ID: 829130
Sample Name:
DHLIN00178.exe
Cookbook: default.jbs
Time: 21:33:08
Date: 17/03/2023
Version: 37.0.0 Beryl

Table of Contents

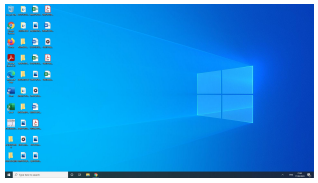
Windows Analysis Report

DHLIN00178.exe

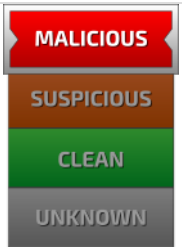
Overview

General Information

Sample Name:	DHLIN00178.exe
Analysis ID:	829130
MD5:	66fdf2df4fc860…
SHA1:	88031f2f9bfbf3…
SHA256:	e07a149d14fc3..
Infos:	



Detection



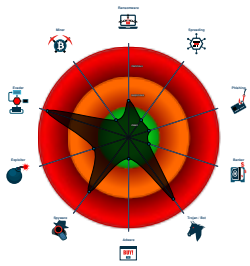
FormBook, GuLoader

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**
- DHLIN00178.exe (PID: 3876 cmdline: C:\Users\user\Desktop\DHLIN00178.exe MD5: 66FDF2DF4FC8601124DF76C284F797E1)
  - DHLIN00178.exe (PID: 1776 cmdline: C:\Users\user\Desktop\DHLIN00178.exe MD5: 66FDF2DF4FC8601124DF76C284F797E1)
    - explorer.exe (PID: 4760 cmdline: C:\Windows\Explorer.EXE MD5: 5EA66FF5AE5612F921BC9DA23BAC95F7)
      - cscript.exe (PID: 1912 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 13783FF4A2B614D7FBD58F5EEBDEDEF6)
        - firefox.exe (PID: 5256 cmdline: C:\Program Files\Mozilla Firefox\Firefox.exe MD5: FA9F4FC5D7ECAB5A20BF7A9D1251C851)
          - WerFault.exe (PID: 2884 cmdline: C:\Windows\system32\WerFault.exe -u -p 5256 -s 284 MD5: 5C06542FED8EE68994D43938E7326D75)
- **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\INetCache\Ghetto\Pointberegningernes241\Chaiselongs\Whatchamacallits76\querciflorae\System.dll	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.9611657134.0000000000600000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000008.00000002.9611657134.0000000000600000.00000040.80000000.00040000.00000000.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
00000008.00000002.9611657134.0000000000600000.00000040.80000000.00040000.00000000.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:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000005.00000002.7003744896.0000000000090000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000005.00000002.7003744896.0000000000090000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x180f5:$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

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)

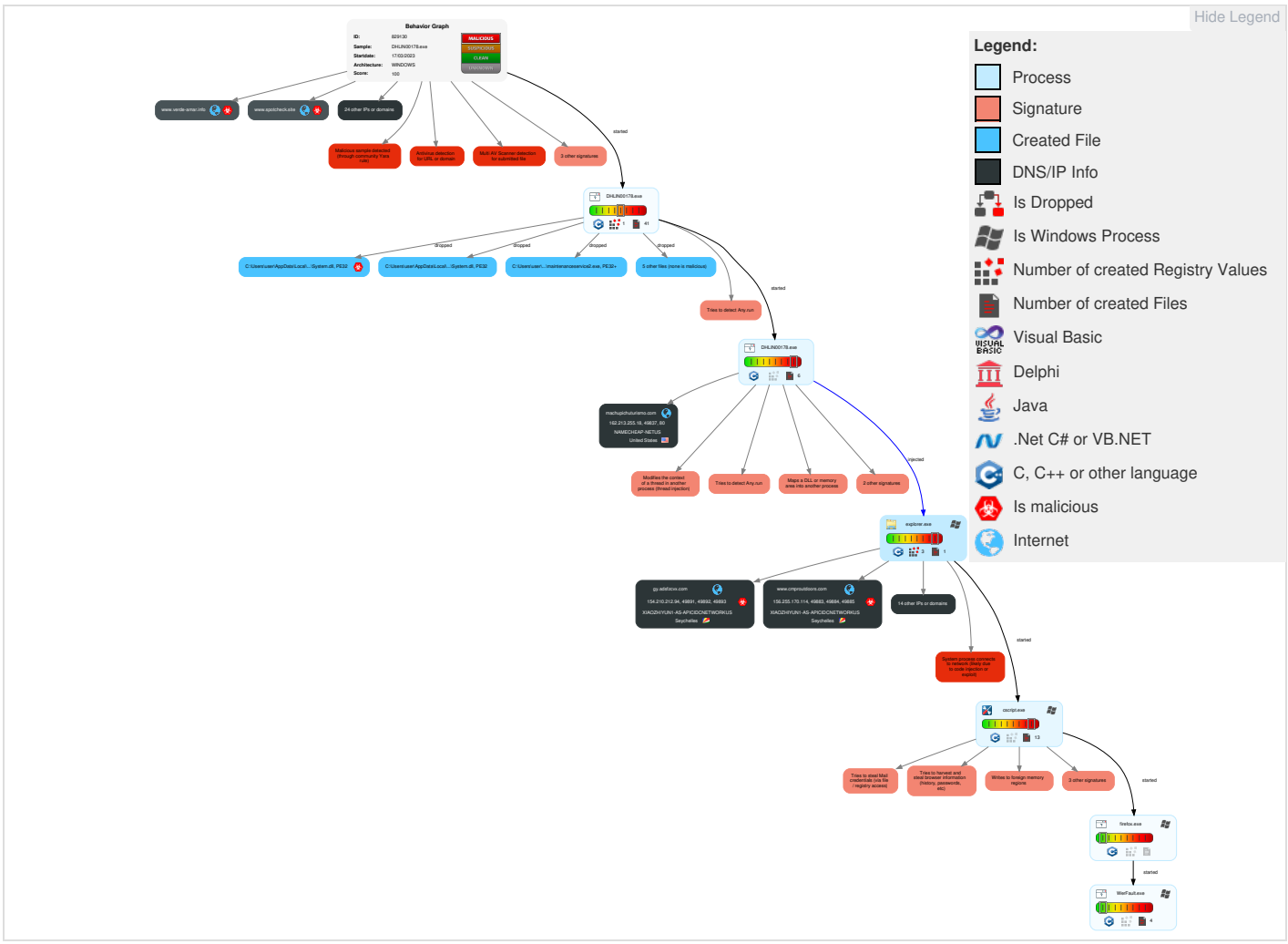
Remote Access Functionality

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 Shared Modules	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	4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Access Token Manipulation	3 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 1 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	1 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 1 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

