

JOeSandbox Cloud BASIC



ID: 626486

Sample Name: Xp7X1Yf3CM

Cookbook: default.jbs

Time: 04:36:29

Date: 14/05/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report Xp7X1Yf3CM	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	5
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Networking	5
E-Banking Fraud	5
Hooking and other Techniques for Hiding and Protection	6
Malware Analysis System Evasion	6
HIPS / PFW / Operating System Protection Evasion	6
Lowering of HIPS / PFW / Operating System Security Settings	6
Stealing of Sensitive Information	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	9
World Map of Contacted IPs	12
Public IPs	13
Private	13
General Information	13
Warnings	14
Simulations	14
Behavior and APIs	14
Joe Sandbox View / Context	14
IPs	14
Domains	14
ASNs	14
JA3 Fingerprints	14
Dropped Files	14
Created / dropped Files	14
C:\ProgramData\Microsoft\Network\Downloader\edb.chk	14
C:\ProgramData\Microsoft\Network\Downloader\edb.log	15
C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	15
C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	15
C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	16
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	16
Static File Info	16
General	16
File Icon	17
Static PE Info	17
General	17
Entrypoint Preview	17
Rich Headers	18
Data Directories	19
Sections	19
Resources	19
Imports	19
Exports	20
Possible Origin	20
Network Behavior	20
TCP Packets	20
HTTP Request Dependency Graph	20
HTTPS Proxied Packets	20

Statistics	21
Behavior	21
System Behavior	21
Analysis Process: loadll64.exePID: 1008, Parent PID: 6124	21
General	21
File Activities	22
Analysis Process: cmd.exePID: 6000, Parent PID: 1008	22
General	22
File Activities	22
Analysis Process: regsvr32.exePID: 5736, Parent PID: 1008	22
General	22
File Activities	22
Analysis Process: rundll32.exePID: 5872, Parent PID: 6000	23
General	23
File Activities	23
File Deleted	23
Analysis Process: rundll32.exePID: 564, Parent PID: 1008	23
General	23
File Activities	23
Analysis Process: regsvr32.exePID: 6204, Parent PID: 5872	24
General	24
Analysis Process: rundll32.exePID: 6212, Parent PID: 1008	24
General	24
File Activities	24
Analysis Process: svchost.exePID: 6452, Parent PID: 568	24
General	24
Analysis Process: svchost.exePID: 6536, Parent PID: 568	25
General	25
File Activities	25
Registry Activities	25
Analysis Process: svchost.exePID: 6608, Parent PID: 568	25
General	25
Registry Activities	25
Analysis Process: svchost.exePID: 6664, Parent PID: 568	26
General	26
Analysis Process: SgrmBroker.exePID: 6712, Parent PID: 568	26
General	26
Analysis Process: svchost.exePID: 6744, Parent PID: 568	26
General	26
Registry Activities	26
Analysis Process: svchost.exePID: 6948, Parent PID: 568	27
General	27
File Activities	27
Analysis Process: svchost.exePID: 7004, Parent PID: 568	27
General	27
File Activities	27
Registry Activities	27
Analysis Process: svchost.exePID: 1008, Parent PID: 568	27
General	27
File Activities	28
Analysis Process: svchost.exePID: 6336, Parent PID: 568	28
General	28
File Activities	28
Analysis Process: svchost.exePID: 6556, Parent PID: 568	28
General	28
File Activities	28
Registry Activities	29
Analysis Process: MpCmdRun.exePID: 6792, Parent PID: 6744	29
General	29
File Activities	29
File Written	29
Analysis Process: conhost.exePID: 6796, Parent PID: 6792	31
General	31
Analysis Process: svchost.exePID: 4708, Parent PID: 568	31
General	31
File Activities	31
Analysis Process: svchost.exePID: 6280, Parent PID: 568	31
General	32
File Activities	32
Disassembly	32

Windows Analysis Report

Xp7X1Yf3CM

Overview

General Information

Sample Name:	Xp7X1Yf3CM (renamed file extension from none to dll)
Analysis ID:	626486
MD5:	02288abc994cf8...
SHA1:	071594ae4d3eab..
SHA256:	0254b8bc80ee39..
Tags:	exe trojan
Infos:	

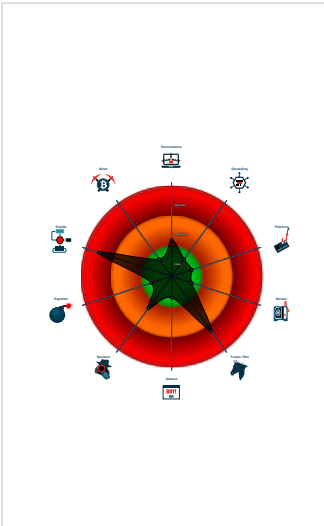
Detection

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Yara detected Emotet
System process connects to network...
Antivirus detection for URL or domain
Query firmware table information (lik...
Changes security center settings (n...
Hides that the sample has been dow...
Queries the volume information (nam...
Contains functionality to check if a d...
Contains functionality to query local...
Deletes files inside the Windows fol...
May sleep (evasive loops) to hinder...
Checks if Antivirus/Antispyware/Fire...

Classification



Process Tree

System is w10x64
loaddll64.exe (PID: 1008 cmdline: loaddll64.exe "C:\Users\user\Desktop\Xp7X1Yf3CM.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
cmd.exe (PID: 6000 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Xp7X1Yf3CM.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
rundll32.exe (PID: 5872 cmdline: rundll32.exe "C:\Users\user\Desktop\Xp7X1Yf3CM.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
regsvr32.exe (PID: 6204 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\KWKbQi\AfskRq\PguzooU.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
regsvr32.exe (PID: 5736 cmdline: regsvr32.exe /s C:\Users\user\Desktop\Xp7X1Yf3CM.dll MD5: D78B75FC68247E8A63ACBA846182740E)
rundll32.exe (PID: 564 cmdline: rundll32.exe C:\Users\user\Desktop\Xp7X1Yf3CM.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
rundll32.exe (PID: 6212 cmdline: rundll32.exe C:\Users\user\Desktop\Xp7X1Yf3CM.dll,DllUnregisterServer MD5: 73C519F050C20580F8A62C849D49215A)
svchost.exe (PID: 6452 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
svchost.exe (PID: 6536 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
svchost.exe (PID: 6608 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
svchost.exe (PID: 6664 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
SgrmBroker.exe (PID: 6712 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
svchost.exe (PID: 6744 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
MpCmdRun.exe (PID: 6792 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
conhost.exe (PID: 6796 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
svchost.exe (PID: 6948 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
svchost.exe (PID: 7004 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
svchost.exe (PID: 1008 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
svchost.exe (PID: 6336 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
svchost.exe (PID: 6556 cmdline: C:\Windows\system32\svchost.exe -k wscsvc -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
svchost.exe (PID: 4708 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
svchost.exe (PID: 6280 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
00000002.00000002.268961112.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.269076253.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.269531970.000001EAA8F30000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.271636704.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.268563839.00000000020D0000.00000040.00001000.00020000.00000000.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.24d00000000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.4e0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.1eaa8f30000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.24d00000000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.1eaa8f30000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 3 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



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)

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)

Lowering of HIPS / PFW / Operating System Security Settings



Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information



Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	1 5 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 Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 Virtualization/Sandbox Evasion	Security Account Manager	1 3 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	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 Hidden Files and Directories	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Obfuscated Files or Information	Cached Domain Credentials	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 Regsvr32	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 Rundll32	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 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

 No Antivirus matches

Dropped Files

 No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.regsvr32.exe.4e0000.1.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
4.2.rundll32.exe.1eaa8f30000.1.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
3.2.rundll32.exe.24d00000000.1.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
2.2.regsvr32.exe.20d0000.0.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File

Domains

 No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://23.239.0.12/default3	100%	Avira URL Cloud	malware	
http://https://23.239.0.12/g	100%	Avira URL Cloud	malware	
http://https://23.239.0.12/Q	100%	Avira URL Cloud	malware	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://23.239.0.12//	100%	Avira URL Cloud	malware	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://cr1.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://23.239.0.12/	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

