ID: 1303888
Sample Name:
Fnvtdhenapsfwu.exe
Cookbook: default.jbs
Time: 22:19:48
Date: 05/09/2023
Version: 38.0.0 Beryl

Table of Contents

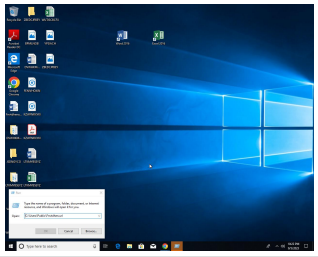
Windows Analysis Report

Fnvtdhenapsfwu.exe

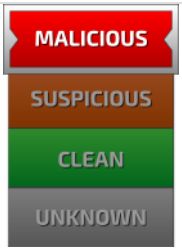
Overview

General Information

Sample Name:	Fnvtdhenapsfwu.exe
Analysis ID:	1303888
MD5:	cffe529403460…
SHA1:	3e03898f87c2c..
SHA256:	56a3dc5c90ad…
Infos:	



Detection



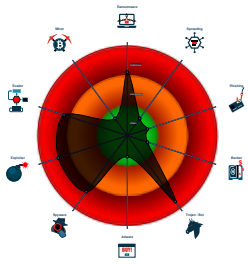
Remcos, DBatLoader

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

Signatures

- Sigma detected: Remcos
- Antivirus detection for URL or domain
- Found malware configuration
- Yara detected UAC Bypass using C…
- Contains functionality to bypass UA…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Remcos RAT
- Yara detected DBatLoader
- Multi AV Scanner detection for drop…
- Contains functionality to steal Firefo…
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- Fnvtdhenapsfwu.exe (PID: 7056 cmdline: C:\Users\user\Desktop\Fnvtdhenapsfwu.exe MD5: CFFE529403460C6AFFE0F52C1E7DE602)
  - SndVol.exe (PID: 7120 cmdline: C:\Windows\System32\SndVol.exe MD5: 1EF1A9B89A984DD25DB61DC1AF2548B8)
- Fnvtdhen.PIF (PID: 6264 cmdline: "C:\Users\Public\Libraries\Fnvtdhen.PIF" MD5: CFFE529403460C6AFFE0F52C1E7DE602)
  - colorcpl.exe (PID: 6388 cmdline: C:\Windows\System32\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Remcos, RemcosRAT	Remcos (acronym of Remote Control & Surveillance Software) is a commercial Remote Access Tool to remotely control computers.Remcos is advertised as legitimate software which can be used for surveillance and penetration testing purposes, but has been used in numerous hacking campaigns.Remcos, once installed, opens a backdoor on the computer, granting full access to the remote user.Remcos is developed by the cybersecurity company BreakingSecurity.	• APT33 • The Gorgon Group	http://malware-traffic-analysis.net/2017/12/22/index.htmlhttps://asec.ahnlab.com/en/32376/https://asec.ahnlab.com/ko/25837/https://asec.ahnlab.com/ko/32101/https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
DBatLoader	This Delphi loader misuses Cloud storage services, such as Google Drive to download the Delphi stager component. The Delphi stager has the actual payload embedded as a resource and starts it.	No Attribution	**http://** https://blog.vincss.net/2020/09/re016-malware-analysis-modiloader-eng.htmlhttps://malcat.fr/blog/exploit-steganography-and-delphi-unpacking-dbatloader/https://malpedia.caad.fkie.fraunhofer.de/details/win.dbatloaderhttps://news.sophos.com/en-us/2020/09/24/email-delivered-modi-rat-attack-pastes-powershell-commandshttps://www.netskope.com/blog/dbatloader-abusing-discord-to-deliver-warzone-rat	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.dbatloader

Malware Configuration

Threatname: Remcos


```
{
  "Host:Port:Password": "tornado.ydns.eu:1972:1orifak.ydns.eu:1972:1",
  "Assigned name": "ES 5th",
  "Copy file": "remcos.exe",
  "Mutex": "RmEEESSSssss-3AINT8",
  "Keylog file": "logs.dat",
  "Screenshot file": "Screenshots",
  "Audio folder": "MicRecords",
  "Copy folder": "Remcos",
  "Keylog folder": "remcos"
}
```


Threatname: DBatLoader


```
{
  "Download Url": "http://wsvdyhrgebwhevawe.ydns.eu/goofeeewsvd/Fnvtdhenaps"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Fnvtdhenapsfwu.exe	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\Fnvtdhen.PIF	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.474312952.00000000007D5000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000008.00000002.253206056.0000000002AB1000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000008.00000003.253042102.0000000002AB1000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000001.00000002.474788319.00000000062F0000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