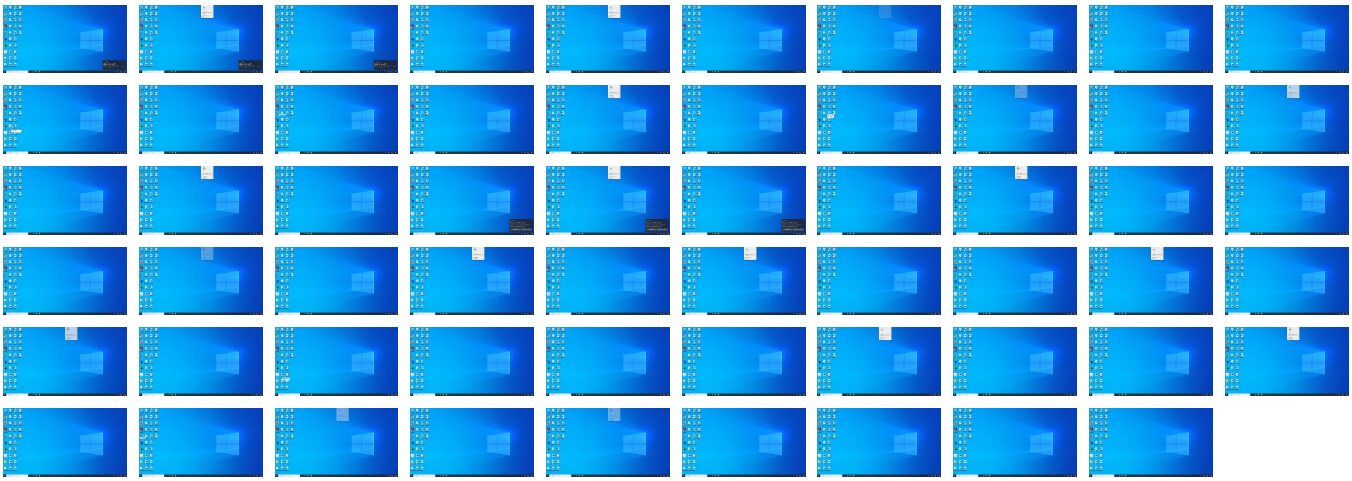
Behavior Graph



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
DHLIN00178.exe	8%	ReversingLabs	Win32.Trojan.Generic	
DHLIN00178.exe	12%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Maattet\SolutionExplorerCLI.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Maattet\System.Security.Cryptography.X509Certificates.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Mandslinien\Characterizable\Senilitetstegnet\percentile.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Pointberegningernes241\Chaiselongs\Whatchamacallits76\querciflorae\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Pointberegningernes241\Chaiselongs\Whatchamacallits76\querciflorae\libdatrie-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Stingily\Nebularise\stormagasiners\libpkcs11-helper-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Stingily\Nebularise\stormagasiners\maintenanceservice2.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsj54D2.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.explorer.exe.14163814.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.DHLIN00178.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
5.0.DHLIN00178.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Source	Detection	Scanner	Label	Link	Download
9.2.firefox.exe.1e1f3814.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.2.cscript.exe.4f33814.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.DHLIN00178.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Domains

Source	Detection	Scanner	Label	Link
td-ccm-168-233.wixdns.net	0%	Virustotal		Browse
popcors.com	1%	Virustotal		Browse
www.riverflow.net	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.sem-jobs.com/i9th/	100%	Avira URL Cloud	malware	
http://www.cmproutdoors.com/i9th/	100%	Avira URL Cloud	malware	
http://www.0w3jy.com/i9th/	0%	Avira URL Cloud	safe	
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	Avira URL Cloud	safe	
http://www.37123.vip/i9th/?eg9JVw4y=QFexSP2v0Nfahq1S1liqATm5JxjoDmOPLniWa5ukQb1HIcv0ZKrmbVZaJMRsWG1ma9D40wKdkkU/v7zCXk+Vmaqrz8TPF5Aljg==&WsTjx=NuByY	100%	Avira URL Cloud	malware	
http://machupichuturismo.com/bBbWIWXVMfEPUqiMugc81.bincj	0%	Avira URL Cloud	safe	
http://www.popcors.com/i9th/	100%	Avira URL Cloud	malware	
http://www.hhkk143.cfd/i9th/	100%	Avira URL Cloud	malware	
http://www.popcors.com/i9th/?WsTjx=NuByY&eg9JVw4y=2Tzmt/R719tLBul7mSD638d/x74EcSC92+f/k2zWdQLWTIlxfL/M90/j5x2SA2nsSzi8rNl8g04ZV+bWcvwPkAs6VEt+1VDvVA==	100%	Avira URL Cloud	malware	
http://www.0w3jy.com/i9th/?WsTjx=NuByY&eg9JVw4y=uGolGY6UqX3sY/9PLVWwN9J/BTzz+6hffrhecVGN5Fjl635Z0j5At+r+BPTklOB2HfIE21jETmQJryl68L/U0+pl2AIDG80kBg==	0%	Avira URL Cloud	safe	
http://www.riverflow.net/i9th/	0%	Avira URL Cloud	safe	
http://www.casinoenligne-france.info/i9th/?WsTjx=NuByY&eg9JVw4y=k6CZcF1ZzBrKa1yLo5gUvle0ANnyvLBM7QyaLf2rdBQJTudoAeDS0wYpaDY8EKJddZnFAls+GzNjbQwIPoLL7cj/l4B8r0J0qw==	100%	Avira URL Cloud	malware	
http://www.hot6s.com/i9th/	100%	Avira URL Cloud	malware	
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	
http://www.sandyhillsagritourism.com/i9th/?WsTjx=NuByY&eg9JVw4y=PDhFruS31XQUb4y36+furUas2tGpUbYkRl+Vt3Aa+IAT3kg40wU83JEX1Y8JNHLK9JPMefgRvvrtwUOOtwZiCVeSdeNGXRAYpw==	100%	Avira URL Cloud	malware	
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://www.spotcheck.site/i9th/	100%	Avira URL Cloud	malware	
http://www.adasoft.info/i9th/	100%	Avira URL Cloud	malware	
http://www.riverflow.net/i9th/?WsTjx=NuByY&eg9JVw4y=djsn1an+GmzwXFTB/MFsKGQXJOZQhusBpj6p6RqECbOdtpCOv2Kvcnth4kqs1edHWjVNJqZCDFfEwc47KO0/1j4B7gbgnVo+SQ==	0%	Avira URL Cloud	safe	
http://www.5319ss.com/i9th/	0%	Avira URL Cloud	safe	
http://www.37123.vip/i9th/	100%	Avira URL Cloud	malware	
http://www.daon3999.net/i9th/	0%	Avira URL Cloud	safe	
http://www.verde-amar.info/i9th/	0%	Avira URL Cloud	safe	
http://www.daon3999.net/i9th/?WsTjx=NuByY&eg9JVw4y=f7i/reR9z/XYtiufs4T2oCgITJHppPIhAuHFUSLntHIlLxYI6+YKRHThES4heztnev1TOQxmA1eDErfm329tx1/Ku+4bHpf60w==	0%	Avira URL Cloud	safe	
http://www.hhkk143.cfd/i9th/?eg9JVw4y=a+ho0UoyjOnZk1ICGpcoaGjEnGbmKf9IFFNpvRdd6kC+DJQ8bYOFaRfvJPlieJPEPcY1cGGv0mjDAZsn1ciiV+pIF0lWDSd4aQ==&WsTjx=NuByY	100%	Avira URL Cloud	malware	
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Avira URL Cloud	safe	
http://www.adasoft.info/i9th/?WsTjx=NuByY&eg9JVw4y=7TOFWM92qV6pcrPqADbwGQbE1m3eI0WOEQ27vaT62sOH8JmND2m/uvMqxI1JrYebWMYnTtk64dqQKbYLv2YomR00aJ+FLC/PKQ==	100%	Avira URL Cloud	malware	
http://machupichuturismo.com/bBbWIWXVMfEPUqiMugc81.bin	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.dinggubd.net/i9th/?WsTjx=NuByY&eg9JVw4y=skpleuUmXVtlsTBo2HC5tT/aGHmA0xfCvZmPrRJBNh0Q4R2Cj+Wk81Dgip66N6Ewmv0qryLoIL5Vk4bBbPirrB4g3sIArb9fSw==	100%	Avira URL Cloud	malware	
http://www.dinggubd.net/i9th/	100%	Avira URL Cloud	malware	
http://www.verde-amar.info/i9th/?eg9JVw4y=k3d2rpkNYMKNWaTFA3t0FG4YoWbTiA9z8X9PQFaufAL9B597B9+6rAPLCs31mdZA/v+HUWU5or1J0geLcv9LMooOfPEJdl/q3g==&WsTjx=NuByY	0%	Avira URL Cloud	safe	
http://www.5319ss.com/i9th/?eg9JVw4y=oRug1p2N3M7f21OO0lOBGqE4PfaV2grEv9VY5puRv4+mIhzAnHI5ZAphwtkKSkIVc0m4kQAL+gvPk8R76uitxElzOZBQuGepJQ==&WsTjx=NuByY	0%	Avira URL Cloud	safe	
http://https://mozilla.org0	0%	Avira URL Cloud	safe	
http://www.sem-jobs.com/i9th/?eg9JVw4y=z7FlOMl2i6pYQmyH2ErzvRvTq7+wkT+xjTHk/876j4Q/5vAls38NbxDvDu1KKOzJ/k110/24aT2WAbPRlApsmRrAhaQg7G9jLg==&WsTjx=NuByY	100%	Avira URL Cloud	malware	
http://www.casinoenligne-france.info/i9th/	100%	Avira URL Cloud	malware	
http://www.spotcheck.site/i9th/?eg9JVw4y=zQVcsXcgs6FlBsavZKdNfD9L9lyDn+uX2155hsx4ti6GChTluvpprxYWozt816wf2SlZqQ0WfllzqwVqRSAw6movAhpuxOp8gg==&WsTjx=NuByY	100%	Avira URL Cloud	malware	
http://www.cmproutdoors.com/i9th/?eg9JVw4y=lqJURYfuPjuznURrThj0aNiAAsaH1/tf+kf9L6kKBxqjEkH5T6yZpcUSZY6yP89JvXg35e6PTbHFvlwlO73OfbEtyEO8MEspLQ==&WsTjx=NuByY	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	• 4%, Virustotal, Browse	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
u4tgw7dr.n.funnull35.com	103.20.61.209	true	true		unknown
adasoft.info	81.88.48.71	true	true		unknown
www.hot6s.com	104.21.8.203	true	true		unknown
machupichuturismo.com	162.213.255.18	true	false		unknown
www.hhkk143.cfd	188.114.96.3	true	true		unknown
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.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.0w3jy.com/i9th/	true	• Avira URL Cloud: safe	unknown
http://www.hhkk143.cfd/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.cmproutdoors.com/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.popcors.com/i9th/?WsTjx=NuByY&eg9JVw4y=2Tzmt/R719tLBul7mSD638d/x74EcSC92+f/k2zWdQLWTIIxfL/M90/j5x2SA2nsSzi8rNl8g04ZV+bWcvwPkAs6VEt+1VDvVA==	true	• Avira URL Cloud: malware	unknown
http://www.popcors.com/i9th/	true	• Avira URL Cloud: malware	unknown

