ID: 830443
Sample Name:
DHLINV000156.exe
Cookbook: default.jbs
Time: 11:51:52
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

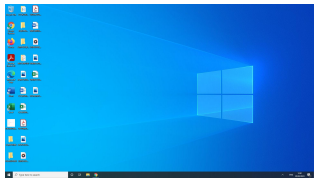
Windows Analysis Report

DHLINV000156.exe

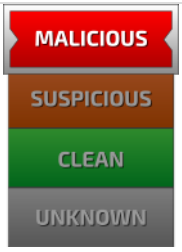
Overview

General Information

Sample Name:	DHLINV000156.exe
Analysis ID:	830443
MD5:	4cef4c9b4785b..
SHA1:	5e00a720edff5...
SHA256:	0a83a6c897b4...
Infos:	



Detection



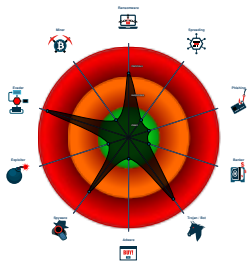
FormBook, GuLoader

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

Signatures

- Multi AV Scanner detection for subm...
- Yara detected FormBook
- Malicious sample detected (through...
- System process connects to networ...
- Antivirus detection for URL or domain
- Yara detected GuLoader
- Sample uses process hollowing tech...
- Tries to steal Mail credentials (via fi...
- Maps a DLL or memory area into an...
- Writes to foreign memory regions
- Tries to detect Any.run
- Injects a PE file into a foreign proce...

Classification



Process Tree

- **System is w10x64native**
- DHLINV000156.exe (PID: 9100 cmdline: C:\Users\user\Desktop\DHLINV000156.exe MD5: 4CEF4C9B4785B2BC5ADCBF1C91185AB9)
  - DHLINV000156.exe (PID: 7624 cmdline: C:\Users\user\Desktop\DHLINV000156.exe MD5: 4CEF4C9B4785B2BC5ADCBF1C91185AB9)
    - explorer.exe (PID: 4592 cmdline: C:\Windows\Explorer.EXE MD5: 5EA66FF5AE5612F921BC9DA23BAC95F7)
      - autoconv.exe (PID: 7192 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 469594005E3B94C5945BCCE7FC521C05)
      - colorcpl.exe (PID: 8804 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: DB71E132EBF1FEB6E93E8A2A0F0C903D)
        - firefox.exe (PID: 1820 cmdline: C:\Program Files\Mozilla Firefox\Firefox.exe MD5: FA9F4FC5D7ECAB5A20BF7A9D1251C851)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Formbook, Formbo	FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.	• SWEED • Cobalt	**http://** blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.htmlhttp://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.htmlhttps://asec.ahnlab.com/en/32149/https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	http://https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INet Cache\Ghetto\internuptial\Smertelig\Registrer\System.dll	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.6881079830.00000000046C0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
0000000C.00000002.6881079830.00000000046C0000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x180f5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17b91:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x181f7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1836f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xaa1a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x16ddc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1de77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ee2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000C.00000002.6881079830.00000000046C0000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1f0c0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xae4f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x182f7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
0000000C.00000002.6880751145.0000000004690000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
0000000C.00000002.6880751145.0000000004690000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x180f5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17b91:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x181f7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1836f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xaa1a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x16ddc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1de77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ee2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 11 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

Yara detected FormBook

Antivirus detection for URL or domain

Networking

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

Yara detected Generic Downloader

E-Banking Fraud

Yara detected FormBook

Spam, unwanted Advertisements and Ransom Demands

Found potential ransomware demand text

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Tries to detect Any.run

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

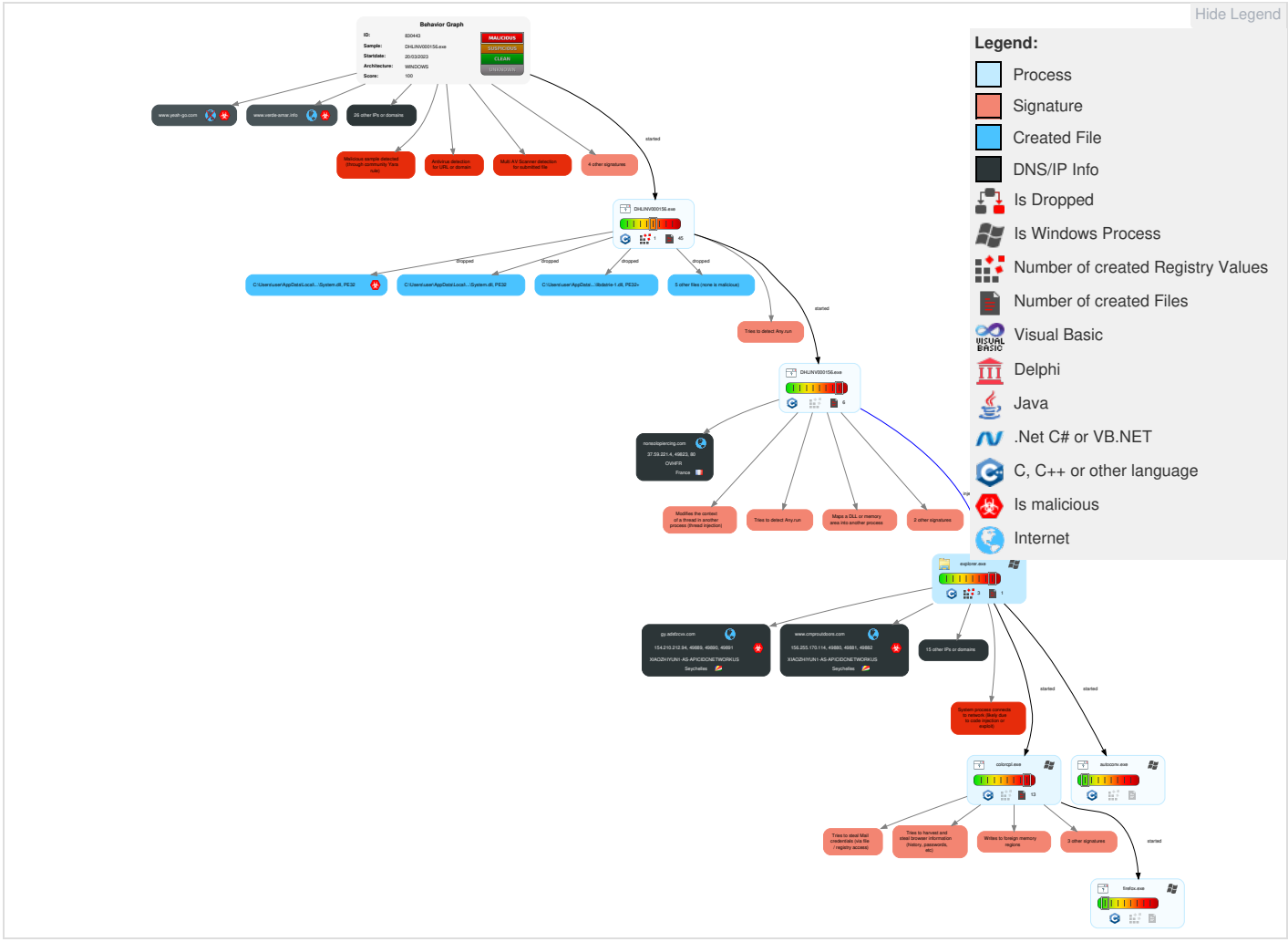
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	3 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/Reboot
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	1 Access Token Manipulation	2 Obfuscated Files or Information	LSASS Memory	4 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	7 1 2 Process Injection	1 Software Packing	Security Account Manager	1 2 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	4 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 Timestomp	NTDS	1 2 Virtualization/Sandbox Evasion	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	2 Process 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 Masquerading	Cached Domain Credentials	1 Application Window 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 2 Virtualization/Sandbox Evasion	DCSync	Network Sniffing	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 Access Token Manipulation	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)	7 1 2 Process Injection	/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