00000001.00000002.474788319.00000000062F0000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.SndVol.exe.400000.0.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
1.2.SndVol.exe.400000.0.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
1.2.SndVol.exe.400000.0.unpack	INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM	Detects Windows exceutables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003)	ditekSHen	• 0x649e8:$guid1: {3E5FC7F9-9A51-4367-9063-A120244FBEC7} • 0x6497c:$s1: CoGetObject • 0x64990:$s1: CoGetObject • 0x649ac:$s1: CoGetObject • 0x6e938:$s1: CoGetObject • 0x6493c:$s2: Elevation:Administrator!new:
1.2.SndVol.exe.400000.0.unpack	Windows_Trojan_Remcos_b296e965	unknown	unknown	• 0x6aaa8:$a1: Remcos restarted by watchdog! • 0x6b020:$a3: %02i:%02i:%02i:%03i
1.2.SndVol.exe.400000.0.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x64afc:$str_a1: C:\Windows\System32\cmd.exe • 0x64a78:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x64a78:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x64f78:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x657a8:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x64b6c:$str_b2: Executing file: • 0x65bec:$str_b3: GetDirectListeningPort • 0x65598:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x65718:$str_b7: \update.vbs • 0x64b94:$str_b9: Downloaded file: • 0x64b80:$str_b10: Downloading file: • 0x64c24:$str_b12: Failed to upload file: • 0x65bb4:$str_b13: StartForward • 0x65bd4:$str_b14: StopForward • 0x65670:$str_b15: fso.DeleteFile " • 0x65604:$str_b16: On Error Resume Next • 0x656a0:$str_b17: fso.DeleteFolder " • 0x64c14:$str_b18: Uploaded file: • 0x64bd4:$str_b19: Unable to delete: • 0x65638:$str_b20: while fso.FileExists(" • 0x650b1:$str_c0: [Firefox StoredLogins not found]
Click to see the 57 entries				

Sigma Signatures

Stealing of Sensitive Information

Sigma detected: Remcos

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Multi AV Scanner detection for dropped file

Exploits

Yara detected UAC Bypass using CMSTP

Privilege Escalation

Contains functionality to bypass UAC (CMSTPLUA)

Networking

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Contains functionality to modify clipboard data

E-Banking Fraud

Yara detected Remcos RAT

Spam, unwanted Advertisements and Ransom Demands

Contains functionalty to change the wallpaper

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected DBatLoader

Persistence and Installation Behavior

Drops PE files with a suspicious file extension

Malware Analysis System Evasion

Delayed program exit found

HIPS / PFW / Operating System Protection Evasion

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected Remcos RAT

Contains functionality to steal Firefox passwords or cookies

Contains functionality to steal Chrome passwords or cookies

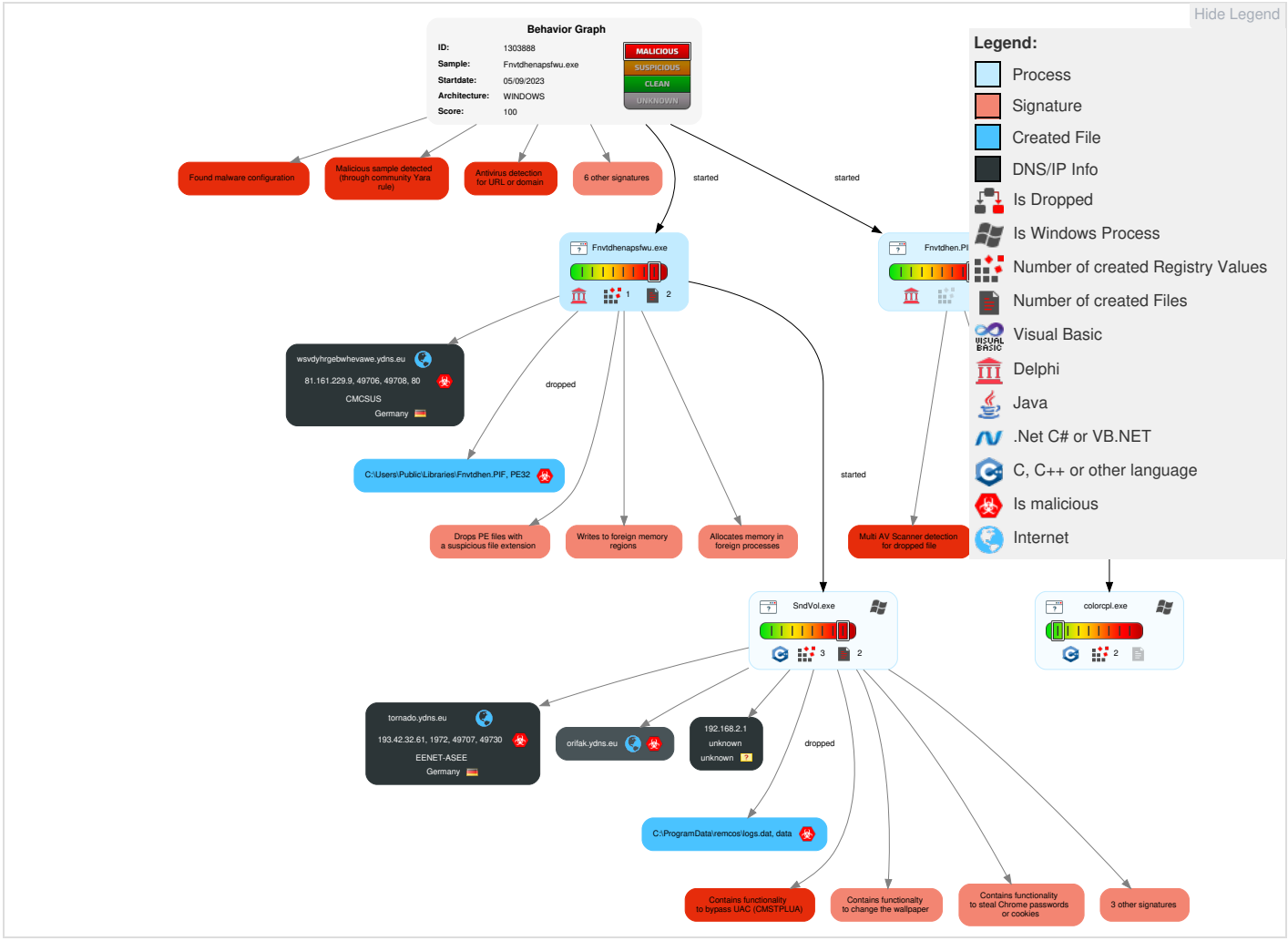
Remote Access Functionality

Yara detected Remcos RAT

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
1 Valid Accounts	1 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/Reboot
Default Accounts	2 Service Execution	1 Valid Accounts	1 Bypass User Access Control	2 Obfuscated Files or Information	2 1 Input Capture	1 Account Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	1 Defacement
Domain Accounts	At (Linux)	1 Windows Service	1 Valid Accounts	1 DLL Side-Loading	2 Credentials In Files	1 System Service Discovery	SMB/Windows Admin Shares	1 2 Clipboard Data	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	1 Registry Run Keys / Startup Folder	1 1 Access Token Manipulation	1 Bypass User Access Control	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 Windows Service	1 1 Masquerading	LSA Secrets	2 4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	3 1 2 Process Injection	1 Valid Accounts	Cached Domain Credentials	1 2 1 Security Software 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	1 Registry Run Keys / Startup Folder	1 Virtualization/Sandbox Evasion	DCSync	1 Virtualization/Sandbox Evasion	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 1 Access Token Manipulation	Proc Filesystem	3 Process Discovery	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)	3 1 2 Process Injection	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

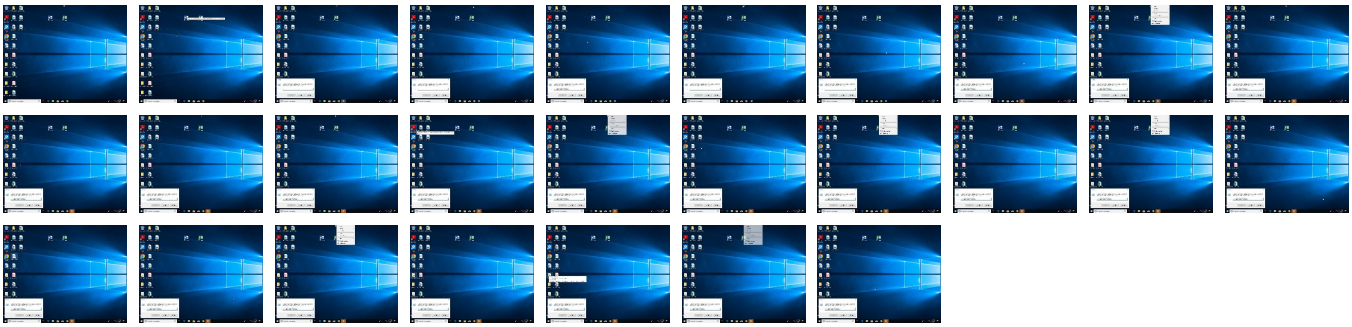
Behavior Graph



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
Fnvtdhenapsfwu.exe	62%	ReversingLabs	Win32.Trojan.Remcos	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Libraries\Fnvtdhen.PIF	62%	ReversingLabs	Win32.Trojan.Remcos	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://geoplugin.net/json.gp	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://geoplugin.net/json.gp/C	0%	URL Reputation	safe	
http://://t.exet.exen	0%	Avira URL Cloud	safe	
http://wsvdyhrgebwhevawe.ydns.eu/goofeeewsvd/Fnvtdhenapsll&=	100%	Avira URL Cloud	phishing	
http://://t.exet.exe	0%	Avira URL Cloud	safe	
http://wsvdyhrgebwhevawe.ydns.eu/goofeeewsvd/Fnvtdhenapsf	100%	Avira URL Cloud	phishing	
http://wsvdyhrgebwhevawe.ydns.eu/goofeeewsvd/FnvtdhenapsDLLq/	100%	Avira URL Cloud	phishing	
http://wsvdyhrgebwhevawe.ydns.eu/	100%	Avira URL Cloud	phishing	
tornado.ydns.eu	100%	Avira URL Cloud	phishing	
http://wsvdyhrgebwhevawe.ydns.eu/goofeeewsvd/Fnvtdhenaps	100%	Avira URL Cloud	phishing	
http://wsvdyhrgebwhevawe.ydns.eu/goofeeewsvd/FnvtdhenapsDLL	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
orifak.ydns.eu	193.42.32.61	true	true		unknown
wsvdyhrgebwhevawe.ydns.eu	81.161.229.9	true	true		unknown
tornado.ydns.eu	193.42.32.61	true	true		unknown

Contacted URLs

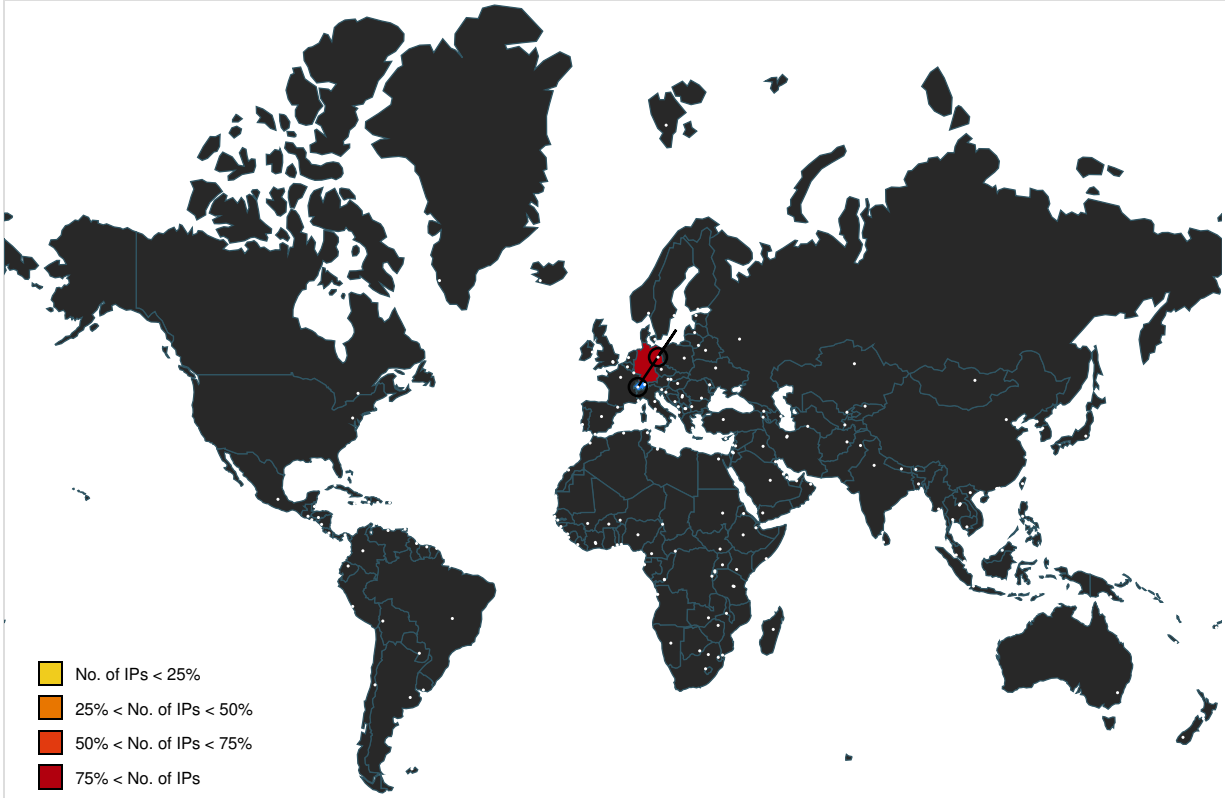
Name	Malicious	Antivirus Detection	Reputation
http://wsvdyhrgebwhevawe.ydns.eu/goofeeewsvd/Fnvtdhenaps	true	• Avira URL Cloud: phishing	unknown
tornado.ydns.eu	true	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://geoplugin.net/json.gp	SndVol.exe	false	• URL Reputation: safe	unknown
http://://t.exet.exen	Fnvtdhenapsfwu.exe, 00000000.00000002.21 6838629.000000000019B000.00000004.000000 10.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://wsvdyhrgebwhevawe.ydns.eu/goofeeewsvd/FnvtdhenapsDLL	Fnvtdhen.PIF, 00000002.00000002.25328954 5.00000000005C5000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://://t.exet.exe	Fnvtdhen.PIF, 00000002.00000002.25323009 7.000000000019B000.00000004.00000010.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://wsvdyhrgebwhevawe.ydns.eu/	Fnvtdhenapsfwu.exe, 00000000.00000002.21 6873929.00000000005C1000.00000004.000000 20.00020000.00000000.sdmp, Fnvtdhen.PIF, 00000002.00000002.253289545.00000000005 D6000.00000004.00000020.00020000.0000000 0.sdmp	true	• Avira URL Cloud: phishing	unknown
http://geoplugin.net/json.gp/C	SndVol.exe, 00000001.00000002.474134003. 0000000000400000.00000040.00001000.00020 000.00000000.sdmp, SndVol.exe, 00000001. 00000002.474788319.00000000062F0000.0000 0040.00000400.00020000.00000000.sdmp, co lorcpl.exe, 00000008.00000002.253322818. 0000000006190000.00000040.00000400.00020 000.00000000.sdmp, colorcpl.exe, 0000000 8.00000002.253136648.0000000000400000.00 000040.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://wsvdyhrgebwhevawe.ydns.eu/goofeeewsvd/Fnvtdhenapsll&=	Fnvtdhenapsfwu.exe, 00000000.00000002.21 6873929.0000000000591000.00000004.000000 20.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://www.pmail.com	Fnvtdhenapsfwu.exe, Fnvtdhenapsfwu.exe, 00000000.00000002.217337311.0000000002CD 9000.00000004.00001000.00020000.00000000.sdmp, Fnvtdhenapsfwu.exe, 00000000.00000002.22133 1055.000000007FD20000.00000004.00001000. 00020000.00000000.sdmp	false		high
