

JoeSandbox Cloud BASIC



ID: 626506

Sample Name: Ru97gvh8ir.dll

Cookbook: default.jbs

Time: 05:24:13

Date: 14/05/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report Ru97gvh8ir.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	5
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Networking	5
E-Banking Fraud	5
Hooking and other Techniques for Hiding and Protection	6
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	13
Public IPs	13
Private	13
General Information	14
Warnings	14
Simulations	14
Behavior and APIs	14
Joe Sandbox View / Context	15
IPs	15
Domains	15
ASNs	15
JA3 Fingerprints	15
Dropped Files	15
Created / dropped Files	15
C:\ProgramData\Microsoft\Network\Downloader\edb.chk	15
C:\ProgramData\Microsoft\Network\Downloader\edb.log	15
C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	16
C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	16
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	17
General	17
File Icon	17
Static PE Info	17
General	17
Entrypoint Preview	18
Rich Headers	19
Data Directories	19
Sections	19
Resources	20
Imports	20
Exports	20
Possible Origin	20
Network Behavior	20
TCP Packets	20
HTTP Request Dependency Graph	21
HTTPS Proxied Packets	21

Statistics	21
Behavior	21
System Behavior	22
Analysis Process: loadll64.exePID: 6304, Parent PID: 1908	22
General	22
File Activities	22
Analysis Process: cmd.exePID: 6316, Parent PID: 6304	22
General	22
File Activities	23
Analysis Process: regsvr32.exePID: 6324, Parent PID: 6304	23
General	23
File Activities	23
File Deleted	23
Analysis Process: rundll32.exePID: 6336, Parent PID: 6316	23
General	23
File Activities	24
Analysis Process: rundll32.exePID: 6352, Parent PID: 6304	24
General	24
File Activities	24
Analysis Process: regsvr32.exePID: 6500, Parent PID: 6324	24
General	24
Analysis Process: rundll32.exePID: 6516, Parent PID: 6304	25
General	25
File Activities	25
Analysis Process: svchost.exePID: 6812, Parent PID: 568	25
General	25
Analysis Process: svchost.exePID: 6856, Parent PID: 568	25
General	25
File Activities	26
Registry Activities	26
Analysis Process: svchost.exePID: 6920, Parent PID: 568	26
General	26
Registry Activities	26
Analysis Process: svchost.exePID: 6980, Parent PID: 568	26
General	26
Analysis Process: SgrmBroker.exePID: 7032, Parent PID: 568	26
General	26
Analysis Process: svchost.exePID: 7060, Parent PID: 568	27
General	27
Registry Activities	27
Analysis Process: svchost.exePID: 1112, Parent PID: 568	27
General	27
File Activities	27
Analysis Process: svchost.exePID: 6092, Parent PID: 568	28
General	28
File Activities	28
Registry Activities	28
Analysis Process: svchost.exePID: 6188, Parent PID: 568	28
General	28
File Activities	28
Analysis Process: svchost.exePID: 6796, Parent PID: 568	28
General	28
File Activities	29
Analysis Process: svchost.exePID: 3356, Parent PID: 568	29
General	29
File Activities	29
Registry Activities	29
Analysis Process: MpCmdRun.exePID: 3672, Parent PID: 7060	29
General	29
File Activities	30
File Written	30
Analysis Process: conhost.exePID: 5836, Parent PID: 3672	31
General	31
Disassembly	31

Windows Analysis Report

Ru97gvh8ir.dll

Overview

General Information

Sample Name:

Ru97gvh8ir.dll

Analysis ID:

626506

MD5:

d0a17f6649895f3.

SHA1:

3df95c0b1a2dd0..

SHA256:

fea10a0d60a2d6..

Tags:

exe

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Emotet

Score:

84

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

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...

