ID: 830431
Sample Name:
DHL_SHIPPING_DOCUMENT.exe
Cookbook: default.jbs
Time: 11:26:09
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

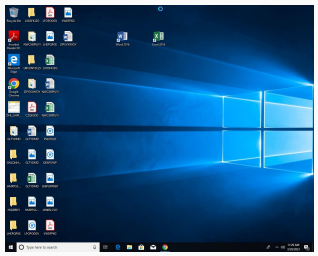
Windows Analysis Report

DHL_SHIPPING_DOCUMENT.exe

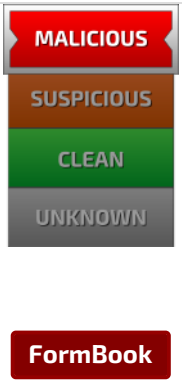
Overview

General Information

Sample Name:	DHL_SHIPPING_DOCUMENT.exe
Analysis ID:	830431
MD5:	04f5c33c1d3f7…
SHA1:	3db181379815…
SHA256:	c0fee78265aef…
Tags:	DHL exe Formbook
Infos:	



Detection



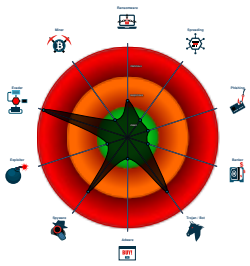
FormBook

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…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- DHL_SHIPPING_DOCUMENT.exe (PID: 3092 cmdline: C:\Users\user\Desktop\DHL_SHIPPING_DOCUMENT.exe MD5: 04F5C33C1D3F795872B58F8C3922B49E)
  - eixfhzlwqd.exe (PID: 2040 cmdline: "C:\Users\user\AppData\Local\Temp\eixfhzlwqd.exe" C:\Users\user\AppData\Local\Temp\lfcykkdw.xwy MD5: 52BD228566EE8DDE1E37102049937D69)
    - conhost.exe (PID: 2168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - eixfhzlwqd.exe (PID: 856 cmdline: C:\Users\user\AppData\Local\Temp\eixfhzlwqd.exe MD5: 52BD228566EE8DDE1E37102049937D69)
      - explorer.exe (PID: 3528 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - help.exe (PID: 2224 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
- **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

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.581265823.0000000002C00000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000005.00000002.581265823.0000000002C00000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1ef80:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xadff:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x18217:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000005.00000002.581265823.0000000002C00000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x18015:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17ab1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x18117:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1828f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa9ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x16cfc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1dd37:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ecea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.357493625.0000000000900000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000003.00000002.357493625.0000000000900000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1ef80:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xadff:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x18217:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Click to see the 13 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.eixfhzlwqd.exe.400000.0.raw.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
3.2.eixfhzlwqd.exe.400000.0.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x20d23:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xcba2:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x19fba:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
3.2.eixfhzlwqd.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x19db8:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x19854:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x19eba:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1a032:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xc76d:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x18a9f:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1fada:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x20a8d:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.eixfhzlwqd.exe.400000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
3.2.eixfhzlwqd.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1ff23:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xbda2:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x191ba:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 81.169.145.88	
Timestamp:	192.168.2.481.169.145.8849695802031412 03/20/23-11:27:41.124513
SID:	2031412
Source Port:	49695
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 104.233.254.113	
Timestamp:	192.168.2.4104.233.254.11349709802031449 03/20/23-11:28:53.219959
SID:	2031449
Source Port:	49709
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 113.52.135.193	
Timestamp:	192.168.2.4113.52.135.19349703802031453 03/20/23-11:28:29.350188
SID:	2031453
Source Port:	49703
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 113.52.135.193	
Timestamp:	192.168.2.4113.52.135.19349703802031412 03/20/23-11:28:29.350188
SID:	2031412
Source Port:	49703
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 81.169.145.88	
Timestamp:	192.168.2.481.169.145.8849695802031453 03/20/23-11:27:41.124513
SID:	2031453
Source Port:	49695
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 199.192.28.110	
Timestamp:	192.168.2.4199.192.28.11049699802031453 03/20/23-11:28:13.420032
SID:	2031453
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.860686532023883 03/20/23-11:29:11.441798
SID:	2023883
Source Port:	60686
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 81.169.145.88	
Timestamp:	192.168.2.481.169.145.8849695802031449 03/20/23-11:27:41.124513
SID:	2031449
Source Port:	49695
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 46.23.69.44	
Timestamp:	192.168.2.446.23.69.4449705802031412 03/20/23-11:28:37.254660
SID:	2031412
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 199.192.28.110	
Timestamp:	192.168.2.4199.192.28.11049699802031412 03/20/23-11:28:13.420032
SID:	2031412
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 113.52.135.193	
Timestamp:	192.168.2.4113.52.135.19349703802031449 03/20/23-11:28:29.350188
SID:	2031449
Source Port:	49703
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 46.23.69.44	
Timestamp:	192.168.2.446.23.69.4449705802031453 03/20/23-11:28:37.254660
SID:	2031453
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 104.233.254.113	
Timestamp:	192.168.2.4104.233.254.11349709802031453 03/20/23-11:28:53.219959
SID:	2031453
Source Port:	49709
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 46.23.69.44	
Timestamp:	192.168.2.446.23.69.4449705802031449 03/20/23-11:28:37.254660
SID:	2031449
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 199.192.28.110	
Timestamp:	192.168.2.4199.192.28.11049699802031449 03/20/23-11:28:13.420032
SID:	2031449
Source Port:	49699

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 104.233.254.113	−
Timestamp:	192.168.2.4104.233.254.11349709802031412 03/20/23-11:28:53.219959
SID:	2031412
Source Port:	49709
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

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)
- Snort IDS alert for network traffic

E-Banking Fraud

- Yara detected FormBook

System Summary

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation

- Detected unpacking (changes PE section rights)

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
- Queues an APC in another process (thread injection)
- Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

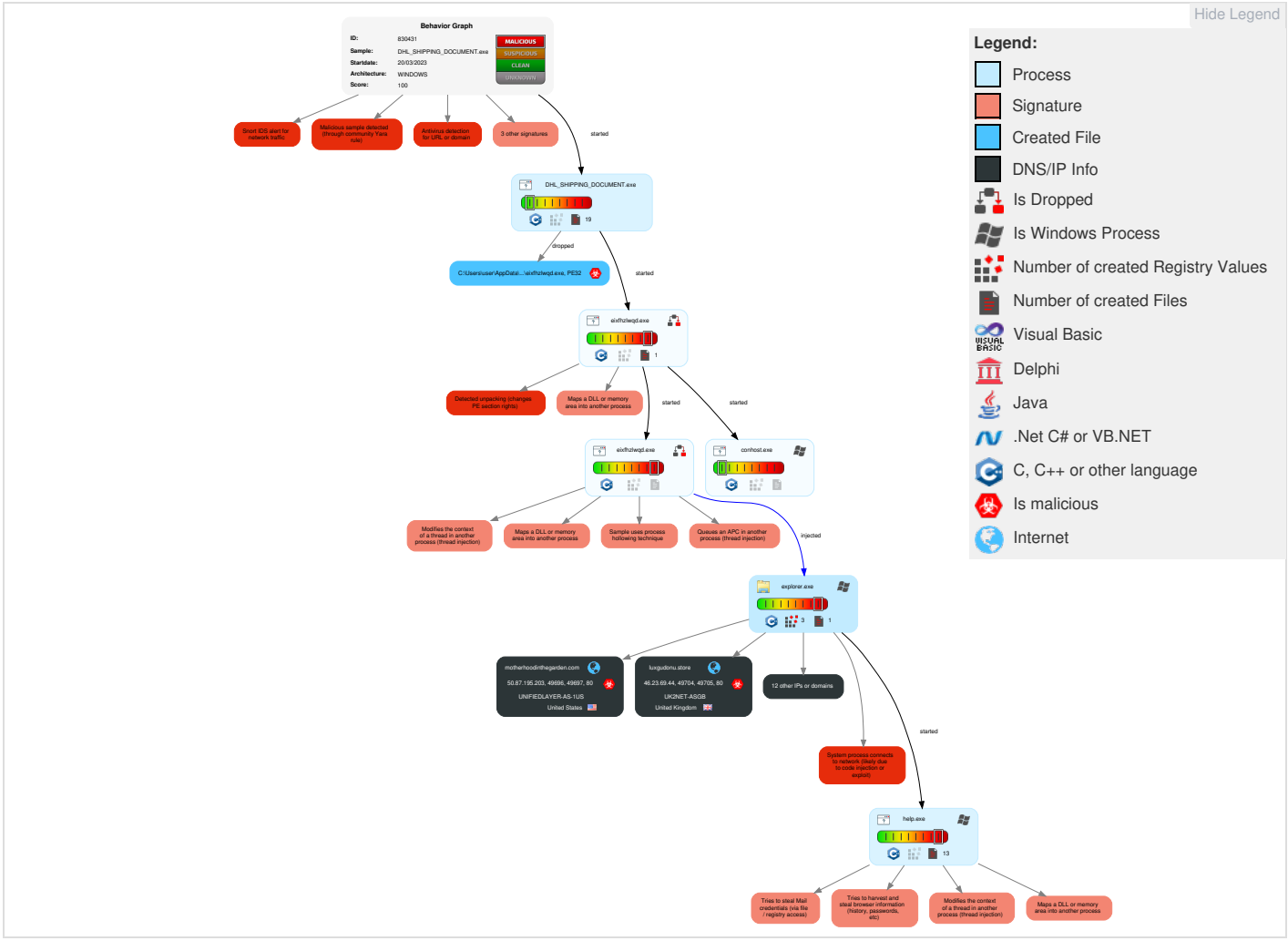
- Yara detected FormBook
- Tries to steal Mail credentials (via file / registry access)
- Tries to harvest and steal browser information (history, passwords, etc)