 No contacted domains info

Contacted URLs

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

URLs from Memory and Binaries

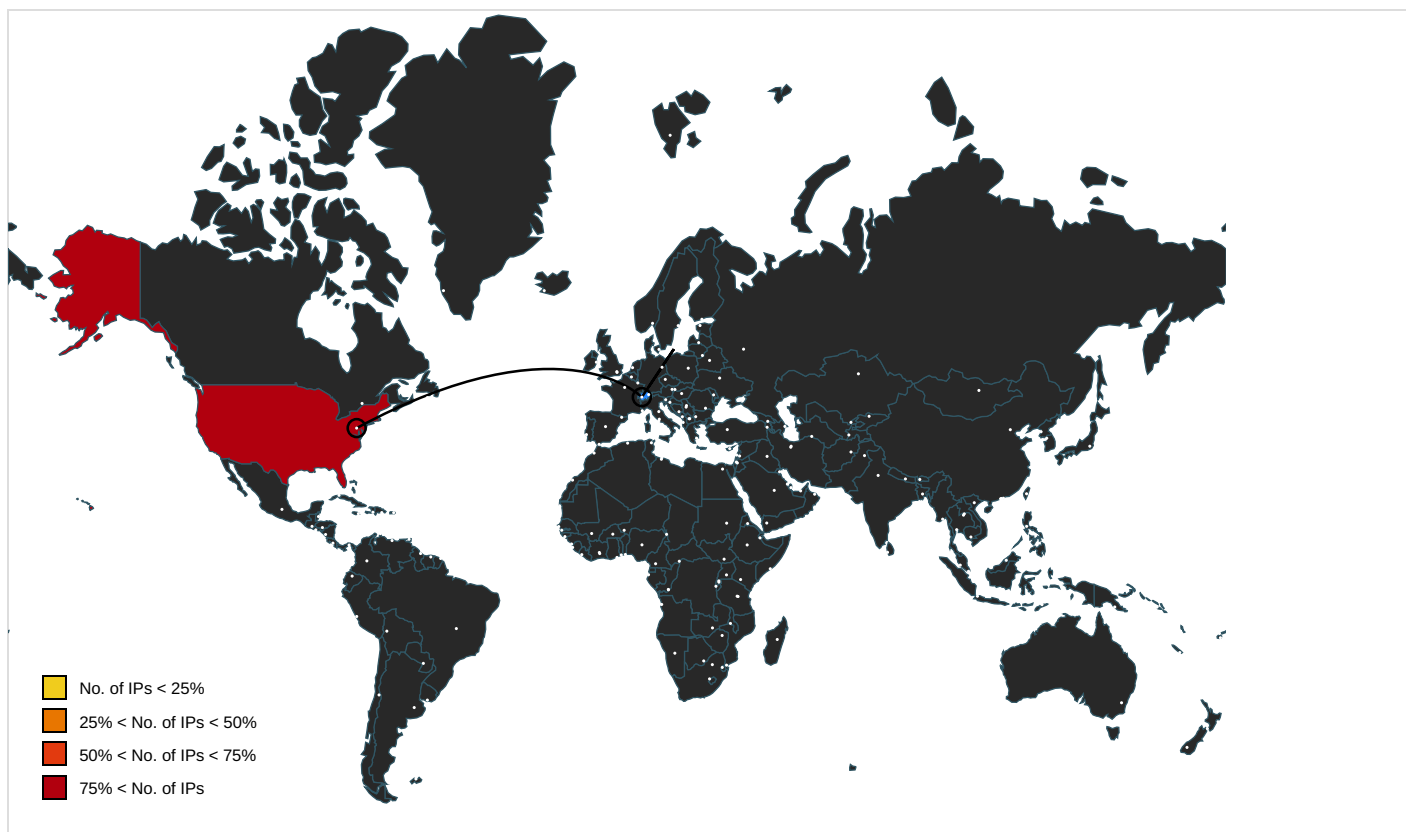
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000D.00000002.326414033.000001803DC3E000.00000004.00000020.00020000.000000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000D.00000003.325699321.000001803DC60000.00000004.00000020.00020000.000000000.sdmp	false		high
http://https://23.239.0.12/default3	regsvr32.exe, 00000005.00000003.341755694.00000000005A2000.00000004.00000020.00020000.000000000.sdmp, regsvr32.exe, 00000005.00000002.783054905.00000000005A2000.00000004.00000020.00020000.000000000.sdmp, regsvr32.exe, 00000005.00000003.341656829.00000000005A2000.00000004.00000020.00020000.000000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000D.00000002.326414033.000001803DC3E000.00000004.00000020.00020000.000000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000D.00000002.326438093.000001803DC54000.00000004.00000020.00020000.000000000.sdmp, svchost.exe, 0000000D.00000003.325689325.000001803DC4F000.00000004.00000020.00020000.000000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000D.00000003.325699321.000001803DC60000.00000004.00000020.00020000.000000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000D.00000003.325742629.000001803DC41000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.326418261.000001803DC42000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://23.239.0.12/g	regsvr32.exe, 00000005.00000003.341755694.000000000005A2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.783054905.000000000005A2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.341656829.000000000005A2000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000D.00000003.325699321.000001803DC60000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000D.00000003.325712400.000001803DC4B000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000D.00000003.303805187.000001803DC31000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000D.00000003.325742629.000001803DC41000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.326418261.000001803DC42000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://23.239.0.12/Q	regsvr32.exe, 00000005.00000003.341715727.000000000005D1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.783098549.000000000005D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.341699831.000000000005CA000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000020.00000003.506337806.0000017583B9C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.506417373.0000017584002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.506353737.0000017583BD5000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.506369168.0000017583BD5000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.506387752.0000017583BBD000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.506404560.0000017583B79000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000020.00000003.506337806.0000017583B9C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.506417373.0000017584002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.506353737.0000017583BD5000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.506369168.0000017583BD5000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.506387752.0000017583BBD000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.506404560.0000017583B79000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.bingmapsportal.com	svchost.exe, 0000000D.00000002.326382614.000001803DC13000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000D.00000002.326414033.000001803DC3E000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000D.00000003.325699321.000001803DC60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://23.239.0.12//	regsvr32.exe, 00000005.00000003.341715727.000000000005D1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.783098549.000000000005D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.341699831.000000000005CA000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000020.00000003.508864000.0000017583B79000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.508751661.0000017583B9C000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000D.00000003.325739063.000001803DC45000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 0000000D.00000003.325684619.000001803DC66000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.326449611.000001803DC69000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000D.00000002.326414033.000001803DC3E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 0000000D.00000003.303805187.000001803DC31000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000D.00000003.325739063.000001803DC45000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ver)	svchost.exe, 00000011.00000002.675155635.000001CF4FC86000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000002.533623859.00000175832EE000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000D.00000003.325727485.000001803DC2C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.326422161.000001803DC47000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.325734615.000001803DC46000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000020.00000003.513231663.0000017583B79000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.513157051.0000017583BD3000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.513123257.0000017583BD3000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.513185679.0000017583B9C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.513196480.0000017583BBD000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000D.00000002.326382614.000001803DC13000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.326414033.000001803DC3E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 0000000B.00000002.782695258.000001F057643000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000D.00000002.326438093.000001803DC54000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.325689325.000001803DC4F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000D.00000003.325699321.000001803DC60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000D.00000003.303805187.000001803DC31000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000D.00000003.325699321.000001803DC60000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.hotspotshield.com/	svchost.exe, 00000020.00000003.506337806 .0000017583B9C000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 0.00000003.506417373.0000017584002000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.506353737 .0000017583BD5000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 0.00000003.506369168.0000017583BD5000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.506387752 .0000017583BBD000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 0.00000003.506404560.0000017583B79000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000D.00000002.326422161 .000001803DC47000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 D.00000003.325734615.000001803DC46000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000020.00000003.508864000 .0000017583B79000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 0.00000003.508751661.0000017583B9C000.00 000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000D.00000003.303805187 .000001803DC31000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000D.00000003.325689325 .000001803DC4F000.00000004.00000020.0002 0000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000D.00000003.325699321 .000001803DC60000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://disneyplus.com/legal	svchost.exe, 00000020.00000003.508864000 .0000017583B79000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 0.00000003.508751661.0000017583B9C000.00 000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000D.00000002.326409621 .000001803DC3A000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 D.00000003.303805187.000001803DC31000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000D.00000002.326422161 .000001803DC47000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 D.00000003.325734615.000001803DC46000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 0000000B.00000002.782695258 .000001F057643000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000D.00000003.325699321 .000001803DC60000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://help.disneyplus.com	svchost.exe, 00000020.00000003.508864000 .0000017583B79000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 0.00000003.508751661.0000017583B9C000.00 000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000B.00000002.782695258 .000001F057643000.00000004.00000020.0002 0000.00000000.sdmp	false	URL Reputation: safe	low
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000D.00000003.325712400 .000001803DC4B000.00000004.00000020.0002 0000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