Classification

Process Tree

System is w10x64

loadll64.exe (PID: 6304 cmdline: loadll64.exe "C:\Users\user\Desktop\Ru97gvh8ir.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)

cmd.exe (PID: 6316 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Ru97gvh8ir.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)

rundll32.exe (PID: 6336 cmdline: rundll32.exe "C:\Users\user\Desktop\Ru97gvh8ir.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)

regsvr32.exe (PID: 6324 cmdline: regsvr32.exe /s C:\Users\user\Desktop\Ru97gvh8ir.dll MD5: D78B75FC68247E8A63ACBA846182740E)

regsvr32.exe (PID: 6500 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\QHTOcg\FaLIWfXNGlBk.dll" MD5: D78B75FC68247E8A63ACBA846182740E)

rundll32.exe (PID: 6352 cmdline: rundll32.exe C:\Users\user\Desktop\Ru97gvh8ir.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)

rundll32.exe (PID: 6516 cmdline: rundll32.exe C:\Users\user\Desktop\Ru97gvh8ir.dll,DllUnregisterServer MD5: 73C519F050C20580F8A62C849D49215A)

svchost.exe (PID: 6812 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 6856 cmdline: c:\windows\system32\svchost.exe -k localService -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 6920 cmdline: c:\windows\system32\svchost.exe -k networkService -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 6980 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

SgrmBroker.exe (PID: 7032 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)

svchost.exe (PID: 7060 cmdline: c:\windows\system32\svchost.exe -k localSystemNetworkRestricted -p -s wscntlm MD5: 32569E403279B3FD2EDB7EBD036273FA)

MpCmdRun.exe (PID: 3672 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)

conhost.exe (PID: 5836 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

svchost.exe (PID: 1112 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 6092 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 6188 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 6796 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe (PID: 3356 cmdline: C:\Windows\system32\svchost.exe -k wscntlm -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)

cleanup

Malware Configuration

No configs have been found

Copyright Joe Security LLC 2022

Page 4 of 31

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.260476507.0000000000DB0000.00000040.00001000.00020000.00000000.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.258276727.0000019B71C10000.00000040.00001000.00020000.00000000.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.648153388.0000000180001000.00000020.00001000.00020000.00000000.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.258391181.0000000180001000.00000020.00001000.00020000.00000000.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.647866634.0000000000E70000.00000040.00001000.00020000.00000000.sdump	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

[Click to see the 3 entries](#)

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.regsvr32.exe.e70000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.db0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.19b71c10000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.db0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.e70000.1.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



Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking



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

E-Banking Fraud



Yara detected Emotet

Hooking and other Techniques for Hiding and Protection



Hides that the sample has been downloaded from the Internet (zone.identifier)

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

Source	Detection	Scanner	Label	Link
Ru97gvh8ir.dll	30%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.regsvr32.exe.e70000.1.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
3.2.rundll32.exe.19b71c10000.1.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
4.2.rundll32.exe.17947080000.1.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.db0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://23.239.0.12/?T	100%	Avira URL Cloud	malware	
http://https://23.239.0.12/yT	100%	Avira URL Cloud	malware	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://23.239.0.12/7	100%	Avira URL Cloud	malware	
http://https://23.239.0.12/;	100%	Avira URL Cloud	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://activity.windows.comr	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