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	Path Interception	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	1 System Time 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	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	5 1 2 Process Injection	2 Obfuscated Files or Information	LSASS Memory	2 File and Directory 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)	Logon Script (Windows)	1 1 Software Packing	Security Account Manager	1 5 System Information 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)	2 Virtualization/Sandbox Evasion	NTDS	4 1 Security Software Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Access Token Manipulation	LSA Secrets	2 Virtualization/Sandbox Evasion	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	5 1 2 Process Injection	Cached Domain Credentials	2 Process 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	Compile After Delivery	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
DHL_SHIPPING_DOCUMENT.exe	26%	ReversingLabs	Win32.Trojan.Nsisx	
DHL_SHIPPING_DOCUMENT.exe	39%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.eixfhzlwqd.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.eixfhzlwqd.exe.20a0000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.afzalhossainantor.com/d2a3/	0%	Avira URL Cloud	safe	
http://www.vanguardfsm.com/d2a3/	0%	Avira URL Cloud	safe	
http://www.afzalhossainantor.comwww.staatslieden.bizF7L99l=8qpwJ	0%	Avira URL Cloud	safe	
http://www.fresnocap.com/d2a3/	0%	Avira URL Cloud	safe	
http://www.on-smooth.comwww.luxgudonu.storeF7L99l=8qpwJ	0%	Avira URL Cloud	safe	
http://www.363ww.top	0%	Avira URL Cloud	safe	
http://www.sowmedia.site/d2a3/?F7L99l=8qpwJ&Mw=IIoejRIoD0NPrvtjG56SffHGubt9bC7l7VozaPHGZoJbvkCik3wIcy97/aKLKqf+leC/SNQQ4bUyJkgTGWAXDnv4xxMA9hLjSw==	100%	Avira URL Cloud	malware	
http://www.espisys-technology.comwww.on-smooth.comF7L99l=8qpwJ)	0%	Avira URL Cloud	safe	
http://www.staatslieden.biz/d2a3/	0%	Avira URL Cloud	safe	
http://www.staatslieden.bizwww.fresnocap.comF7L99l=8qpwJ	0%	Avira URL Cloud	safe	
http://www.xefordbienhoa.com/d2a3/	0%	Avira URL Cloud	safe	
http://www.worldhortihealth.com	0%	Avira URL Cloud	safe	
http://www.getpay.life/d2a3/?F7L99l=8qpwJ&Mw=VQWJd0zbMmoZh8qz35kMD56sFoyc6gTYso/MZ3BJ/Q0NuTQy4/HeuFqYJgzXZamkeMaLAEsOyVyJpFsiRVW3jp2QSfHijAqmyw==	100%	Avira URL Cloud	malware	
http://www.worldhortihealth.comwww.afzalhossainantor.comF7L99l=8qpwJ	0%	Avira URL Cloud	safe	
http://www.363ww.top/d2a3/	100%	Avira URL Cloud	malware	
http://www.sowmedia.site	100%	Avira URL Cloud	malware	
http://perldancer.org/	0%	Avira URL Cloud	safe	
http://www.on-smooth.com/d2a3/	100%	Avira URL Cloud	malware	
http://www.luxgudonu.store/d2a3/	100%	Avira URL Cloud	malware	
http://www.espisys-technology.com	0%	Avira URL Cloud	safe	
http://www.sowmedia.site/d2a3/	100%	Avira URL Cloud	malware	
http://www.rw-bau.com/d2a3/	100%	Avira URL Cloud	malware	
http://www.motherhoodinthegarden.com/d2a3/?Mw=cN5AEPknHvfgRR2crmYFAZMRCOFajc7CFMghZAmOXZ6v62v+A/wOpED6FQaDJ/tGFUb6Y91ZfjLOaofoM8qmjHtlEGMmc9VxCg==&F7L99l=8qpwJ	100%	Avira URL Cloud	malware	
http://www.vanguardfsm.com	0%	Avira URL Cloud	safe	
http://www.afzalhossainantor.com	0%	Avira URL Cloud	safe	
http://www.on-smooth.com	0%	Avira URL Cloud	safe	
http://www.yh78898.com	0%	Avira URL Cloud	safe	
http://www.yh78898.com/d2a3/?Mw=/rn7tSorYChcOKKpyJYvjsebDE1EetOtUlfXV6ATVt8jMTNnk8PtnAR6Iam3VdBxJXQPah1uBiYgzGnhkXQp6MgBOVaGh7iMCA==&F7L99l=8qpwJ	100%	Avira URL Cloud	malware	
http://www.worldhortihealth.com/d2a3/	100%	Avira URL Cloud	malware	
http://www.fresnocap.com	0%	Avira URL Cloud	safe	
http://www.motherhoodinthegarden.com	0%	Avira URL Cloud	safe	
http://www.rw-bau.comwww.worldhortihealth.comF7L99l=8qpwJ	0%	Avira URL Cloud	safe	
http://www.espisys-technology.com/d2a3/	100%	Avira URL Cloud	malware	
http://www.getpay.life	100%	Avira URL Cloud	malware	
http://www.363ww.topwww.rw-bau.comF7L99l=8qpwJ	0%	Avira URL Cloud	safe	
http://www.vanguardfsm.comwww.xefordbienhoa.comF7L99l=8qpwJr	0%	Avira URL Cloud	safe	
http://www.luxgudonu.store	0%	Avira URL Cloud	safe	
http://www.luxgudonu.store/d2a3/?Mw=OjO/noXVMTk40sLqqWNUhETz5fwNQfL3iZv4zuTHX4FsBRg0F7vbWW3nqcxNlOGl4ZCA660VFsqTMG20zBTe2NhxC9mrQabZ6Q==&F7L99l=8qpwJ	100%	Avira URL Cloud	malware	
http://www.espisys-technology.com/d2a3/?Mw=HRt8t1hC6ylxzqu69JiO+2+wCg/IpDjUJ4ODvXLX3JGoHCx8OnZPShMSZXcaT/6Kc192JGOxG+z3HQLrZrJeLIMi1PhqwEBrHA==&F7L99l=8qpwJ	100%	Avira URL Cloud	malware	
http://www.motherhoodinthegarden.com/d2a3/	100%	Avira URL Cloud	malware	
http://www.xefordbienhoa.com	0%	Avira URL Cloud	safe	
http://www.versicherungsgott.com/d2a3/	100%	Avira URL Cloud	malware	
http://www.yh78898.com/d2a3/	100%	Avira URL Cloud	malware	
http://www.sowmedia.sitewww.yh78898.comF7L99l=8qpwJ	0%	Avira URL Cloud	safe	
http://motherhoodinthegarden.com/d2a3/?Mw=cN5AEPknHvfgRR2crmYFAZMRCOFajc7CFMghZAmOXZ6v62v	100%	Avira URL Cloud	malware	
http://www.rw-bau.com	0%	Avira URL Cloud	safe	
http://www.yh78898.comwww.363ww.topF7L99l=8qpwJ	0%	Avira URL Cloud	safe	
http://www.luxgudonu.storewww.sowmedia.siteF7L99l=8qpwJ	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.on-smooth.com/d2a3/?F7L99l=8qpwJ&Mw=LnB6L7dnOzftoEr5UpUEPAqnd7gAmYo0E1h8Hr8XDrTV/RCVTRWGXzxgMAjKYD2ZiMi0DXBclY2V/N6w7Ub5K9/YRO3kcEW/Xg==	100%	Avira URL Cloud	malware	
http://www.versicherungsgott.com/d2a3/?F7L99l=8qpwJ&Mw=3fW4twhu5lX2LSkBcFVlWjxiVco4zHJfqjvATlwHU7q8puaymE5DWsW8adrpP96Z6UNtMOOwQnTRLGoNrAuAplzT11t8CH71vQ==	100%	Avira URL Cloud	malware	
http://www.staatslieden.biz	0%	Avira URL Cloud	safe	
http://www.getpay.life/d2a3/	100%	Avira URL Cloud	malware	
http://www.versicherungsgott.com	0%	Avira URL Cloud	safe	
http://www.fresnocap.comwww.vanguardfsm.comF7L99l=8qpwJ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.363ww.top	39.109.117.109	true	true		unknown
www.getpay.life	199.192.28.110	true	true		unknown
www.espisys-technology.com	217.160.0.32	true	true		unknown
sowmedia.site	37.97.254.29	true	true		unknown
versicherungsgott.com	81.169.145.88	true	true		unknown
motherhoodinthegarden.com	50.87.195.203	true	true		unknown
www.yh78898.com	104.233.254.113	true	true		unknown
luxgudonu.store	46.23.69.44	true	true		unknown
on-smooth.com	113.52.135.193	true	true		unknown
www.luxgudonu.store	unknown	unknown	true		unknown
www.on-smooth.com	unknown	unknown	true		unknown
www.motherhoodinthegarden.com	unknown	unknown	true		unknown
www.versicherungsgott.com	unknown	unknown	true		unknown
www.sowmedia.site	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.sowmedia.site/d2a3/?F7L99l=8qpwJ&Mw=IIoejRloD0NPrvtjG56SffHGubt9bC7l7VozaPHGZoJbvkCik3wIcy97/aKLKqf+leC/SNQQ4bUyJkgTGWAXDnv4xxMA9hLjSw==	true	• Avira URL Cloud: malware	unknown
http://www.on-smooth.com/d2a3/	true	• Avira URL Cloud: malware	unknown
http://www.getpay.life/d2a3/?F7L99l=8qpwJ&Mw=VQWJd0zbMmoZh8qz35kMD56sFoyc6gTYso/MZ3BJ/Q0NuTQy4/HeuFqYJgzXZamkeMaLAEsOyVyJpFsiRVW3jp2QSfHijAqmyw==	true	• Avira URL Cloud: malware	unknown
http://www.luxgudonu.store/d2a3/	true	• Avira URL Cloud: malware	unknown
http://www.sowmedia.site/d2a3/	true	• Avira URL Cloud: malware	unknown
http://www.motherhoodinthegarden.com/d2a3/?Mw=cN5AEPknHvfgRR2crmYFAZMRCOFajc7CFMghZAmOXZ6v62v+A/wOpED6FQaDJ/tGFUb6Y91ZfjLOaofoM8qmjHtlEGMmc9VxCg==&F7L99l=8qpwJ	true	• Avira URL Cloud: malware	unknown
http://www.yh78898.com/d2a3/?Mw=/rn7tSorYChcOKKpyJYvjsebDE1EetOtUlfXV6ATVt8jMTNnk8PtnAR6Iam3VdBxJXQPah1uBiYgzGnhkXQp6MgBOVaGh7iMCA==&F7L99l=8qpwJ	true	• Avira URL Cloud: malware	unknown
http://www.espisys-technology.com/d2a3/	true	• Avira URL Cloud: malware	unknown
http://www.luxgudonu.store/d2a3/?Mw=OjO/noXVMTk40sLqqWNUhETz5fwNQfL3iZv4zuTHX4FsBRg0F7vbWW3nqcxNlOGl4ZCA660VFsqTMG20zBTe2NhxC9mrQabZ6Q==&F7L99l=8qpwJ	true	• Avira URL Cloud: malware	unknown
http://www.espisys-technology.com/d2a3/?Mw=HRt8t1hC6ylxzqu69JiO+2+wCg/lpDjUJ4ODvXLX3JGoHCx8OnZPShMSZXcaT/6Kc192JGOxG+z3HQLrZrJeLIMi1PhqwEBrHA==&F7L99l=8qpwJ	true	• Avira URL Cloud: malware	unknown
http://www.motherhoodinthegarden.com/d2a3/	true	• Avira URL Cloud: malware	unknown
http://www.yh78898.com/d2a3/	true	• Avira URL Cloud: malware	unknown
http://www.on-smooth.com/d2a3/?F7L99l=8qpwJ&Mw=LnB6L7dnOzftoEr5UpUEPAqnd7gAmYo0E1h8Hr8XDrTV/RCVTRWGXzxgMAjKYD2ZiMi0DXBclY2V/N6w7Ub5K9/YRO3kcEW/Xg==	true	• Avira URL Cloud: malware	unknown
http://www.versicherungsgott.com/d2a3/?F7L99l=8qpwJ&Mw=3fW4twhu5lX2LSkBcFVlWjxiVco4zHJfqjvATlwHU7q8puaymE5DWsW8adrpP96Z6UNtMOOwQnTRLGoNrAuAplzT11t8CH71vQ==	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.getpay.life/d2a3/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