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

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626486
Start date and time: 14/05/202204:36:29	2022-05-14 04:36:29 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Xp7X1Yf3CM (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:	38
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:	mal76.troj.evad.winDLL@29/6@0/2

EGA Information:	Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	- Successful, ratio: 99% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Adjust boot time - Enable AMSI - Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, WMIADAP.exe, backgroundTaskHost.exe, WmiPrvSE.exe, UsoClient.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.4.86, 20.49.150.241, 20.223.24.244
- Excluded domains from analysis (whitelisted): fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, settings-win.data.microsoft.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, go.microsoft.com, settings-prod-uks-2.uksouth.cloudapp.azure.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaiized.net, prod.fs.microsoft.com.akadns.net, atm-settingsfe-prod-geo.trafficmanager.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.
- VT rate limit hit for: Xp7X1Yf3CM.dll

Simulations

Behavior and APIs

Time	Type	Description
04:38:08	API Interceptor	12x Sleep call for process: svchost.exe modified
04:39:01	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process: C:\Windows\System32\svchost.exe

File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:ShaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF3180
Malicious:	false
Preview:	*.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....*.....

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24943125406421562
Encrypted:	false
SSDEEP:	1536:BJiRdIVzkZm3lyf49uyc0ga04PdHs9LrM/oVMUdSRU4j:BJiRdwfu2SRU4j
MD5:	C9B69AD24B56E5D05703283BF09823F9
SHA1:	378CD57403FEDE55B79B726DBFF8A0432AD6D06E
SHA-256:	CC15C2F3A3A9F3CA451FBF25590B1DF153ADDDF476D77EC03DD4A987EF29A3F5
SHA-512:	9B2CD3EEC0E0FC0998B89995784207EF6C70F473AA0FB0A213A4E125431E3635DFE17FC9011FD8BF7CD6178E15CF0FD619FB5799A8DA5C8572DEDD6A8BE55CD8
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 0xd3505601, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25071193549470316
Encrypted:	false
SSDEEP:	384:pbm+W0StseCJ48EApW0StseCJ48E2rTSjIK/ebmLerYRSRY1J2:pbJSB2nSB2RSjIK/+mLesOj1J2
MD5:	0B8F20E19BC239C73CB26AFE8699C673
SHA1:	3BDC85282E48C3F374117BD7C5DD444BB04DC58C
SHA-256:	C2213C8DC45B472D6913F51D0FCA316CC8E26C4988A616875FA237C81BBF899D
SHA-512:	431189D44754ED3C4C29D86D268F45DF45EA703190EE8EBA860864726A2BB1C0F09817129409E7B8DB23016FAC0BB46DF84FEDD72FF6831F851D64B62FCA8A7
Malicious:	false
Preview:	.PV....ef.3...w.....).....)....z...&...z?.h.(.....)....z....).....3...w.....B.....@....."z.v.)...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):	0.0769246725658165
Encrypted:	false

SSDEEP:	3:OS7vtytvKqXIN0fsDMkgEukagf9fLzgEXiYII3VkttlmInI:NrSvK3b8f+3
MD5:	F17347206F758969DB47E5C0055D969D
SHA1:	1E665E1EDFC2359812488F4DF5BAF5CD3EDF0248
SHA-256:	299D6F87C6BD2C6F9F8EDF232AF256A0D244BCA0F57E59D9E7C508D8FF62EBB0
SHA-512:	79521BD85A97A361388DD0810577BB469CE4635E61F1123E64209C50F3D5CEE7748F272199A7A7F3DF784A4AA1D3E7E7F75202240DE8A6498A2E05201C923A14
Malicious:	false
Preview:	2.....3...w...&...z?...z.....)...z...)...z.9...)...z.u.....)...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:YMRl83Xl2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA CA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.1636012365831876
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3z5+O:j+s+v+b+P+m+0+Q+q+q+O
MD5:	A712CDD447B0EB1AAEAA73F94CBB24E0
SHA1:	90869C031A35A2088EB90CCB1AAF2A76EA2EEF3C
SHA-256:	04517E3F97804EAC19C7DD88E175757461554371F89AC491086E35E3A34806F2
SHA-512:	F17960B9F67BBDF2EE173C7E9DFBEA22D06FD266C5DDD2984E12EE43B527562FAF1976B110449277BCD50383F70DED41A0439A19FBBCE34030774F5DFD6542 E
Malicious:	false
Preview:	Mp.C.m.d.R.u.n.:.C.o.m.m.a.n.d. . Line.: "C:\P.r.o.g.r.a.m. .F.i.l.e.s\W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\m.p.c.m.d.r.u.n...e.x.e.". -w.d.e.n.a.b.l.e.....S.t.a.r.t. .T.i.m.e.:. .T.h.u. .J.u.n. .2.7. .2.0.1.9. .0. 1.:2.9.:4.9.....M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:.h.r. =. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:.M.p.W.D.E.n.a.b.l.e.(T.R.U.E). .f.a.i.l.e.d. . (8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:.E.n.d. .T.i.m.e.:. .T.h.u. .J.u.n. .2.7. .2.0.1.9. .0.1.:2.9.:4.9.....