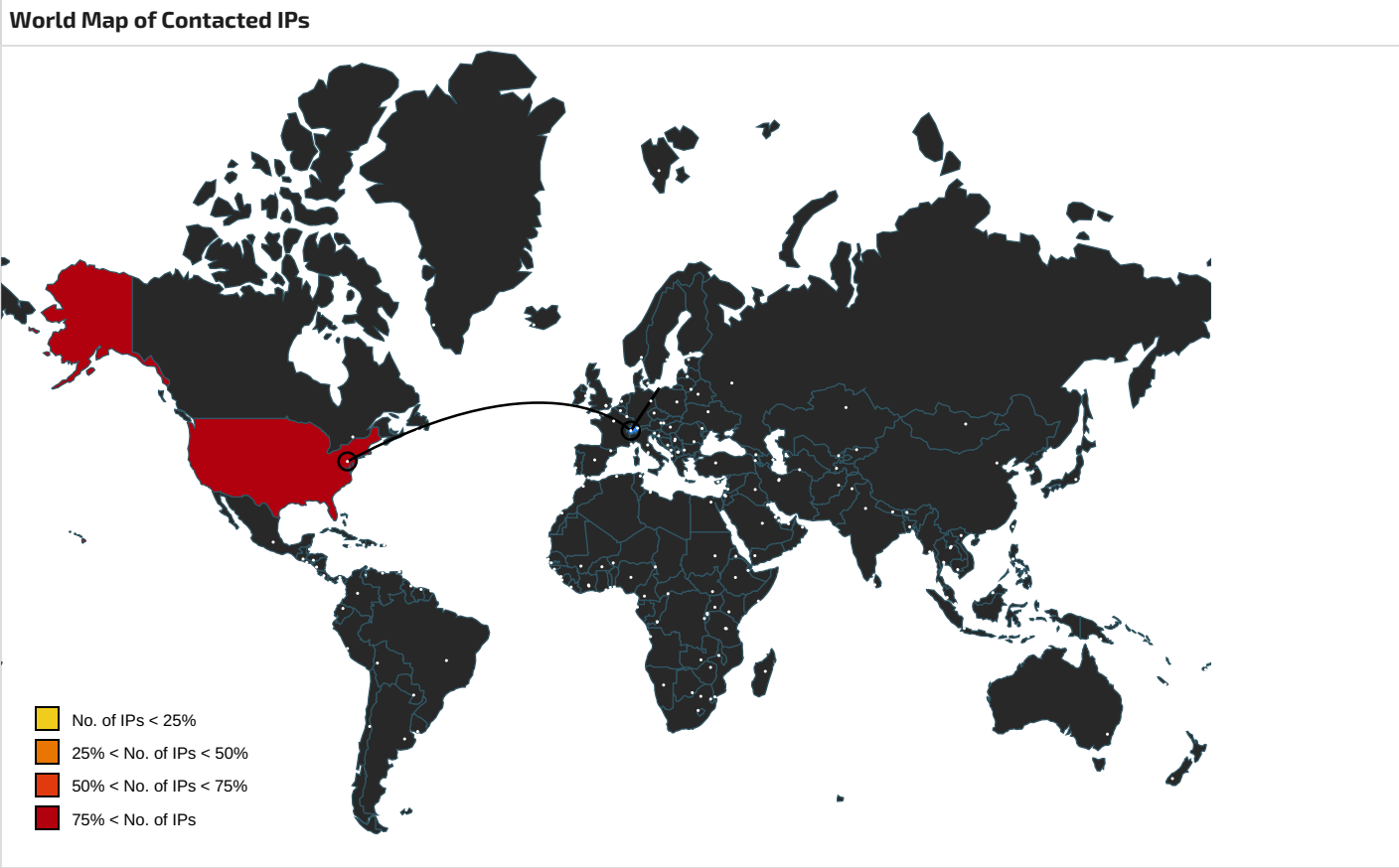
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000D.00000002.318792183.00000226EE43E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000D.00000003.318354950.00000226EE462000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000D.00000002.318792183.00000226EE43E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000D.00000002.318835280.00000226EE45D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318374543.00000226EE45B000.0000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000D.00000003.318419162.00000226EE446000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.318812314.00000226EE447000.0000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318390455.00000226EE441000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000D.00000003.318354950.00000226EE462000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://23.239.0.12/?T	regsvr32.exe, 00000005.00000003.332877829.0000000000C64000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.647653042.0000000000C75000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://23.239.0.12/yT	regsvr32.exe, 00000005.00000003.332877829.0000000000C64000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.647653042.0000000000C75000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000D.00000003.318429092.00000226EE442000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318390455.00000226EE441000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.318806583.00000226EE443000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000D.00000003.318354950.00000226EE462000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000D.00000002.318737872.00000226EE429000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318374543.00000226EE45B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000D.00000003.296600069.00000226EE432000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000D.00000003.318429092.00000226EE442000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318390455.00000226EE441000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.318806583.00000226EE443000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000015.00000003.410672122.00000270A5602000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410599081.00000270A51AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410771133.00000270A51AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410791747.00000270A5619000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410692294.00000270A5603000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.41067456.00000270A519C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410743577.00000270A518A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000015.00000003.410672122.00000270A5602000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410599081.00000270A51AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410771133.00000270A51AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410791747.00000270A5619000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410692294.00000270A5603000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.41067456.00000270A519C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410743577.00000270A518A000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.bingmapsportal.com	svchost.exe, 0000000D.00000002.318724342.00000226EE413000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000D.00000002.318737872.00000226EE429000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copy right/	svchost.exe, 0000000D.00000002.318792183.00000226EE43E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000D.00000003.318354950.00000226EE462000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000015.00000003.414863193.00000270A51A2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.414985699.00000270A5190000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.414970747.00000270A5189000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000D.00000003.318419162.00000226EE446000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318390455.00000226EE441000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://23.239.0.12/7	regsvr32.exe, 00000005.00000003.33287782.9.0000000000C64000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.647508689.0000000000C64000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 0000000D.00000003.318338732.00000226EE469000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318869002.00000226EE46B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000D.00000002.318792183.00000226EE43E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 0000000D.00000002.318737872.00000226EE429000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://23.239.0.12/;	regsvr32.exe, 00000005.00000003.33287782.9.0000000000C64000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.647508689.0000000000C64000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000D.00000003.318419162.00000226EE446000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318390455.00000226EE441000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ver)	svchost.exe, 00000012.00000002.609573425.00000151B5016000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000002.437352499.00000270A48EA000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000D.00000002.318839985.00000226EE45F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318390455.00000226EE441000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318368166.00000226EE45E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000015.00000003.418543495.00000270A5602000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.418463858.00000270A519F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.418409275.00000270A518E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.418295891.00000270A51B5000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.418216286.00000270A51B5000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://activity.windows.comr	svchost.exe, 0000000B.00000002.647553491.0000023A28044000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000D.00000002.318792183.00000226EE43E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.318724342.00000226EE413000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://%s.xboxlive.com	svchost.exe, 0000000B.00000002.647553491.0000023A28044000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000D.00000003.318419162.00000226EE446000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.318812314.00000226EE447000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318390455.00000226EE441000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000D.00000003.318354950.00000226EE462000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000D.00000003.296600069.00000226EE432000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000D.00000003.318354950.00000226EE462000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 00000015.00000003.410672122.00000270A5602000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410599081.00000270A51AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410771133.00000270A51AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410692294.00000270A5603000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.410743577.00000270A518A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000D.00000002.318839985.00000226EE45F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318368166.00000226EE45E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000015.00000003.414863193.00000270A51A2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.414985699.00000270A5190000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.414970747.00000270A5189000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000D.00000002.318835280.00000226EE45D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318374543.00000226EE45B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	svchost.exe, 00000012.00000003.609101929.00000151AF8AB000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.609492780.00000151AF8AB000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000D.00000003.318390455.00000226EE441000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.318806583.00000226EE443000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000D.00000003.318354950.00000226EE462000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://disneyplus.com/legal	svchost.exe, 00000015.00000003.414863193.00000270A51A2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.414985699.00000270A5190000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.414970747.00000270A5189000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000D.00000003.296600069.00000226EE432000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318448471.00000226EE43B000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000D.00000002.318839985.00000226EE45F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318368166.00000226EE45E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 0000000B.00000002.647553491.0000023A28044000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000D.00000003.318354950.00000226EE462000.00000004.00000020.00020000.00000000.sdmp	false		high
http://help.disneyplus.com.	svchost.exe, 00000015.00000003.414863193.00000270A51A2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.414985699.00000270A5190000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.414970747.00000270A5189000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000B.00000002.647553491.0000023A28044000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000D.00000002.318835280.00000226EE45D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.318374543.00000226EE45B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000D.00000003.318374543.00000226EE45B000.00000004.00000020.00020000.00000000.sdmp	false		high