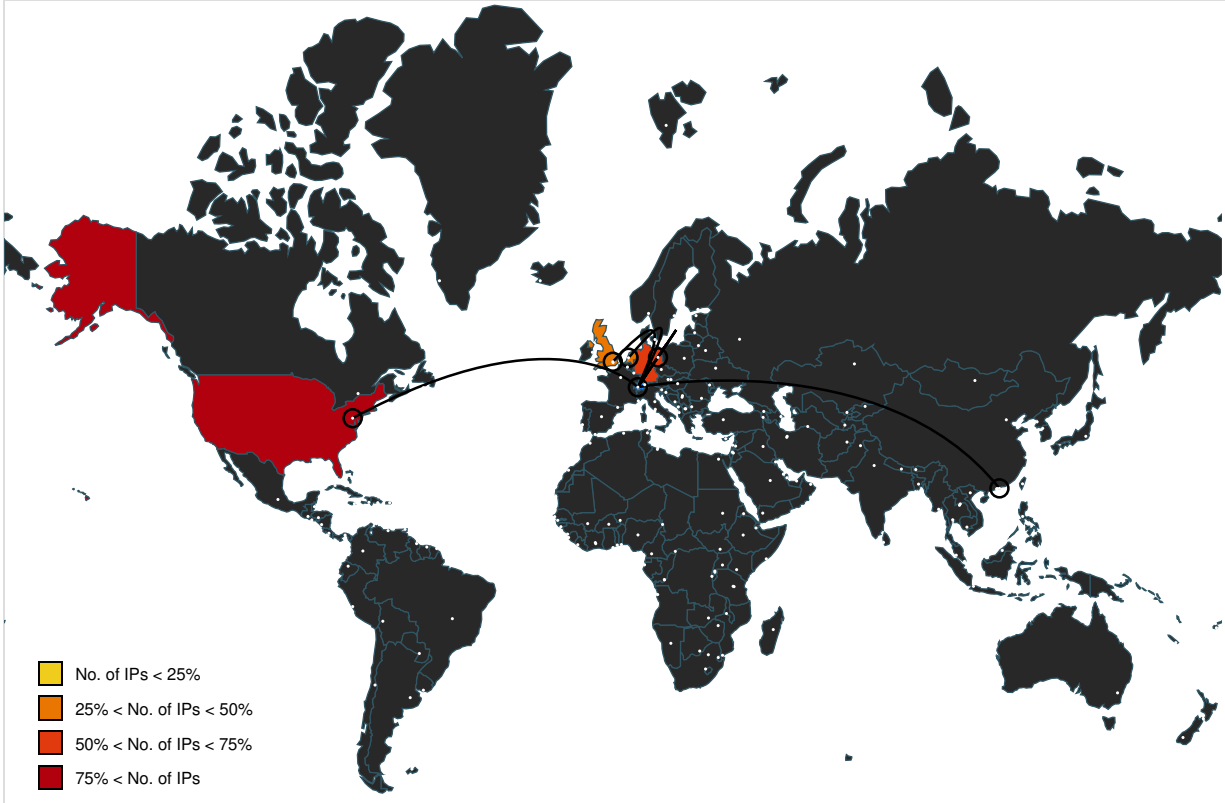
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	help.exe, 00000005.00000003.398334454.000000000069B000.00000004.00000020.00020000.00000000.sdmp, 35-7052c.5.dr	false		high
http://www.vanguardfsm.com/d2a3/	explorer.exe, 00000004.00000002.585709062.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.afzalhossainantor.com/d2a3/	explorer.exe, 00000004.00000002.585709062.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	35-7052c.5.dr	false		high
http://www.afzalhossainantor.comwww.staatslieden.bizF7L99l=8qpwJ	explorer.exe, 00000004.00000003.557927500.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.451404045.0000000005A2E000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://perldancer.org/	help.exe, 00000005.00000002.582591092.00000000D30000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.on-smooth.comwww.luxgudonu.storeF7L99l=8qpwJ	explorer.exe, 00000004.00000003.451404045.0000000005A2E000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.espisys-technology.comwww.on-smooth.comF7L99l=8qpwJ)	explorer.exe, 00000004.00000003.451404045.0000000005A2E000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://search.yahoo.com?fr=crmas_sfpf	help.exe, 00000005.00000003.398334454.000000000069B000.00000004.00000020.00020000.00000000.sdmp, 35-7052c.5.dr	false		high
http://www.363ww.top	explorer.exe, 00000004.00000003.557927500.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.451404045.0000000005A2E000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fresnocap.com/d2a3/	explorer.exe, 00000004.00000002.585709062.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sowmedia.site	explorer.exe, 00000004.00000003.557927500.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.451404045.0000000005A2E000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.staatslieden.biz/d2a3/	explorer.exe, 00000004.00000002.585709062.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.xefordbienhoa.com/d2a3/	explorer.exe, 00000004.00000002.585709062.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.363ww.top/d2a3/	explorer.exe, 00000004.00000002.585709062.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.staatslieden.bizwww.fresnocap.comF7L99l=8qpwJ	explorer.exe, 00000004.00000003.557927500.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.451404045.0000000005A2E000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.0000000005A9E000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.worldhortihealth.com	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.worldhortihealth.comwww.afzalhossainantor.com F7L99l=8qpwJ	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.espisys-technology.com	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rw-bau.com/d2a3/	explorer.exe, 00000004.00000002.58570906 2.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.afzalhossainantor.com	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.motherhoodinthegarden.com	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.vanguardfsm.com	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.on-smooth.com	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.yh78898.com	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fresnocap.com	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.worldhortihealth.com/d2a3/	explorer.exe, 00000004.00000002.58570906 2.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.rw-bau.comwww.worldhortihealth.comF7L99l=8qpwJ	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	help.exe, 00000005.00000003.398334454.00 0000000069B000.00000004.00000020.0002000 0.00000000.sdmp, 35-7052c.5.dr	false		high
http://www.getpay.life	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.363ww.topwww.rw-bau.comF7L99l=8qpwJ	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.vanguardfsm.comwww.xefordbienhoa.comF7L99l=8qpwJr	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.luxgudonu.store	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	35-7052c.5.dr	false		high
http://www.sowmedia.sitewww.yh78898.comF7L99l=8qpwJ	explorer.exe, 00000004.00000003.45140404 5.0000000005A2E000.00000004.00000001.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	help.exe, 00000005.00000003.398334454.00 0000000069B000.00000004.00000020.0002000 0.00000000.sdmp, 35-7052c.5.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	DHL_SHIPPING_DOCUMENT.exe	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	help.exe, 00000005.00000003.398334454.00 0000000069B000.00000004.00000020.0002000 0.00000000.sdmp, 35-7052c.5.dr	false		high
http://www.xefordbienhoa.com	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.versicherungsgott.com/d2a3/	explorer.exe, 00000004.00000002.58570906 2.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://ac.ecosia.org/autocomplete?q=	35-7052c.5.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	help.exe, 00000005.00000003.398334454.00 0000000069B000.00000004.00000020.0002000 0.00000000.sdmp, 35-7052c.5.dr	false		high
http://motherhoodinthegarden.com/d2a3/?Mw=cN5AEPknHvfgRR2crmYFAZMRCOFajc7CFMghZAmOXZ6v62v	help.exe, 00000005.00000002.582591092.00 000000036E8000.00000004.10000000.0004000 0.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.rw-bau.com	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.yh78898.comwww.363ww.topF7L99l=8qpwJ	explorer.exe, 00000004.00000003.45140404 5.0000000005A2E000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.luxgudonu.storewww.sowmedia.siteF7L99l=8qpwJ	explorer.exe, 00000004.00000003.45140404 5.0000000005A2E000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.staatslieden.biz	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	35-7052c.5.dr	false		high
http://www.versicherungsgott.com	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fresnocap.comwww.vanguardfsm.comF7L99l=8qpwJ	explorer.exe, 00000004.00000003.55792750 0.0000000005A9E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.451404045.0000000005A2E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.585709062.000000 0005A9E000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.87.195.203	motherhoodinthegarden.com	United States		46606	UNIFIEDLAYER-AS-1US	true
37.97.254.29	sowmedia.site	Netherlands		20857	TRANSIP-ASAmsterdamtheNetherlandsNL	true
46.23.69.44	luxgudonu.store	United Kingdom		13213	UK2NET-ASGB	true
217.160.0.32	www.espisys-technology.com	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
104.233.254.113	www.yh78898.com	United States		137443	ANCHGLOBAL-AS-APAnchnetAsiaLimitedHK	true
199.192.28.110	www.getpay.life	United States		22612	NAMECHEAP-NETUS	true
81.169.145.88	versicherungsgott.com	Germany		6724	STRATOSTRATOAGDE	true
113.52.135.193	on-smooth.com	Hong Kong		133380	LAYER-ASLayerstackLimitedHK	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830431
Start date and time:	2023-03-20 11:26:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	10
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:	DHL_SHIPPING_DOCUMENT.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@12/5@9/8
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 73.7% (good quality ratio 67.2%) • Quality average: 74% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:27:20	API Interceptor	506x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\35-7052c