http://wsvdyhrgebwhevawe.ydns.eu/goofeeewsvd/Fnvtdhenapsf	Fnvtdhen.PIF, 00000002.00000002.25328954 5.00000000005A1000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://wsvdyhrgebwhevawe.ydns.eu/goofeeewsvd/Fnvtdhenapsdllq/	Fnvtdhen.PIF, 00000002.00000002.2532895450000000005C5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
81.161.229.9	wsvdyhrgebwhevawe.ydns.eu	Germany		33657	CMCSUS	true
193.42.32.61	orifak.ydns.eu	Germany		3221	EENET-ASEE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	38.0.0 Beryl
Analysis ID:	1303888
Start date and time:	2023-09-05 22:19:48 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
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
Sample file name:	Fnvtdhenapsfwu.exe
Detection:	MAL
Classification:	mal100.rans.troj.spyw.expl.evad.winEXE@6/3@4/3
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 21.3% (good quality ratio 20.2%) • Quality average: 81.6% • Quality standard deviation: 26%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, geover.prod.do.dsp.mp.microsoft.com, kv501.prod.do.dsp.mp.microsoft.com, fs.microsoft.com, geo.prod.do.dsp.mp.microsoft.com, tse1.mm.bing.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenFile calls found.
- 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 NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: Fnvtdhenapsfwu.exe

Simulations

Behavior and APIs

Time	Type	Description
22:20:39	API Interceptor	1x Sleep call for process: Fnvtdhenapsfwu.exe modified
22:20:44	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Fnvtdhen C:\Users\Public\Fnvtdhen.url
22:20:53	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Fnvtdhen C:\Users\Public\Fnvtdhen.url
22:20:54	API Interceptor	1x Sleep call for process: Fnvtdhen.PIF 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\remcos\logs.dat

Process:	C:\Windows\SysWOW64\SndVol.exe
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.369167134696068
Encrypted:	false
SSDEEP:	3:rmlql7lQNd/lnq5JWRal2Jl+7R0DAlBG4moojklovDl6v:KlRNi5YcleeDAlS1gWAv
MD5:	0E6C4C6494E8D563882175A365488D13
SHA1:	45B37A739A9868BECEC3DE9C5ADC0B654AE8959A
SHA-256:	7EBF554F6B4C8ED72A2144EA1395BAFC4FB99AE4A56DEA9BF2A368D80E32E5A1
SHA-512:	2311DD2FBE44074C33169F91EF8148FB776AEDE01944EF3B54A890599A4E9C0F3BAD20D7C2061340AE2E433A8BCAE55D8AFC7FD7B9D65F18A0BAC9C5D7C213 51
Malicious:	**true**
Reputation:	low
Preview:	....[.2.0.2.3./.0.9./.0.5. .2.2.:.2.0.:.4.4. .O.f.f.l.i.n.e. .K.e.y.l.o.g.g.e.r. .S.t.a.r.t.e.d.].....[.R.u.n.].....[.P.r.o.g.r.a.m. .M.a.n.a.g.e.r.].....

C:\Users\Public\Fnvtdhen.url

Process:	C:\Users\user\Desktop\Fnvtdhenapsfwu.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\Fnvtdhen.PIF">), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	99
Entropy (8bit):	4.9763390393549205
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMTRuL1EysbxovtKRPK:HRYFVmTWDyz08BZExytK9K
MD5:	928836AD0DD52122BB9A9A40825BC079
SHA1:	C26578D2CA5F86A0B4C86270FF63F581344EB445
SHA-256:	AAC3F8C4BC51B6B1BC4572E288916BC5D7E8B643935F022D1B4FC44246F35338
SHA-512:	F7832BDB19624D5502DB5A245E7175967096AB7F12E70112699AAC18DDF369B618FA62F61AFD5B59632F089EA074B65DE957B30D44F136B0171FB83F6BF8AE9D
Malicious:	false
Reputation:	low
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\Fnvtdhen.PIF"..IconIndex=9..HotKey=37..