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:	626506
Start date and time: 14/05/202205:24:13	2022-05-14 05:24:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ru97gvh8ir.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	35
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:	mal84.troj.evad.winDLL@27/6@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms

Warnings
• Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, WMIADAP.exe, backgroundTaskHost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 23.211.4.86, 20.223.24.244, 51.11.168.232, 20.49.150.241 • 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, iris.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, settings-prod-uks-1.uksouth.cloudapp.azure.com, 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.

Simulations		
Behavior and APIs		
Time	Type	Description
05:25:54	API Interceptor	1x Sleep call for process: svchost.exe modified
05:26:41	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF3160
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):	0.24943767283333948
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU45:BJiRdwfu2SRU45
MD5:	E684E45F64C4CB31FE5A56503E5A5C01
SHA1:	BCDEA2FFC1DAB538F60E92A82FC9F2BB37A03AB0
SHA-256:	FB79D1DD86392EF33CB9CFACF32E7D02C226810A9C62D015A4CAC43CFE4F0774
SHA-512:	92A5EC75545DE44240F5610C53E3CA35EE83887B1F536FE5DDE23F88EC0906BA2DC69A1724F65568E27CA765CC976EF1F1C8B6B872BDD07EEDF54BF6C2CCB72
Malicious:	false

Preview:	V.d.....@..@.3..w.....3..w.....C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....Ou.....@...@.....d#.....
----------	--

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x7d998954, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2505391752286642
Encrypted:	false
SSDEEP:	384:QzZ+W0StseCJ48EApW0StseCJ48E2rTSjIK/ebmLerYSRSY1J2:QzySB2nSB2RSjIK/+mLesOj1J2
MD5:	BDC53BBF35781DFBFBB5B64C69C1B1F6
SHA1:	E12030164F15A6277D45475CAC926A80CB03D161
SHA-256:	65B3B97C5B945076A4413642E41FB285F2AEC64B332A415B99437C318F75AEFD
SHA-512:	83C3394C1353BBBA0CCB51D99C0403BE61A1E072C1DBC749C268DEA1D5EFFFD61370E2C030D2A48C12FF7FB51C81810525955A20CB928062DDA9E8B28FE62100
Malicious:	false
Preview:	}.T... ..e.f.3..w.....)......Z..6...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):	0.07383250156300065
Encrypted:	false
SSDEEP:	3:/Sill/J7vTXMUI/XaigfSxd2I/all3Vktlmlnl:aCJrTDigfz42d3
MD5:	A45672FA5C1D99BDAC4158CADE5DA1BA
SHA1:	70FC8EA9625D8859E7EA6FA03CBFE78D539DE682
SHA-256:	CFC587504377375B1C2F4BD8C576A86D6CEB076C64A29D5470D4554A557AB3DB
SHA-512:	A064A5AD32AC4743DFE6AEC1873D6123BF432C1CD2DF5B51505BF11628EFA32D15CC547804142251EA76A72CF7EBF3B2B8BB306575CC1C87E5519FD8B0205EDB
Malicious:	false
Preview:	V.....3..w...6...z...z.....z.....z.E.....z.....z.....

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83xfAw2fHbY:YMRI83X12f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECDD90B959FEB2F503AC258D7C0A235D6FE9
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 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 00007F8AA92E9ED7h
call 00007F8AA92EC064h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007F8AA92E9D80h
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 00007F8AA92F8A5Ah
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h

Instruction
je 00007F8AA92E9F13h
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 00007F8AA92F8A08h
jmp 00007F8AA92E9EF4h
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	0x2dfffc	.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x52000	0x3d5f	0x3e00	False	0.355405745968	data	5.39367324642	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x56000	0x20d8	0x1200	False	0.180772569444	data	2.18161586025	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x59000	0xe1c	0x1000	False	0.44580078125	data	4.98556265168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x5a000	0x2dffc	0x2e000	False	0.839408542799	data	7.73448363752	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0x6f8	0x800	False	0.1796875	data	1.81179169858	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

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

Imports	
DLL	Import
KERNEL32.dll	ExitProcess, VirtualAlloc, CompareStringW, CompareStringA, GetTimeZoneInformation, GetLocaleInfoW, GetCurrentThreadId, FlsSetValue, GetCommandLineA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RtlVirtualUnwind, RtlLookupFunctionEntry, RtlCaptureContext, EncodePointer, DecodePointer, TlsAlloc, FlsGetValue, FlsFree, SetLastError, GetLastError, GetCurrentThread, FlsAlloc, HeapFree, Sleep, GetModuleHandleW, GetProcAddress, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, HeapSetInformation, HeapCreate, HeapDestroy, RtlUnwindEx, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, LeaveCriticalSection, FatalAppExitA, EnterCriticalSection, HeapAlloc, HeapReAlloc, WriteFile, SetConsoleCtrlHandler, FreeLibrary, LoadLibraryA, InitializeCriticalSectionAndSpinCount, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetDateFormatA, GetTimeFormatA, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, HeapSize, SetEnvironmentVariableA
ole32.dll	CoTaskMemFree, CoLoadLibrary, CoTaskMemAlloc

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

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

Network Behavior				
TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 05:25:54.255302906 CEST	49742	443	192.168.2.3	23.239.0.12
May 14, 2022 05:25:54.255337000 CEST	443	49742	23.239.0.12	192.168.2.3
May 14, 2022 05:25:54.255414963 CEST	49742	443	192.168.2.3	23.239.0.12
May 14, 2022 05:25:54.329833031 CEST	49742	443	192.168.2.3	23.239.0.12
May 14, 2022 05:25:54.329853058 CEST	443	49742	23.239.0.12	192.168.2.3
May 14, 2022 05:25:54.871645927 CEST	443	49742	23.239.0.12	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 05:25:54.871757030 CEST	49742	443	192.168.2.3	23.239.0.12
May 14, 2022 05:25:55.265436888 CEST	49742	443	192.168.2.3	23.239.0.12
May 14, 2022 05:25:55.265492916 CEST	443	49742	23.239.0.12	192.168.2.3
May 14, 2022 05:25:55.265772104 CEST	443	49742	23.239.0.12	192.168.2.3
May 14, 2022 05:25:55.265885115 CEST	49742	443	192.168.2.3	23.239.0.12
May 14, 2022 05:25:55.270133018 CEST	49742	443	192.168.2.3	23.239.0.12
May 14, 2022 05:25:55.312505960 CEST	443	49742	23.239.0.12	192.168.2.3
May 14, 2022 05:25:56.222610950 CEST	443	49742	23.239.0.12	192.168.2.3
May 14, 2022 05:25:56.222680092 CEST	443	49742	23.239.0.12	192.168.2.3
May 14, 2022 05:25:56.222781897 CEST	49742	443	192.168.2.3	23.239.0.12
May 14, 2022 05:25:56.222819090 CEST	49742	443	192.168.2.3	23.239.0.12
May 14, 2022 05:25:56.223576069 CEST	49742	443	192.168.2.3	23.239.0.12
May 14, 2022 05:25:56.223607063 CEST	443	49742	23.239.0.12	192.168.2.3

HTTP Request Dependency Graph

- 23.239.0.12

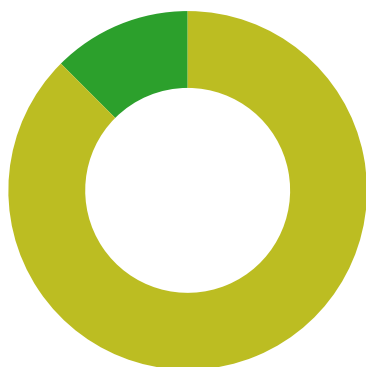
HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49742	23.239.0.12	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-14 03:25:55 UTC	0	OUT	GET / HTTP/1.1 Cookie: OQiV=BMo4RobL5HoeZiKj+kuwo42M2Kxxn+tZOzmZqou2w96cYgK0+BWxqw8XT37HlgNZpnFxoJ86xPlg a8L99Q/lanZogVAknbnVfqY3U+8qYNkBB04er0H369wwwAD8YXE6SUdN2TO4RVu1wTct90w1DIV6+Kh+PtKy8R3DB2L AH7/fbJokLH7oS9tCfdvv4l6KsNzS1hmQFEOn5cQjVCJqStPcrhK/n5acAKbznMorepJgL4aYQ3wwwISKLxvWlvn8+A 2QZ+7fUmnLZYyig2G0zP9WbMTEh8WkBG3N4n9tE3o+BKTrmizHb+q9ggF87pwIG3qjSd5Yfid7rXj1EReIX9Af2 Host: 23.239.0.12 Connection: Keep-Alive Cache-Control: no-cache
2022-05-14 03:25:56 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 14 May 2022 03:25:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2022-05-14 03:25:56 UTC	0	IN	Data Raw: 62 37 0d 0a a2 b0 c4 42 64 78 3a d9 41 af af de 69 f7 65 8c 09 ea e0 5c e0 1b 9d 4b 46 6a 65 9e 72 e2 07 24 ed d0 da a8 a3 57 dd 66 40 95 c6 8e 29 58 5f 77 86 97 75 fb 3c 43 ef 79 59 4c 39 f1 84 a6 06 be f0 e7 d3 9a 59 87 11 96 7d 09 28 75 29 88 84 b2 13 1e de 6f 14 09 e0 c0 59 3a b4 d1 a6 b7 72 82 9b b1 00 36 45 4d 88 f9 de d8 cc 4e 83 67 a9 ce 96 be fd fa 5e 4a 33 5f cd b1 e3 77 d0 a8 0e eb b5 ae 1b bb 50 21 1c 7d 34 75 c5 14 33 38 16 09 4d 46 f8 a2 72 74 3a 3b 5a 10 f1 40 61 5f ee a2 36 75 15 a4 ed a0 12 c8 c7 d9 77 c7 c3 ab c7 0b 9a 0b 18 93 46 45 cb 0d 0a 30 0d 0a 0d 0a Data Ascii: b7Bdx:AieIKFjer\$Wf@)X_wu<CyYL9Y}(u)oY:r6EMNg^J3_wP!j4u38MFrt::Z@a_6uwFEO

Statistics

Behavior

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



- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- MpCmdRun.exe
- conhost.exe

💡 Click to jump to process

System Behavior

Analysis Process: **loaddll64.exe** PID: 6304, Parent PID: 1908

General	
Target ID:	0
Start time:	05:25:16
Start date:	14/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\Ru97gvh8ir.dll"
Imagebase:	0x7ff6495a0000
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: 6316, Parent PID: 6304

General	
Target ID:	1
Start time:	05:25:17
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\Ru97gvh8ir.dll",#1
Imagebase:	0x7ff619a00000
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: 6324, Parent PID: 6304

General

Target ID:	2
Start time:	05:25:17
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\Ru97gvh8ir.dll
Imagebase:	0x7ff72a9c0000
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: 00000002.00000002.260476507.0000000000DB0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.260944985.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\QHTOcglFaLIWfXNGIbK.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: 6336, Parent PID: 6316

General

Target ID:	3
Start time:	05:25:17
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\Ru97gvh8ir.dll",#1
Imagebase:	0x7ff7a57a0000
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: 00000003.00000002.258276727.0000019B71C10000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.258039137.0000000180001000.00000020.00001000.00020000.00000000.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: 6352, Parent PID: 6304

General

Target ID:	4
Start time:	05:25:18
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Ru97gvh8ir.dll,DllRegisterServer
Imagebase:	0x7ff7a57a0000
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: 00000004.00000002.258391181.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.258788281.0000017947080000.00000040.00001000.00020000.00000000.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: 6500, Parent PID: 6324

General

Target ID:	5
Start time:	05:25:21
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\QHTOcglFaLIWfXNGIbK.dll"
Imagebase:	0x7ff72a9c0000
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: 00000005.00000002.648153388.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.647866634.0000000000E70000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6516, Parent PID: 6304**General**

Target ID:	6
Start time:	05:25:22
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Ru97gvh8ir.dll,DllUnregisterServer
Imagebase:	0x7ff7a57a0000
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: 6812, Parent PID: 568**General**

Target ID:	10
Start time:	05:25:36
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: 6856, Parent PID: 568**General**

Target ID:	11
Start time:	05:25:37
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities						
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.						
File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities							
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6920, Parent PID: 568	
General	
Target ID:	12
Start time:	05:25:38
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities								
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.								
Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6980, Parent PID: 568	
General	
Target ID:	13
Start time:	05:25:38
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 7032, Parent PID: 568	
General	
Target ID:	14
Start time:	05:25:39
Start date:	14/05/2022

Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff73b750000
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: 7060, Parent PID: 568

General

Target ID:	15
Start time:	05:25:40
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	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: 1112, Parent PID: 568

General

Target ID:	16
Start time:	05:25:42
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: 6092, Parent PID: 568**General**

Target ID:	18
Start time:	05:25:52
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: 6188, Parent PID: 568**General**

Target ID:	19
Start time:	05:26:05
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k 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: 6796, Parent PID: 568**General**

Target ID:	21
------------	----

Start time:	05:26:18
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
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
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: svchost.exe PID: 3356, Parent PID: 568

General	
Target ID:	28
Start time:	05:26:35
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: 3672, Parent PID: 7060

General	
Target ID:	29
Start time:	05:26:40
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\ImpCmdRun.log	8156	182	0d 00 0a 00 0d 00 0a 00 2d 00 0d 00 0a 00	----- ----- -----	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\ImpCmdRun.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 35 00 3a 00 32 00 36 00 3a 00 34 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 05:26 :41	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\ImpCmdRun.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\ImpCmdRun.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 35 00 3a 00 32 00 36 00 3a 00 34 00 31 00 0d 00 0a 00	MpCmdRun: End Time: Sat May 14 2022 05:26:41	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8888	174	2d 00 0d 00 0a 00	----- ----- -----	success or wait	1	7FF7B034BC96	WriteFile

Analysis Process: conhost.exe PID: 5836, Parent PID: 3672	
General	
Target ID:	30
Start time:	05:26:41
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

Disassembly
 No disassembly