Static File Info	
General	
File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.482106783381786
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:	Xp7X1Yf3CM.dll
File size:	545280
MD5:	02288abc994cf899ca0dc3d554eb284a
SHA1:	071594ae4d3eabc482032a69fe6b6019f1968b95

SHA256:	0254b8bc80ee3949cabbe9c64c6a1b8967259642e26c080c4b7c95bd97bba938
SHA512:	e34e81eeeadc791d9ed12cd2c4730e7fbafe5c42c00b74ddad90324ee5bffa169a5aab105549964a6cac19c048a59a902dd073c283fff81217e6f6cc22405aca
SSDEEP:	12288:B4UJY9B+TenWsSEPHjMOUP9uXdt7JpfYNvr9RM54RutCTdJGqloTCZ4eEsZHHxHy:B4UJY9BSenZSEPHjMOUP9Udt7JpfYNVP
TLSH:	87C4CFA5435C08FCE762C3395C975BC5B1F7BDAE0664AF260BC18DA05E1BA90F53A381
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 00007FC92875E697h
call 00007FC928760824h
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 00007FC92875E540h
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 00007FC92876D21Ah
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007FC92875E6D3h
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 00007FC92876D1C8h
jmp 00007FC92875E6B4h
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	0x2dff	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x59000	0xe1c	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0x1d8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x52000	0x288	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x504ca	0x50600	False	0.389081940124	zlib compressed data	5.26882252971	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x52000	0x3d5f	0x3e00	False	0.355342741935	data	5.3927335582	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.data	0x56000	0x20d8	0x1200	False	0.180772569444	data	2.18161586025	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x59000	0xe1c	0x1000	False	0.44580078125	data	4.98556265168	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x5a000	0x2dff	0x2e000	False	0.839408542799	data	7.73448363752	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0x6f8	0x800	False	0.1796875	data	1.81179169858	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

DLL	Import
ole32.dll	CoTaskMemFree, CoLoadLibrary, CoTaskMemAlloc

Exports		
Name	Ordinal	Address
DllRegisterServer	1	0x180042050
DllUnregisterServer	2	0x180042080

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

Network Behavior				
TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 04:38:14.668498993 CEST	49745	443	192.168.2.3	23.239.0.12
May 14, 2022 04:38:14.668550968 CEST	443	49745	23.239.0.12	192.168.2.3
May 14, 2022 04:38:14.668674946 CEST	49745	443	192.168.2.3	23.239.0.12
May 14, 2022 04:38:14.695267916 CEST	49745	443	192.168.2.3	23.239.0.12
May 14, 2022 04:38:14.695306063 CEST	443	49745	23.239.0.12	192.168.2.3
May 14, 2022 04:38:15.252432108 CEST	443	49745	23.239.0.12	192.168.2.3
May 14, 2022 04:38:15.252568960 CEST	49745	443	192.168.2.3	23.239.0.12
May 14, 2022 04:38:15.797986984 CEST	49745	443	192.168.2.3	23.239.0.12
May 14, 2022 04:38:15.798012018 CEST	443	49745	23.239.0.12	192.168.2.3
May 14, 2022 04:38:15.798300028 CEST	443	49745	23.239.0.12	192.168.2.3
May 14, 2022 04:38:15.799674988 CEST	49745	443	192.168.2.3	23.239.0.12
May 14, 2022 04:38:15.804275990 CEST	49745	443	192.168.2.3	23.239.0.12
May 14, 2022 04:38:15.844505072 CEST	443	49745	23.239.0.12	192.168.2.3
May 14, 2022 04:38:16.650969982 CEST	443	49745	23.239.0.12	192.168.2.3
May 14, 2022 04:38:16.651042938 CEST	443	49745	23.239.0.12	192.168.2.3
May 14, 2022 04:38:16.651138067 CEST	49745	443	192.168.2.3	23.239.0.12
May 14, 2022 04:38:16.651187897 CEST	49745	443	192.168.2.3	23.239.0.12
May 14, 2022 04:38:16.651643991 CEST	49745	443	192.168.2.3	23.239.0.12
May 14, 2022 04:38:16.651660919 CEST	443	49745	23.239.0.12	192.168.2.3

HTTP Request Dependency Graph
23.239.0.12

HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49745	23.239.0.12	443	C:\Windows\System32\regsvr32.exe
Timestamp	kBytes transferred	Direction	Data		

Timestamp	kBytes transferred	Direction	Data
2022-05-14 02:38:15 UTC	0	OUT	GET / HTTP/1.1 Cookie: TgcenRvYsT=Ylh08jWDXMh8HJcxJPKpZsCBPxbkXnKV0Ywocuph5vbaWbOyx1yPJWsxIZtRv6+7LpHShc pjfeOPEEFoMdGc3nq/EDmkJ5XKAG86gVddDyP7E2S+aKcpK/fFmThBOO7yCq8UgXOOMeNjQMqnznww1LypRr4fUc8l Ysobu5EDOD1jkaCoePpopUDRWnTelxuHsD5c/bZUFN7g3HjUxiuk4yNbKQoEvBGIAJPfp4AWpRmeI4505O3PoYJSv PlpGT7K94JrT7+FK+rSjUS5iJ0R4uq6W7kb/CIK3S1S+BFkY= Host: 23.239.0.12 Connection: Keep-Alive Cache-Control: no-cache
2022-05-14 02:38:16 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 14 May 2022 02:38:16 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2022-05-14 02:38:16 UTC	0	IN	Data Raw: 32 34 66 0d 0a bc c4 01 8a fb b9 df c1 5c a9 a8 46 6f 07 9b 80 01 e1 2f 14 12 1f ac 2f d8 64 81 c8 60 3a 61 1a 95 8a 10 45 d4 4b 6d 1b a6 6f 20 85 5f 97 a7 09 49 05 fa 6c 44 1d ac 24 07 91 87 47 7d 60 16 18 51 45 6f 65 a3 1c c3 e5 e1 a4 bc 13 45 0d c0 16 df c6 79 cd c3 1d 9c d8 f4 99 27 5f f3 95 86 af 57 20 4b f7 37 50 dc 85 36 c2 64 8a 89 47 00 79 ba 6c 22 b1 be cb 8d c2 65 aa 76 07 93 de c6 3d bd 3b 7b 96 ee db b0 89 89 c2 e8 4f c8 73 53 82 5c ea 17 de f7 b2 25 ce 24 04 9a eb 0d 58 48 37 4a a7 8c d5 36 8d e3 80 86 68 4a a9 60 0b 4f 73 28 b2 45 0b 76 c7 13 5a 0e 31 5e 49 0f dd 4c ba f0 ef d7 01 f9 f4 c9 1c b5 4d f6 29 01 92 0c 30 c1 ca dc 7e c5 47 05 af 21 1c af 17 59 7c 56 91 d2 a2 bf c1 fb 66 06 29 13 d2 b9 99 9b 96 55 e5 83 f3 0d 56 8b cd 51 8f cd 16 Data Ascii: 24fFo/d':aEKmo _lID\$G}'QEoeEy'_W K7P6dGyl"ev={OsS!%\$XH7J6hJ'Os(EvZ1^lLM)0-Gi'Y Vf)UVQ

Statistics

Behavior



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

 Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 1008, Parent PID: 6124

General

Target ID:	0
Start time:	04:37:37
Start date:	14/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\Xp7X1Yf3CM.dll"
Imagebase:	0x7ff651af0000
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: 6000, Parent PID: 1008

General

Target ID:	1
Start time:	04:37:37
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\Xp7X1Yf3CM.dll",#1
Imagebase:	0x7ff709750000
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: 5736, Parent PID: 1008

General

Target ID:	2
Start time:	04:37:38
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\Xp7X1Yf3CM.dll
Imagebase:	0x7ff708980000
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: 00000002.00000002.268961112.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.268563839.00000000020D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: rundll32.exe PID: 5872, Parent PID: 6000

General

Target ID:	3
Start time:	04:37:38
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\Xp7X1Yf3CM.dll",#1
Imagebase:	0x7ff68fda0000
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: 00000003.00000002.271636704.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.272116119.0000024D00000000.00000040.00001000.00020000.00000000.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\KWKbQi\AfskRqPguzooU.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: 564, Parent PID: 1008

General

Target ID:	4
Start time:	04:37:38
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Xp7X1Yf3CM.dll,DllRegisterServer
Imagebase:	0x7ff68fda0000
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: 00000004.00000002.269076253.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.269531970.000001EAA8F30000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: regsvr32.exe PID: 6204, Parent PID: 5872

General

Target ID:	5
Start time:	04:37:42
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\KWKbQi\AfskRqPguzooU.dll"
Imagebase:	0x7ff708980000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.783254222.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.782535445.0000000004E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6212, Parent PID: 1008

General

Target ID:	6
Start time:	04:37:42
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Xp7X1Yf3CM.dll,DllUnregisterServer
Imagebase:	0x7ff68fda0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: svchost.exe PID: 6452, Parent PID: 568

General

Target ID:	10
Start time:	04:37:53
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:	0x7ff73c930000

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

Analysis Process: svchost.exe PID: 6536, Parent PID: 568

General

Target ID:	11
Start time:	04:37:56
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
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	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

Analysis Process: svchost.exe PID: 6608, Parent PID: 568

General

Target ID:	12
Start time:	04:37:57
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

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

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

Analysis Process: svchost.exe PID: 6664, Parent PID: 568

General

Target ID:	13
Start time:	04:37:58
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: 6712, Parent PID: 568

General

Target ID:	14
Start time:	04:37:59
Start date:	14/05/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7c6ea0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6744, Parent PID: 568

General

Target ID:	15
Start time:	04:37:59
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsv
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol
----------	------------	-------	----------------	--------

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

Analysis Process: svchost.exe PID: 6948, Parent PID: 568

General

Target ID:	16
Start time:	04:38:05
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
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: 7004, Parent PID: 568

General

Target ID:	17
Start time:	04:38:07
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:	0x7ff73c930000
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: 1008, Parent PID: 568

General

Target ID:	19
------------	----

Start time:	04:38:42
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:	0x7ff73c930000
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: 6336, Parent PID: 568

General	
Target ID:	20
Start time:	04:38:48
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:	0x7ff73c930000
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: 6556, Parent PID: 568

General	
Target ID:	25
Start time:	04:38:51
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:	0x7ff73c930000
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
----------	------	------	----------	----------	------------	-------	----------------	--------

Analysis Process: MpCmdRun.exe PID: 6792, Parent PID: 6744

General

Target ID:	27
Start time:	04:39:00
Start date:	14/05/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7b0320000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8156	182	0d 00 0a 00 0d 00 0a 00 2d 00 0d 00 0a 00	----- ----- -----	success or wait	1	7FF7B034BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8338	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 61 00 74 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 31 00 34 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 34 00 3a 00 33 00 39 00 3a 00 30 00 31 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Sat May 14 2022 04:39 :01	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8596	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8682	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8702	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8788	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 61 00 74 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 31 00 34 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 34 00 3a 00 33 00 39 00 3a 00 30 00 31 00 0d 00 0a 00	MpCmdRun: End Time: Sat May 14 2022 04:39:01	success or wait	1	7FF7B034BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\IcmdRun.log	8888	174	2d 00 0d 00 0a 00	----- ----- -----	success or wait	1	7FF7B034BC96	WriteFile

Analysis Process: conhost.exe PID: 6796, Parent PID: 6792	
General	
Target ID:	28
Start time:	04:39:01
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4708, Parent PID: 568	
General	
Target ID:	30
Start time:	04:39:06
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:	0x7ff73c930000
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: 6280, Parent PID: 568	
---	--

General	
Target ID:	32
Start time:	04:39:19
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:	0x7ff73c930000
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