C:\Users\Public\Libraries\Fnvtdhen.PIF

Process:	C:\Users\user\Desktop\Fnvtdhenapsfwu.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1243648
Entropy (8bit):	6.2960091515949825
Encrypted:	false
SSDEEP:	24576:ORTaL+A2f8Zhp8bYm1EnyWjkf0eFuPD+4m:gTaKsh
MD5:	CFFE529403460C6AFFE0F52C1E7DE602
SHA1:	3E03898F87C2CC47D57893C3DD55302281E9F2B5
SHA-256:	56A3DC5C90ADE897E349BA0FD0433770DCDDA32B5BD2A1C6608B2AF2F9B34C05
SHA-512:	C94045AE5B144141A33C2EE980F1B276C7DED8B1F574C91B6F6E57F4B410CE93440255FCF64DF493526959155C67280159829D10360CE595EBE42E7732269AC1
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: C:\Users\Public\Libraries\Fnvtdhen.PIF, Author: Joe Security
Antivirus:	• Antivirus: ReversingLabs, Detection: 62%
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....t.....@.....@.....0..r.... ...^.....@.....p..... 9..... .....text... v.....x..... ..`.itext..8.....|..... ..`.data....O.....P.....@....bss....8.....idata..r....0...0.....@....tls....@....`.. .....rdata.....p.....@..@.reloc..@.....@..B.rsrc....^... ...^.....@..@.....@..@..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.2960091515949825
TrID:	• Win32 Executable (generic) a (10002005/4) 99.38% • InstallShield setup (43055/19) 0.43% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	Fnvtdhenapsfwu.exe
File size:	1'243'648 bytes
MD5:	cffe529403460c6affe0f52c1e7de602
SHA1:	3e03898f87c2cc47d57893c3dd55302281e9f2b5
SHA256:	56a3dc5c90ade897e349ba0fd0433770dcdda32b5bd2a1c6608b2af2f9b34c05
SHA512:	c94045ae5b144141a33c2ee980f1b276c7ded8b1f574c91b6f6e57f4b410ce93440255fcf64df493526959155c67280159829d10360ce595ebe42e7732269ac1
SSDEEP:	24576:ORTaL+A2f8Zhp8bYm1EnyWjkf0eFuPD+4m:gTaKsh
TLSH:	E5457DE2A354CC72F06A3578C849B6C0382A7DED693A5CCD666C794A1A73761793C03F
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	71e191928686b3a5

Static PE Info

General

Entrypoint:	0x489900
Entrypoint Section:	.itext
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	beefa6546dd4570bf21020f1082d8b97

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 00488360h
call 00007FC438DF3901h
mov eax, dword ptr [0050EDBCh]
mov eax, dword ptr [eax]
push eax

Instruction
mov eax, dword ptr [0050EDD0h]
mov eax, dword ptr [eax]
push eax
mov eax, dword ptr [0050ECBCh]
mov eax, dword ptr [eax]
push eax
mov eax, dword ptr [005117FCh]
push eax
call 00007FC438E74F72h
call 00007FC438DF147Dh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x113000	0x2e72	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x122000	0x15e00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x118000	0x9340	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x117000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x113920	0x72c	.idata
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	0x87620	0x87800	False	0.5196807973939115	data	6.548203907656841	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.itext	0x89000	0x938	0xa00	False	0.58359375	data	6.10757289766183	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x8a000	0x84fd4	0x85000	False	0.344478750587406	data	4.487974311252079	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0x10f000	0x3884	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x113000	0x2e72	0x3000	False	0.3133951822916667	data	4.995784798933046	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.tls	0x116000	0x40	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x117000	0x18	0x200	False	0.05078125	data	0.2108262677871819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x118000	0x9340	0x9400	False	0.6007970861486487	data	6.675728362695167	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x122000	0x15e00	0x15e00	False	0.14052455357142857	data	3.8426006120251004	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_CURSOR	0x12333c	0x134	Targa image data - Map 64 x 65536 x 1 +32 "\001"	English	United States	0.38636363636363635
RT_CURSOR	0x123470	0x134	data	English	United States	0.4642857142857143
RT_CURSOR	0x1235a4	0x134	data	English	United States	0.4805194805194805
RT_CURSOR	0x1236d8	0x134	data	English	United States	0.38311688311688313
RT_CURSOR	0x12380c	0x134	data	English	United States	0.36038961038961037
RT_CURSOR	0x123940	0x134	data	English	United States	0.4090909090909091
RT_CURSOR	0x123a74	0x134	Targa image data - RGB 64 x 65536 x 1 +32 "\001"	English	United States	0.4967532467532468
RT_BITMAP	0x123ba8	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360	English	United States	0.43103448275862066
RT_BITMAP	0x123d78	0x1e4	Device independent bitmap graphic, 36 x 19 x 4, image size 380	English	United States	0.46487603305785125
RT_BITMAP	0x123f5c	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360	English	United States	0.43103448275862066
RT_BITMAP	0x12412c	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360	English	United States	0.39870689655172414
RT_BITMAP	0x1242fc	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360	English	United States	0.4245689655172414
RT_BITMAP	0x1244cc	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360	English	United States	0.5021551724137931
RT_BITMAP	0x12469c	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360	English	United States	0.5064655172413793
RT_BITMAP	0x12486c	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360	English	United States	0.39655172413793105
RT_BITMAP	0x124a3c	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360	English	United States	0.5344827586206896
RT_BITMAP	0x124c0c	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360	English	United States	0.39655172413793105
RT_BITMAP	0x124ddc	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States	0.39864864864864863
RT_BITMAP	0x124f04	0x128	Device independent bitmap graphic, 19 x 16 x 4, image size 192	English	United States	0.3885135135135135
RT_BITMAP	0x12502c	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States	0.3885135135135135
RT_BITMAP	0x125154	0xe8	Device independent bitmap graphic, 13 x 16 x 4, image size 128	English	United States	0.36637931034482757
RT_BITMAP	0x12523c	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States	0.3614864864864865
RT_BITMAP	0x125364	0x128	Device independent bitmap graphic, 20 x 16 x 4, image size 192	English	United States	0.3783783783783784
RT_BITMAP	0x12548c	0xd0	Device independent bitmap graphic, 13 x 13 x 4, image size 104	English	United States	0.49038461538461536
RT_BITMAP	0x12555c	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States	0.3716216216216216
RT_BITMAP	0x125684	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States	0.2905405405405405
RT_BITMAP	0x1257ac	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States	0.38175675675675674
RT_BITMAP	0x1258d4	0x128	Device independent bitmap graphic, 19 x 16 x 4, image size 192	English	United States	0.3783783783783784
RT_BITMAP	0x1259fc	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States	0.3783783783783784

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_BITMAP	0x125b24	0xe8	Device independent bitmap graphic, 12 x 16 x 4, image size 128	English	United States	0.3620689655172414
RT_BITMAP	0x125c0c	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States	0.3581081081081081
RT_BITMAP	0x125d34	0x128	Device independent bitmap graphic, 20 x 16 x 4, image size 192	English	United States	0.375
RT_BITMAP	0x125e5c	0xd0	Device independent bitmap graphic, 13 x 13 x 4, image size 104	English	United States	0.47115384615384615