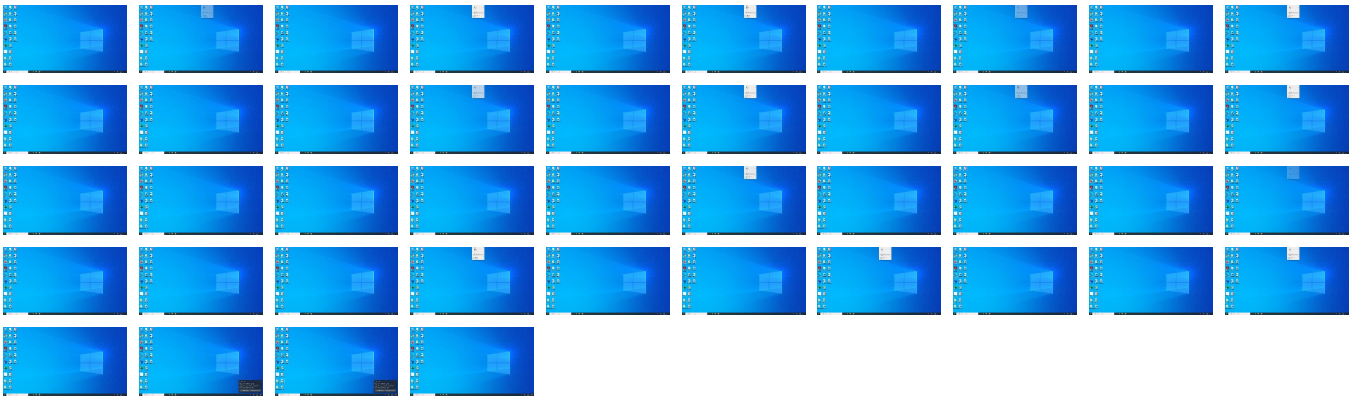
Behavior Graph

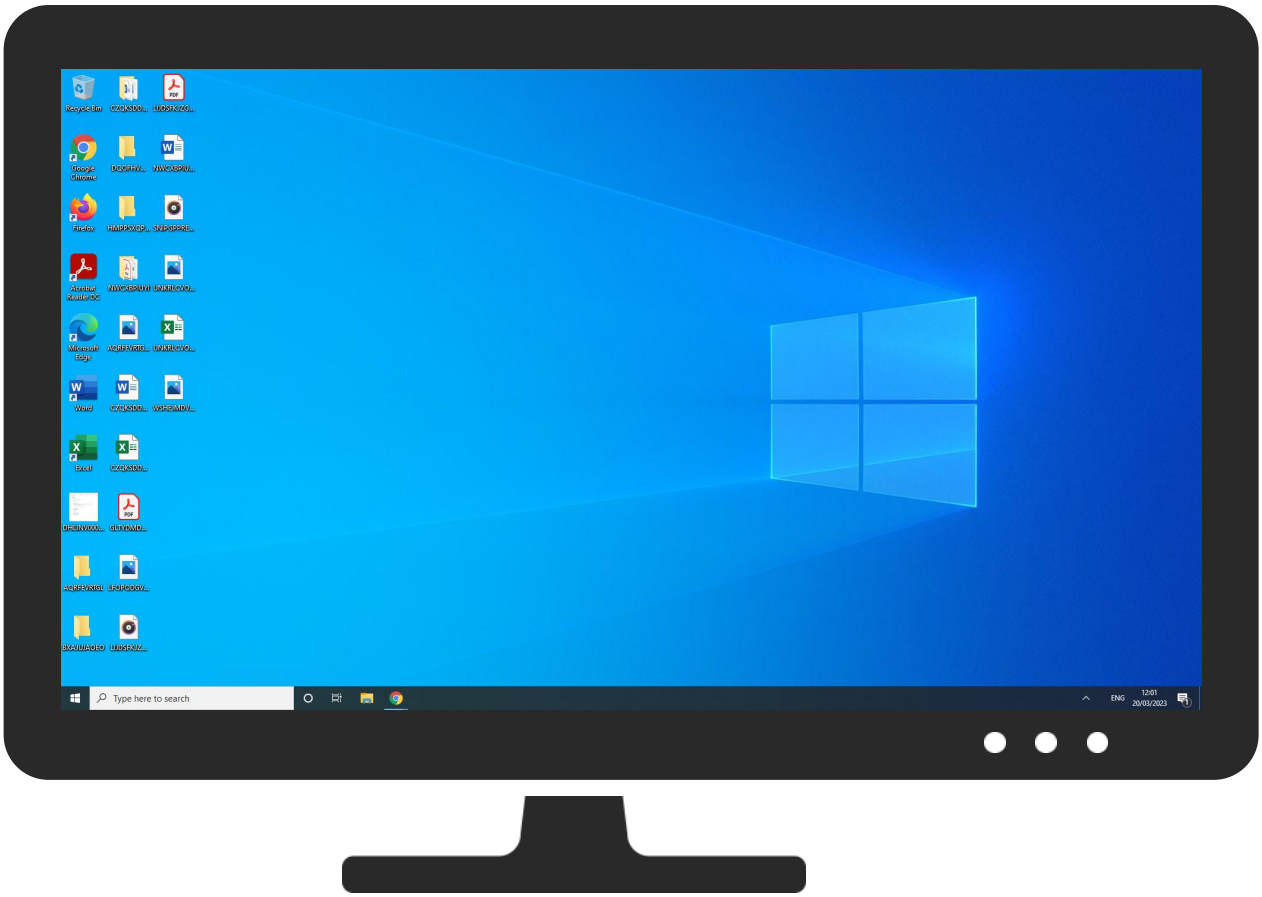


Screenshots

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
DHLINV000156.exe	22%	Virustotal		Browse
DHLINV000156.exe	23%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Glitteringly\pinckneya\Administrerbarest\Fyringssedlens\SolutionExplorerCLI.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Styringsmidlernes\Pinkfishes109\Supersensitizations172\Smaskforvirrede\libpkcs11-helper-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Styringsmidlernes\Pinkfishes109\Supersensitizations172\Smaskforvirrede\maintenanceservice2.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Styringsmidlernes\Pinkfishes109\Supersensitizations172\Smaskforvirrede\percentile.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Supergallantness\afstres\Archives\Sadelmagernaalenes\System.Security.Cryptography.X509Certificates.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\internuptial\Smertelig\Registrer\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\internuptial\Smertelig\Registrer\libdatrie-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsxCFC.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.DHLINV000156.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
8.0.DHLINV000156.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Source	Detection	Scanner	Label	Link	Download
10.2.explorer.exe.14413814.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.DHLINV000156.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
12.2.colorcpl.exe.4bb3814.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.2.firefox.exe.b5d3814.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
td-ccm-168-233.wixdns.net	0%	Virustotal		Browse
popcors.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://schemas.microsoft.c	0%	Avira URL Cloud	safe	
http://www.popcors.com/i9th/	100%	Avira URL Cloud	malware	
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	0%	Avira URL Cloud	safe	
http://www.adasoft.info/i9th/www.adasoft.info	100%	Avira URL Cloud	malware	
http://www.hhkk143.cfd/i9th/?YM=a+ho0UoyjOnZk1ICGpcoaGjEnGbmKf9IFFNpvRdd6kC+DJQ8bYOFaRfvJPlieJPEPcY1cGGv0mjDAZsn1ciiV+plF0lWDSd4aQ==&F20=_ng1IJ	100%	Avira URL Cloud	malware	
http://www.hot6s.comF20=_ng1IJ	0%	Avira URL Cloud	safe	
http://www.globaltourguide.org8KC=R_sQOWT9q	0%	Avira URL Cloud	safe	
http://nonsolopiercing.com/wp-content/vSvXWEFHsgTrbgVnnEpdo45.binystemR0	0%	Avira URL Cloud	safe	
http://www.adasoft.info	0%	Avira URL Cloud	safe	
http://www.riverflow.net/i9th/	0%	Avira URL Cloud	safe	
http://www.popcors.com/i9th/?F20=_ng1IJ&YM=2Tzmt/R719tLBuI7mSD638d/x74EcSC92+f/k2zWdQLWTIlxfL/M90/j5x2SA2nsSzi8rNI8g04ZV+bWcvwPkAs6VEt+1VDvVA==	100%	Avira URL Cloud	malware	
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	
http://www.hayuterce.com	100%	Avira URL Cloud	malware	
http://www.yeah-go.com/i9th/www.yeah-go.com	0%	Avira URL Cloud	safe	
http://www.daon3999.net/i9th/	0%	Avira URL Cloud	safe	
http://www.popcors.com/i9th/www.popcors.com	100%	Avira URL Cloud	malware	
http://www.sandyhillsagritourism.com/i9th/?F20=_ng1IJ&YM=PDhFruS31XQUb4y36+furUas2tGpUbYkRI+Vt3Aa+IAT3kg40wU83JEX1Y8JNHLK9JPMefgRvvrtwUOOtwZiCVeSdeNGXRAYpw==	100%	Avira URL Cloud	malware	
http://www.daon3999.net	0%	Avira URL Cloud	safe	
http://www.hayuterce.com8KC=R_sQOWT9q	0%	Avira URL Cloud	safe	
http://www.dinggubd.netF20=_ng1IJ	0%	Avira URL Cloud	safe	
http://www.popcors.comF20=_ng1IJ	0%	Avira URL Cloud	safe	
http://nonsolopiercing.com/wp-content/vSvXWEFHsgTrbgVnnEpdo45.binv	0%	Avira URL Cloud	safe	
http://www.dinggubd.net/i9th/	100%	Avira URL Cloud	malware	
http://www.spotcheck.site	100%	Avira URL Cloud	malware	
http://nonsolopiercing.com/wp-content/vSvXWEFHsgTrbgVnnEpdo45.bin	0%	Avira URL Cloud	safe	
http://https://www.cmproutdoors.com/i9th/?YM=lqJURYfuPjuznURrThj0aNiAAsaH1/tf	0%	Avira URL Cloud	safe	
http://www.adasoft.infoF20=_ng1IJ	0%	Avira URL Cloud	safe	
http://www.casinoenligne-france.infoF20=_ng1IJ	0%	Avira URL Cloud	safe	
http://https://outlook.comE	0%	Avira URL Cloud	safe	
http://www.daon3999.net:80/i9th/?F20=_ng1IJ&YM=f7i/reR9z/XYtiufs4T2oCglTJHppPIhAuHFUSLntHIlLxYI6	0%	Avira URL Cloud	safe	
http://www.hayuterce.com/i9th/www.hayuterce.com	100%	Avira URL Cloud	malware	
http://www.37123.vip/i9th/www.37123.vip	100%	Avira URL Cloud	malware	
http://www.globaltourguide.org/i9th/www.globaltourguide.org	0%	Avira URL Cloud	safe	
http://www.sem-jobs.comF20=_ng1IJ	0%	Avira URL Cloud	safe	
http://www.5319ss.com/i9th/?YM=oRug1p2N3M7f21OO0lOBGqE4PfaV2grEv9VY5puRv4+mIhzAnHI5ZAphwtkKSkIVc0m4kQAL+gvPk8R76uitxElzOZBQuGepJQ==&F20=_ng1IJ	0%	Avira URL Cloud	safe	
http://www.dinggubd.net/i9th/?F20=_ng1IJ&YM=skpIeuUmXVtlsTBo2HC5tT/aGHmA0xfCvZmPrRJBNh0Q4R2Cj+Wk81Dgip66N6Ewmv0qryLoIL5Vk4bBbPirrB4g3slArb9fSw==	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://www.spotcheck.siteF20=_ng1IJ	0%	Avira URL Cloud	safe	
http://www.casinoenligne-france.info	0%	Avira URL Cloud	safe	
http://www.yeah-go.com	0%	Avira URL Cloud	safe	
http://www.verde-amar.info/i9th/?YM=k3d2rpkNYMKNWaTFA3t0FG4YoWbTiA9z8X9PQFaufAL9B597B9+6rAPLCs31mdZA/v+HUWU5or1J0geLcv9LMooOfPEJdl/q3g==&F20=_ng1IJ	0%	Avira URL Cloud	safe	
http://www.casinoenligne-france.info/i9th/	100%	Avira URL Cloud	malware	
http://www.yeah-go.com/i9th/	0%	Avira URL Cloud	safe	
http://www.hot6s.com/i9th/www.hot6s.com	100%	Avira URL Cloud	malware	
http://www.hhkk143.cfd/i9th/	100%	Avira URL Cloud	malware	
http://www.hot6s.com	100%	Avira URL Cloud	malware	
http://www.casinoenligne-france.info/i9th/www.casinoenligne-france.info	100%	Avira URL Cloud	malware	
http://www.hhkk143.cfdF20=_ng1IJ	0%	Avira URL Cloud	safe	
http://www.nortonseecurity.com8KC=R_sQOWT9q	0%	Avira URL Cloud	safe	
http://www.sandyhillsagritourism.comF20=_ng1IJ	0%	Avira URL Cloud	safe	
http://www.hot6s.com/i9th/	100%	Avira URL Cloud	malware	
http://schemas.micro	0%	Avira URL Cloud	safe	
http://www.37123.vipF20=_ng1IJ	0%	Avira URL Cloud	safe	
http://www.cmproutdoors.comF20=_ng1IJ	0%	Avira URL Cloud	safe	
http://www.daon3999.net/i9th/?F20=_ng1IJ&YM=f7i/reR9z/XYtiufs4T2oCglTJHppPIhAuHFUSLntHIlLxYI6+YKRHThES4heztnev1TOQxmA1eDErfm329tx1/Ku+4bHpf60w==	0%	Avira URL Cloud	safe	
http://www.cmproutdoors.com/i9th/www.cmproutdoors.com	100%	Avira URL Cloud	malware	
http://www.riverflow.net/i9th/?F20=_ng1IJ&YM=djsn1an+GmzwXFTB/MFsKGQXJOZQhusBpj6p6RqECbOdtpCOv2Kvcnth4kqs1edHWjVNJqZCDFfEwc47KO0/1j4B7gbgnVo+SQ==	0%	Avira URL Cloud	safe	
http://www.37123.vip	0%	Avira URL Cloud	safe	
http://www.spotcheck.site/i9th/	100%	Avira URL Cloud	malware	
http://www.0w3jy.com/i9th/?F20=_ng1IJ&YM=uGolGY6UqX3sY/9PLVWwN9J/BTzz+6hffrhecVGN5FjI635Z0j5At+r+BPTklOB2HfIE21jETmQJryl68L/U0+pl2AIDG80kBg==	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://www.verde-amar.info/i9th/	0%	Avira URL Cloud	safe	
http://www.dinggubd.net	0%	Avira URL Cloud	safe	
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://www.globaltourguide.org/i9th/	0%	Avira URL Cloud	safe	
http://www.spotcheck.site/i9th/www.spotcheck.site	100%	Avira URL Cloud	malware	
http://www.adasoft.info/i9th/?F20=_ng1IJ&YM=7TOFWM92qV6pcrPqADbwGQbE1m3eI0WOEQ27vaT62sOH8JmND2m/uvMqxI1JrYebWMYnTtk64dqQKbYLv2YomR00aJ+FLC/PKQ==	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
td-ccm-168-233.wixdns.net	34.117.168.233	true	true	• 0%, Virustotal, Browse	unknown