Process:	C:\Windows\SysWOW64\help.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\eixfhzlwqd.exe

Process:	C:\Users\user\Desktop\DHL_SHIPPING_DOCUMENT.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	95744
Entropy (8bit):	6.2261764317924495
Encrypted:	false
SSDEEP:	1536:V0ZlV4KXc4OxQEsGZDmS+jtBaK/eRuZocSZUpxwkyBp+NnFsSW81kxgsWJjcdvbk:ed4KALsGZDN+x/yuZocSTkyBw9y8eASY

MD5:	52BD228566EE8DDE1E37102049937D69
SHA1:	B04481BE94D6AE60469226B33382139271D0A549
SHA-256:	82281D2CEDDE42F2564C5506652128954061C5208D5C59BA5237875A96FA38C8
SHA-512:	50350D708465FA51CA74050BEF07AF63EAEA9770E5A7A507BD62C4C4214EF6040CEC4FF3A3AAE6C87BD8FAE94D2999551825922A594FD7C22A99DC3BA2D2EE E4
Malicious:	**true**
Reputation:	low
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......7...s...s...s...8...y...8.......8...g......U......b......`...8...j...s...........r.......r...Richs...........PE..L......d...............!.....|......"............@..|k.......................................^................................]..@............................ ....text.............................. ..`.rdata...f.......h..................@..@.data...l............l..............@.. ....

C:\Users\user\AppData\Local\Temp\lfcykkdw.xwy

Process:	C:\Users\user\Desktop\DHL_SHIPPING_DOCUMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	5585
Entropy (8bit):	7.185773983646611
Encrypted:	false
SSDEEP:	96:Farc6oYV7OWg/DrYuTk2XO5oSwsBcWsYdfOQQSB+FCV76RdoT1uHDfRnTomtC8B3:FarcRQyJLhX1ShCvwjkMVWQ8JDtC8Mm9
MD5:	DD97B27860101C0989FEB9552ABBD29B
SHA1:	BC39A79D85EAE4EA267084C7253D18BF47398B87
SHA-256:	323E755E8354C0AD25CA44CF297BAC5A7ECAD26C1578953566D20DB95110F93D
SHA-512:	4343A67064EB05DD1493E052260577C2ECEDD9531DF9BAE9B0F8897210A011E9010817948EA9C56AF5487EBC95E5B728B16CD13C42F0BBCD34990156011B4DB
Malicious:	false
Reputation:	low
Preview:	.005m..f.F<...05o.:......?v>.3.3.<......M.knl.02a..c.E<...42c. ......4.D63.6.3.?.....E.gni.53P..805.p8.q?.2.8.u .a..beabo.H0..v..v.@3.`..i/7.p.6.t(2..g.}.u<..G-.0.3.h.f....w8L$.m.r .D;F...okc..m.;4.q.?.<@.4.0...m..u<f...@%.`4..D'd.O$..A5..=..<r..4M.knl.82a..Q..401ec.t4.M4...D;.D..d580..E9....E....3.u.mje.18e..`W..480.x<.p=.4.4.p-P..6.c.!....D%.|.eX. ....+..t..0....e.a..`beP..580.p=.t>.8.5.p,XE..Md.....M9..e...@4......F1..u.|c.....Lq.}<...v<+480.}<;.&<.>..r.^.q8F0....q.^.q8F0...^..M...3uc.....}<F...kloe.=8e...548.r...t..w.(058. q..v..l.0A..q..34.q.p.}...u.{.w....}.p013......u.L.4F".u..04.t.t.q..p.x.u....q.8580..Y...}..E.4D'.q..80.}.t.t..w.p.p...X+AK..M......v.ZXK.J.E.....}.]..O.F.....u.X_.M.M......H...X...K.D.....}. \&....A..B....G...P5..O.E..P....\...Y...K.E..a....B...].4.T.4.q0.p..q..~<1|..x.q.>.t&.u.|1,.t..w.pe..\...w.p..u.T.4.Q.0.}.;.q%..5M%.}.;.qm..tL9.}.5013.6.].5.u...K...P3480..u...dR0. m...D4...B358.q.0342.}.e......dX4R0]<048[3^2^8Z5..p...d.a..

C:\Users\user\AppData\Local\Temp\mvmtumtue.nvj

Process:	C:\Users\user\Desktop\DHL_SHIPPING_DOCUMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	210477
Entropy (8bit):	**7.998822054659917**
Encrypted:	**true**
SSDEEP:	3072:cY/mWoc3Tt/pj+DHK2cytCbzE2OYnxjbRQJvDRxeqVKwBYcQfG8LssuEXUhivzCe:3735G3cFzE2O8orRxeqVzbhjqzJWG
MD5:	33B5DE50DB0BB7122119E41416DE2573
SHA1:	9C557EB9394E46FAFE4ADCE3643666E74EE05974
SHA-256:	BA6A2D48F1BA514A8302F8E0B1A656D1243CFCDAF4B0408ED5CFCF598E129411
SHA-512:	CB1C24ACBBD4AA76CC295875A02282FDC8078CADEFE6CF3DC6EF804E037D2B00FE802E971FDB423BD4A8C160ADCD92F100506BFBCC8141CD9F48BE03EAF5 BA9E
Malicious:	false
Preview:	,.7l.z.....8.h./..+('.x.S.P.nyt....V....v...._.....'?G.u...b........r..d.6.^=..V..S......d'.:...O.E..6x.A.*...x........j...g0.....7...."tv...xNC.-n.B.......,.e;4.....\h@.Q...O*.r..f.Y.J........;./. O.O..=.j.S.. ....../...\:69..:%........0f.>...kz..........>......a.mn. .ny.....V.....J...._.....'?G.u.......< 0;8........(..:B.`T.Z....A..?...lBOu..,.Y...G.x......6........f{S1|Y.W.?.%o7...-..^......7y..md.J....\h@... _.*.r....HaS.\:.&..;./.qO5........^.......hN..\669.(.%..........f.....kz................a.m.P.nyt....V....v...._.....'?G.u.......< 0;8........(..:B.`T.Z....A..?...lBOu..,.Y...G.x......6........f{S1|Y.W.?.% o7...-..^......7y..md.J....\h@.Q...O*.r;.f.HeS.\.;&...;./.qO5.....j.........hN..\669.(.%..........f.....kz................a.m.P.nyt....V....v...._.....'?G.u.......< 0;8........(..:B.`T.Z....A..?...lBO u..,.Y...G.x......6........f{S1|Y.W.?.%o7...-..^......7y..md.J....\h@.Q...O*.r;.f.HeS.\.;&...;./.qO5.....j.........

C:\Users\user\AppData\Local\Temp\nsu5B23.tmp

Process:	C:\Users\user\Desktop\DHL_SHIPPING_DOCUMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	320868
Entropy (8bit):	7.627351926435029
Encrypted:	false
SSDEEP:	6144:D735G3cFzE2O8orRxeqVzbhjqzJWlaGKGsGZExocCk:Ds3cdoFxeW/aGKGsHG
MD5:	877CEC6DAEAB0B4B42C7AB77077772C5

SHA1:	90292679B84F9F1D096753521E4E87B0456D3DBA
SHA-256:	6EA18BC067BD0206119ECB96AA6BA6326CCF32FBAACA5691091AD8F9E46B4E6B
SHA-512:	A3A00F05D6C071146661BD24B6982103E5F940158D661C2FDFFE739AF08FFF51B80C871589489937FA2D1FACDE7A274E9853E3F8BAC4B79544B87FEF53739BEE
Malicious:	false
Preview:	V#.....,.....i...@.....".....V#.....*..... .....G.....j.....N..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	5.937523402259023
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:	DHL_SHIPPING_DOCUMENT.exe
File size:	730562
MD5:	04f5c33c1d3f795872b58f8c3922b49e
SHA1:	3db181379815210d6fb0491d9660ddefff263224
SHA256:	c0fee78265aef8793cb49690cc68fdf3debb84ab529bd59a2883a0c63ee0a6f5
SHA512:	f91d065389d15ccc22ac765b9432fc7df44b6141618ae902fe8179eb2311a85e31796b87e15550d2240db835486ef8f5084be00cb71ed9dec9ff9b9d4af2c110
SSDEEP:	12288:4YGGr4VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVHdx7OkVaa3bIsYyPouzayEtiQ:4Yed5ODdCPXzHE4Q
TLSH:	D5F44AE1D68484E9FC6A4B76A8339C3A15677D7EB9B4601D661EB6312B732C30077C0B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	71915e442028d505

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
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:	0x614F9B1F [Sat Sep 25 21:56:47 2021 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:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp

Instruction
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FB81882765Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FB81882762Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0x6a3b8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
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	0x8000	0x2b0	.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	0x6676	0x6800	False	0.6568134014423077	data	6.4174599871908855	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.141066817170598	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.110582127654237	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3b000	0x6a3b8	0x6a400	False	0.1916015625	data	3.688576847107456	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b358	0x42028	Device independent bitmap graphic, 256 x 512 x 32, image size 262144	English	United States
RT_ICON	0x7d380	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0x8dba8	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States
RT_ICON	0x97050	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736	English	United States
RT_ICON	0x9c4d8	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0xa0700	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0xa2ca8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0xa3d50	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States
RT_ICON	0xa46d8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_DIALOG	0xa4b40	0x100	data	English	United States
RT_DIALOG	0xa4c40	0x11c	data	English	United States
RT_DIALOG	0xa4d60	0x60	data	English	United States
RT_GROUP_ICON	0xa4dc0	0x84	data	English	United States
RT_VERSION	0xa4e48	0x230	data	English	United States
RT_MANIFEST	0xa5078	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

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

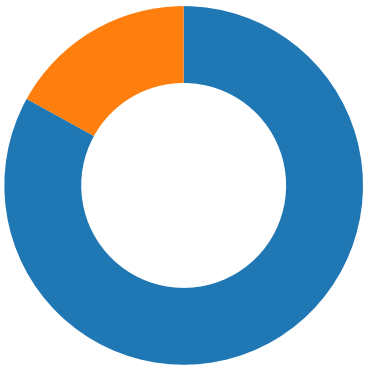
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.481.169.145.8849695802031412 03/20/23-11:27:41.124513	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49695	80	192.168.2.4	81.169.145.88
192.168.2.4104.233.254.11349709802031449 03/20/23-11:28:53.219959	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49709	80	192.168.2.4	104.233.254.113
192.168.2.4113.52.135.19349703802031453 03/20/23-11:28:29.350188	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49703	80	192.168.2.4	113.52.135.193
192.168.2.4113.52.135.19349703802031412 03/20/23-11:28:29.350188	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49703	80	192.168.2.4	113.52.135.193
192.168.2.481.169.145.8849695802031453 03/20/23-11:27:41.124513	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49695	80	192.168.2.4	81.169.145.88
192.168.2.4199.192.28.11049699802031453 03/20/23-11:28:13.420032	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49699	80	192.168.2.4	199.192.28.110
192.168.2.48.8.8.8.860686532023883 03/20/23-11:29:11.441798	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	60686	53	192.168.2.4	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.481.169.145.88 49695802031449 03/20/23-11:27:41.124513	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49695	80	192.168.2.4	81.169.145.88
192.168.2.446.23.69.4449 705802031412 03/20/23-11:28:37.254660	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49705	80	192.168.2.4	46.23.69.44
192.168.2.4199.192.28.11 049699802031412 03/20/23-11:28:13.420032	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49699	80	192.168.2.4	199.192.28.110
192.168.2.4113.52.135.19 349703802031449 03/20/23-11:28:29.350188	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49703	80	192.168.2.4	113.52.135.193
192.168.2.446.23.69.4449 705802031453 03/20/23-11:28:37.254660	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49705	80	192.168.2.4	46.23.69.44
192.168.2.4104.233.254.1 1349709802031453 03/20/23-11:28:53.219959	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49709	80	192.168.2.4	104.233.254.113
192.168.2.446.23.69.4449 705802031449 03/20/23-11:28:37.254660	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49705	80	192.168.2.4	46.23.69.44
192.168.2.4199.192.28.11 049699802031449 03/20/23-11:28:13.420032	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49699	80	192.168.2.4	199.192.28.110
192.168.2.4104.233.254.1 1349709802031412 03/20/23-11:28:53.219959	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49709	80	192.168.2.4	104.233.254.113

Network Port Distribution



Total Packets: 53

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:27:41.103671074 CET	49695	80	192.168.2.4	81.169.145.88
Mar 20, 2023 11:27:41.124280930 CET	80	49695	81.169.145.88	192.168.2.4
Mar 20, 2023 11:27:41.124399900 CET	49695	80	192.168.2.4	81.169.145.88
Mar 20, 2023 11:27:41.124512911 CET	49695	80	192.168.2.4	81.169.145.88
Mar 20, 2023 11:27:41.144968033 CET	80	49695	81.169.145.88	192.168.2.4
Mar 20, 2023 11:27:41.146936893 CET	80	49695	81.169.145.88	192.168.2.4
Mar 20, 2023 11:27:41.147181034 CET	80	49695	81.169.145.88	192.168.2.4
Mar 20, 2023 11:27:41.148864031 CET	49695	80	192.168.2.4	81.169.145.88
Mar 20, 2023 11:27:41.154973984 CET	49695	80	192.168.2.4	81.169.145.88
Mar 20, 2023 11:27:41.174519062 CET	80	49695	81.169.145.88	192.168.2.4
Mar 20, 2023 11:27:51.205352068 CET	49696	80	192.168.2.4	50.87.195.203
Mar 20, 2023 11:27:51.390180111 CET	80	49696	50.87.195.203	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:27:51.390422106 CET	49696	80	192.168.2.4	50.87.195.203
Mar 20, 2023 11:27:51.390614033 CET	49696	80	192.168.2.4	50.87.195.203
Mar 20, 2023 11:27:51.575270891 CET	80	49696	50.87.195.203	192.168.2.4
Mar 20, 2023 11:27:51.819456100 CET	80	49696	50.87.195.203	192.168.2.4
Mar 20, 2023 11:27:51.819508076 CET	80	49696	50.87.195.203	192.168.2.4
Mar 20, 2023 11:27:51.819648027 CET	49696	80	192.168.2.4	50.87.195.203
Mar 20, 2023 11:27:52.892504930 CET	49696	80	192.168.2.4	50.87.195.203
Mar 20, 2023 11:27:53.909151077 CET	49697	80	192.168.2.4	50.87.195.203
Mar 20, 2023 11:27:54.093878984 CET	80	49697	50.87.195.203	192.168.2.4
Mar 20, 2023 11:27:54.098609924 CET	49697	80	192.168.2.4	50.87.195.203
Mar 20, 2023 11:27:54.098740101 CET	49697	80	192.168.2.4	50.87.195.203
Mar 20, 2023 11:27:54.283379078 CET	80	49697	50.87.195.203	192.168.2.4
Mar 20, 2023 11:27:54.881174088 CET	80	49697	50.87.195.203	192.168.2.4
Mar 20, 2023 11:27:54.923999071 CET	49697	80	192.168.2.4	50.87.195.203
Mar 20, 2023 11:28:04.891547918 CET	80	49697	50.87.195.203	192.168.2.4
Mar 20, 2023 11:28:04.891773939 CET	49697	80	192.168.2.4	50.87.195.203
Mar 20, 2023 11:28:04.906358957 CET	49697	80	192.168.2.4	50.87.195.203
Mar 20, 2023 11:28:05.090928078 CET	80	49697	50.87.195.203	192.168.2.4
Mar 20, 2023 11:28:09.970515013 CET	49698	80	192.168.2.4	199.192.28.110
Mar 20, 2023 11:28:10.138561010 CET	80	49698	199.192.28.110	192.168.2.4
Mar 20, 2023 11:28:10.139292955 CET	49698	80	192.168.2.4	199.192.28.110
Mar 20, 2023 11:28:10.139673948 CET	49698	80	192.168.2.4	199.192.28.110
Mar 20, 2023 11:28:10.307205915 CET	80	49698	199.192.28.110	192.168.2.4
Mar 20, 2023 11:28:10.410506964 CET	80	49698	199.192.28.110	192.168.2.4
Mar 20, 2023 11:28:10.410605907 CET	80	49698	199.192.28.110	192.168.2.4
Mar 20, 2023 11:28:10.410754919 CET	49698	80	192.168.2.4	199.192.28.110
Mar 20, 2023 11:28:11.960941076 CET	49698	80	192.168.2.4	199.192.28.110
Mar 20, 2023 11:28:13.250793934 CET	49699	80	192.168.2.4	199.192.28.110
Mar 20, 2023 11:28:13.418484926 CET	80	49699	199.192.28.110	192.168.2.4
Mar 20, 2023 11:28:13.419913054 CET	49699	80	192.168.2.4	199.192.28.110
Mar 20, 2023 11:28:13.420032024 CET	49699	80	192.168.2.4	199.192.28.110
Mar 20, 2023 11:28:13.587511063 CET	80	49699	199.192.28.110	192.168.2.4
Mar 20, 2023 11:28:13.697813988 CET	80	49699	199.192.28.110	192.168.2.4
Mar 20, 2023 11:28:13.697864056 CET	80	49699	199.192.28.110	192.168.2.4
Mar 20, 2023 11:28:13.698159933 CET	49699	80	192.168.2.4	199.192.28.110
Mar 20, 2023 11:28:13.698652983 CET	49699	80	192.168.2.4	199.192.28.110
Mar 20, 2023 11:28:13.866168022 CET	80	49699	199.192.28.110	192.168.2.4
Mar 20, 2023 11:28:18.763628960 CET	49700	80	192.168.2.4	217.160.0.32
Mar 20, 2023 11:28:18.786365986 CET	80	49700	217.160.0.32	192.168.2.4
Mar 20, 2023 11:28:18.788248062 CET	49700	80	192.168.2.4	217.160.0.32
Mar 20, 2023 11:28:18.788455009 CET	49700	80	192.168.2.4	217.160.0.32
Mar 20, 2023 11:28:18.811074972 CET	80	49700	217.160.0.32	192.168.2.4
Mar 20, 2023 11:28:18.816607952 CET	80	49700	217.160.0.32	192.168.2.4
Mar 20, 2023 11:28:18.816633940 CET	80	49700	217.160.0.32	192.168.2.4
Mar 20, 2023 11:28:18.816771984 CET	49700	80	192.168.2.4	217.160.0.32
Mar 20, 2023 11:28:20.301188946 CET	49700	80	192.168.2.4	217.160.0.32
Mar 20, 2023 11:28:21.318445921 CET	49701	80	192.168.2.4	217.160.0.32
Mar 20, 2023 11:28:21.341140985 CET	80	49701	217.160.0.32	192.168.2.4
Mar 20, 2023 11:28:21.341253996 CET	49701	80	192.168.2.4	217.160.0.32
Mar 20, 2023 11:28:21.341408014 CET	49701	80	192.168.2.4	217.160.0.32
Mar 20, 2023 11:28:21.367325068 CET	80	49701	217.160.0.32	192.168.2.4
Mar 20, 2023 11:28:21.374430895 CET	80	49701	217.160.0.32	192.168.2.4
Mar 20, 2023 11:28:21.374499083 CET	80	49701	217.160.0.32	192.168.2.4
Mar 20, 2023 11:28:21.374721050 CET	49701	80	192.168.2.4	217.160.0.32
Mar 20, 2023 11:28:21.375020027 CET	49701	80	192.168.2.4	217.160.0.32
Mar 20, 2023 11:28:21.397676945 CET	80	49701	217.160.0.32	192.168.2.4
Mar 20, 2023 11:28:26.419450998 CET	49702	80	192.168.2.4	113.52.135.193
Mar 20, 2023 11:28:26.623085022 CET	80	49702	113.52.135.193	192.168.2.4
Mar 20, 2023 11:28:26.623271942 CET	49702	80	192.168.2.4	113.52.135.193

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:28:26.623491049 CET	49702	80	192.168.2.4	113.52.135.193
Mar 20, 2023 11:28:26.827152014 CET	80	49702	113.52.135.193	192.168.2.4
Mar 20, 2023 11:28:26.827330112 CET	80	49702	113.52.135.193	192.168.2.4
Mar 20, 2023 11:28:26.827353001 CET	80	49702	113.52.135.193	192.168.2.4
Mar 20, 2023 11:28:26.827411890 CET	49702	80	192.168.2.4	113.52.135.193
Mar 20, 2023 11:28:28.130045891 CET	49702	80	192.168.2.4	113.52.135.193
Mar 20, 2023 11:28:29.146186113 CET	49703	80	192.168.2.4	113.52.135.193
Mar 20, 2023 11:28:29.349519014 CET	80	49703	113.52.135.193	192.168.2.4
Mar 20, 2023 11:28:29.349842072 CET	49703	80	192.168.2.4	113.52.135.193
Mar 20, 2023 11:28:29.350188017 CET	49703	80	192.168.2.4	113.52.135.193
Mar 20, 2023 11:28:29.553194046 CET	80	49703	113.52.135.193	192.168.2.4
Mar 20, 2023 11:28:29.553384066 CET	80	49703	113.52.135.193	192.168.2.4
Mar 20, 2023 11:28:29.553415060 CET	80	49703	113.52.135.193	192.168.2.4
Mar 20, 2023 11:28:29.553632975 CET	49703	80	192.168.2.4	113.52.135.193
Mar 20, 2023 11:28:29.553765059 CET	49703	80	192.168.2.4	113.52.135.193
Mar 20, 2023 11:28:29.756839037 CET	80	49703	113.52.135.193	192.168.2.4
Mar 20, 2023 11:28:34.640928030 CET	49704	80	192.168.2.4	46.23.69.44
Mar 20, 2023 11:28:34.668648958 CET	80	49704	46.23.69.44	192.168.2.4
Mar 20, 2023 11:28:34.668832064 CET	49704	80	192.168.2.4	46.23.69.44
Mar 20, 2023 11:28:34.700421095 CET	49704	80	192.168.2.4	46.23.69.44
Mar 20, 2023 11:28:34.728221893 CET	80	49704	46.23.69.44	192.168.2.4
Mar 20, 2023 11:28:34.733566046 CET	80	49704	46.23.69.44	192.168.2.4
Mar 20, 2023 11:28:34.733638048 CET	80	49704	46.23.69.44	192.168.2.4
Mar 20, 2023 11:28:34.733741999 CET	49704	80	192.168.2.4	46.23.69.44
Mar 20, 2023 11:28:36.209743023 CET	49704	80	192.168.2.4	46.23.69.44
Mar 20, 2023 11:28:37.225220919 CET	49705	80	192.168.2.4	46.23.69.44
Mar 20, 2023 11:28:37.253339052 CET	80	49705	46.23.69.44	192.168.2.4
Mar 20, 2023 11:28:37.253623009 CET	49705	80	192.168.2.4	46.23.69.44
Mar 20, 2023 11:28:37.254659891 CET	49705	80	192.168.2.4	46.23.69.44

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:27:41.073858976 CET	56572	53	192.168.2.4	8.8.8.8
Mar 20, 2023 11:27:41.092590094 CET	53	56572	8.8.8.8	192.168.2.4
Mar 20, 2023 11:27:51.185725927 CET	50911	53	192.168.2.4	8.8.8.8
Mar 20, 2023 11:27:51.203722954 CET	53	50911	8.8.8.8	192.168.2.4
Mar 20, 2023 11:28:09.934638023 CET	59683	53	192.168.2.4	8.8.8.8
Mar 20, 2023 11:28:09.969444990 CET	53	59683	8.8.8.8	192.168.2.4
Mar 20, 2023 11:28:18.710139036 CET	64167	53	192.168.2.4	8.8.8.8
Mar 20, 2023 11:28:18.761651993 CET	53	64167	8.8.8.8	192.168.2.4
Mar 20, 2023 11:28:26.393294096 CET	58565	53	192.168.2.4	8.8.8.8
Mar 20, 2023 11:28:26.418127060 CET	53	58565	8.8.8.8	192.168.2.4
Mar 20, 2023 11:28:34.576559067 CET	52239	53	192.168.2.4	8.8.8.8
Mar 20, 2023 11:28:34.612303972 CET	53	52239	8.8.8.8	192.168.2.4
Mar 20, 2023 11:28:42.362283945 CET	56807	53	192.168.2.4	8.8.8.8
Mar 20, 2023 11:28:42.404155016 CET	53	56807	8.8.8.8	192.168.2.4
Mar 20, 2023 11:28:50.041943073 CET	61007	53	192.168.2.4	8.8.8.8
Mar 20, 2023 11:28:50.077486038 CET	53	61007	8.8.8.8	192.168.2.4
Mar 20, 2023 11:29:11.441797972 CET	60686	53	192.168.2.4	8.8.8.8
Mar 20, 2023 11:29:12.049052954 CET	53	60686	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 11:27:41.073858976 CET	192.168.2.4	8.8.8.8	0x8ccb	Standard query (0)	www.versicherungsgott.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:27:51.185725927 CET	192.168.2.4	8.8.8.8	0x8af	Standard query (0)	www.motherhoodintheg arden.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 11:28:09.934638023 CET	192.168.2.4	8.8.8.8	0x77a1	Standard query (0)	www.getpay.life	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:28:18.710139036 CET	192.168.2.4	8.8.8.8	0x8ebc	Standard query (0)	www.espisys-technology.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:28:26.393294096 CET	192.168.2.4	8.8.8.8	0x6924	Standard query (0)	www.on-smooth.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:28:34.576559067 CET	192.168.2.4	8.8.8.8	0x759e	Standard query (0)	www.luxgudonu.store	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:28:42.362283945 CET	192.168.2.4	8.8.8.8	0x5976	Standard query (0)	www.sowmedia.site	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:28:50.041943073 CET	192.168.2.4	8.8.8.8	0x9a04	Standard query (0)	www.yh78898.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:11.441797972 CET	192.168.2.4	8.8.8.8	0x8ddd	Standard query (0)	www.363ww.top	A (IP address)	IN (0x0001)	false

DNS Answers

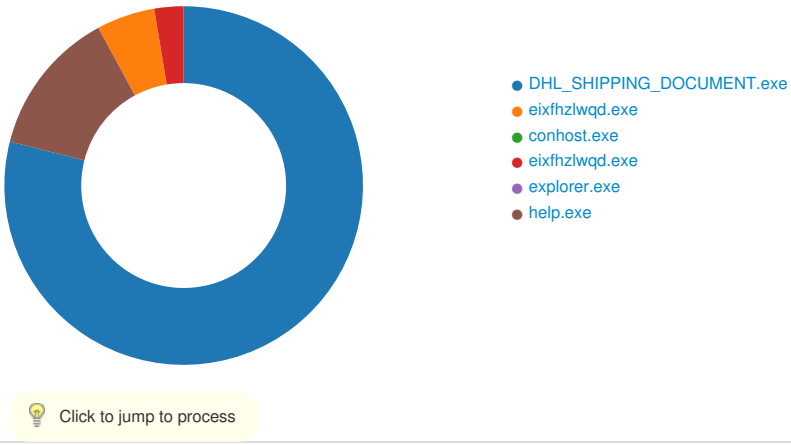
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 11:27:41.092590094 CET	8.8.8.8	192.168.2.4	0x8ccb	No error (0)	www.versicherungsgott.com	versicherungsgott.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:27:41.092590094 CET	8.8.8.8	192.168.2.4	0x8ccb	No error (0)	versicherungsgott.com		81.169.145.88	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:27:51.203722954 CET	8.8.8.8	192.168.2.4	0x8af	No error (0)	www.motherhoodinthegarden.com	motherhoodinthegarden.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:27:51.203722954 CET	8.8.8.8	192.168.2.4	0x8af	No error (0)	motherhoodinthegarden.com		50.87.195.203	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:28:09.969444990 CET	8.8.8.8	192.168.2.4	0x77a1	No error (0)	www.getpay.life		199.192.28.110	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:28:18.761651993 CET	8.8.8.8	192.168.2.4	0x8ebc	No error (0)	www.espisys-technology.com		217.160.0.32	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:28:26.418127060 CET	8.8.8.8	192.168.2.4	0x6924	No error (0)	www.on-smooth.com	on-smooth.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:28:26.418127060 CET	8.8.8.8	192.168.2.4	0x6924	No error (0)	on-smooth.com		113.52.135.193	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:28:34.612303972 CET	8.8.8.8	192.168.2.4	0x759e	No error (0)	www.luxgudonu.store	luxgudonu.store		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:28:34.612303972 CET	8.8.8.8	192.168.2.4	0x759e	No error (0)	luxgudonu.store		46.23.69.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:28:42.404155016 CET	8.8.8.8	192.168.2.4	0x5976	No error (0)	www.sowmedia.site	sowmedia.site		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:28:42.404155016 CET	8.8.8.8	192.168.2.4	0x5976	No error (0)	sowmedia.site		37.97.254.29	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:28:50.077486038 CET	8.8.8.8	192.168.2.4	0x9a04	No error (0)	www.yh78898.com		104.233.254.113	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:12.049052954 CET	8.8.8.8	192.168.2.4	0x8ddd	No error (0)	www.363ww.top		39.109.117.109	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.versicherungsgott.com
- www.motherhoodinthegarden.com
- www.getpay.life
- www.espisys-technology.com
- www.on-smooth.com
- www.luxgudonu.store
- www.sowmedia.site
- www.yh78898.com

Statistics

Behavior



System Behavior

Analysis Process: DHL_SHIPPING_DOCUMENT.exe PID: **3092**, Parent PID: **3528**

General	
Target ID:	0
Start time:	11:27:07
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\DHL_SHIPPING_DOCUMENT.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL_SHIPPING_DOCUMENT.exe
Imagebase:	0x400000
File size:	730562 bytes
MD5 hash:	04F5C33C1D3F795872B58F8C3922B49E
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: eixfhzlwqd.exe PID: **2040**, Parent PID: **3092**

General

Target ID:	1
Start time:	11:27:07
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\eixfhzlwqd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\eixfhzlwqd.exe" C:\Users\user\AppData\Local\Temp\lfcykkdw.xwy
Imagebase:	0x400000
File size:	95744 bytes
MD5 hash:	52BD228566EE8DDE1E37102049937D69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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:\Users\user\AppData\Local\Temp\lfcykkdw.xwy	unknown	4096	success or wait	1	407824	ReadFile
C:\Users\user\AppData\Local\Temp\lfcykkdw.xwy	unknown	4096	success or wait	1	407824	ReadFile

Analysis Process: conhost.exe PID: **2168**, Parent PID: **2040**

General

Target ID:	2
Start time:	11:27:07
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: eixfhzlwqd.exe PID: **856**, Parent PID: **2040**

General

Target ID:	3
Start time:	11:27:08
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\eixfhzlwqd.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\eixfhzlwqd.exe

Imagebase:	0x400000
File size:	95744 bytes
MD5 hash:	52BD228566EE8DDE1E37102049937D69
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: 00000003.00000002.357493625.0000000000900000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.357493625.0000000000900000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.357493625.0000000000900000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.357465550.00000000008D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.357465550.00000000008D0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.357465550.00000000008D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.357347266.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.357347266.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.357347266.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41E59A	NtReadFile

Analysis Process: explorer.exe PID: **3528**, Parent PID: **856**

General

Target ID:	4
Start time:	11:27:13
Start date:	20/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff618f60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	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	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: help.exe PID: 2224, Parent PID: 3528

General

Target ID:	5
Start time:	11:27:25
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0x3b0000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
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: 00000005.00000002.581265823.0000000002C00000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.581265823.0000000002C00000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.581265823.0000000002C00000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000005.00000002.581153913.0000000002900000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.581153913.0000000002900000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.581153913.0000000002900000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000005.00000002.579126869.0000000000510000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.579126869.0000000000510000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.579126869.0000000000510000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
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\AppData\Local\Temp\eixfhzlwqd.exe	success or wait	1	2C1C827	NtDeleteFile
C:\Users\user\AppData\Local\Temp\35-7052c	object name not found	1	2C1C827	NtDeleteFile
C:\Users\user\AppData\Local\Temp\35-7052c	sharing violation	1	2C1C827	NtDeleteFile
C:\Users\user\AppData\Local\Temp\35-7052c	sharing violation	1	2C1C827	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	1622408	success or wait	1	2C1C7F7	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Disassembly

No disassembly