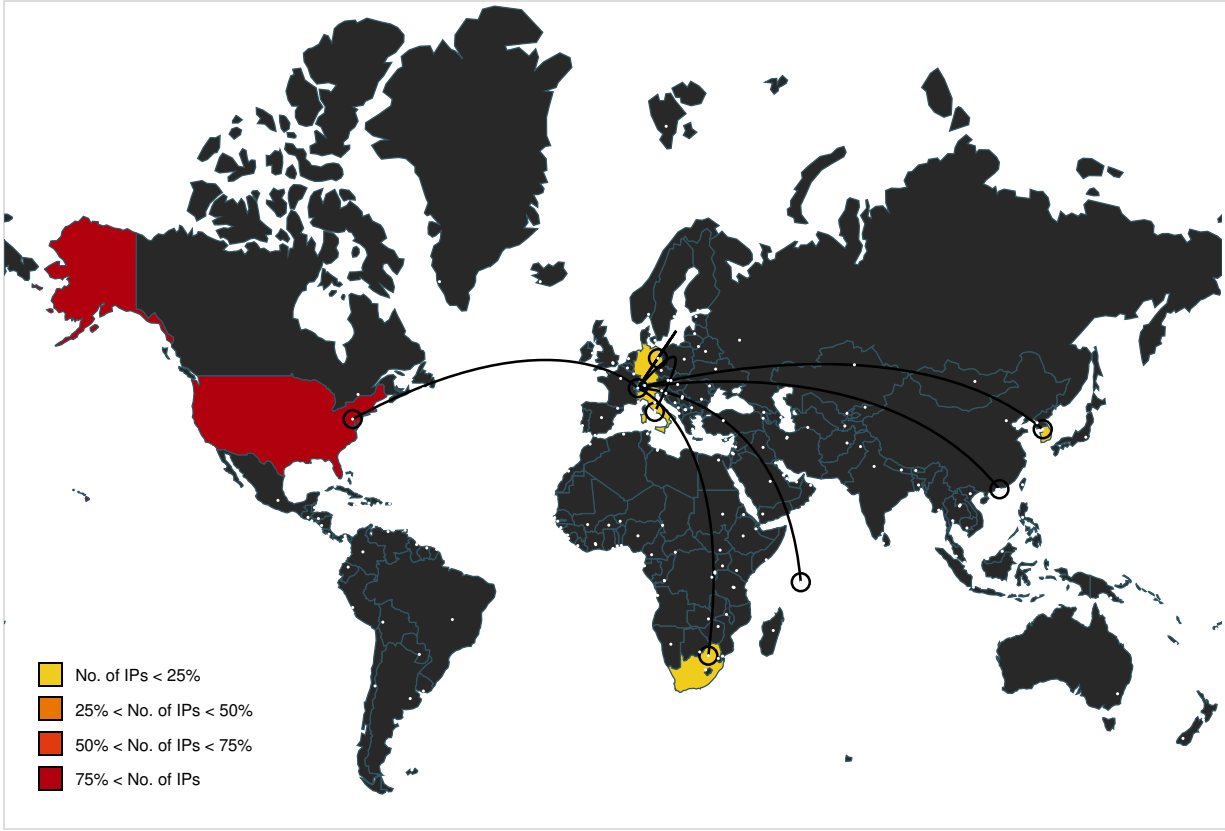
Name	Malicious	Antivirus Detection	Reputation
http://www.37123.vip/i9th/?eg9JVw4y=QFexSP2v0Nfahq1S1liqATm5JxjoDmOPLniWa5ukQb1HIcv0ZKrmbVZaJMRsWG1ma9D40wKdkkU/v7zCXk+Vmaqrz8TPF5AIjg==&WsTjx=NuByY	true	• Avira URL Cloud: malware	unknown
http://www.sem-jobs.com/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.0w3jy.com/i9th/?WsTjx=NuByY&eg9JVw4y=uGolGY6UqX3sY/9PLVWwN9J/BTzz+6hffrhecVGN5FjI635Z0j5At+r+BPTkIOB2HfIE21jETmQJryI68L/U0+pl2AIDG80kBg==	true	• Avira URL Cloud: safe	unknown
http://www.hot6s.com/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.riverflow.net/i9th/	true	• Avira URL Cloud: safe	unknown
http://www.casinoenligne-france.info/i9th/?WsTjx=NuByY&eg9JVw4y=k6CZcF1ZzBrKa1yLo5gUvle0ANnyvLBM7QyaLf2rdBQJTudoAeDS0wYpaDY8EKJddZnFAls+GzNjbQwIPoLL7cj/l4B8r0J0qw==	true	• Avira URL Cloud: malware	unknown
http://www.adasoft.info/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.sandyhillsagritourism.com/i9th/?WsTjx=NuByY&eg9JVw4y=PDhFruS31XQUb4y36+furUas2tGpUbYkRl+Vt3Aa+IAT3kg40wU83JEX1Y8JNHLK9JPMefgRvvrtwUOOtwZiCVeSdeNGXRAYpw==	true	• Avira URL Cloud: malware	unknown
http://www.spotcheck.site/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.riverflow.net/i9th/?WsTjx=NuByY&eg9JVw4y=djsn1an+GmzwXFTB/MFsKGQXJOZQhusBpj6p6RqECbOdtpCOv2Kvcnth4kqs1edHWjVNJqZCDFfEwc47KO0/1j4B7gbgnVo+SQ==	true	• Avira URL Cloud: safe	unknown
http://www.5319ss.com/i9th/	true	• Avira URL Cloud: safe	unknown
http://www.37123.vip/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.daon3999.net/i9th/	true	• Avira URL Cloud: safe	unknown
http://www.verde-amar.info/i9th/	true	• Avira URL Cloud: safe	unknown
http://www.daon3999.net/i9th/?WsTjx=NuByY&eg9JVw4y=f7i/reR9z/XYtiufs4T2oCgITJHppPIhAuHFUSLntHIlLxYI6+YKRHThES4heztnev1TOQxmA1eDErfm329tx1/Ku+4bHpf60w==	true	• Avira URL Cloud: safe	unknown
http://www.hhkk143.cfd/i9th/?eg9JVw4y=a+ho0UoyjOnZk1ICGpcoaGjEnGbmKf9IFFNpvRdd6kC+DJQ8bYOFaRfvJPIieJPEPcY1cGGv0mjDAZsn1ciiV+pIF0lWDSd4aQ==&WsTjx=NuByY	true	• Avira URL Cloud: malware	unknown
http://www.adasoft.info/i9th/?WsTjx=NuByY&eg9JVw4y=7TOFWM92qV6pcrPqADbwGQbE1m3eI0WOEQ27vaT62sOH8JmND2m/uvMqxI1JrYebWMYnTtk64dqQKbYLv2YomR00aJ+FLC/PKQ==	true	• Avira URL Cloud: malware	unknown
http://machupichuturismo.com/bBbWIWXVMfEPUqiMugc81.bin	false	• Avira URL Cloud: safe	unknown
http://www.dinggubd.net/i9th/?WsTjx=NuByY&eg9JVw4y=skpIeuUmXVtlsTBo2HC5tT/aGHmA0xfCvZmPrRJBNh0Q4R2Cj+Wk81Dgip66N6Ewmv0qryLoIL5Vk4bBbPirrB4g3sIArb9fSw==	true	• Avira URL Cloud: malware	unknown
http://www.dinggubd.net/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.verde-amar.info/i9th/?eg9JVw4y=k3d2rpkNYMKNWaTFA3t0FG4YoWbTiA9z8X9PQFaufAL9B597B9+6rAPLCs31mdZA/v+HUWU5or1J0geLcv9LMooOfPEJdI/q3g==&WsTjx=NuByY	true	• Avira URL Cloud: safe	unknown
http://www.5319ss.com/i9th/?eg9JVw4y=oRug1p2N3M7f21OO0lOBGqE4PfaV2grEv9VY5puRv4+mIhzAnHI5ZAphwtkKSkIVc0m4kQAL+gvPk8R76uitxElzOZBQuGepJQ==&WsTjx=NuByY	true	• Avira URL Cloud: safe	unknown
http://www.sem-jobs.com/i9th/?eg9JVw4y=z7FIOMl2i6pYQmyH2ErzvRvTq7+wkT+xjTHk/876j4Q/5vAls38NbxDvDu1KKOzJ/k110/24aT2WAbPRlApsmRrAhaQg7G9jLg==&WsTjx=NuByY	true	• Avira URL Cloud: malware	unknown
http://www.casinoenligne-france.info/i9th/	true	• Avira URL Cloud: malware	unknown
http://www.spotcheck.site/i9th/?eg9JVw4y=zQVcsXcgs6FIBsavZKdNfD9L9IyDn+uX2155hsx4ti6GChTIuvpprxYWozt816wf2SlZqQ0WfIlzqwVqRSAw6movAhpuxOp8gg==&WsTjx=NuByY	true	• Avira URL Cloud: malware	unknown
http://www.cmproutdoors.com/i9th/?eg9JVw4y=lqJURYfuPjuznURrThj0aNiAAsaH1/tf+kf9L6kKBxqjEkH5T6yZpcUSZY6yP89JvXg35e6PTbHFvlwlO73OfbEtyEO8MEspLQ==&WsTjx=NuByY	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://machupichuturismo.com/bBbWIWXVMfEPUqiMugc81.bincj	DHLIN00178.exe, 00000005.00000003.691482 3773.00000000076A0000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.thawte.com0	DHLIN00178.exe, 00000001.00000003.468458 8231.00000000029A4000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	DHLIN00178.exe, 00000005.00000001.590793 7864.0000000000649000.00000020.00000001. 01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	DHLIN00178.exe, 00000001.00000000.4561346773.0000000000409000.00000008.00000001.01000000.00000003.sdmp, DHLIN00178.exe, 00000001.00000002.6089742553.0000000000409000.00000004.00000001.01000000.00000003.sdmp, DHLIN00178.exe, 00000005.00000000.5906874308.0000000000409000.00000008.00000001.01000000.00000003.sdmp	false		high
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	DHLIN00178.exe, 00000005.00000001.5907937864.0000000000626000.00000020.00000001.01000000.00000005.sdmp	false		high
http://www.gopher.ftp://ftp.	DHLIN00178.exe, 00000005.00000001.5907937864.0000000000649000.00000020.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/cps0(	DHLIN00178.exe, 00000001.00000003.4684588231.00000000029A4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/dotnet/runtime	DHLIN00178.exe, 00000001.00000003.4687395558.00000000029AC000.00000004.00000020.00020000.00000000.sdmp, DHLIN00178.exe, 00000001.00000003.4688853178.00000000029AB000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	DHLIN00178.exe, 00000005.00000001.5907937864.00000000005F2000.00000020.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_Error	DHLIN00178.exe, DHLIN00178.exe, 00000001.00000000.4561346773.0000000000409000.00000008.00000001.01000000.00000003.sdmp, DHLIN00178.exe, 00000001.00000002.6089742553.0000000000409000.00000004.00000001.01000000.00000003.sdmp, DHLIN00178.exe, 00000005.00000000.5906874308.0000000000409000.00000008.00000001.01000000.00000003.sdmp	false		high
http://https://aka.ms/dotnet-warnings/	DHLIN00178.exe, 00000001.00000003.4687395558.00000000029AC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	DHLIN00178.exe, 00000001.00000003.4684588231.00000000029A4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.symauth.com/rpa00	DHLIN00178.exe, 00000001.00000003.4684588231.00000000029A4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.nero.com	DHLIN00178.exe, 00000001.00000003.4684588231.00000000029A4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	DHLIN00178.exe, 00000005.00000001.5907937864.0000000000649000.00000020.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	DHLIN00178.exe, 00000005.00000001.5907937864.00000000005F2000.00000020.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://mozilla.org0	DHLIN00178.exe, 00000001.00000003.4691888119.00000000029AA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	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
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
3.9.182.46	www.casinoenligne-france.info	United States		16509	AMAZON-02US	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
103.20.61.209	u4tgw7dr.n.funnull35.com	Hong Kong		133380	LAYER-ASLayerstackLimitedHK	true
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
162.213.255.18	machupichuturismo.com	United States		22612	NAMECHEAP-NETUS	false
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:	829130
Start date and time:	2023-03-17 21:33:08 +01:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 17m 3s
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:	14
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:	DHLIN00178.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@8/11@19/17
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 6.4% (good quality ratio 6.1%) • Quality average: 78.4% • Quality standard deviation: 27.4%
HCA Information:	• Successful, ratio: 96% • 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, UserOOBEBroker.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.190.160.14, 40.126.32.136, 20.190.160.22, 40.126.32.68, 20.190.160.20, 40.126.32.138, 40.126.32.76, 40.126.32.140
- Excluded domains from analysis (whitelisted): prdv6a.aadg.msidentity.com, wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, www.tm.v6.a.prd.aadg.akadns.net, login.msa.msidentity.com, www.tm.lg.prod.aadmsa.trafficmanager.net
- Execution Graph export aborted for target DHLIN00178.exe, PID 1776 because there are no executed function
- 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 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\Maattet\Dystonia.Fis116

Process:	C:\Users\user\Desktop\DHLIN00178.exe
File Type:	ASCII text, with very long lines (53810), with no line terminators
Category:	dropped
Size (bytes):	53810
Entropy (8bit):	2.6910915446582364
Encrypted:	false
SSDEEP:	768:m5Bw4mEWCEEEEE87pG5nZpb+fPM3kgjx/6yE2xNLXnF+yB54yLvBkhBYq7oP8n5j:mlUnZpxU6xRLM2Lclp5weok
MD5:	7FB8B546EC10F0822FC0B4089E560733
SHA1:	2CEFF57E58D87662C329D3F1978CCBC6FCEB16DF
SHA-256:	6D868BCFDE2ECCB7EBD58E727C3DC32434DA3F21E0EF80AEA2C89E5F5A7F3642
SHA-512:	3F25762F1393CB4C9538B6005F00B8E122C029F05E542229D17EE6D761F0A91954C2CA79426650A8F1DE0310CB850E8E27AC2A713764BEB2719EBDE17A4CC59
Malicious:	false
Reputation:	low
Preview:	00000F005B001A1A00004C000000540000000E300E9E90033000000DDDDDD00000000005C5C000000006700003A000054005D0000003636360000 4F4F00006D6D0000FFFFFFFFFF009E000086868600F30000A6A6A6A6000001000000141414140018000000262600303000B8000000000083002020006600480086000000000F2F2F200000C00000000CF000000060600000030300078008700001C00BA00000000000000F3F300CB00C6C6C6C600500000000F000E3E300D1D1D100D9009A9A000024000 00EDED000100000000000007070700000004B4B00000026003700A60036363600000042000 0A1000000C200BDBDBD005C5C002C000000F70000000000000007E7E7E7E7E00001E1E00ED00004C004C0000AB00002C2C007F7F0000007C00000E0000B40000BFBFBFBF000000AE000000000000888800FCFCFCFC00515100 0000C6C6C6007777770000CBCBCBCBCBCBCBCB0000DCDC000000000009797000064640012120 0AE000000DA001C003F3F00000000CCCC00003333 330080808080808000000000032009B9B0023232300004A000000A0A0A000000F0F00FF00008B00E7E7004400E5E50000E3E3E3E3E3002020000000020007900001F1F0000007300000D00A100FAFA0003000072000000005A5A00E2E200B7B7B7B700000000002300A6A600720000002B005D000000838383

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Maattet\Skrddersjlenes.Nou

Process:	C:\Users\user\Desktop\DHLIN00178.exe
File Type:	data
Category:	dropped
Size (bytes):	260228
Entropy (8bit):	7.296059267389181
Encrypted:	false
SSDEEP:	3072:Frjq0MSUGUC72zwV6xCFAGSsIb0N1YK+S6RSojl8XfHtc9LtR866+Tq8oD7xYCBs:F0ZGUCT/Ib0NKSogfNc3HnW8oDHtswe
MD5:	3AE902DED608BA446C2B6FF0804D96BE
SHA1:	D3B6BF0FFA9F017DACA457F4569A04AA086CD263
SHA-256:	377721BE18CEB08A0D3181A3C375C08F5B918FE7CB0509046AB911C9030CDB95
SHA-512:	FECA207CF6E38A4DC94A266F02D84E86BDE14C6EC5F6859EADC38369955103BD707B97D09DEBEAD7CB5600D99E0A9043AF234FDBA221B674041844E926934FE8
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Maattet\SolutionExplorerCLI.dll

Process:	C:\Users\user\Desktop\DHLIN00178.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..:.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\Maattet\System.Security.Cryptography.X509Certificates.dll

Process:	C:\Users\user\Desktop\DHLIN00178.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\Mandslinien\Characterizable\Senilitetstegnet\percentile.dll

Process:	C:\Users\user\Desktop\DHLIN00178.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\Pointberegningernes241\Chaiselongs\Whatchamacallits76\querciflorae\System.dll

Process:	C:\Users\user\Desktop\DHLIN00178.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\Pointberegningernes241\Chaiselongs\Whatchamacallits76\querciflorae\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..;..l..;..Q..;..Y..;..a..;..i..;..q..;..y..;....; ...;....;..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Ghetto\Pointberegningernes241\Chaiselongs\Whatchamacallits76\querciflorae\libdatrie-1.dll

Process:	C:\Users\user\Desktop\DHLIN00178.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\Microsoft\Windows\INetCache\Ghetto\Stingily\Nebularise\stormagasiners\libpkcs11-helper-1.dll

Process:	C:\Users\user\Desktop\DHLIN00178.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\Stingily\Nebularise\stormagasiners\maintenanceservice2.exe

Process:	C:\Users\user\Desktop\DHLIN00178.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\Temp\AeL-0b1QRQ

Process:	C:\Windows\SysWOW64\cscript.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\nsj54D2.tmp\System.dll

Process:	C:\Users\user\Desktop\DHLIN00178.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):	7.477730016942703
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:	DHLIN00178.exe
File size:	888192
MD5:	66fdf2df4fc8601124df76c284f797e1
SHA1:	88031f2f9bfbf3eb0b069c68fd4ed4ee288daf9f
SHA256:	e07a149d14fc37367e7331342d07dc45aec9ef7bbce780ea636c5d04f6c26f3f
SHA512:	a1fc53925d4fd04a81d2d7dc8bb26ed15fef14e9cd38945fbba55ef7b67a13b67c9527ed7c5388f9ed9013c287df67f343248bb4261838f389d34f42959c3720
SSDEEP:	12288:AwFjJnKlHcG+glWs89TbTjb8E5UcKcZnY4UKwp7hVOZCbgjvwhaD:A6jklHcGtlF89TbfccUNEZCbgjV
TLSH:	4715CFD7B845528CE9B99EB3712B1C2213701FBA662C104D76CC329D09FD1627EDE86E
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:	6e8d166f696a6661

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=Misbehadden@Anstdsstenenes.Sta, OU="Seksdageslb Tredjebehandles ", O=Konfirmeres, L=Bondues, S=Hauts-de-France, C=FR
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	• 27/05/2022 07:04:34 26/05/2025 07:04:34
Subject Chain	• E=Misbehadden@Anstdsstenenes.Sta, OU="Seksdageslb Tredjebehandles ", O=Konfirmeres, L=Bondues, S=Hauts-de-France, C=FR
Version:	3
Thumbprint MD5:	EF5809104A07E21FDB714DE7D3F4CB3B
Thumbprint SHA-1:	E5B83F0AF141BAF75894E4585A5133459235BDBF
Thumbprint SHA-256:	AC8EC8BCA9EDDE54EDCCFD81C53BCAB60DEB5C8F53E2C46EB232990CA73252D7
Serial:	7D95432F108C131FEDA31C4FE788119FC24ED14C

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi

Instruction
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 00007FDC79015AB3h
push ebx
call 00007FDC79018B9Bh
cmp eax, ebx
je 00007FDC79015AA9h
push 00000C00h
call eax
mov esi, 00407298h
push esi
call 00007FDC79018B17h
push esi
call dword ptr [00407098h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FDC79015A8Dh
push 0000000Ah
call 00007FDC79018B6Fh
push 00000008h
call 00007FDC79018B68h
push 00000006h
mov dword ptr [00423704h], eax
call 00007FDC79018B5Ch
cmp eax, ebx
je 00007FDC79015AB1h
push 0000001Eh
call eax
test eax, eax
je 00007FDC79015AA9h
or byte ptr [0042370Fh], 00000040h
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	0x34260	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xd6b18	0x2268	
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	0x34260	0x34400	False	0.20456414473684212	data	4.299804646716883	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x36208	0x33828	Device independent bitmap graphic, 199 x 512 x 32, image size 203776, resolution 3779 x 3779 px/m	English	United States
RT_DIALOG	0x69a30	0x100	data	English	United States
RT_DIALOG	0x69b30	0x11c	data	English	United States
RT_DIALOG	0x69c50	0xc4	data	English	United States
RT_DIALOG	0x69d18	0x60	data	English	United States
RT_GROUP_ICON	0x69d78	0x14	data	English	United States
RT_VERSION	0x69d90	0x190	data	English	United States
RT_MANIFEST	0x69f20	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

DLL	Import
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

Total Packets: 69

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 21:37:33.052336931 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.220213890 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.220441103 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.221458912 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.396615028 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.396702051 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.396770000 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.396832943 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.396862984 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.396863937 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.396897078 CET	80	49837	162.213.255.18	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 21:37:33.396944046 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.396960974 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.397025108 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.397063017 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.397063017 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.397092104 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.397133112 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.397156000 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.397221088 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.397255898 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.397316933 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.397316933 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.397500038 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.564837933 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.564940929 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.565017939 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.565088034 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.565100908 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.565160036 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.565177917 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.565223932 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.565253973 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.565275908 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.565332890 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.565390110 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.565407038 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.565454006 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.565483093 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.565517902 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.565556049 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.565587997 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.565656900 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.565742970 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.565743923 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.565772057 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.565897942 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.565938950 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.566005945 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.566019058 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.566067934 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.566148043 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.566226959 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.566251040 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.566318035 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.566324949 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.566396952 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.566452026 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.566471100 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.566515923 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.566545963 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.566577911 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.566647053 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.566783905 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.734282017 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.734411955 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.734515905 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.734520912 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.734611034 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.734636068 CET	80	49837	162.213.255.18	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 21:37:33.734750032 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.734767914 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.734818935 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.734863043 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.734958887 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.734982014 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.735025883 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.735101938 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.735182047 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.735220909 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.735250950 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.735327959 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.735425949 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.735445023 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.735476971 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.735563993 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.735634089 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.735665083 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.735718012 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.735757113 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.735863924 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.735867023 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.735964060 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.736005068 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.736057997 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.736068964 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.736174107 CET	80	49837	162.213.255.18	192.168.11.20
Mar 17, 2023 21:37:33.736182928 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.736249924 CET	49837	80	192.168.11.20	162.213.255.18
Mar 17, 2023 21:37:33.736272097 CET	80	49837	162.213.255.18	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 21:37:32.723170042 CET	58030	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:37:33.046544075 CET	53	58030	1.1.1.1	192.168.11.20
Mar 17, 2023 21:39:18.686295033 CET	62586	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:39:18.725651026 CET	53	62586	1.1.1.1	192.168.11.20
Mar 17, 2023 21:39:33.868172884 CET	58897	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:39:34.203830957 CET	53	58897	1.1.1.1	192.168.11.20
Mar 17, 2023 21:39:46.897708893 CET	55202	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:39:46.928004026 CET	53	55202	1.1.1.1	192.168.11.20
Mar 17, 2023 21:39:59.629028082 CET	59279	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:40:00.230015993 CET	53	59279	1.1.1.1	192.168.11.20
Mar 17, 2023 21:40:14.046832085 CET	60805	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:40:14.119550943 CET	53	60805	1.1.1.1	192.168.11.20
Mar 17, 2023 21:40:26.966200113 CET	60613	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:40:26.986928940 CET	53	60613	1.1.1.1	192.168.11.20
Mar 17, 2023 21:40:39.635067940 CET	58472	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:40:39.985469103 CET	53	58472	1.1.1.1	192.168.11.20
Mar 17, 2023 21:40:53.178683996 CET	49296	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:40:53.192972898 CET	53	49296	1.1.1.1	192.168.11.20
Mar 17, 2023 21:41:06.707278013 CET	61538	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:41:07.026993990 CET	53	61538	1.1.1.1	192.168.11.20
Mar 17, 2023 21:41:21.188827991 CET	53222	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:41:21.207340002 CET	53	53222	1.1.1.1	192.168.11.20
Mar 17, 2023 21:41:35.545300961 CET	50570	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:41:36.560158968 CET	50570	53	192.168.11.20	9.9.9.9
Mar 17, 2023 21:41:37.020494938 CET	53	50570	1.1.1.1	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 21:41:37.353796959 CET	53	50570	9.9.9.9	192.168.11.20
Mar 17, 2023 21:41:50.884869099 CET	63114	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:41:51.192102909 CET	53	63114	1.1.1.1	192.168.11.20
Mar 17, 2023 21:42:04.725537062 CET	52456	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:42:05.741060972 CET	52456	53	192.168.11.20	9.9.9.9
Mar 17, 2023 21:42:06.574141026 CET	53	52456	1.1.1.1	192.168.11.20
Mar 17, 2023 21:42:06.817251921 CET	53	52456	9.9.9.9	192.168.11.20
Mar 17, 2023 21:42:21.425585985 CET	65151	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:42:21.853430033 CET	53	65151	1.1.1.1	192.168.11.20
Mar 17, 2023 21:42:35.609678030 CET	54072	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:42:35.920783997 CET	53	54072	1.1.1.1	192.168.11.20
Mar 17, 2023 21:42:48.576221943 CET	63581	53	192.168.11.20	1.1.1.1
Mar 17, 2023 21:42:48.607541084 CET	53	63581	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 17, 2023 21:37:32.723170042 CET	192.168.11.20	1.1.1.1	0x7fcb	Standard query (0)	machupichu turismo.com	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:39:18.686295033 CET	192.168.11.20	1.1.1.1	0xc897	Standard query (0)	www.sandyh illsagrito urism.com	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:39:33.868172884 CET	192.168.11.20	1.1.1.1	0xb713	Standard query (0)	www.sem-jo bs.com	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:39:46.897708893 CET	192.168.11.20	1.1.1.1	0x2334	Standard query (0)	www.casino enligne-fr ance.info	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:39:59.629028082 CET	192.168.11.20	1.1.1.1	0x9baa	Standard query (0)	www.37123.vip	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:40:14.046832085 CET	192.168.11.20	1.1.1.1	0xa56c	Standard query (0)	www.adasoft.info	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:40:26.966200113 CET	192.168.11.20	1.1.1.1	0xcfe	Standard query (0)	www.hhkk14 3.cfd	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:40:39.635067940 CET	192.168.11.20	1.1.1.1	0x4b01	Standard query (0)	www.popcor s.com	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:40:53.178683996 CET	192.168.11.20	1.1.1.1	0x4dd1	Standard query (0)	www.spotch eck.site	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:41:06.707278013 CET	192.168.11.20	1.1.1.1	0xd571	Standard query (0)	www.dinggu bd.net	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:41:21.188827991 CET	192.168.11.20	1.1.1.1	0x2a07	Standard query (0)	www.hot6s.com	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:41:35.545300961 CET	192.168.11.20	1.1.1.1	0x49ef	Standard query (0)	www.0w3jy.com	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:41:36.560158968 CET	192.168.11.20	9.9.9.9	0x49ef	Standard query (0)	www.0w3jy.com	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:41:50.884869099 CET	192.168.11.20	1.1.1.1	0xc593	Standard query (0)	www.cmprou tdoors.com	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:42:04.725537062 CET	192.168.11.20	1.1.1.1	0x9ba6	Standard query (0)	www.daon39 99.net	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:42:05.741060972 CET	192.168.11.20	9.9.9.9	0x9ba6	Standard query (0)	www.daon39 99.net	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:42:21.425585985 CET	192.168.11.20	1.1.1.1	0xc8ca	Standard query (0)	www.5319ss .com	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:42:35.609678030 CET	192.168.11.20	1.1.1.1	0xef7b	Standard query (0)	www.riverf low.net	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:42:48.576221943 CET	192.168.11.20	1.1.1.1	0xe4b8	Standard query (0)	www.verde-amar.info	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 17, 2023 21:37:33.046544075 CET	1.1.1.1	192.168.11.20	0x7fcb	No error (0)	machupichu turismo.com		162.213.255.1 8	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:39:18.725651026 CET	1.1.1.1	192.168.11.20	0xc897	No error (0)	www.sandyh illsagrito urism.com	gcdn0.wixdns. net		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 17, 2023 21:39:18.725651026 CET	1.1.1.1	192.168.11.20	0xc897	No error (0)	gcdn0.wixdns.net	td-ccm-168-233.wixdns.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 17, 2023 21:39:18.725651026 CET	1.1.1.1	192.168.11.20	0xc897	No error (0)	td-ccm-168-233.wixdns.net		34.117.168.233	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:39:34.203830957 CET	1.1.1.1	192.168.11.20	0xb713	No error (0)	www.sem-jobs.com		85.13.156.177	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:39:46.928004026 CET	1.1.1.1	192.168.11.20	0x2334	No error (0)	www.casinoenligne-france.info		3.9.182.46	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:40:00.230015993 CET	1.1.1.1	192.168.11.20	0x9baa	No error (0)	www.37123.vip	ehbw3ftr-u.funnull01.vip		CNAME (Canonical name)	IN (0x0001)	false
Mar 17, 2023 21:40:00.230015993 CET	1.1.1.1	192.168.11.20	0x9baa	No error (0)	ehbw3ftr-u.funnull01.vip	u4tgw7dr.n.funnull35.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 17, 2023 21:40:00.230015993 CET	1.1.1.1	192.168.11.20	0x9baa	No error (0)	u4tgw7dr.n.funnull35.com		103.20.61.209	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:40:00.230015993 CET	1.1.1.1	192.168.11.20	0x9baa	No error (0)	u4tgw7dr.n.funnull35.com		103.20.61.210	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:40:00.230015993 CET	1.1.1.1	192.168.11.20	0x9baa	No error (0)	u4tgw7dr.n.funnull35.com		103.20.61.207	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:40:14.119550943 CET	1.1.1.1	192.168.11.20	0xa56c	No error (0)	www.adasoft.info	adasoft.info		CNAME (Canonical name)	IN (0x0001)	false
Mar 17, 2023 21:40:14.119550943 CET	1.1.1.1	192.168.11.20	0xa56c	No error (0)	adasoft.info		81.88.48.71	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:40:26.986928940 CET	1.1.1.1	192.168.11.20	0xcfe	No error (0)	www.hhkk143.cfd		188.114.96.3	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:40:26.986928940 CET	1.1.1.1	192.168.11.20	0xcfe	No error (0)	www.hhkk143.cfd		188.114.97.3	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:40:39.985469103 CET	1.1.1.1	192.168.11.20	0x4b01	No error (0)	www.popcors.com	popcors.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 17, 2023 21:40:39.985469103 CET	1.1.1.1	192.168.11.20	0x4b01	No error (0)	popcors.com		173.230.227.171	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:40:53.192972898 CET	1.1.1.1	192.168.11.20	0x4dd1	No error (0)	www.spotcheck.site		199.192.30.193	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:41:07.026993990 CET	1.1.1.1	192.168.11.20	0xd571	No error (0)	www.dingqubd.net		38.163.2.19	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:41:21.207340002 CET	1.1.1.1	192.168.11.20	0x2a07	No error (0)	www.hot6s.com		104.21.8.203	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:41:21.207340002 CET	1.1.1.1	192.168.11.20	0x2a07	No error (0)	www.hot6s.com		172.67.157.215	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:41:37.020494938 CET	1.1.1.1	192.168.11.20	0x49ef	No error (0)	www.0w3jy.com	hk.ygrcw.cn		CNAME (Canonical name)	IN (0x0001)	false
Mar 17, 2023 21:41:37.020494938 CET	1.1.1.1	192.168.11.20	0x49ef	No error (0)	hk.ygrcw.cn		164.88.122.250	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:41:37.353796959 CET	9.9.9.9	192.168.11.20	0x49ef	No error (0)	www.0w3jy.com	hk.ygrcw.cn		CNAME (Canonical name)	IN (0x0001)	false
Mar 17, 2023 21:41:37.353796959 CET	9.9.9.9	192.168.11.20	0x49ef	No error (0)	hk.ygrcw.cn		164.88.122.250	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:41:51.192102909 CET	1.1.1.1	192.168.11.20	0xc593	No error (0)	www.cmproutdoors.com		156.255.170.114	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:42:06.574141026 CET	1.1.1.1	192.168.11.20	0x9ba6	No error (0)	www.daon3999.net	daon3999.net		CNAME (Canonical name)	IN (0x0001)	false

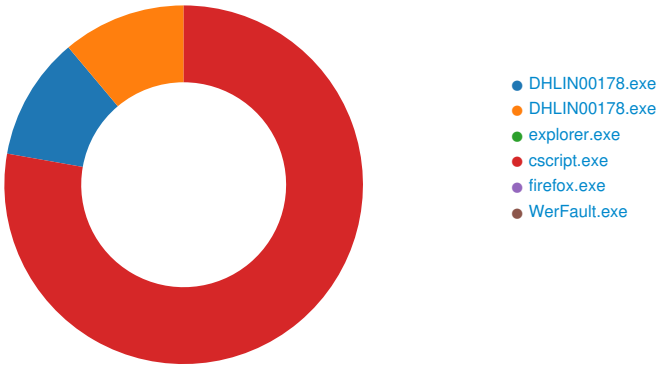
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 17, 2023 21:42:06.574141026 CET	1.1.1.1	192.168.11.20	0x9ba6	No error (0)	daon3999.net		222.122.213.231	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:42:06.817251921 CET	9.9.9.9	192.168.11.20	0x9ba6	No error (0)	www.daon3999.net	daon3999.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 17, 2023 21:42:06.817251921 CET	9.9.9.9	192.168.11.20	0x9ba6	No error (0)	daon3999.net		222.122.213.231	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:42:21.853430033 CET	1.1.1.1	192.168.11.20	0xc8ca	No error (0)	www.5319ss.com	gy.adsfzcvx.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 17, 2023 21:42:21.853430033 CET	1.1.1.1	192.168.11.20	0xc8ca	No error (0)	gy.adsfzcvx.com		154.210.212.94	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:42:35.920783997 CET	1.1.1.1	192.168.11.20	0xef7b	No error (0)	www.riverflow.net		64.190.63.111	A (IP address)	IN (0x0001)	false
Mar 17, 2023 21:42:48.607541084 CET	1.1.1.1	192.168.11.20	0xe4b8	No error (0)	www.verde-amar.info		185.53.177.54	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- machupichuturismo.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

Statistics

Behavior



System Behavior

Analysis Process: DHLIN00178.exe PID: 3876, Parent PID: 4760

General

Target ID:	1
Start time:	21:35:02
Start date:	17/03/2023
Path:	C:\Users\user\Desktop\DHLIN00178.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHLIN00178.exe
Imagebase:	0x400000
File size:	888192 bytes
MD5 hash:	66FDF2DF4FC8601124DF76C284F797E1
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: 00000001.00000002.6092061877.000000000A021000.00000040.00001000.00020000.00000000.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: DHLIN00178.exe PID: 1776, Parent PID: 3876

General

Target ID:	5
Start time:	21:37:16
Start date:	17/03/2023
Path:	C:\Users\user\Desktop\DHLIN00178.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHLIN00178.exe
Imagebase:	0x400000
File size:	888192 bytes
MD5 hash:	66FDF2DF4FC8601124DF76C284F797E1
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: 00000005.00000002.7003744896.0000000000090000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.7003744896.0000000000090000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.7003744896.0000000000090000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000005.00000002.7003407706.0000000000060000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.7003407706.0000000000060000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.7003407706.0000000000060000.00000040.10000000.00040000.00000000.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: **4760**, Parent PID: **1776**

General

Target ID:	7
Start time:	21:38:58
Start date:	17/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff71ac00000
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: cscript.exe PID: **1912**, Parent PID: **4760**

General

Target ID:	8
Start time:	21:39:03
Start date:	17/03/2023
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0x6a0000
File size:	144896 bytes
MD5 hash:	13783FF4A2B614D7FBD58F5EEBDEDEF6
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: 00000008.00000002.9611657134.0000000000600000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.9611657134.0000000000600000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.9611657134.0000000000600000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.9612907079.0000000002CC0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.9612907079.0000000002CC0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.9612907079.0000000002CC0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.9614713149.0000000002FF0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.9614713149.0000000002FF0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.9614713149.0000000002FF0000.00000004.00000800.00020000.00000000.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\DHLIN00178.exe	cannot delete	1	61C947	NtDeleteFile
C:\Users\user\AppData\Local\Temp\AeL-0b1QRQ	object name not found	1	61C947	NtDeleteFile
C:\Users\user\AppData\Local\Temp\AeL-0b1QRQ	sharing violation	1	61C947	NtDeleteFile
C:\Users\user\AppData\Local\Temp\AeL-0b1QRQ	sharing violation	1	61C947	NtDeleteFile
C:\Users\user\AppData\Local\Temp\AeL-0b1QRQ	sharing violation	1	61C947	NtDeleteFile
C:\Users\user\AppData\Local\Temp\AeL-0b1QRQ	sharing violation	1	61C947	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	61C917	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: **5256**, Parent PID: **1912**

General

Target ID:	9
Start time:	21:39:24
Start date:	17/03/2023
Path:	C:\Program Files\Mozilla Firefox\firefox.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Mozilla Firefox\Firefox.exe
Imagebase:	0x7ff739710000
File size:	597432 bytes
MD5 hash:	FA9F4FC5D7ECAB5A20BF7A9D1251C851
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: WerFault.exe PID: **2884**, Parent PID: **5256**

General

Target ID:	12
Start time:	21:39:29
Start date:	17/03/2023
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 5256 -s 284
Imagebase:	0x7ff6e2850000
File size:	568632 bytes
MD5 hash:	5C06542FED8EE68994D43938E7326D75
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

Disassembly

No disassembly