popcors.com	173.230.227.171	true	true	• 1%, Virustotal, Browse	unknown
www.spotcheck.site	199.192.30.193	true	true		unknown
gy.adsfzcvx.com	154.210.212.94	true	true		unknown
www.riverflow.net	64.190.63.111	true	true		unknown
hk.ygrcw.cn	164.88.122.250	true	true		unknown
www.sem-jobs.com	85.13.156.177	true	true		unknown
www.dinggubd.net	38.163.2.19	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
u4tgw7dr.n.funnull35.com	20.239.65.138	true	true		unknown
nonsolopiercing.com	37.59.221.4	true	false		unknown
adasoft.info	81.88.48.71	true	true		unknown
www.hot6s.com	104.21.8.203	true	true		unknown
www.hhkk143.cfd	188.114.96.3	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
daon3999.net	222.122.213.231	true	true		unknown
www.casinoenligne-france.info	3.9.182.46	true	true		unknown
www.cmproutdoors.com	156.255.170.114	true	true		unknown
www.verde-amar.info	185.53.177.54	true	true		unknown
www.popcors.com	unknown	unknown	true		unknown
www.sandyhillsagritourism.com	unknown	unknown	true		unknown
www.0w3jy.com	unknown	unknown	true		unknown
www.yeah-go.com	unknown	unknown	true		unknown
www.37123.vip	unknown	unknown	true		unknown
www.daon3999.net	unknown	unknown	true		unknown
www.5319ss.com	unknown	unknown	true		unknown
www.adasoft.info	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.hhkk143.cfd/i9th/?YM=a+ho0UoyjOnZk1ICGpcoaGjEnGbmKf9IFFNpvRdd6kC+DJQ8bYOFaRfvJPlieJPEPcY1cGGv0mjDAZsn1ciiV+plF0lWDSd4aQ==&F20=_ng1lJ	true	• Avira URL Cloud: malware	unknown
http://www.popcors.com/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.riverflow.net/i9th/	true	• Avira URL Cloud: safe	unknown
http://www.popcors.com/i9th/?F20=_ng1lJ&YM=2Tzmt/R719tLBul7mSD638d/x74EcSC92+f/k2zWdQLWTIlxfL/M90/j5x2SA2nsSzi8rNl8g04ZV+bWcvwPkAs6VEt+1VDvVA==	true	• Avira URL Cloud: malware	unknown
http://www.sandyhillsagritourism.com/i9th/?F20=_ng1lJ&YM=PDhFruS31XQUb4y36+furUas2tGpUbYkRl+Vt3Aa+IAT3kg40wU83JEX1Y8JNHLK9JPMefgRvvrtwUOOtwZiCVeSdeNGXRAYpw==	true	• Avira URL Cloud: malware	unknown
http://www.daon3999.net/i9th/	true	• Avira URL Cloud: safe	unknown
http://nonsolopiercing.com/wp-content/vSvXWEFHsgTrbgVnnEpdo45.bin	false	• Avira URL Cloud: safe	unknown
http://www.dinggubd.net/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.5319ss.com/i9th/?YM=oRug1p2N3M7f21OO0lOBGqE4PfaV2grEv9VY5puRv4+mIhzAnHI5ZAphwtkKSkIVc0m4kQAL+gvPk8R76uitxElzOZBQuGepJQ==&F20=_ng1lJ	true	• Avira URL Cloud: safe	unknown
http://www.dinggubd.net/i9th/?F20=_ng1lJ&YM=skpIeuUmXVtlsTBo2HC5tT/aGHmA0xfCvZmPrRJBNh0Q4R2Cj+Wk81Dgip66N6Ewmv0qryLoIL5Vk4bBbPirrB4g3slArb9fSw==	true	• Avira URL Cloud: malware	unknown
http://www.verde-amar.info/i9th/?YM=k3d2rpkNYMKNWaTFA3t0FG4YoWbTiA9z8X9PQFaufAL9B597B9+6rAPLCs31mdZA/v+HUWU5or1J0geLcv9LMooOfPEJdl/q3g==&F20=_ng1lJ	true	• Avira URL Cloud: safe	unknown
http://www.casinoenligne-france.info/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.yeah-go.com/i9th/	true	• Avira URL Cloud: safe	unknown
http://www.hhkk143.cfd/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.hot6s.com/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.daon3999.net/i9th/?F20=_ng1lJ&YM=f7i/reR9z/XYtiufs4T2oCglTJHppPIhAuHFUSLntHIlLxYI6+YKRHThES4heztnev1TOQxmA1eDErfm329tx1/Ku+4bHpf60w==	true	• Avira URL Cloud: safe	unknown
http://www.riverflow.net/i9th/?F20=_ng1lJ&YM=djsn1an+GmzwXFTB/MFsKGQXJOZQhusBpj6p6RqECbOdtpCOv2Kvcnth4kqs1edHWjVNJqZCDFfEwc47KO0/1j4B7gbgnVo+SQ==	true	• Avira URL Cloud: safe	unknown
http://www.0w3jy.com/i9th/?F20=_ng1lJ&YM=uGolGY6UqX3sY/9PLVWwN9J/BTzz+6hffrhecVGN5FjI635Z0j5At+r+BPTklOB2HfIE21jETmQJryl68L/U0+pl2AIDG80kBg==	true	• Avira URL Cloud: safe	unknown
http://www.spotcheck.site/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.verde-amar.info/i9th/	true	• Avira URL Cloud: safe	unknown
http://www.adasoft.info/i9th/?F20=_ng1lJ&YM=7TOFWM92qV6pcrPqADbwGQbE1m3eI0WOEQ27vaT62sOH8JmND2m/uvMqxI1JrYebWMYnTtk64dqQKbYLv2YomR00aJ+FLC/PKQ==	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.hot6s.comF20=_ng1lJ	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	colorcpl.exe, 0000000C.00000002.68903409 19.0000000007503000.00000004.00000020.00 020000.00000000.sdmp, colorcpl.exe, 0000 000C.00000003.3401883899.000000000749500 0.00000004.00000020.00020000.00000000.sdmp, AeL-0b1QRQ.12.dr	false		high
http://www.adasoft.info	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://uk.search.yahoo.com/favicon.icohttps://uk.searc h.yahoo.com/search	colorcpl.exe, 0000000C.00000002.68903409 19.0000000007503000.00000004.00000020.00 020000.00000000.sdmp, colorcpl.exe, 0000 000C.00000003.3401883899.000000000749500 0.00000004.00000020.00020000.00000000.sdmp, AeL-0b1QRQ.12.dr	false		high
http://www.adasoft.info/i9th/www.adasoft.info	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/ac/?q=	colorcpl.exe, 0000000C.00000003.34018838 99.0000000007495000.00000004.00000020.00 020000.00000000.sdmp, AeL-0b1QRQ.12.dr	false		high
http://nonsolopiercing.com/wp-content/vSvXWEFHsgTrbgVnnEpdo45.binystemR0	DHLINV000156.exe, 00000008.00000002.3257 887473.0000000003138000.00000004.0000002 0.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://api.msn.com:443/v1/news/Feed/Windows?	explorer.exe, 0000000A.00000002.69144732 74.000000000F76E000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.3152133955.0000000009BE000 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000002.6889834307.000 0000009BE0000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.3171009246.000000000F76E000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	DHLINV000156.exe, 00000008.00000001.2368 782551.0000000000649000.00000020.0000000 1.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.microsoft.c	explorer.exe, 0000000A.00000002.69144732 74.000000000F76E000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.3171009246.000000000F76E00 0.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://excel.office.com	explorer.exe, 0000000A.00000003.36220023 35.000000000D6AA000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000003.3627191346.000000000D6B500 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000002.6902699355.000 000000D6AA000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.3162334795.000000000D6AA000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://www.globaltourguide.org8KC=R_sQOWT9q	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	DHLINV000156.exe, 00000008.00000001.2368 782551.0000000000626000.00000020.0000000 1.01000000.00000006.sdmp	false		high
http://www.gopher.ftp://ftp.	DHLINV000156.exe, 00000008.00000001.2368 782551.0000000000649000.00000020.0000000 1.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en-us/news/world/uk-climate-activis:	explorer.exe, 0000000A.00000002.68860578 21.0000000005A37000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.3148668525.0000000005A3700 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.daon3999.net	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://activity.windows.com/UserActivity.ReadWrite.CreatedByApp$	explorer.exe, 0000000A.00000003.36267547 47.000000000D651000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.3162334795.000000000D65300 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.popcors.com/i9th/www.popcors.com	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.yeah-go.com/i9th/www.yeah-go.com	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