RT_BITMAP	0x125f2c	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States	0.36824324324324326
RT_BITMAP	0x126054	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States	0.28716216216216217
RT_BITMAP	0x12617c	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States	0.3885135135135135
RT_BITMAP	0x1262a4	0x128	Device independent bitmap graphic, 19 x 16 x 4, image size 192	English	United States	0.375
RT_BITMAP	0x1263cc	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States	0.375
RT_BITMAP	0x1264f4	0xe8	Device independent bitmap graphic, 13 x 16 x 4, image size 128	English	United States	0.36637931034482757
RT_BITMAP	0x1265dc	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States	0.35135135135135137
RT_BITMAP	0x126704	0x128	Device independent bitmap graphic, 20 x 16 x 4, image size 192	English	United States	0.36486486486486486
RT_BITMAP	0x12682c	0xd0	Device independent bitmap graphic, 13 x 13 x 4, image size 104	English	United States	0.47115384615384615
RT_BITMAP	0x1268fc	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States	0.3581081081081081
RT_BITMAP	0x126a24	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States	0.28716216216216217
RT_BITMAP	0x126b4c	0xe8	Device independent bitmap graphic, 16 x 16 x 4, image size 128	English	United States	0.4870689655172414
RT_ICON	0x126c34	0x1bc8	Device independent bitmap graphic, 72 x 144 x 8, image size 5184, 256 important colors			0.12570303712035996
RT_ICON	0x1287fc	0x608	Device independent bitmap graphic, 20 x 40 x 8, image size 400, 256 important colors			0.23056994818652848
RT_ICON	0x128e04	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 21600			0.04953789279112754
RT_ICON	0x12e28c	0x3a48	Device independent bitmap graphic, 60 x 120 x 32, image size 14880			0.05630026809651475
RT_ICON	0x131cd4	0x1a68	Device independent bitmap graphic, 40 x 80 x 32, image size 6720			0.08994082840236686
RT_ICON	0x13373c	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400			0.16639344262295083
RT_ICON	0x1340c4	0x6b8	Device independent bitmap graphic, 20 x 40 x 32, image size 1680			0.19883720930232557
RT_ICON	0x13477c	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088			0.18882978723404256
RT_DIALOG	0x134be4	0x52	data			0.7682926829268293
RT_DIALOG	0x134c38	0x52	data			0.7560975609756098
RT_STRING	0x134c8c	0x27c	data			0.4748427672955975
RT_STRING	0x134f08	0x3ec	data			0.4213147410358566
RT_STRING	0x1352f4	0x4c8	data			0.38480392156862747
RT_STRING	0x1357bc	0x9c	data			0.717948717948718
RT_STRING	0x135858	0xec	data			0.6271186440677966
RT_STRING	0x135944	0x1a4	data			0.5357142857142857
RT_STRING	0x135ae8	0x43c	data			0.38468634686346864
RT_STRING	0x135f24	0x348	data			0.4119047619047619
RT_STRING	0x13626c	0x370	data			0.34545454545454546
RT_STRING	0x1365dc	0x390	data			0.40789473684210525
RT_STRING	0x13696c	0xd0	data			0.5721153846153846
RT_STRING	0x136a3c	0xa0	data			0.65
RT_STRING	0x136adc	0x2b8	data			0.4540229885057471
RT_STRING	0x136d94	0x474	data			0.29385964912280704
RT_STRING	0x137208	0x38c	data			0.3876651982378855
RT_STRING	0x137594	0x2b4	data			0.42052023121387283

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_RCDATA	0x137848	0x10	data			1.5
RT_RCDATA	0x137858	0x398	data			0.6945652173913044
RT_GROUP_CURSOR	0x137bf0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.25
RT_GROUP_CURSOR	0x137c04	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.25
RT_GROUP_CURSOR	0x137c18	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.3
RT_GROUP_CURSOR	0x137c2c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.3
RT_GROUP_CURSOR	0x137c40	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.3
RT_GROUP_CURSOR	0x137c54	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.3
RT_GROUP_CURSOR	0x137c68	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States	1.3
RT_GROUP_ICON	0x137c7c	0x76	data			0.7542372881355932

Imports

DLL	Import
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
user32.dll	GetKeyboardType, DestroyWindow, LoadStringA, MessageBoxA, CharNextA
kernel32.dll	GetACP, Sleep, VirtualFree, VirtualAlloc, GetTickCount, QueryPerformanceCounter, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, CompareStringA, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
user32.dll	CreateWindowExA, WindowFromPoint, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, ShowCaret, SetWindowsHookExA, SetWindowPos, SetWindowPlacement, SetWindowLongW, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageW, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageW, PeekMessageA, OpenClipboard, OffsetRect, OemToCharA, NotifyWinEvent, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowUnicode, IsWindowEnabled, IsWindow, IsRectEmpty, IsMenu, IsIconic, IsDialogMessageW, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, HideCaret, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongW, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessagePos, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutNameA, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassLongA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumChildWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawStateA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawEdge, DispatchMessageW, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CharNextW, ChangeDisplaySettingsA, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
opengl32.dll	wglMakeCurrent, wglDeleteContext
gdi32.dll	UnrealizeObject, SwapBuffers, StretchBlt, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, Polygon, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPointA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetRgnBox, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, GdiFlush, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
kernel32.dll	lstrcpyA, WriteProcessMemory, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtectEx, VirtualProtect, VirtualAlloc, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryExA, LoadLibraryA, LeaveCriticalSection, IsBadReadPtr, InitializeCriticalSection, GlobalUnlock, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetStdHandle, GetProcAddress, GetModuleHandleW, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetFileAttributesA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCurrentProcess, GetCPInfo, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteFileA, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle

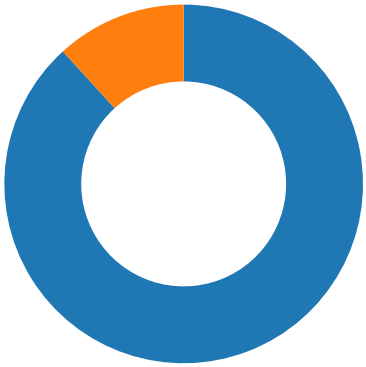
DLL	Import
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegFlushKey, RegCloseKey
glu32.dll	gluDisk, gluCylinder
opengl32.dll	glVertex3f, glTranslatef, glRotatef, glPushMatrix, glPopMatrix, glPolygonMode, glNormal3f, glLoadIdentity, glEnd, glEnable, glDisable, glColor3f, glClear, glCallList, glBegin
oleaut32.dll	GetErrorInfo, VariantInit, SysFreeString
ole32.dll	CoUninitialize, CoInitialize
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopyInd, VariantCopy, VariantClear, VariantInit
comctl32.dll	_TrackMouseEvent, ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Replace, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create
ntdll	NtAllocateVirtualMemory
oleacc.dll	LresultFromObject
winmm.dll	sndPlaySoundA
advapi32	GetTokenInformation
ntdll	NtWriteVirtualMemory, NtProtectVirtualMemory
uRL	TelnetProtocolHandler

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 34

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 5, 2023 22:20:41.968466043 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.194540977 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.194904089 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.195539951 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.421448946 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.421928883 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.422004938 CEST	80	49706	81.161.229.9	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 5, 2023 22:20:42.422024012 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.422048092 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.422068119 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.422086954 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.422105074 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.422123909 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.422122955 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.422142982 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.422166109 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.422173977 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.422174931 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.422228098 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.648080111 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648175955 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648250103 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648308992 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648319960 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.648369074 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648379087 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.648431063 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648492098 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648504019 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.648552895 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648613930 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648619890 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.648678064 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648740053 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.648741007 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648802996 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648865938 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.648869038 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648931026 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648992062 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.648997068 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.649055004 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.649111032 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.649152040 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.649173021 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.649241924 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.649245024 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.649327040 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.649411917 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.875397921 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.875504971 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.875556946 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.875603914 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.875649929 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.875694036 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.875739098 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.875782967 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.875825882 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.875869989 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.875912905 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.875924110 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.875956059 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876000881 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876045942 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876051903 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.876091957 CEST	80	49706	81.161.229.9	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 5, 2023 22:20:42.876135111 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876163006 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.876178026 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876224995 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876235008 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.876271009 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876306057 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.876316071 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876359940 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876405954 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876418114 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.876451969 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876485109 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.876497984 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876543999 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876586914 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.876588106 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876632929 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876672983 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.876677990 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876722097 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876748085 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.876768112 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876812935 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876853943 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.876857996 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876904011 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876929998 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.876948118 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.876992941 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.877010107 CEST	49706	80	192.168.2.4	81.161.229.9
Sep 5, 2023 22:20:42.877038956 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.877084017 CEST	80	49706	81.161.229.9	192.168.2.4
Sep 5, 2023 22:20:42.877127886 CEST	80	49706	81.161.229.9	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 5, 2023 22:20:41.582685947 CEST	53819	53	192.168.2.4	8.8.8.8
Sep 5, 2023 22:20:41.961239100 CEST	53	53819	8.8.8.8	192.168.2.4
Sep 5, 2023 22:20:46.337424994 CEST	60316	53	192.168.2.4	8.8.8.8
Sep 5, 2023 22:20:47.062622070 CEST	53	60316	8.8.8.8	192.168.2.4
Sep 5, 2023 22:20:56.427208900 CEST	51816	53	192.168.2.4	8.8.8.8
Sep 5, 2023 22:20:56.809474945 CEST	53	51816	8.8.8.8	192.168.2.4
Sep 5, 2023 22:21:49.649444103 CEST	54388	53	192.168.2.4	8.8.8.8
Sep 5, 2023 22:21:50.043793917 CEST	53	54388	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 5, 2023 22:20:41.582685947 CEST	192.168.2.4	8.8.8.8	0x59b0	Standard query (0)	wsvdyhrgebwhevawe.ydns.eu	A (IP address)	IN (0x0001)	false
Sep 5, 2023 22:20:46.337424994 CEST	192.168.2.4	8.8.8.8	0x1530	Standard query (0)	tornado.ydns.eu	A (IP address)	IN (0x0001)	false
Sep 5, 2023 22:20:56.427208900 CEST	192.168.2.4	8.8.8.8	0x6204	Standard query (0)	wsvdyhrgebwhevawe.ydns.eu	A (IP address)	IN (0x0001)	false
Sep 5, 2023 22:21:49.649444103 CEST	192.168.2.4	8.8.8.8	0x3d44	Standard query (0)	orifak.ydns.eu	A (IP address)	IN (0x0001)	false

DNS Answers

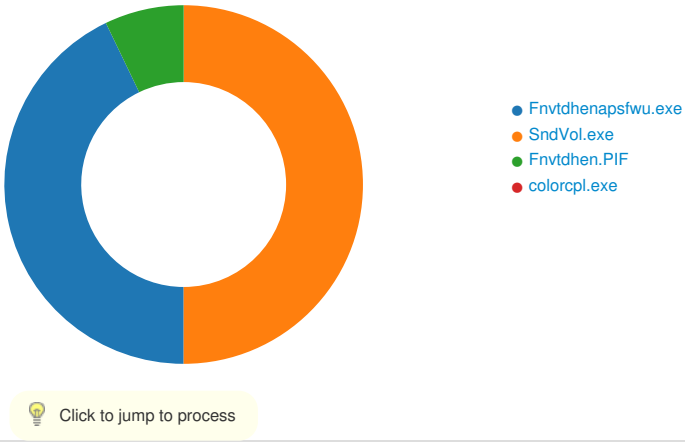
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 5, 2023 22:20:41.961239100 CEST	8.8.8.8	192.168.2.4	0x59b0	No error (0)	wsvdyhrgebwhevawe.ydns.eu		81.161.229.9	A (IP address)	IN (0x0001)	false
Sep 5, 2023 22:20:47.062622070 CEST	8.8.8.8	192.168.2.4	0x1530	No error (0)	tornado.ydns.eu		193.42.32.61	A (IP address)	IN (0x0001)	false
Sep 5, 2023 22:20:56.809474945 CEST	8.8.8.8	192.168.2.4	0x6204	No error (0)	wsvdyhrgebwhevawe.ydns.eu		81.161.229.9	A (IP address)	IN (0x0001)	false
Sep 5, 2023 22:21:50.043793917 CEST	8.8.8.8	192.168.2.4	0x3d44	No error (0)	orifak.ydns.eu		193.42.32.61	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- wsvdyhrgebwhevawe.ydns.eu

Statistics

Behavior



System Behavior

Analysis Process: Fnvtdhenapsfwu.exe PID: 7056, Parent PID: 3512

General

Target ID:	0
Start time:	22:20:39
Start date:	05/09/2023
Path:	C:\Users\user\Desktop\Fnvtdhenapsfwu.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Fnvtdhenapsfwu.exe
Imagebase:	0x400000
File size:	1'243'648 bytes
MD5 hash:	CFFE529403460C6AFFE0F52C1E7DE602
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low
Has exited:	true

File Activities

Registry Activities

Analysis Process: SndVol.exe PID: **7120**, Parent PID: **7056**

General

Target ID:	1
Start time:	22:20:44
Start date:	05/09/2023
Path:	C:\Windows\SysWOW64\SndVol.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\SndVol.exe
Imagebase:	0x950000
File size:	226'264 bytes
MD5 hash:	1EF1A9B89A984DD25DB61DC1AF2548B8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000001.00000002.474312952.00000000007D5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000002.474788319.00000000062F0000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000001.00000002.474788319.00000000062F0000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM, Description: Detects Windows exceutables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003), Source: 00000001.00000002.474788319.00000000062F0000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000001.00000002.474788319.00000000062F0000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000001.00000002.474788319.00000000062F0000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000002.474134003.0000000000400000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000001.00000002.474134003.0000000000400000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM, Description: Detects Windows exceutables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003), Source: 00000001.00000002.474134003.0000000000400000.00000040.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000001.00000002.474134003.0000000000400000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000001.00000002.474134003.0000000000400000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	moderate
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40A6D0	CreateDirectoryW
C:\ProgramData\remcos\logs.dat	append data or add subdirectory or create pipe instance | read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	41C388	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\remcos\logs.dat	0	162	0d 00 0a 00 5b 00 32 00 30 00 32 00 33 00 2f 00 30 00 39 00 2f 00 30 00 35 00 20 00 32 00 32 00 3a 00 32 00 30 00 3a 00 34 00 34 00 20 00 4f 00 66 00 66 00 6c 00 69 00 6e 00 65 00 20 00 4b 00 65 00 79 00 6c 00 6f 00 67 00 67 00 65 00 72 00 20 00 53 00 74 00 61 00 72 00 74 00 65 00 64 00 5d 00 0d 00 0a 00 0d 00 0a 00 5b 00 52 00 75 00 6e 00 5d 00 0d 00 0a 00 0d 00 0a 00 5b 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 4d 00 61 00 6e 00 61 00 67 00 65 00 72 00 5d 00 0d 00 0a 00	[2023/09/05 22:20:44 Offline Keylogger Started][Run][Program Manager]	success or wait	1	41C3C2	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\RmEEESSSssss-3AINT8\	success or wait	1	4136D2	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\RmEEESSSssss-3AINT8	exepath	binary	5D 86 94 21 89 64 03 EF 02 F0 1A 8C 18 48 83 BA F5 1E 0B B2 CE 87 9E CE 97 84 C0 F9 9F 69 84 3D 1B 14 72 6F 18 CA 83 73 B4 9E 44 F0 36 32 12 19 BB 77 BA 85 96 6A A6 47 93 FE 15 95 D1 96	success or wait	1	4136FA	RegSetValueExA
HKEY_CURRENT_USER\Software\RmEEESSSssss-3AINT8	licence	unicode	D3596CEE7D5C07A9162C55F49655DE72	success or wait	1	4136FA	RegSetValueExA
HKEY_CURRENT_USER\Software\RmEEESSSssss-3AINT8	time	dword	1693952130	success or wait	1	4137F4	RegSetValueExA

Analysis Process: Fnvtdhen.PIF PID: **6264**, Parent PID: **3512**

General

Target ID:	2
Start time:	22:20:53
Start date:	05/09/2023
Path:	C:\Users\Public\Libraries\Fnvtdhen.PIF
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\Libraries\Fnvtdhen.PIF"
Imagebase:	0x400000
File size:	1'243'648 bytes
MD5 hash:	CFFE529403460C6AFFE0F52C1E7DE602
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: C:\Users\Public\Libraries\Fnvtdhen.PIF, Author: Joe Security
Antivirus matches:	• Detection: 62%, ReversingLabs
Reputation:	low
Has exited:	true

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Fnvtdhen.PIF	unknown	1243648	success or wait	1	2BBCC45	NtReadFile

Analysis Process: colorcpl.exe PID: **6388**, Parent PID: **6264**

General

Target ID:	8
Start time:	22:21:00
Start date:	05/09/2023
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\colorcpl.exe
Imagebase:	0x60000
File size:	86'528 bytes
MD5 hash:	746F3B5E7652EA0766BA10414D317981
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000002.253206056.0000000002AB1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.253042102.0000000002AB1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.253092372.0000000002AB1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.253076423.0000000002AD0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000008.00000002.253136648.0000000000400000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000002.253136648.0000000000400000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM, Description: Detects Windows exceutables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003), Source: 00000008.00000002.253136648.0000000000400000.00000040.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000008.00000002.253136648.0000000000400000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000008.00000002.253136648.0000000000400000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000008.00000002.253322818.0000000006190000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000002.253322818.0000000006190000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM, Description: Detects Windows exceutables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003), Source: 00000008.00000002.253322818.0000000006190000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000008.00000002.253322818.0000000006190000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000008.00000002.253322818.0000000006190000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	high
Has exited:	true

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	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly