

JoeSandbox Cloud BASIC



ID: 626489

Sample Name: r0hiaXHscs.dll

Cookbook: default.jbs

Time: 04:55:57

Date: 14/05/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report r0hiaXHscs.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	4
Memory Dumps	4
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Networking	5
E-Banking Fraud	5
Hooking and other Techniques for Hiding and Protection	5
HIPS / PFW / Operating System Protection Evasion	6
Stealing of Sensitive Information	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	9
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	9
World Map of Contacted IPs	10
Public IPs	11
General Information	11
Warnings	12
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASNs	12
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
Static File Info	12
General	13
File Icon	13
Static PE Info	13
General	13
Entrypoint Preview	13
Rich Headers	15
Data Directories	15
Sections	15
Resources	15
Imports	16
Exports	16
Possible Origin	16
Network Behavior	16
TCP Packets	16
HTTP Request Dependency Graph	16
HTTPS Proxied Packets	17
Statistics	17
Behavior	17
System Behavior	17
Analysis Process: loaddll64.exePID: 7072, Parent PID: 5640	17
General	17
File Activities	18
Analysis Process: cmd.exePID: 7092, Parent PID: 7072	18
General	18
File Activities	18

Analysis Process: regsvr32.exePID: 7136, Parent PID: 7072	18
General	18
File Activities	19
File Deleted	19
Analysis Process: rundll32.exePID: 7148, Parent PID: 7092	19
General	19
File Activities	19
Analysis Process: rundll32.exePID: 3504, Parent PID: 7072	19
General	19
File Activities	20
Analysis Process: rundll32.exePID: 3980, Parent PID: 7072	20
General	20
File Activities	20
Analysis Process: regsvr32.exePID: 6392, Parent PID: 7136	20
General	20
Analysis Process: svchost.exePID: 3272, Parent PID: 588	20
General	20
Analysis Process: svchost.exePID: 2332, Parent PID: 588	21
General	21
File Activities	21
Analysis Process: svchost.exePID: 5740, Parent PID: 588	21
General	21
File Activities	21
Analysis Process: svchost.exePID: 6148, Parent PID: 588	22
General	22
File Activities	22
Analysis Process: svchost.exePID: 6092, Parent PID: 588	22
General	22
File Activities	22
Analysis Process: svchost.exePID: 3440, Parent PID: 588	22
General	22
File Activities	23
Disassembly	23

Windows Analysis Report

r0hiaXHscs.dll

Overview

General Information

Sample Name:

r0hiaXHscs.dll

Analysis ID:

626489

MD5:

28fd92e0ce7538..

SHA1:

483d573cd7d464..

SHA256:

198a1b06c69382..

Tags:

exe

trojan

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Emotet

Score:

76

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

Yara detected Emotet

System process connects to networ...

Antivirus detection for URL or domain

Hides that the sample has been dow...

Queries the volume information (nam...

Contains functionality to check if a d...

Contains functionality to query local...

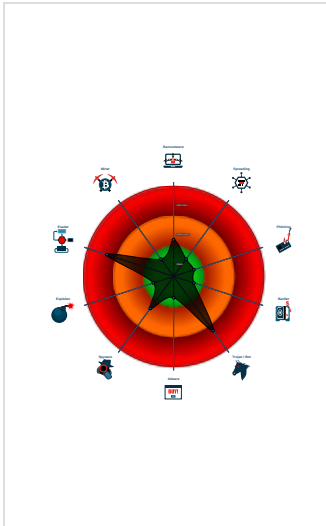
Deletes files inside the Windows fol...

May sleep (evasive loops) to hinder...

Uses code obfuscation techniques (...)

Creates files inside the system direc...

Classification



Process Tree

System is w10x64

loaddll64.exe

(PID: 7072 cmdline: loaddll64.exe "C:\Users\user\Desktop\r0hiaXHscs.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)

cmd.exe

(PID: 7092 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\r0hiaXHscs.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)

rundll32.exe

(PID: 7148 cmdline: rundll32.exe "C:\Users\user\Desktop\r0hiaXHscs.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)

regsvr32.exe

(PID: 7136 cmdline: regsvr32.exe /s C:\Users\user\Desktop\r0hiaXHscs.dll MD5: D78B75FC68247E8A63ACBA846182740E)

regsvr32.exe

(PID: 6392 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\FxQLsR\IONbDjBVKT.dll" MD5: D78B75FC68247E8A63ACBA846182740E)

rundll32.exe

(PID: 3504 cmdline: rundll32.exe C:\Users\user\Desktop\r0hiaXHscs.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)

rundll32.exe

(PID: 3980 cmdline: rundll32.exe C:\Users\user\Desktop\r0hiaXHscs.dll,DllUnregisterServer MD5: 73C519F050C20580F8A62C849D49215A)

svchost.exe

(PID: 3272 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe

(PID: 2332 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe

(PID: 5740 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe

(PID: 6148 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe

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

svchost.exe

(PID: 3440 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
00000006.00000002.776811676.0000000180001000.0000020.00001000.00020000.00000000.sdmf	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Copyright Joe Security LLC 2022

Page 4 of 23

Source	Rule	Description	Author	Strings
00000004.00000002.398034910.0000000180001000.00000020.00001000.00020000.00000000.sdm	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.775504614.0000000002C40000.00000040.00001000.00020000.00000000.sdm	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.399182634.0000013444F90000.00000040.00001000.00020000.00000000.sdm	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.395798586.000002165C820000.00000040.00001000.00020000.00000000.sdm	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 3 entries

Unpacked PEs				
Source	Rule	Description	Author	Strings
4.2.rundll32.exe.13444f90000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.2165c820000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.5a0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.regsvr32.exe.2c40000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.13444f90000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 3 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking

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

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

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



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

Stealing of Sensitive Information



Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Native API	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	2 Virtualization/Sandbox Evasion	LSASS Memory	2 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 1 1 Process Injection	Security Account Manager	2 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 Hidden Files and Directories	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Regsvr32	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Rundll32	DCSync	2 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph

Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
r0hiaXHscs.dll	35%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.regsvr32.exe.2c40000.1.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
3.2.rundll32.exe.2165c820000.1.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
2.2.regsvr32.exe.5a0000.0.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
4.2.rundll32.exe.13444f90000.1.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File

Domains

No Antivirus matches

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

Domains and IPs	
Contacted Domains	
 No contacted domains info	

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

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000017.00000003.736113156 .000001F25DB8E000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.735828686.000001F25DBA0000.00 000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000017.00000003.736113156 .000001F25DB8E000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.735828686.000001F25DBA0000.00 000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000017.00000003.729809833 .000001F25DBA0000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.729965849.000001F25DBB0000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.729933938 .000001F25DB8E000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.729828603.000001F25DBB0000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.729850048 .000001F25E002000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.730030081.000001F25E019000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.729874316 .000001F25E003000.00000004.00000020.0002 0000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.pango.co/privacy	svchost.exe, 00000017.00000003.729809833.000001F25DBA0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.729965849.000001F25DBB0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.729933938.000001F25DB8E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.729874316.000001F25E002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.729850048.000001F25E002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.729874316.000001F25E003000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 00000017.00000003.736113156.000001F25DB8E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.735828686.000001F25DBA0000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://23.239.0.12/aw	regsvr32.exe, 00000006.00000003.467319252.00000000013E1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.775356330.00000000013E1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.467211849.00000000013E1000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://crl.ver)	svchost.exe, 00000017.00000002.766213350.000001F25D2ED000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://https://www.tiktok.com/legal/report	svchost.exe, 00000017.00000003.745516041.000001F25DB8E000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000017.00000003.745558940.000001F25E002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.745533948.000001F25DB9F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.745516041.000001F25DB8E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.745454811.000001F25DBB5000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://help.disneyplus.com.	svchost.exe, 00000017.00000003.736113156.000001F25DB8E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.735828686.000001F25DBA0000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://support.hotspotshield.com/	svchost.exe, 00000017.00000003.729809833.000001F25DBA0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.729965849.000001F25DBB0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.729933938.000001F25DB8E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.729874316.000001F25E002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.729850048.000001F25E002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.729874316.000001F25E003000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.microsoft	svchost.exe, 0000000E.00000002.548646295.000001A6FB27B000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626489
Start date and time: 14/05/202204:55:57	2022-05-14 04:55:57 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	r0hiaXHscs.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:	25
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@19/0@0/1
EGA Information:	Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, arc.msn.com, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, 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

 No simulations

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files

 No created / dropped files found

Static File Info

General	
File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.4820900629981555
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:	r0hiaXHscs.dll
File size:	545280
MD5:	28fd92e0ce7538516dcea70e239fb177
SHA1:	483d573cd7d464b01c880998e0321970a635e8d0
SHA256:	198a1b06c69382d00cf775aa56d2172f6d0412f31753bda078620107ee998283
SHA512:	aa78a2ce9c6118faa00b9a3d8adcc2603c607ddd3816a106155f1cac91a1a6c3aaab1d51954563af7a10477b8046e78adf509d2f5527f7fea65aa25ca1a3b402
SSDEEP:	12288:B4UJY9B+TenWsSEPHjMOUP9uXdt7JpfYNNv9RM54RutCTdJGqloTCZ4eEsZFhHy:B4UJY9BSenZSEPHjMOUP9Udt7JpfYNNv
TLSH:	22C4CFA5435C08FCE762C3395C975BC5B1F7BDAE0664AF260BC18DA05E1BA90F53A381
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	

Instruction
jne 00007FB74CBB1BC7h
call 00007FB74CBB3D54h
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 00007FB74CBB1A70h
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 00007FB74CBC074Ah
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007FB74CBB1C03h
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]

Instruction
dec eax
mov edx, dword ptr [esp+60h]
xor ecx, ecx
call 00007FB74CBC06F8h
jmp 00007FB74CBB1BE4h
dec eax
mov eax, dword ptr [eax+eax+00000000h]

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

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

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x504ca	0x50600	False	0.389081940124	zlib compressed data	5.26882252971	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x52000	0x3d5f	0x3e00	False	0.355405745968	data	5.39330874285	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.data	0x56000	0x20d8	0x1200	False	0.180772569444	data	2.18161586025	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x59000	0xe1c	0x1000	False	0.44580078125	data	4.98556265168	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x5a000	0x2dffc	0x2e000	False	0.839408542799	data	7.73448363752	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0x6f8	0x800	False	0.1796875	data	1.81179169858	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

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

Imports	
DLL	Import
KERNEL32.dll	ExitProcess, VirtualAlloc, CompareStringW, CompareStringA, GetTimeZoneInformation, GetLocaleInfoW, GetCurrentThreadId, FlsSetValue, GetCommandLineA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RtlVirtualUnwind, RtlLookupFunctionEntry, RtlCaptureContext, EncodePointer, DecodePointer, TlsAlloc, FlsGetValue, FlsFree, SetLastError, GetLastError, GetCurrentThread, FlsAlloc, HeapFree, Sleep, GetModuleHandleW, GetProcAddress, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, HeapSetInformation, HeapCreate, HeapDestroy, RtlUnwindEx, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, LeaveCriticalSection, FatalAppExitA, EnterCriticalSection, HeapAlloc, HeapReAlloc, WriteFile, SetConsoleCtrlHandler, FreeLibrary, LoadLibraryA, InitializeCriticalSectionAndSpinCount, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetDateFormatA, GetTimeFormatA, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, HeapSize, SetEnvironmentVariableA
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 04:57:53.988490105 CEST	49772	443	192.168.2.6	23.239.0.12
May 14, 2022 04:57:53.988554955 CEST	443	49772	23.239.0.12	192.168.2.6
May 14, 2022 04:57:53.988698006 CEST	49772	443	192.168.2.6	23.239.0.12
May 14, 2022 04:57:54.029891014 CEST	49772	443	192.168.2.6	23.239.0.12
May 14, 2022 04:57:54.029942989 CEST	443	49772	23.239.0.12	192.168.2.6
May 14, 2022 04:57:54.571053982 CEST	443	49772	23.239.0.12	192.168.2.6
May 14, 2022 04:57:54.571193933 CEST	49772	443	192.168.2.6	23.239.0.12
May 14, 2022 04:57:55.201952934 CEST	49772	443	192.168.2.6	23.239.0.12
May 14, 2022 04:57:55.202007055 CEST	443	49772	23.239.0.12	192.168.2.6
May 14, 2022 04:57:55.202414036 CEST	443	49772	23.239.0.12	192.168.2.6
May 14, 2022 04:57:55.202596903 CEST	49772	443	192.168.2.6	23.239.0.12
May 14, 2022 04:57:55.216537952 CEST	49772	443	192.168.2.6	23.239.0.12
May 14, 2022 04:57:55.260504007 CEST	443	49772	23.239.0.12	192.168.2.6
May 14, 2022 04:57:56.068161011 CEST	443	49772	23.239.0.12	192.168.2.6
May 14, 2022 04:57:56.068233013 CEST	443	49772	23.239.0.12	192.168.2.6
May 14, 2022 04:57:56.068325996 CEST	49772	443	192.168.2.6	23.239.0.12
May 14, 2022 04:57:56.068365097 CEST	49772	443	192.168.2.6	23.239.0.12
May 14, 2022 04:57:56.069004059 CEST	49772	443	192.168.2.6	23.239.0.12
May 14, 2022 04:57:56.069027901 CEST	443	49772	23.239.0.12	192.168.2.6

HTTP Request Dependency Graph
23.239.0.12

HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49772	23.239.0.12	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-14 02:57:55 UTC	0	OUT	GET / HTTP/1.1 Cookie: Gg=8GHy3N4Xm4BasGI7yF4aqbYZ+UfwCGyAbOIBL+16WxGiVKGpNRlXTVpgGtiVDv4o6m2fAcCSHbC7mYM UPTjqe4US1mRyANHQL7kUXdkMIV97NOv6NIFY6ltHTPKLQm3cab3RqaCCTHdeUJgOXpfGnYvQigwPZkv1S1NderwB dUbUrQpVsTBxEAdf7eBMQneqNUwyO1NGdrv9JdDXBeFHpBIJABa3NfDOXQ+k98+uc8fHA== Host: 23.239.0.12 Connection: Keep-Alive Cache-Control: no-cache
2022-05-14 02:57:56 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 14 May 2022 02:57:55 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2022-05-14 02:57:56 UTC	0	IN	Data Raw: 32 35 31 0d 0a e5 09 5c cb b4 0b 45 71 b9 0d 63 89 8a a1 4c 32 be a8 03 f1 d7 47 67 c4 00 8c dc 92 a3 71 49 d9 f3 c4 aa 67 b2 f3 4a a7 39 d0 87 67 0c 1d 78 75 44 8f 06 3c 82 76 22 91 49 52 6a 51 c7 50 6d a1 5a 9c 4a 21 ce 14 80 13 bb ac c0 f6 1d 68 a8 6a 13 a8 b5 6b ac 0c 26 eb ac ad ef 44 3e 68 6d 50 00 78 73 57 23 ba a1 63 c6 22 53 bd 0b 82 cc be 87 0f a3 e3 19 88 af 18 45 fa aa 8c 4f f1 14 51 9f 6d f5 5e 7c 7b b1 43 3d c3 01 e3 b6 4d 6b b7 e9 1a 97 73 e8 f0 79 45 77 bb 09 fb e3 4a 3e aa db cd b6 0e 2a 4f b6 a9 4e be 93 05 66 f6 f8 57 18 ba d9 6d 5d b2 1b 02 3e 53 44 06 d0 b6 91 a4 ee 56 da 75 9c 51 af ac 14 f2 94 9e aa 37 77 66 b9 60 51 e7 01 19 bf 3a 91 01 85 f8 1f 99 0d 1d fb b3 f5 a3 ae 40 7e 75 8e fb bc d1 25 6c 23 89 58 3c bd 69 db f7 3d eb bf b9 Data Ascii: 251\Eqcl2GgqlgJ9gxuD<v"IRjQPmZJ!hjk&D>hmPxSW#c"SEOQm^ {C=MksyEwJ>*ONfWm]>SDVuQ 7wf'Q:@~u%l#X<=

Statistics

Behavior



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

 Click to jump to process

System Behavior	
Analysis Process: loaddll64.exe PID: 7072, Parent PID: 5640	
General	
Target ID:	0
Start time:	04:57:14
Start date:	14/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\r0hiaXHscs.dll"

Imagebase:	0x7ff7fbfc0000
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: 7092, Parent PID: 7072

General

Target ID:	1
Start time:	04:57:15
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\r0hiaXHscs.dll",#1
Imagebase:	0x7ff6edb0000
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: 7136, Parent PID: 7072

General

Target ID:	2
Start time:	04:57:16
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\r0hiaXHscs.dll
Imagebase:	0x7ff655080000
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: 00000002.00000002.401404502.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.401159904.00000000005A0000.00000040.00001000.00020000.00000000.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\FxQLsR\IONbDJBVK.T.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: 7148, Parent PID: 7092	
General	
Target ID:	3
Start time:	04:57:16
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\r0hiaXHscs.dll",#1
Imagebase:	0x7ff71b1e0000
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: 00000003.00000002.395798586.000002165C820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.395299440.0000000180001000.00000020.00001000.00020000.00000000.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: 3504, Parent PID: 7072	
General	
Target ID:	4
Start time:	04:57:17
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\r0hiaXHscs.dll,DllRegisterServer
Imagebase:	0x7ff71b1e0000
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: 00000004.00000002.398034910.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.399182634.0000013444F90000.00000040.00001000.00020000.00000000.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: 3980, Parent PID: 7072	
General	
Target ID:	5
Start time:	04:57:21
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\r0hiaXHscs.dll,DllUnregisterServer
Imagebase:	0x7ff71b1e0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

Analysis Process: regsvr32.exe PID: 6392, Parent PID: 7136	
General	
Target ID:	6
Start time:	04:57:22
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\FxQLsR\ONbDjBVKT.dll"
Imagebase:	0x7ff655080000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.776811676.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.775504614.0000000002C40000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: 3272, Parent PID: 588	
General	
Target ID:	10
Start time:	04:57:54

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:	0x7ff726010000
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: 2332, Parent PID: 588

General

Target ID:	14
Start time:	04:58:27
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

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

Analysis Process: svchost.exe PID: 5740, Parent PID: 588

General

Target ID:	19
Start time:	04:59:00
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:	0x7ff726010000
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: 6148, Parent PID: 588**General**

Target ID:	20
Start time:	04:59:09
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff726010000
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: 588**General**

Target ID:	21
Start time:	04:59:28
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff726010000
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: 3440, Parent PID: 588**General**

Target ID:	23
Start time:	04:59:46
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:	0x7ff726010000
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