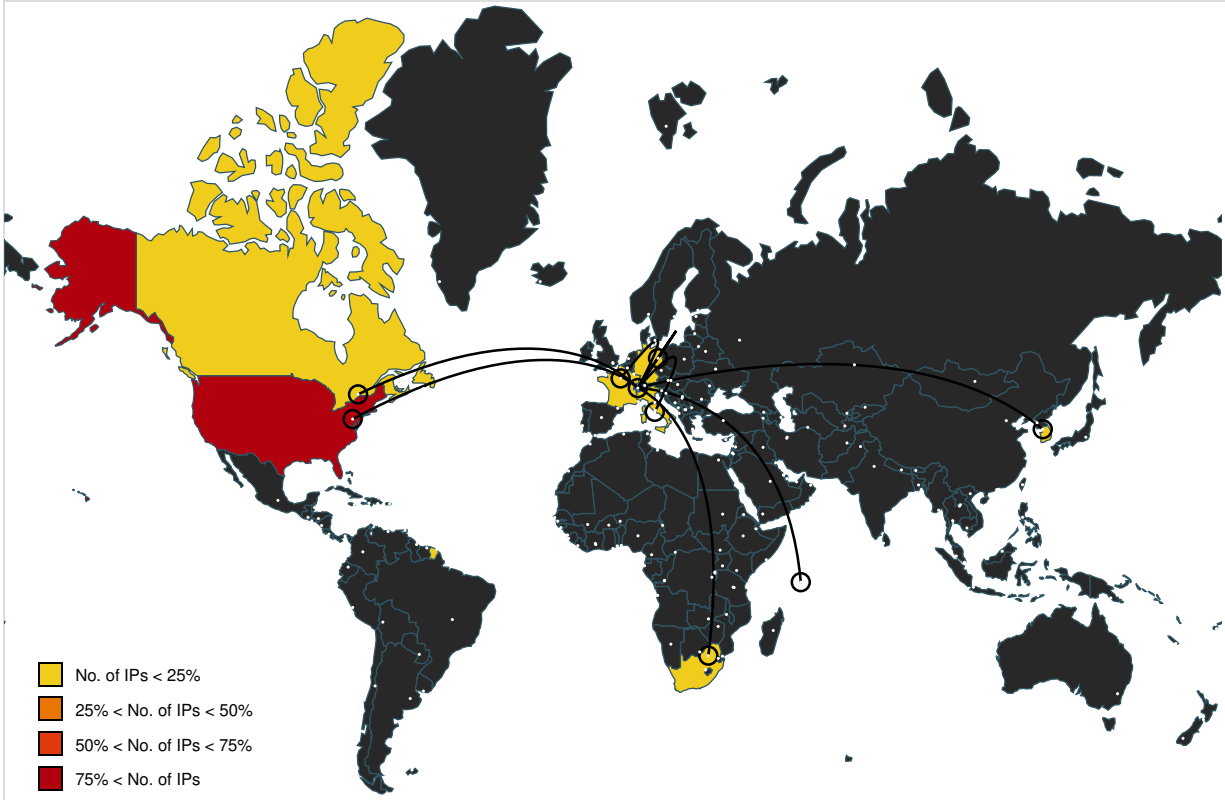
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.hayuterce.com8KC=R_sQOWT9q	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.msn.com/en-us/news/us/texas-gov-abbott-sends-miles-of-cars-along-border-to-deter-migrant	explorer.exe, 0000000A.00000000.31521339 55.0000000009BE0000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000002.6889834307.0000000009BE000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.hayuterce.com	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://android.notify.windows.com/iOSv	explorer.exe, 0000000A.00000000.31655901 23.000000000DA63000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000003.3616659566.000000000DA6300 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.dinggubd.netF20=_ng1lJ	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://uk.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	colorcpl.exe, 0000000C.00000002.68903409 19.0000000007503000.00000004.00000020.00 020000.00000000.sdmp, colorcpl.exe, 0000 000C.00000003.3401883899.000000000749500 0.00000004.00000020.00020000.00000000.sdmp, AeL-0b1QRQ.12.dr	false		high
http://www.popcors.comF20=_ng1lJ	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://nonsolopiercing.com/wp-content/vSvXWEFHsgTrbgVnnEpdo45.binv	DHLINV000156.exe, 00000008.00000002.3258 366023.000000000318B000.00000004.0000002 0.00020000.00000000.sdmp, DHLINV000156.exe, 00000008.00000003.3132388903.0000000 00318B000.00000004.00000020.00020000.000 00000.sdmp, DHLINV000156.exe, 00000008.0 0000003.3131797147.000000000318B000.0000 0004.00000020.00020000.00000000.sdmp, DH LINV000156.exe, 00000008.00000003.313292 7450.000000000318B000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.cmproutdoors.com/i9th/?YM=lqJURYfuPjuznURrThj0aNiAAsaH1/tf	explorer.exe, 0000000A.00000002.69246854 09.000000001591C000.00000004.80000000.00 040000.00000000.sdmp, colorcpl.exe, 0000 000C.00000002.6887012764.00000000060BC00 0.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://assets.msn.com/weathermapdata/1/static/svg/72/MostlySunnyDay.svg	explorer.exe, 0000000A.00000000.31521339 55.0000000009BE0000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000002.6889834307.0000000009BE000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.spotcheck.site	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.adasoft.infoF20=_ng1lJ	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://word.office.com	explorer.exe, 0000000A.00000000.31736926 42.000000000FAB6000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000002.6914647937.000000000FA9700 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000002.6902699355.000 000000D60A000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.3161433559.000000000D607000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://https://www.msn.com/en-us/tv/celebrity/tarek-el-moussa-tests-positive-for-covid-19-shuts-down-filmin	explorer.exe, 0000000A.00000000.31521339 55.0000000009BE0000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000002.6889834307.0000000009BE000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.casinoenligne-france.infoF20=_ng1lJ	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://outlook.comE	explorer.exe, 0000000A.00000000.31408638 53.00000000013A4000.00000004.00000020.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000002.6874670041.00000000013A400 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.daon3999.net:80/i9th/?F20=_ng1IJ&YM=f7i/reR9z/XYtiufs4T2oCglTJHppPIhAuHFUSLntHIlLxYl6	explorer.exe, 0000000A.00000002.69246854 09.0000000015AAE000.00000004.80000000.00 040000.00000000.sdmp, colorcpl.exe, 0000 000C.00000002.6887012764.000000000624E00 0.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en-us/news/technology/facebook-oversight-board-reviewing-xcheck-system-for-vips/	explorer.exe, 0000000A.00000000.31521339 55.0000000009BE0000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000002.6889834307.0000000009BE000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	colorcpl.exe, 0000000C.00000003.34018838 99.0000000007495000.00000004.00000020.00 020000.00000000.sdmp, AeL-0b1QRQ.12.dr	false		high
http://www.hayuterce.com/i9th/www.hayuterce.com	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://nsis.sf.net/NSIS_ErrorError	DHLINV000156.exe	false		high
http://www.37123.vip/i9th/www.37123.vip	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.globaltourguide.org/i9th/www.globaltourguide.org	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/cps0(	DHLINV000156.exe, 00000002.00000003.1944 530759.00000000028ED000.00000004.0000002 0.00020000.00000000.sdmp, SolutionExplorerCLI.dll.2.dr	false		high
http://https://outlook.com	explorer.exe, 0000000A.00000002.69026993 55.000000000D60A000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.3161433559.000000000D60700 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.sem-jobs.comF20=_ng1IJ	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.msn.com/v1/news/Feed/Windows?activityId=5696A836803C42E0B53F7BB2770E5342&timeOut=10000&o	explorer.exe, 0000000A.00000000.31521339 55.0000000009BE0000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000002.6889834307.0000000009BE000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_Error	DHLINV000156.exe	false		high
http://www.symauth.com/rpa00	DHLINV000156.exe, 00000002.00000003.1944 530759.00000000028ED000.00000004.0000002 0.00020000.00000000.sdmp, SolutionExplorerCLI.dll.2.dr	false		high
http://www.casinoenligne-france.info	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://android.notify.windows.com/iOS	explorer.exe, 0000000A.00000000.31655901 23.000000000DA63000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000003.3616659566.000000000DA6300 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.nero.com	DHLINV000156.exe, 00000002.00000003.1944 530759.00000000028ED000.00000004.0000002 0.00020000.00000000.sdmp, SolutionExplorerCLI.dll.2.dr	false		high
http://www.yeah-go.com	explorer.exe, 0000000A.00000002.68981396 35.000000000B78B000.00000040.80000000.00 040000.00000000.sdmp, explorer.exe, 0000 000A.00000002.6914647937.000000000FA9700 0.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.spotcheck.siteF20=_ng1IJ	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.msn.com/v1/news/Feed/Windows?	explorer.exe, 0000000A.00000000.31711668 54.000000000FA10000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000002.6914647937.000000000FA1000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.hot6s.com/i9th/www.hot6s.com	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://sedo.com/search/details/?partnerid=324561&language=d&domain=riverflow.net&origin=sales_lande	explorer.exe, 0000000A.00000002.69246854 09.0000000015DD2000.00000004.80000000.00 040000.00000000.sdmp, colorcpl.exe, 0000 000C.00000002.6887012764.000000000657200 0.00000004.10000000.00040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.hot6s.com	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.casinoenligne-france.info/i9th/www.casinoenligne-france.info	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.nortonseecurity.com8KC=R_sQOWT9q	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://support.google.com/chrome/?p=plugin_flash	colorcpl.exe, 0000000C.00000002.68903409 19.0000000007480000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://www.hhkk143.cfdF20=_ng1lJ	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.msn.com/en-us/news/politics/democratic-su	explorer.exe, 0000000A.00000000.31486685 25.0000000005A37000.00000004.00000001.00 020000.00000000.sdmp	false		high
http://push.zhanzhang.baidu.com/push.js	explorer.exe, 0000000A.00000002.69246854 09.0000000015466000.00000004.80000000.00 040000.00000000.sdmp, colorcpl.exe, 0000 000C.00000002.6890151620.000000000715000 0.00000004.00000800.00020000.00000000.sdmp, colorcpl.exe, 0000000C.00000002.6887012764.000 0000005C06000.00000004.10000000.00040000 .00000000.sdmp	false		high
http://www.sandyhillsagritourism.comF20=_ng1lJ	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://schemas.micro	explorer.exe, 0000000A.00000000.31582268 68.000000000AD20000.00000002.00000001.00 040000.00000000.sdmp, explorer.exe, 0000 000A.00000002.6880934450.00000000037F000 0.00000002.00000001.00040000.00000000.sdmp, explorer.exe, 0000000A.00000000.3157646797.000 000000A240000.00000002.00000001.00040000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.37123.vipF20=_ng1lJ	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.cmproutdoors.comF20=_ng1lJ	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.msn.com/en-us/news/politics/white-house-chaos-as-video-shows-joe-biden-aides-stop-report	explorer.exe, 0000000A.00000002.68860578 21.0000000005A37000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.3148668525.0000000005A3700 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://github.com/dotnet/runtime	DHLINV000156.exe, 00000002.00000003.1947 032871.00000000028EA000.00000004.0000002 0.00020000.00000000.sdmp, DHLINV000156.exe, 00000002.00000003.1948493703.0000000 0028E4000.00000004.00000020.00020000.000 00000.sdmp, System.Security.Cryptography.X509Certificates.dll.2.dr, System.dll.2.dr	false		high
http://https://aka.ms/odirm	explorer.exe, 0000000A.00000002.68902234 05.0000000009D46000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.3153873762.0000000009D4600 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.37123.vip	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.cmproutdoors.com/i9th/www.cmproutdoors.com	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	DHLINV000156.exe, 00000008.00000001.2368 782551.00000000005F2000.00000020.0000000 1.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/dotnet-warnings/	DHLINV000156.exe, 00000002.00000003.1947 032871.00000000028EA000.00000004.0000002 0.00020000.00000000.sdmp, System.Security.Cryptography.X509Certificates.dll.2.dr	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	DHLINV000156.exe, 00000002.00000003.1944 530759.00000000028ED000.00000004.0000002 0.00020000.00000000.sdmp, SolutionExplorerCLI.dll.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.dinggubd.net	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.globaltourguide.org/i9th/	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://inference.location.live.net/inferenceservice/v21/ Pox/GetLocationUsingFingerprinte1e71f6b-214	DHLINV000156.exe, 00000008.00000001.2368 782551.0000000000649000.00000020.0000000 1.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.spotcheck.site/i9th/www.spotcheck.site	explorer.exe, 0000000A.00000002.69146479 37.000000000FA97000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.8.203	www.hot6s.com	United States		13335	CLOUDFLARENETUS	true
156.255.170.114	www.cmproutdoors.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
222.122.213.231	daon3999.net	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
34.117.168.233	td-ccm-168-233.wixdns.net	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	true
64.190.63.111	www.riverflow.net	United States		11696	NBS11696US	true
37.59.221.4	nonsolopiercing.com	France		16276	OVHFR	false
3.9.182.46	www.casinoenligne-france.info	United States		16509	AMAZON-02US	true
20.239.65.138	u4tgw7dr.n.funnull35.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
199.192.30.193	www.spotcheck.site	United States		22612	NAMECHEAP-NETUS	true
38.163.2.19	www.dinggubd.net	United States		174	COGENT-174US	true
185.53.177.54	www.verde-amar.info	Germany		61969	TEAMINTERNET-ASDE	true
188.114.96.3	www.hhkk143.cfd	European Union		13335	CLOUDFLARENETUS	true
154.210.212.94	gy.adsfzcvx.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.13.156.177	www.sem-jobs.com	Germany		34788	NMM-ASD-02742FriedersdorfHauptstrasse68DE	true
164.88.122.250	hk.ygrcw.cn	South Africa		137951	CLAYERLIMITED-AS-APClayerLimitedHK	true
81.88.48.71	adasoft.info	Italy		39729	REGISTER-ASIT	true
173.230.227.171	popcors.com	United States		12180	INTERNAP-2BLKUS	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830443
Start date and time:	2023-03-20 11:51:52 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	DHLINV000156.exe
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winEXE@10/11@20/18
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 18% (good quality ratio 17.5%) • Quality average: 83.7% • Quality standard deviation: 24.5%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, audiodg.exe, UserOOBEBroker.exe, RuntimeBroker.exe, ShellExperienceHost.exe, WMIADAP.exe, SIHClient.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, wdcp.microsoft.com, fe3cr.delivery.mp.microsoft.com
- 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 NtEnumerateKey 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 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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Glitteringly\pinckneya\Administrerbarest\Fyringssedlens\Discouple.Lab

Process:	C:\Users\user\Desktop\DHLINV000156.exe
File Type:	data
Category:	dropped
Size (bytes):	257335
Entropy (8bit):	7.2826392494429175
Encrypted:	false
SSDEEP:	6144:oUf41w76GaZg+f3kqYlmWwgN9ST+oR9nNyBCjzDb:Vfcw7Lag8ElRp9wJyk3Db
MD5:	A91E61BC886E6E67E5441F96377A9B0C
SHA1:	4A3D5D529C0328EED76371ED3A36D10684227303
SHA-256:	4DC27F3A2440B1826B4E1BFE993BEE9D647F4789D775B612439F55EC76D55044
SHA-512:	FCDFCBCACD8115866F29D273A6561AE5E015C7F3616D7F7FE09D4865EC1E70B7DD1FF1A4BB9C4123CF0339C846030D8BE0E1F005CE707CB81925639E7C14D(79
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Glitteringly\pinckneya\Administrerbarest\Fyringssedlens\Hny.Com

Process:	C:\Users\user\Desktop\DHLINV000156.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	75512
Entropy (8bit):	2.680395278497968
Encrypted:	false
SSDEEP:	1536:yv2XdmPwwnBCTEHke5XYnaswxUSErZJqXKSDgiumhUocp3:0BPAzp3
MD5:	06284E5EABF1CB10DA1D5C6C6B64EACB
SHA1:	E8430493BC1415193507E442B4596F819BE5256B

SHA-256:	0805F6DC1F08E82F6A7C397C19DC33E63B3EAA770F735829FB3E15EE7B344CE6
SHA-512:	5E918BEB4D036CB1B8F3A5E8DA99771EF8D91580F06E8F03E53EE387E956A78B2A4A67FF0B0C6FAA72B566265D07E4F448DE6186DEF2BB1C57C785CE1DC947BC
Malicious:	false
Preview:	00450000000000000D60000C30000000E00D7D7D7D700DB00004400E5000000000041005D00B7000000EB0000000000000000ED00BCBCBC00000000 9D9D9D0000000000000048006A00222222220000B3B3B3004848000037000019191900000CF00000000A60000EC00666600B3B3B3000009000009004C4C006600004E 000000EAEAEAEA0000CFCFCF003A3A3A3A004848000E00000000009C9C9C00000000757575000F000000000600FF0000C9C90000000000068680000D9 D9D900A8A8A8000000001600 9C000000000000000E9E900009797970032320000D4D40008004B001900DB00BABA00C2000000858500A3000045450000000000001C00 000000D4D4D4000038380000660 0ECECECECECECECEC00EF000000009700320000D0D0000A0A000CB00121200002323000000140000000000000000 0000000000000032000000 8A8A8A000000000410028280065650052000007D7D000000000606000000000E4E4E400AB0000003E00FA000005050000000000006464 64006D000000000000848400005858004000 0A1A1A1000A0000810029292900 9C0000DCDCDCDC002C2C00BCBC00004C000026006D00B7005200A7A7 A7000000AFAFAF000000DB00670000000606007C7C00008400D4D4D4D40000424242008E8E006D6D00C30000F1F1F10000000000B900E2000000000000000008E00

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Glitteringly\pinckneya\Administrerbarest\Fyringssedlens\SolutionExplorerCLI.dll

Process:	C:\Users\user\Desktop\DHLINV000156.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	75248
Entropy (8bit):	6.149004775364808
Encrypted:	false
SSDEEP:	1536:GmY7dQU8l75gS4SqQR27YZW1cwvbTxUd6Rw:GmacliS49QR27YZW1vn2dWw
MD5:	3A03B61FA01DCDFF3E595D279F159D6E
SHA1:	94900C28C23AD01D311C389A0813277CFB30345C
SHA-256:	4F4D6511BEC955B4E8A30371ED743EA5EBC87CEB0BF93FE21F0A378AA2C05A01
SHA-512:	0D04D3486911DFE0439449554E90FB68B4D85EEE025A9B89910C306DE33CBFDBBEF1ABCAC5D4CD3B3CC1B1F445B7C67DC341C9363C9B127810ABD0498EC94AC4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.:.:.:.:.:.:.:.:.].:.:.]..:.:.]..:.:.]..:.:.u..:.:.u.:.:.:.u...:.Rich.:..... ....PE..L...w..U.....!.....:.....dG.....P.....@.....p....@.....<...P.... .....0.....P..8.....R..@.....P.....(Q.. H.....text...!8.....:..... ..`.rdata.....P.....>.....@..@.data.....@....rsrc..... .....@..@.reloc.. ....0.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Styringsmidlernes\Pinkfishes109\Supersensitizations172\Smaskforvirrede\libpkcs11-helper-1.dll

Process:	C:\Users\user\Desktop\DHLINV000156.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	130344
Entropy (8bit):	6.2622011397185
Encrypted:	false
SSDEEP:	3072:tKInqqVjbm+1Vi5R6QQU7k1TAH1OobTrWHEE+jFpCOx:tVzjvi5R6QQU7k1TAH1OobTrWHExFpdx
MD5:	2455841538BA8A502398C18781CC3CEB
SHA1:	86CFD513FEE46EBC2C35225B27372679BE6ADA91
SHA-256:	F37BE7BD8C46D58CA931810536C8A2BEC36D06FF3281740FE0AD177F022AC781
SHA-512:	BC1DCDDE074150616DED7EAACC3FC44BDD2487EB5E550172F5EA46432AA76F19443A9FD6CEF61577B7803C1B083FFCBCEAF9ADC3114A97B547A78C2654F757E3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....&".....".....\d.....P.....z... ..`... .....X....0.....x....@..... ..(.....P.....text...8!.....".....`.P`.data.....@.....&..... .....@.`..rdata...^...P...`...(.....@.`@.pdata.....@.0@.xdata.....@.0@.bss.....`..edata.....@.0@.idata.. X.....@.0..CRT....X.....@.@..tls....h.... .....@.`..rsrc.....0.....@.0..reloc.....@.....@.0B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Styringsmidlernes\Pinkfishes109\Supersensitizations172\Smaskforvirrede\maintenanceservice2.exe

Process:	C:\Users\user\Desktop\DHLINV000156.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	227256

Entropy (8bit):	6.388677533277947
Encrypted:	false
SSDEEP:	6144:ue/rKQgYva3o4vj272BNvlJuQlf2qIHL2:uYrK4a3PvKw7ufg2
MD5:	49A2E97304EF8E044EEBD7ACCAD37E11
SHA1:	7D0F26591C8BD4CAB1718E323B65706CBEA5DE7A
SHA-256:	83EAFBF165642C563CD468D12BC85E3A9BAEDE084E5B18F99466E071149FD15F
SHA-512:	AC206C5EF6F373A0005902D09110A95A7F5FB4F524653D30C3A65182717272FE244694A6698D40884BEA243B2CA00D7741CED796DF7AE8C633F513B8C6FCD6C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...J..b....."....:.....@.....Y.....`..... .....`..h....X.....(....P.....(...h.....text....9.....:..... ..`.rdata.....P.....>..... @..@.data....!...0.....@....pdata..h....`.....*.....@..@.00cfg.....D.....@..@.tls.....F.....@....rsrc.....H.....@..@.reloc..... .....P.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Styringsmidlernes\Pinkfishes109\Supersensitizations172\Smaskforvirr ede\percentile.dll

Process:	C:\Users\user\Desktop\DHLINV000156.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	102577
Entropy (8bit):	5.075179901575448
Encrypted:	false
SSDEEP:	768:t9H5uXFjJeEoPsznZgkZNhFdS2E0fVnSdNPfZ5+uKIu7aQzTgp37CtHRMX6NX0:tJ5wJeEoU9g0Nhav09nahfYxDRx0
MD5:	3144FDFEC817D0AC6FE3F4642B70328B
SHA1:	756C3513DC10CF00B517C72B2D3AB3E20895A46C
SHA-256:	BF17F5B38DCF35B55B1E0FAD462D4095ABAAA4CD8F1EDBDC8657C0249EF5D4D3
SHA-512:	012D9A3B88BA5D5090E8B47B49FE50E518489AB05FAAC6A1A0743F29A369B7D67F39B8E113B34740607137F2D67D75116DBE2A76E8E1DBE699BA4973F8037684
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...rL.`.<.....& ...$.....6.....P.....U.. ..`... .....Y.....P.....`.....A..(.....text.....`.P`.data...p....0..... .....@. P..rdata..p....@.....".....@.`@.pdata.....P.....*.....@.0@.xdata..I...`.....@.0@.bss.....p.....`..edata..Y.....0.....@.0@.idata.. .....2.....@.0..CRT....X.....6.....@.@..tls.....8.....@.@..reloc..`.....:.....@.0B/4.....<.....@.PB/19.....C.....@..... .....@..B/31.....`.....@..B/45..... .....@..B/57.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Supergallantness\afstres\Archives\Sadelmagernaalenes\System.Securit y.Cryptography.X509Certificates.dll

Process:	C:\Users\user\Desktop\DHLINV000156.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	485488
Entropy (8bit):	6.710350474742332
Encrypted:	false
SSDEEP:	6144:1E5AW+0VyAaOKxFf8r6S2rGjF0KAmdHCKsCZcufvh7OzxQxQ5JVIRVrk:KGWlaOKC2a0tmFChCOFeqLIRpk
MD5:	84D7B1FB924AEEFCF4A2C7A687FE2EF1
SHA1:	A2C2C7DE9096328A3FEF0C7FCEA262A294C0807B
SHA-256:	32A54C24B18B3C087E06F4F19885FB410304AB4AF2263154020D3F5CDCE36D99
SHA-512:	E75F91DA415B15CA0B19519179021FD88C0FC68FE4EF2A68B899B121BD511C04AECCB58101318C86CB0458D7310208C358DBB9155A02D62DE73C04128ECC59
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....fW....." .....`..... ..`...@.....@..... .....1...D..p$...P.....0..T.....H.....text..... ..`.data...wy.....z..... .....@....reloc.....P.....:.....@..B.....0.....T.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F.i .l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0.....d...C.o.m.m.e.n.t.s...I.n.t.e.r.n.a.l. .i.m.p.l.e.m.e.n.t.a.t.i.o.n. .p.a.c.k.a.g.e. .n.o.t. .m .e.a.n.t. .f.o.r. .d.i.r.e.c.t. .c.o.n.s.u.m.p.t.i.o.n... .P.l.e.a.s.e. .d.o. .n.o.t. .r.e.f.e.r.e.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\internuptial\Smertelig\Registrer\System.dll

Process:	C:\Users\user\Desktop\DHLINV000156.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	49768

Entropy (8bit):	5.650496280667822
Encrypted:	false
SSDEEP:	768:4vuoy1c6A2ZX8TRNH5JVbOd502zq1TntV5fljM:4vuoO3ZX8Q5jzC35NjM
MD5:	BCC32F5B608C99F89508921B6333B329
SHA1:	5F70BB4A3A812C399D8D2A2954C9A715574CFF61
SHA-256:	5D4FF9A8E3B3CA26F53CD2CC4C557C5F2074A431B9CD029AE7F7A7B8902FA3C1
SHA-512:	99C7623BCA873C75A3B804C815DF178ACC88E043A36473C785216CD26DC73F0525FE336F17F0F2C8CA6473FBD407A953D4650D093C52440D93ECF07C1440FAE
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\internuptial\Smertelig\Registrer\System.dll, Author: Joe Security
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....." ..0..... ....`.....O.....h$.....T..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....P .....`.....BSJB.....v4.0.30319.....l...$;..#~...;...R..#Strings....4.....#US.8.....#GUID...H..... #Blob.....T.....3...../.....=.....=....J=...=.....V...}.....h.. ....J.. ....1.. ..j.. .., AF..a.AF.....R..e..=.....;....;....;..)..;..1..;..9..; ..A..;..I..;..Q..;..Y..;..a..;..i..;..q..;..y..;....; ....;....;..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\internuptial\Smertelig\Registrer\libdatrie-1.dll

Process:	C:\Users\user\Desktop\DHLINV000156.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	36029
Entropy (8bit):	5.699900454607003
Encrypted:	false
SSDEEP:	768:Hm5z53y6m/LHlM6GnPGUvMrsztd/sLLhF3VI:a53y6Gy6GuU5d/OhF3G
MD5:	8A54723090530190EB11AFCD5B702B1B
SHA1:	DFA923EC796A754BD21C4F9E504305848A4CB1B2
SHA-256:	738F67F45FAA07CC387BAF390604EE4CE709CBE7C223D9A043EE06F7CB360D5B
SHA-512:	E0D310458C8259112E07B153EDC86FDFF29E1B09648FED8D163D44DEB3BEE1545E7AD37BB00E9255DF6514844B21A829750848DA42F85FA77BEF376CE09750CF
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....<.....&".....R.....0.....h.....^.. ....`.....(.....text...HP.....R.....`.P`.data.....p.....V.....@. P..rdata.....X.....@.`@.pdata.....b.....@.0@.xdata.....j.....@.0@.bss.... .....`..edata.....r.....@.0@.idata..... ...v.....@.0..CRT....X.....~.....@.@..tls.....@.@..reloc..`.....@.0B..... .....

C:\Users\user\AppData\Local\Temp\AeL-0b1QRQ

Process:	C:\Windows\SysWOW64\colorcpl.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 5, database pages 59, cookie 0x4f, schema 4, UTF-8, version-valid-for 5
Category:	dropped
Size (bytes):	122880
Entropy (8bit):	1.1305327154874678
Encrypted:	false
SSDEEP:	192:oLt4nKTjebGAUJp/XH9euJDvphC+KRmquPWSTVumQ6:it4nsJp/39RDhw+KRmqu+cVumQ
MD5:	D331C900DDE8ACB523C51D9448205C0A
SHA1:	BDB3366F54876E78F76A6244EDA7A4C302FEB91D
SHA-256:	F199798DF1C37E3A8F6FFF1E208F083CF687F5C6A220DCAD42BB68F2120181CD
SHA-512:	415E4F4F26D4F861063676EA786C2941DB8DB7E248E32D84595BC7D531CE19669AFDCB447BC18B0B723839984CD15269FF6E89EBCD168D8EBD0EC7AF86CC92E7
Malicious:	false
Preview:	SQLite format 3.....@ .....;.....O.....O}.....5..... ....

C:\Users\user\AppData\Local\Temp\nsxCFC.tmp\System.dll

Process:	C:\Users\user\Desktop\DHLINV000156.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.854901984552606

Encrypted:	false
SSDEEP:	192:qPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4U:F7VpNo8gmOyRsVc4
MD5:	0063D48AFE5A0CDC02833145667B6641
SHA1:	E7EB614805D183ECB1127C62DECB1A6BE1B4F7A8
SHA-256:	AC9DFE3B35EA4B8932536ED7406C29A432976B685CC5322F94EF93DF920FEDE7
SHA-512:	71CBBCAEB345E09306E368717EA0503FE8DF485BE2E95200FEBC61BCD8BA74FB4211CD263C232F148C0123F6C6F2E3FD4EA20BDECC4070F5208C35C6920240F0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....]..... .....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.597743551355423
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	DHLINV000156.exe
File size:	800224
MD5:	4cef4c9b4785b2bc5adcbf1c91185ab9
SHA1:	5e00a720edff53c27a6ee5fe4606a42cc2ab3a02
SHA256:	0a83a6c897b43357c341190cc93e0310cc8063f4e569853aba1c912ede95229f
SHA512:	efae339a37af259aa445015dd022beaec68fab00170615beccbed38af7bbc7bfbf874daa5f1426c85fb2856900f266141485cb2dd84108e074c9716686a59ca7
SSDEEP:	12288:myiYQS2zqcAMFVJV6xYaU/XnKcZnY4UKwp7hVOZCbgjvwr:ZiYG/FVD6WHicUNEZCbgjG
TLSH:	19051297A2618296FDE74BB0193B8D2902777E7A7DB2C54F26A577B21FB32C20017407
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... (...F...F...F.*.....F...G.w.F.*.....F...v...F...@...F.Rich..F.....PE..L.....]..... .....`.....52.....p....@

File Icon

Icon Hash:	4501012101010100

Static PE Info

General

Entrypoint:	0x403235
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x5DF6D4E3 [Mon Dec 16 00:50:43 2019 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:	e9c0657252137ac61c1eeeba4c021000

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	E=Disambiguations@acropora.Gav, OU="Underprioriteres Interessekonflikter ", O=Nontrigonometrical, L=Mahaffey, S=Pennsylvania, C=US
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 06/02/2023 08:11:54 05/02/2026 08:11:54
Subject Chain	• E=Disambiguations@acropora.Gav, OU="Underprioriteres Interessekonflikter ", O=Nontrigonometrical, L=Mahaffey, S=Pennsylvania, C=US
Version:	3
Thumbprint MD5:	7AA203D6AB689907A6C41BAEE5BDC189
Thumbprint SHA-1:	4DDF250E49818DE396B187AD3A3F34130F0E4D5A
Thumbprint SHA-256:	B577E1E8F47010ED802D38B4B8E5E3E1CE2B6005A883A5BB8D225D3AD933F1AC
Serial:	4E44313213E3991CC4F5945A8D82C0D78DD7307E

Entrypoint Preview
Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004070A0h]
call dword ptr [0040709Ch]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042370Ch], eax
je 00007F9D2CDCAB53h
push ebx
call 00007F9D2CDCDC3Bh
cmp eax, ebx
je 00007F9D2CDCAB49h
push 00000C00h
call eax
mov esi, 00407298h
push esi
call 00007F9D2CDCDBB7h
push esi
call dword ptr [00407098h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F9D2CDCAB2Dh
push 0000000Ah
call 00007F9D2CDCDC0Fh
push 00000008h
call 00007F9D2CDCDC08h
push 00000006h
mov dword ptr [00423704h], eax
call 00007F9D2CDCDBFCh
cmp eax, ebx
je 00007F9D2CDCAB51h
push 0000001Eh
call eax
test eax, eax
je 00007F9D2CDCAB49h
or byte ptr [0042370Fh], 00000040h

Instruction
push ebp
call dword ptr [00407040h]
push ebx
call dword ptr [00407284h]
mov dword ptr [004237D8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041ECC8h
call dword ptr [00407178h]
push 00409188h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7430	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x36000	0x1e3f8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xc1330	0x22b0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x7000	0x294	.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	0x5f7d	0x6000	False	0.6680094401041666	data	6.466064816043304	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x123e	0x1400	False	0.4275390625	data	4.989734782278587	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1a818	0x400	False	0.638671875	data	5.130817636118804	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x24000	0x12000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x36000	0x1e3f8	0x1e400	False	0.26598011363636365	data	3.27208167704045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x362f8	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536, resolution 5905 x 5905 px/m	English	United States
RT_ICON	0x46b20	0x537d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4bea0	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384, resolution 5905 x 5905 px/m	English	United States
RT_ICON	0x500c8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216, resolution 5905 x 5905 px/m	English	United States
RT_ICON	0x52670	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096, resolution 5905 x 5905 px/m	English	United States
RT_ICON	0x53718	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024, resolution 5905 x 5905 px/m	English	United States
RT_DIALOG	0x53b80	0x100	data	English	United States
RT_DIALOG	0x53c80	0x11c	data	English	United States
RT_DIALOG	0x53da0	0xc4	data	English	United States
RT_DIALOG	0x53e68	0x60	data	English	United States
RT_GROUP_ICON	0x53ec8	0x5a	data	English	United States
RT_VERSION	0x53f28	0x190	data	English	United States
RT_MANIFEST	0x540b8	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

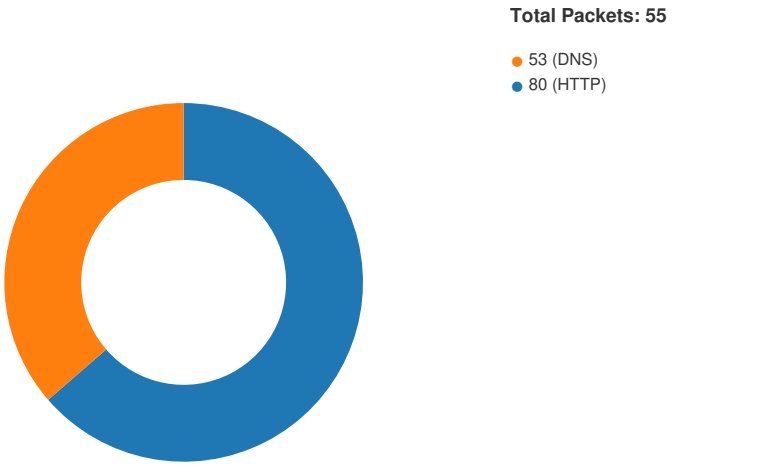
DLL	Import
KERNEL32.dll	GetTempPathA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetEnvironmentVariableA, Sleep, GetTickCount, GetCommandLineA, lstrlenA, GetVersion, SetErrorMode, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GetWindowsDirectoryA, SetFileAttributesA, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, ReadFile, WriteFile, lstrcpyA, MoveFileExA, lstrcatA, GetSystemDirectoryA, GetProcAddress, GetExitCodeProcess, WaitForSingleObject, CompareFileTime, SetFileTime, GetFileAttributesA, SetCurrentDirectoryA, MoveFileA, GetFullPathNameA, GetShortPathNameA, SearchPathA, CloseHandle, lstrcmpiA, CreateThread, GlobalLock, lstrcmpA, DeleteFileA, FindFirstFileA, FindNextFileA, FindClose, SetFilePointer, GetPrivateProfileStringA, WritePrivateProfileStringA, MulDiv, MultiByteToWideChar, FreeLibrary, LoadLibraryExA, GetModuleHandleA, GlobalAlloc, GlobalFree, ExpandEnvironmentStringsA
USER32.dll	GetSystemMenu, SetClassLongA, EnableMenuItem, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, ScreenToClient, GetWindowRect, GetDlgItem, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, EndDialog, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, LoadImageA, CreateDialogParamA, SetTimer, SetWindowTextA, SetForegroundWindow, ShowWindow, SetWindowLongA, SendMessageTimeoutA, FindWindowExA, IsWindow, AppendMenuA, TrackPopupMenu, CreatePopupMenu, DrawTextA, EndPaint, DestroyWindow, wsprintfA, PostQuitMessage
GDI32.dll	SelectObject, SetTextColor, SetBkMode, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, GetDeviceCaps, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExA, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, SHFileOperationA
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExA, RegOpenKeyExA, SetFileSecurityA, OpenProcessToken, LookupPrivilegeValueA, RegEnumValueA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:54:48.264178038 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.286770105 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.287147999 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.287543058 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.308059931 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.310060024 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.310151100 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.310216904 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.310281038 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.310328960 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.310329914 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.310343027 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.310409069 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.310410023 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.310473919 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.310532093 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.310538054 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.310533047 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.310601950 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.310602903 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.310671091 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.310714960 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.310714960 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.310899973 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.331321001 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.331412077 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.331963062 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.331963062 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.332298994 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.332432032 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.332498074 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.332559109 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.332602024 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.332602978 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.332622051 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.332680941 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.332684994 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.332747936 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.332792997 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.332792997 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.332809925 CET	80	49823	37.59.221.4	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:54:48.332863092 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.332873106 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.332936049 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.332971096 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.333002090 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.333065033 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.333138943 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.333199024 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.333316088 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.353630066 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.353718996 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.353779078 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.353836060 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.353893042 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.353949070 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354002953 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354043961 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.354060888 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354115009 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.354116917 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354172945 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354228973 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354284048 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354338884 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354393005 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354448080 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354502916 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354507923 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.354557991 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354613066 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354666948 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354677916 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.354722977 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354779005 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354834080 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354888916 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.354944944 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.355036020 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.355175972 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.376204967 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.376279116 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.376400948 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.376461029 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.376486063 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.376517057 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.376571894 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.376626968 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.376682043 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.376737118 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.376794100 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.376827002 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.376851082 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.376877069 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.376907110 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.376961946 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.377008915 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.377008915 CET	49823	80	192.168.11.20	37.59.221.4
Mar 20, 2023 11:54:48.377017021 CET	80	49823	37.59.221.4	192.168.11.20
Mar 20, 2023 11:54:48.377073050 CET	80	49823	37.59.221.4	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:54:48.232134104 CET	60124	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:54:48.259109974 CET	53	60124	1.1.1.1	192.168.11.20
Mar 20, 2023 11:56:18.481327057 CET	61205	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:56:18.681103945 CET	53	61205	1.1.1.1	192.168.11.20
Mar 20, 2023 11:56:33.820898056 CET	56676	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:56:33.872941971 CET	53	56676	1.1.1.1	192.168.11.20
Mar 20, 2023 11:56:46.959852934 CET	55519	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:56:46.994508028 CET	53	55519	1.1.1.1	192.168.11.20
Mar 20, 2023 11:56:59.956497908 CET	49708	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:57:00.713232994 CET	53	49708	1.1.1.1	192.168.11.20
Mar 20, 2023 11:57:14.389786959 CET	62343	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:57:14.457936049 CET	53	62343	1.1.1.1	192.168.11.20
Mar 20, 2023 11:57:27.293910027 CET	52082	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:57:27.315874100 CET	53	52082	1.1.1.1	192.168.11.20
Mar 20, 2023 11:57:39.963136911 CET	59432	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:57:40.315663099 CET	53	59432	1.1.1.1	192.168.11.20
Mar 20, 2023 11:57:53.506364107 CET	52181	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:57:53.526247025 CET	53	52181	1.1.1.1	192.168.11.20
Mar 20, 2023 11:58:07.019270897 CET	57800	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:58:07.343427896 CET	53	57800	1.1.1.1	192.168.11.20
Mar 20, 2023 11:58:21.515594006 CET	52585	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:58:21.531311035 CET	53	52585	1.1.1.1	192.168.11.20
Mar 20, 2023 11:58:35.215946913 CET	63093	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:58:36.231028080 CET	63093	53	192.168.11.20	9.9.9.9
Mar 20, 2023 11:58:36.377612114 CET	53	63093	1.1.1.1	192.168.11.20
Mar 20, 2023 11:58:36.969326973 CET	53	63093	9.9.9.9	192.168.11.20
Mar 20, 2023 11:58:50.274959087 CET	52457	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:58:50.445172071 CET	53	52457	1.1.1.1	192.168.11.20
Mar 20, 2023 11:59:03.993531942 CET	53320	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:59:05.005743027 CET	53320	53	192.168.11.20	9.9.9.9
Mar 20, 2023 11:59:05.512342930 CET	53	53320	1.1.1.1	192.168.11.20
Mar 20, 2023 11:59:05.816593885 CET	53	53320	9.9.9.9	192.168.11.20
Mar 20, 2023 11:59:19.362520933 CET	50719	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:59:19.809180021 CET	53	50719	1.1.1.1	192.168.11.20
Mar 20, 2023 11:59:33.562340021 CET	65422	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:59:33.684478998 CET	53	65422	1.1.1.1	192.168.11.20
Mar 20, 2023 11:59:46.340909958 CET	57010	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:59:46.370095015 CET	53	57010	1.1.1.1	192.168.11.20
Mar 20, 2023 12:02:05.421128035 CET	53661	53	192.168.11.20	1.1.1.1
Mar 20, 2023 12:02:05.717917919 CET	53	53661	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 11:54:48.232134104 CET	192.168.11.20	1.1.1.1	0x9978	Standard query (0)	nonsolopiercing.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:56:18.481327057 CET	192.168.11.20	1.1.1.1	0xbbc	Standard query (0)	www.sandyhillsagritourism.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:56:33.820898056 CET	192.168.11.20	1.1.1.1	0x6463	Standard query (0)	www.sem-jobs.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:56:46.959852934 CET	192.168.11.20	1.1.1.1	0x5ffa	Standard query (0)	www.casinoenligne-france.info	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:56:59.956497908 CET	192.168.11.20	1.1.1.1	0xd479	Standard query (0)	www.37123.vip	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:14.389786959 CET	192.168.11.20	1.1.1.1	0xc445	Standard query (0)	www.adasoft.info	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:27.293910027 CET	192.168.11.20	1.1.1.1	0xccf9	Standard query (0)	www.hhkk143.cfd	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 11:57:39.963136911 CET	192.168.11.20	1.1.1.1	0x2485	Standard query (0)	www.popcors.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:53.506364107 CET	192.168.11.20	1.1.1.1	0xad88	Standard query (0)	www.spotcheck.site	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:58:07.019270897 CET	192.168.11.20	1.1.1.1	0xbc56	Standard query (0)	www.dinggubd.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:58:21.515594006 CET	192.168.11.20	1.1.1.1	0x6fcd	Standard query (0)	www.hot6s.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:58:35.215946913 CET	192.168.11.20	1.1.1.1	0x95b4	Standard query (0)	www.0w3jy.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:58:36.231028080 CET	192.168.11.20	9.9.9.9	0x95b4	Standard query (0)	www.0w3jy.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:58:50.274959087 CET	192.168.11.20	1.1.1.1	0x14ed	Standard query (0)	www.cmproutdoors.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:59:03.993531942 CET	192.168.11.20	1.1.1.1	0xe44	Standard query (0)	www.daon3999.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:59:05.005743027 CET	192.168.11.20	9.9.9.9	0xe44	Standard query (0)	www.daon3999.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:59:19.362520933 CET	192.168.11.20	1.1.1.1	0xec5c	Standard query (0)	www.5319ss.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:59:33.562340021 CET	192.168.11.20	1.1.1.1	0xeae	Standard query (0)	www.riverflow.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:59:46.340909958 CET	192.168.11.20	1.1.1.1	0xf373	Standard query (0)	www.verde-amar.info	A (IP address)	IN (0x0001)	false
Mar 20, 2023 12:02:05.421128035 CET	192.168.11.20	1.1.1.1	0xee47	Standard query (0)	www.yeah-go.com	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
Mar 20, 2023 11:54:48.259109974 CET	1.1.1.1	192.168.11.20	0x9978	No error (0)	nonsolopiercing.com		37.59.221.4	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:56:18.681103945 CET	1.1.1.1	192.168.11.20	0xbbc	No error (0)	www.sandyhillsagritourism.com	gcdn0.wixdns.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:56:18.681103945 CET	1.1.1.1	192.168.11.20	0xbbc	No error (0)	gcdn0.wixdns.net	td-ccm-168-233.wixdns.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:56:18.681103945 CET	1.1.1.1	192.168.11.20	0xbbc	No error (0)	td-ccm-168-233.wixdns.net		34.117.168.233	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:56:33.872941971 CET	1.1.1.1	192.168.11.20	0x6463	No error (0)	www.sem-jobs.com		85.13.156.177	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:56:46.994508028 CET	1.1.1.1	192.168.11.20	0x5ffa	No error (0)	www.casinoenligne-france.info		3.9.182.46	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:00.713232994 CET	1.1.1.1	192.168.11.20	0xd479	No error (0)	www.37123.vip	ehbw3ftr-u.funnull01.vip		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:57:00.713232994 CET	1.1.1.1	192.168.11.20	0xd479	No error (0)	ehbw3ftr-u.funnull01.vip	u4tgw7dr.n.funnull35.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:57:00.713232994 CET	1.1.1.1	192.168.11.20	0xd479	No error (0)	u4tgw7dr.n.funnull35.com		20.239.65.138	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:00.713232994 CET	1.1.1.1	192.168.11.20	0xd479	No error (0)	u4tgw7dr.n.funnull35.com		103.20.61.207	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:00.713232994 CET	1.1.1.1	192.168.11.20	0xd479	No error (0)	u4tgw7dr.n.funnull35.com		103.20.61.209	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:00.713232994 CET	1.1.1.1	192.168.11.20	0xd479	No error (0)	u4tgw7dr.n.funnull35.com		103.20.61.210	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:00.713232994 CET	1.1.1.1	192.168.11.20	0xd479	No error (0)	u4tgw7dr.n.funnull35.com		20.24.81.22	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:00.713232994 CET	1.1.1.1	192.168.11.20	0xd479	No error (0)	u4tgw7dr.n.funnull35.com		20.239.64.71	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 11:57:00.713232994 CET	1.1.1.1	192.168.11.20	0xd479	No error (0)	u4tgw7dr.n.funnull35.com		20.239.64.84	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:14.457936049 CET	1.1.1.1	192.168.11.20	0xc445	No error (0)	www.adasoft.info	adasoft.info		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:57:14.457936049 CET	1.1.1.1	192.168.11.20	0xc445	No error (0)	adasoft.info		81.88.48.71	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:27.315874100 CET	1.1.1.1	192.168.11.20	0xccf9	No error (0)	www.hhkk143.cfd		188.114.96.3	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:27.315874100 CET	1.1.1.1	192.168.11.20	0xccf9	No error (0)	www.hhkk143.cfd		188.114.97.3	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:40.315663099 CET	1.1.1.1	192.168.11.20	0x2485	No error (0)	www.popcors.com	popcors.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:57:40.315663099 CET	1.1.1.1	192.168.11.20	0x2485	No error (0)	popcors.com		173.230.227.171	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:57:53.526247025 CET	1.1.1.1	192.168.11.20	0xad88	No error (0)	www.spotcheck.site		199.192.30.193	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:58:07.343427896 CET	1.1.1.1	192.168.11.20	0xbc56	No error (0)	www.dingqubd.net		38.163.2.19	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:58:21.531311035 CET	1.1.1.1	192.168.11.20	0x6fcd	No error (0)	www.hot6s.com		104.21.8.203	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:58:21.531311035 CET	1.1.1.1	192.168.11.20	0x6fcd	No error (0)	www.hot6s.com		172.67.157.215	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:58:36.377612114 CET	1.1.1.1	192.168.11.20	0x95b4	No error (0)	www.0w3jy.com	hk.ygrcw.cn		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:58:36.377612114 CET	1.1.1.1	192.168.11.20	0x95b4	No error (0)	hk.ygrcw.cn		164.88.122.250	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:58:36.969326973 CET	9.9.9.9	192.168.11.20	0x95b4	No error (0)	www.0w3jy.com	hk.ygrcw.cn		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:58:36.969326973 CET	9.9.9.9	192.168.11.20	0x95b4	No error (0)	hk.ygrcw.cn		164.88.122.250	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:58:50.445172071 CET	1.1.1.1	192.168.11.20	0x14ed	No error (0)	www.cmproutdoors.com		156.255.170.114	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:59:05.512342930 CET	1.1.1.1	192.168.11.20	0xe44	No error (0)	www.daon3999.net	daon3999.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:59:05.512342930 CET	1.1.1.1	192.168.11.20	0xe44	No error (0)	daon3999.net		222.122.213.231	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:59:05.816593885 CET	9.9.9.9	192.168.11.20	0xe44	No error (0)	www.daon3999.net	daon3999.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:59:05.816593885 CET	9.9.9.9	192.168.11.20	0xe44	No error (0)	daon3999.net		222.122.213.231	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:59:19.809180021 CET	1.1.1.1	192.168.11.20	0xec5c	No error (0)	www.5319ss.com	gy.adsfzcvx.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:59:19.809180021 CET	1.1.1.1	192.168.11.20	0xec5c	No error (0)	gy.adsfzcvx.com		154.210.212.94	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:59:33.684478998 CET	1.1.1.1	192.168.11.20	0xeae	No error (0)	www.riverflow.net		64.190.63.111	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:59:46.370095015 CET	1.1.1.1	192.168.11.20	0xf373	No error (0)	www.verde-amar.info		185.53.177.54	A (IP address)	IN (0x0001)	false
Mar 20, 2023 12:02:05.717917919 CET	1.1.1.1	192.168.11.20	0xee47	No error (0)	www.yeah-go.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 12:02:05.717917919 CET	1.1.1.1	192.168.11.20	0xee47	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)	false

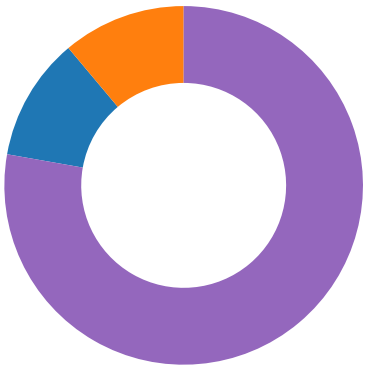
HTTP Request Dependency Graph

- nonsolopiercing.com
- www.sandyhillsagritourism.com
- www.sem-jobs.com
- www.casinoenligne-france.info
- www.37123.vip
- www.adasoft.info
- www.hhkk143.cfd
- www.popcors.com
- www.spotcheck.site
- www.dinggubd.net
- www.hot6s.com
- www.0w3jy.com
- www.cmproutdoors.com
- www.daon3999.net
- www.5319ss.com
- www.riverflow.net
- www.verde-amar.info
- www.yeah-go.com

Statistics

Behavior

- DHLINV000156.exe
- DHLINV000156.exe
- explorer.exe
- autoconv.exe
- colorcpl.exe
- firefox.exe



Click to jump to process

System Behavior

Analysis Process: DHLINV000156.exe PID: 9100, Parent PID: 4592

General

Target ID:	2
Start time:	11:53:46
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\DHLINV000156.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHLINV000156.exe
Imagebase:	0x400000
File size:	800224 bytes
MD5 hash:	4CEF4C9B4785B2BC5ADCBF1C91185AB9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.2465676378.000000000505A000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: DHLINV000156.exe PID: 7624, Parent PID: 9100

General

Target ID:	8
Start time:	11:54:40
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\DHLINV000156.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHLINV000156.exe
Imagebase:	0x400000
File size:	800224 bytes

MD5 hash:	4CEF4C9B4785B2BC5ADCBF1C91185AB9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.3226190234.0000000000090000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.3226190234.0000000000090000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.3226190234.0000000000090000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.3225862883.0000000000060000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.3225862883.0000000000060000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.3225862883.0000000000060000.00000040.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1696752	success or wait	1	41E68A	NtReadFile

Analysis Process: explorer.exe PID: **4592**, Parent PID: **7624**

General

Target ID:	10
Start time:	11:55:58
Start date:	20/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff7ac7d0000
File size:	4849904 bytes
MD5 hash:	5EA66FF5AE5612F921BC9DA23BAC95F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: autoconv.exe PID: **7192**, Parent PID: **4592**

General

Target ID:	11
Start time:	11:56:03
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x2a0000
File size:	851968 bytes
MD5 hash:	469594005E3B94C5945BCCE7FC521C05
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: colorcpl.exe PID: **8804**, Parent PID: **4592**

General

Target ID:	12
Start time:	11:56:03
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\colorcpl.exe
Imagebase:	0x60000
File size:	86528 bytes
MD5 hash:	DB71E132EBF1FEB6E93E8A2A0F0C903D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 0000000C.00000002.6881079830.00000000046C0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.6881079830.00000000046C0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000C.00000002.6881079830.00000000046C0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 0000000C.00000002.6880751145.0000000004690000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.6880751145.0000000004690000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000C.00000002.6880751145.0000000004690000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 0000000C.00000002.6874962433.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.6874962433.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000C.00000002.6874962433.00000000028B0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DHLINV000156.exe	cannot delete	1	28CC947	NtDeleteFile
C:\Users\user\AppData\Local\Temp\AeL-0b1QRQ	object name not found	1	28CC947	NtDeleteFile
C:\Users\user\AppData\Local\Temp\AeL-0b1QRQ	sharing violation	1	28CC947	NtDeleteFile

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AeL-0b1QRQ	sharing violation	1	28CC947	NtDeleteFile
C:\Users\user\AppData\Local\Temp\AeL-0b1QRQ	sharing violation	1	28CC947	NtDeleteFile
C:\Users\user\AppData\Local\Temp\AeL-0b1QRQ	sharing violation	1	28CC947	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1696752	success or wait	1	28CC917	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: firefox.exe PID: **1820**, Parent PID: **8804**

General

Target ID:	13
Start time:	11:56:24
Start date:	20/03/2023
Path:	C:\Program Files\Mozilla Firefox\firefox.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Mozilla Firefox\Firefox.exe
Imagebase:	0x7ff71d500000
File size:	597432 bytes
MD5 hash:	FA9F4FC5D7ECAB5A20BF7A9D1251C851
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

No disassembly