82DB1905B6
SHA1:	5D1466F577C4C8B68060FB2A13B9718A8E1E2700
SHA-256:	077E85DA7D7D045B8680FDF82B04E9A5BA48191448330A9A4F16433AC5261C15
SHA-512:	0372A572C11DE60FF4CDEF69716DE199D05D3416CF92ED020C2FC998078F5F7AE31E9E80E260EB321D53FFF983132186A7DA9497F2D5D435B85C7429067DD9A
Malicious:	false
Preview:	.JZ{.....3...w..9!...z/..%...z.....%...z...%...z.....%...z.e.....~[..%...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):	6.482098733128464
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:	yj81rxDZIp.dll
File size:	545280
MD5:	4f1cdae4390ecb862267f2eaaf826c74
SHA1:	082de69d51991350ddfc05350073a55571c3ce5d

SHA256:	c4e2c26fd37189447fcd387393974199933fdbffaadf2faaaac5347d1b0a8ef5
SHA512:	04e5e7f0086810c82e1ae0e21fb953df25873f8361da4f20f5d844778d91a77cb3b71489d005ebd4fa7535f2a96db3bfbcca632cebe12d9022f899fab7efee0e
SSDEEP:	12288:B4UJY9B+TenWsSEPHjMOUP9uXdt7JpfYNVr9RM54RutCTdJGqIoTCZ4eEsZiHxHy:B4UJY9BSenZSEPHjMOUP9Udt7JpfYNVe
TLSH:	33C4CFA5435C08FCE762C3395C975BC5B1F7BDAE0664AF260BC18DA05E1BA90F53A381
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 00007F698C737937h
call 00007F698C739AC4h
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]

Instruction
dec eax
add esp, 20h
pop edi
jmp 00007F698C7377E0h
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 00007F698C7464BAh
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007F698C737973h
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 00007F698C746468h
jmp 00007F698C737954h
dec eax
mov eax, dword ptr [eax+eax+00000000h]

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x55cf0	0x6f	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5544c	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5a000	0x2dffc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x59000	0xe1c	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0x1d8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x52000	0x288	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x504ca	0x50600	False	0.389081940124	zlib compressed data	5.26882252971	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x52000	0x3d5f	0x3e00	False	0.355405745968	data	5.39334203825	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

DLL	Import
ole32.dll	CoTaskMemFree, CoLoadLibrary, CoTaskMemAlloc

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x180042050
DllUnregisterServer	2	0x180042080

Possible Origin

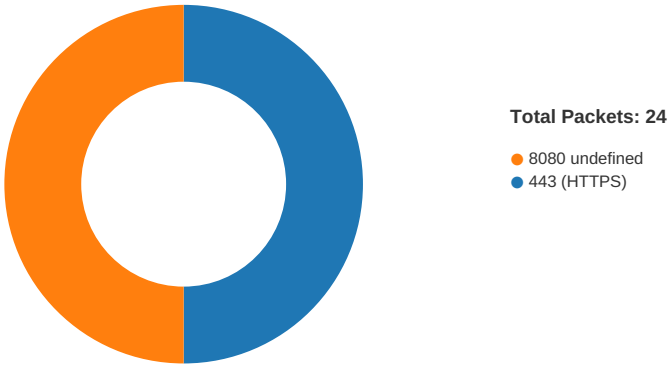
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5150.95.66.124 4977580802404312 05/14/22-04:33:59.725234	TCP	2404312	ET CNC Feodo Tracker Reported CnC Server TCP group 7	49775	8080	192.168.2.5	150.95.66.124

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 04:33:56.379163027 CEST	49773	443	192.168.2.5	23.239.0.12
May 14, 2022 04:33:56.379209042 CEST	443	49773	23.239.0.12	192.168.2.5
May 14, 2022 04:33:56.379298925 CEST	49773	443	192.168.2.5	23.239.0.12
May 14, 2022 04:33:56.414200068 CEST	49773	443	192.168.2.5	23.239.0.12
May 14, 2022 04:33:56.414246082 CEST	443	49773	23.239.0.12	192.168.2.5
May 14, 2022 04:33:56.960381985 CEST	443	49773	23.239.0.12	192.168.2.5
May 14, 2022 04:33:56.960558891 CEST	49773	443	192.168.2.5	23.239.0.12
May 14, 2022 04:33:58.667026043 CEST	49773	443	192.168.2.5	23.239.0.12
May 14, 2022 04:33:58.667067051 CEST	443	49773	23.239.0.12	192.168.2.5
May 14, 2022 04:33:58.667361975 CEST	443	49773	23.239.0.12	192.168.2.5
May 14, 2022 04:33:58.667604923 CEST	49773	443	192.168.2.5	23.239.0.12
May 14, 2022 04:33:58.671036005 CEST	49773	443	192.168.2.5	23.239.0.12

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 04:33:58.712493896 CEST	443	49773	23.239.0.12	192.168.2.5
May 14, 2022 04:33:58.843278885 CEST	443	49773	23.239.0.12	192.168.2.5
May 14, 2022 04:33:58.843379021 CEST	443	49773	23.239.0.12	192.168.2.5
May 14, 2022 04:33:58.843453884 CEST	49773	443	192.168.2.5	23.239.0.12
May 14, 2022 04:33:58.843478918 CEST	49773	443	192.168.2.5	23.239.0.12
May 14, 2022 04:33:58.846863031 CEST	49773	443	192.168.2.5	23.239.0.12
May 14, 2022 04:33:58.846904039 CEST	443	49773	23.239.0.12	192.168.2.5
May 14, 2022 04:33:58.846919060 CEST	49773	443	192.168.2.5	23.239.0.12
May 14, 2022 04:33:58.846963882 CEST	49773	443	192.168.2.5	23.239.0.12
May 14, 2022 04:33:59.725234032 CEST	49775	8080	192.168.2.5	150.95.66.124
May 14, 2022 04:33:59.922143936 CEST	8080	49775	150.95.66.124	192.168.2.5
May 14, 2022 04:33:59.925414085 CEST	49775	8080	192.168.2.5	150.95.66.124
May 14, 2022 04:33:59.926034927 CEST	49775	8080	192.168.2.5	150.95.66.124
May 14, 2022 04:34:00.122863054 CEST	8080	49775	150.95.66.124	192.168.2.5
May 14, 2022 04:34:00.138585091 CEST	8080	49775	150.95.66.124	192.168.2.5
May 14, 2022 04:34:00.138623953 CEST	8080	49775	150.95.66.124	192.168.2.5
May 14, 2022 04:34:00.138844013 CEST	49775	8080	192.168.2.5	150.95.66.124
May 14, 2022 04:34:00.299082041 CEST	49775	8080	192.168.2.5	150.95.66.124
May 14, 2022 04:34:00.497375965 CEST	8080	49775	150.95.66.124	192.168.2.5
May 14, 2022 04:34:00.497461081 CEST	49775	8080	192.168.2.5	150.95.66.124
May 14, 2022 04:34:00.498275042 CEST	49775	8080	192.168.2.5	150.95.66.124
May 14, 2022 04:34:00.732228994 CEST	8080	49775	150.95.66.124	192.168.2.5
May 14, 2022 04:34:01.423486948 CEST	8080	49775	150.95.66.124	192.168.2.5
May 14, 2022 04:34:01.423706055 CEST	49775	8080	192.168.2.5	150.95.66.124
May 14, 2022 04:34:04.423486948 CEST	8080	49775	150.95.66.124	192.168.2.5
May 14, 2022 04:34:04.423563957 CEST	8080	49775	150.95.66.124	192.168.2.5
May 14, 2022 04:34:04.423650026 CEST	49775	8080	192.168.2.5	150.95.66.124
May 14, 2022 04:34:04.424582005 CEST	49775	8080	192.168.2.5	150.95.66.124
May 14, 2022 04:35:46.266910076 CEST	49775	8080	192.168.2.5	150.95.66.124
May 14, 2022 04:35:46.266943932 CEST	49775	8080	192.168.2.5	150.95.66.124

HTTP Request Dependency Graph

- 23.239.0.12

HTTPS Proxied Packets

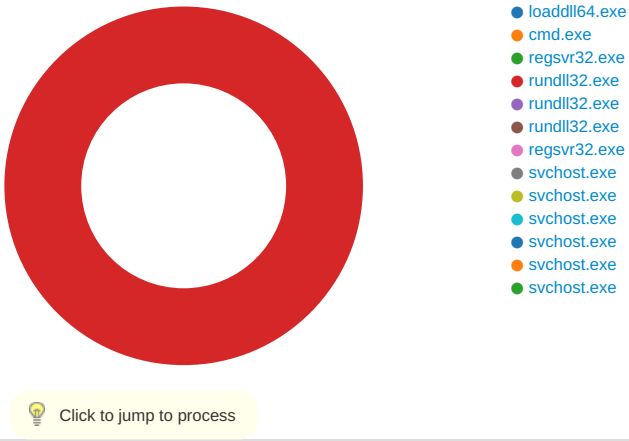
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49773	23.239.0.12	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-14 02:33:58 UTC	0	OUT	GET / HTTP/1.1 Cookie: QplU=hBL9qJmGvW/2EuZ+GBF9bH2Pgx/JXOgEgUtSMs/Xr65WzDcqetddaWzwuXh5JGx39JgIR932OSnFY 7E9phFJznqERMAUy3kUCUPxgga7CbKI6PBLY6I638PGhOIVZSUw305F9rapXw/czJXriHFq3NWcZgk0+SEeip6YZgc +3gUrtVrVeMEIF9KknYl3mfXEDIMIpUXTxabJMjN6Z50nL/WUTE7lAATo6Fjj4ZuuVOtxKlmhmkYxOI9E6JidVirta 2dbsnCt+uBB1ViBVc3HvZOhdAwkTZXZin4oG8ahn7usXUw+DZruLwhbao/dbbpRRY9R4mVWuKxe55MemWZ4R6k= Host: 23.239.0.12 Connection: Keep-Alive Cache-Control: no-cache
2022-05-14 02:33:58 UTC	0	IN	HTTP/1.1 503 Service Temporarily Unavailable Server: nginx Date: Sat, 14 May 2022 02:33:58 GMT Content-Type: text/html Content-Length: 494 Connection: close ETag: "605d14d6-1ee"

Timestamp	kBytes transferred	Direction	Data
2022-05-14 02:33:58 UTC	0	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 45 72 72 6f 72 3c 2f 74 69 74 6c 65 3e 0a 3c 73 74 79 6c 65 3e 0a 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 33 35 65 6d 3b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 54 61 68 6f 6d 61 2c 20 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 2e 3c 2f 68 31 3e 0a 3c 70 3e 53 6f 72 72 79 2c 20 74 68 65 20 70 61 67 65 20 79 6f 75 20 61 72 Data Ascii: <!DOCTYPE html><html><head><title>Error</title><style> body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; }</style></head><body><h1>An error occurred.</h1><p>Sorry, the page you ar

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **7068**, Parent PID: **2504**

General

Target ID:	0
Start time:	04:33:22
Start date:	14/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\yj81rxDZIp.dll"
Imagebase:	0x7ff7e2710000
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: **7080**, Parent PID: **7068**

General

Target ID:	1
Start time:	04:33:22
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\yj81rxDZIp.dll",#1
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **7092**, Parent PID: **7068**

General

Target ID:	2
Start time:	04:33:23
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\yj81rxDZIp.dll
Imagebase:	0x7ff703e50000
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: 00000002.00000002.434632880.0000000000CE0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.435422797.0000000180001000.00000020.00001000.00020000.00000000.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: **7080**

General

Target ID:	3
Start time:	04:33:23
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\yj81rxDZIp.dll",#1
Imagebase:	0x7ff7d6be0000
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: 00000003.00000002.436780201.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.437553196.0000012A08A10000.00000040.00001000.00020000.00000000.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\KZsiDdn\sdxQuTDjzsbvXJ.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: **7112**, Parent PID: **7068**

General

Target ID:	4
Start time:	04:33:23
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\yj81rxDZIp.dll,DllRegisterServer
Imagebase:	0x7ff7d6be0000
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: 00000004.00000002.434955422.000001A2C05E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.434704633.0000000180001000.00000020.00001000.00020000.00000000.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: **3384**, Parent PID: **7068**

General

Target ID:	5
Start time:	04:33:27

Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\yj81rxDZIp.dll,DllUnregisterServer
Imagebase:	0x7ff7d6be0000
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: **2532**, Parent PID: **7104**

General

Target ID:	6
Start time:	04:33:27
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\KZsiDdn\sdxQuTDjzsbvXJ.dll"
Imagebase:	0x7ff703e50000
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: 00000006.00000002.944705463.0000000000B80000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.944856611.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: **1300**, Parent PID: **580**

General

Target ID:	12
Start time:	04:33:44
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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: **5756**, Parent PID: **580**

General

Target ID:	14
Start time:	04:33:50
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6356**, Parent PID: **580**

General

Target ID:	15
Start time:	04:33:54
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **7160**, Parent PID: **580**

General	
Target ID:	16
Start time:	04:33:59
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **6696**, Parent PID: **580**

General	
Target ID:	17
Start time:	04:34:09
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:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **1592**, Parent PID: **580**

General	
Target ID:	22
Start time:	04:34:26
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly