ID: 830322
Sample Name:
OUTSTANDING_PAYMENT.exe
Cookbook: default.jbs
Time: 09:06:45
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

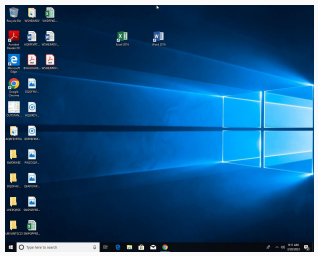
Windows Analysis Report

OUTSTANDING_PAYMENT.exe

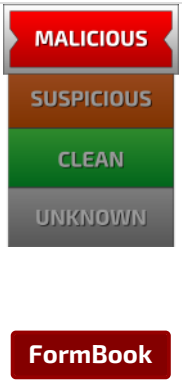
Overview

General Information

Sample Name:	OUTSTANDING_PAYMENT.exe
Analysis ID:	830322
MD5:	4832e17c1f684..
SHA1:	d7ad36c7bee5…
SHA256:	d0ac15eeb53f6..
Tags:	exe Formbook
Infos:	



Detection



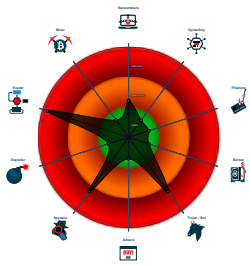
FormBook

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…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- 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…

Classification



Process Tree

- **System is w10x64**
- OUTSTANDING_PAYMENT.exe (PID: 4224 cmdline: C:\Users\user\Desktop\OUTSTANDING_PAYMENT.exe MD5: 4832E17C1F6841AEE2E1984A429ED946)
  - qhcqh.exe (PID: 5156 cmdline: "C:\Users\user\AppData\Local\Temp\qhcqh.exe" C:\Users\user\AppData\Local\Temp\bpgvtpbkoxw.z MD5: 41C9E29A7ED3640682A0003BE2DF4D93)
    - qhcqh.exe (PID: 5124 cmdline: C:\Users\user\AppData\Local\Temp\qhcqh.exe MD5: 41C9E29A7ED3640682A0003BE2DF4D93)
      - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - rundll32.exe (PID: 4948 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **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
0000000D.00000002.777131854.0000000000C40000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
0000000D.00000002.777131854.0000000000C40000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1f0d0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xae3f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x182f7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
0000000D.00000002.777131854.0000000000C40000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x180f5:$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:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xaa0a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x16ddc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1de87:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ee3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.303713415.0000000000F30000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000002.00000002.303713415.0000000000F30000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1f0d0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xae3f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x182f7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Click to see the 13 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.qhcqh.exe.400000.0.raw.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
2.2.qhcqh.exe.400000.0.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x20eb3:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xcc22:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1a0da:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
2.2.qhcqh.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x19ed8:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x19974:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x19fda:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1a152:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xc7ed:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x18bbf:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1fc6a:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x20c1d:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.qhcqh.exe.400000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
2.2.qhcqh.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x200b3:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xbe22:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x192da:$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: 192.168.2.3 - Destination IP: 185.151.30.181

Timestamp:	192.168.2.3185.151.30.18149711802031453 03/20/23-09:09:32.876293
SID:	2031453
Source Port:	49711
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 192.64.116.162

Timestamp:	192.168.2.3192.64.116.16249717802031449 03/20/23-09:09:54.051496
SID:	2031449
Source Port:	49717
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 5.181.216.141

Timestamp:	192.168.2.35.181.216.14149705802031449 03/20/23-09:09:09.878629
SID:	2031449
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 192.64.116.162

Timestamp:	192.168.2.3192.64.116.16249717802031412 03/20/23-09:09:54.051496
SID:	2031412
Source Port:	49717
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 5.181.216.141

Timestamp:	192.168.2.35.181.216.14149705802031453 03/20/23-09:09:09.878629
SID:	2031453
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 192.64.116.162

Timestamp:	192.168.2.3192.64.116.16249717802031453 03/20/23-09:09:54.051496
SID:	2031453
Source Port:	49717
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 185.151.30.181

Timestamp:	192.168.2.3185.151.30.18149711802031449 03/20/23-09:09:32.876293
SID:	2031449
Source Port:	49711
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.851139532023883 03/20/23-09:09:48.362224
SID:	2023883
Source Port:	51139
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 5.181.216.141	−
Timestamp:	192.168.2.35.181.216.14149705802031412 03/20/23-09:09:09.878629
SID:	2031412
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 185.151.30.181	−
Timestamp:	192.168.2.3185.151.30.18149711802031412 03/20/23-09:09:32.876293
SID:	2031412
Source Port:	49711
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
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample

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
- Sample has a suspicious name (potential lure to open the executable)

Malware Analysis System Evasion

- Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

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)

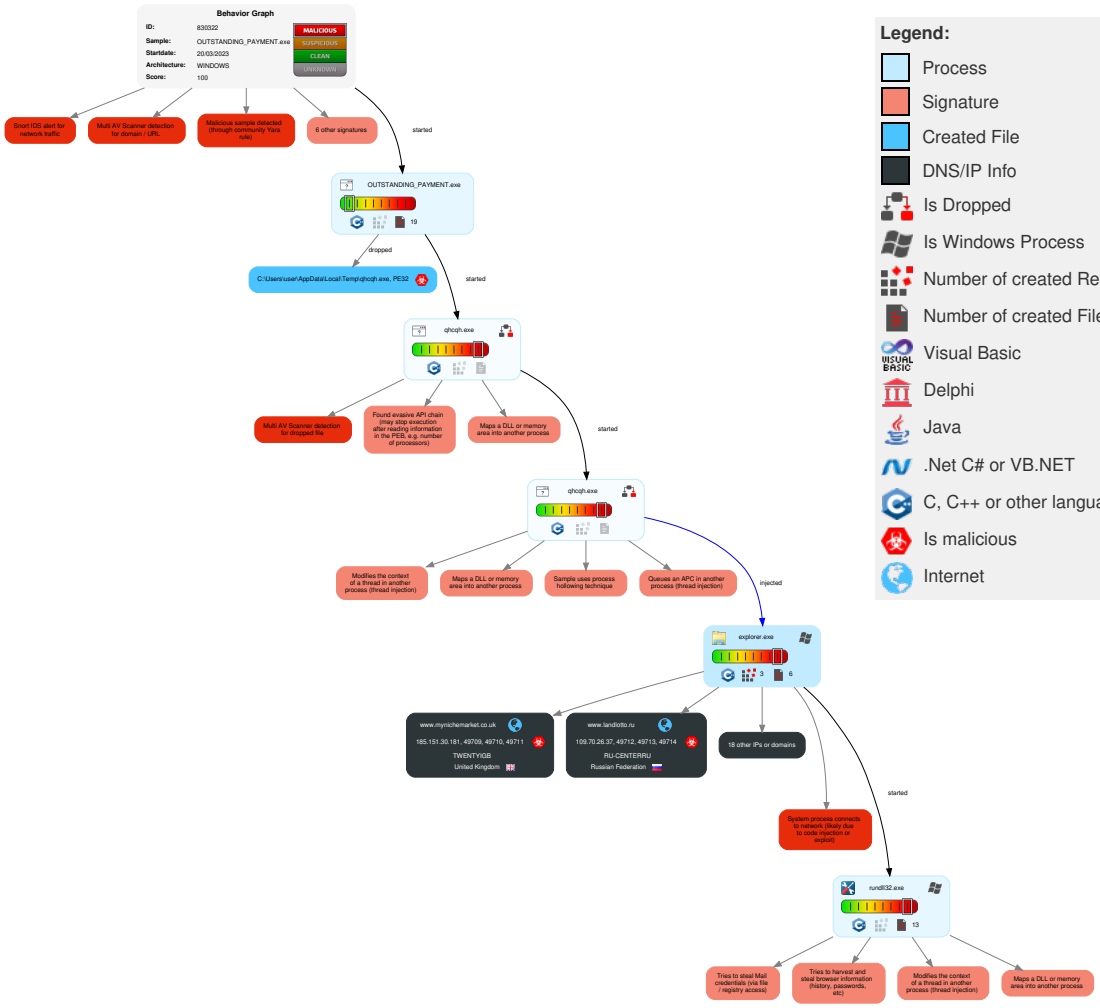
Remote Access Functionality

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 2 Native API	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	1 Shared Modules	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 Software Packing	Security Account Manager	1 6 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)	1 Masquerading	NTDS	1 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	2 Virtualization/Sandbox Evasion	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	1 Access Token Manipulation	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	5 1 2 Process Injection	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	1 Rundll32	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

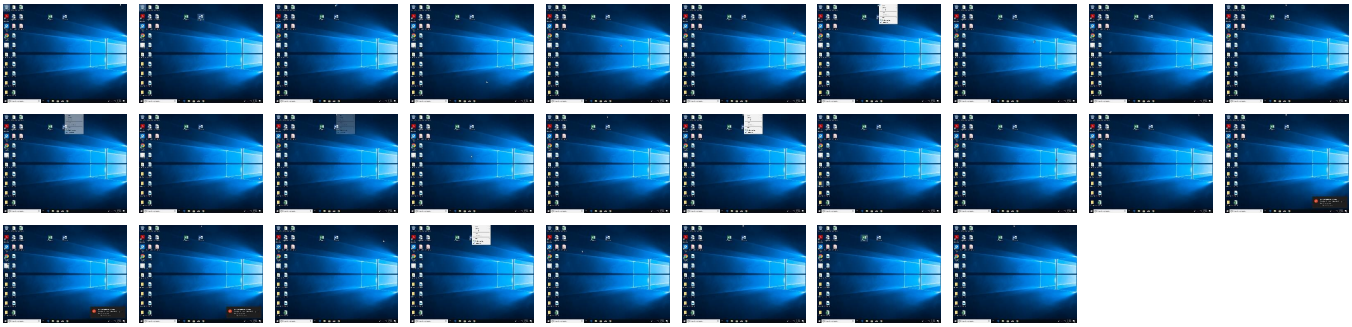
Behavior Graph



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
OUTSTANDING_PAYMENT.exe	72%	ReversingLabs	Win32.Trojan.Leoncem	
OUTSTANDING_PAYMENT.exe	72%	Virustotal		Browse
OUTSTANDING_PAYMENT.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\qhcqh.exe	51%	ReversingLabs	Win32.Trojan.Tnega	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.rundll32.exe.4f53814.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.2.qhcqh.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.qhcqh.exe.980000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
13.2.rundll32.exe.30544f8.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.OUTSTANDING_PAYMENT.exe.28ebe10.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
dirdikyepedia.com	9%	Virustotal		Browse
allison2patrick.online	6%	Virustotal		Browse
www.gorwly.top	3%	Virustotal		Browse
glb-mobility.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.karlscurry.co.uk/0oqq/?ICHyvj5=/wt4JY4W3l+DpUlEm50j75nj98dXbWC1Jam/Xyx5jEHfTH+E1ePLpr1g8eshFzfVb4/25r9KS6bvXq1NrjcG6ioEuox+na//qA==&qt9TW=60_ljPJoqo6d2	0%	Avira URL Cloud	safe	
http://www.hudsonandbailey.uk	0%	Avira URL Cloud	safe	
http://www.fanversewallet.com/0oqq/qt9TW=60_ljPJoqo6d2	100%	Avira URL Cloud	malware	
http://www.g2fm.co.uk/0oqq/?ICHyvj5=mrlIldvmtur7mkt/rPLDu6zCaW7pq/FSfCj+/pKGfo5WkxwlgZbXON4VpSp8r5ryJHF0PKr2dhp3lAxH7D3LGu58YX7EcXy0Ow==&qt9TW=60_ljPJoqo6d2	0%	Avira URL Cloud	safe	
http://www.karlscurry.co.uk/0oqq/	0%	Avira URL Cloud	safe	
http://www.dirdikyepedia.com/0oqq/?qt9TW=60_ljPJoqo6d2&ICHyvj5=PRQC41TmcI9bvUwILfW251fDqJjDWsulERfzYnlMN4HgHjqryKViH0BFVe/NE6lVKE81tYv052d7aHxIDF6KpDCDELCE9pYayA==	100%	Avira URL Cloud	malware	
http://www.ty23vip.com/0oqq/qt9TW=60_ljPJoqo6d2	0%	Avira URL Cloud	safe	
http://www.fanversewallet.com/0oqq/?qt9TW=60_ljPJoqo6d2&ICHyvj5=Yikzj9CFq5vqEc2vNlbzxihd8s3DrMcGxuzxagcCy5X6CzTVIy/a14lT5vlHy5RQ1Z7Px0aDVF6+DD/SwGM+3qMYWad3MBh6/g==	100%	Avira URL Cloud	malware	
http://www.thelastwill.net/0oqq/	0%	Avira URL Cloud	safe	
http://www.mynichemarket.co.uk/0oqq/	0%	Avira URL Cloud	safe	
http://www.glb-mobility.com	0%	Avira URL Cloud	safe	
http://www.thelastwill.net/0oqq/qt9TW=60_ljPJoqo6d2	0%	Avira URL Cloud	safe	
http://www.gorwly.top/0oqq/qt9TW=60_ljPJoqo6d2	100%	Avira URL Cloud	malware	
http://www.brennmansoluciones.com	0%	Avira URL Cloud	safe	
http://www.glb-mobility.com/0oqq/?ICHyvj5=L0mSdT0ooJoC+WTAff+ZGzvWM+chwjv3Dy0WIeNakQkmi/ixITEkKFHCL0Q8UzGKK5QpSY+AVQ3lyxgaFTuxUTcmK0rro2dEnw==&qt9TW=60_ljPJoqo6d2	0%	Avira URL Cloud	safe	
http://www.allison2patrick.online/0oqq/	100%	Avira URL Cloud	malware	
http://www.karlscurry.co.uk	0%	Avira URL Cloud	safe	
http://www.glb-mobility.com/0oqq/	0%	Avira URL Cloud	safe	
http://www.g2fm.co.uk/0oqq/	0%	Avira URL Cloud	safe	
http://www.thelastwill.net	0%	Avira URL Cloud	safe	
http://www.sexopornoxx.store/0oqq/	100%	Avira URL Cloud	malware	
http://www.thebang.sbs	0%	Avira URL Cloud	safe	
http://www.ty23vip.com/0oqq/	0%	Avira URL Cloud	safe	
http://www.fanversewallet.com/0oqq/	100%	Avira URL Cloud	malware	
http://www.ketoibabal.cyou/0oqq/	0%	Avira URL Cloud	safe	
http://www.ty23vip.com	0%	Avira URL Cloud	safe	
http://www.landlotto.ru/0oqq/	100%	Avira URL Cloud	malware	
http://https://tiao2022.vip:12306/?u=	0%	Avira URL Cloud	safe	
http://www.gorwly.top	100%	Avira URL Cloud	malware	
http://www.mynichemarket.co.uk	0%	Avira URL Cloud	safe	
http://www.dirdikyepedia.com/0oqq/	100%	Avira URL Cloud	malware	
http://www.themssterofssuepnse.rest	100%	Avira URL Cloud	malware	
http://www.karlscurry.co.uk/0oqq/qt9TW=60_ljPJoqo6d2	0%	Avira URL Cloud	safe	
http://www.fanversewallet.com	100%	Avira URL Cloud	malware	
http://www.allison2patrick.online	0%	Avira URL Cloud	safe	
http://www.brennmansoluciones.com/0oqq/qt9TW=60_ljPJoqo6d2	0%	Avira URL Cloud	safe	
http://www.leewanyam.com/0oqq/polb=tYchV8	0%	Avira URL Cloud	safe	
http://www.brennmansoluciones.com/0oqq/	0%	Avira URL Cloud	safe	
http://www.gorwly.top/0oqq/	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://www.glb-mobility.com/0oqq/qt9TW=60_ljPJoqo6d2	0%	Avira URL Cloud	safe	
http://www.brennmansoluciones.com/0oqq/polb=tYchV8	0%	Avira URL Cloud	safe	
http://www.mynichemarket.co.uk/0oqq/?qt9TW=60_ljPJoqo6d2&ICHyvj5=bPiAqCboB3xuuR9jBd2d5kx4kdlhaJ3zm41TCptSu6l9zHYblFc2aOuFx07ZodW9tNkBHFGkWniHGpAg445zXTdag0fAcLuZfA==	0%	Avira URL Cloud	safe	
http://www.leewanyam.com/0oqq/	0%	Avira URL Cloud	safe	
http://https://www.fasthosts.co.uk/domain-names/search/?domain=$	0%	Avira URL Cloud	safe	
http://https://fasthosts.co.uk/	0%	Avira URL Cloud	safe	
http://www.themssterofssuepnse.rest/0oqq/	100%	Avira URL Cloud	malware	
http://www.landlotto.ru/0oqq/qt9TW=60_ljPJoqo6d2	100%	Avira URL Cloud	malware	
http://www.mynichemarket.co.uk/0oqq/qt9TW=60_ljPJoqo6d2	0%	Avira URL Cloud	safe	
http://www.ketoibabal.cyou	0%	Avira URL Cloud	safe	
http://https://www.fasthosts.co.uk/get-online?utm_source=domainparking&utm_medium=referral&utm_campaign=fh_	0%	Avira URL Cloud	safe	
http://www.virginhairweave.co.uk/0oqq/	0%	Avira URL Cloud	safe	
http://www.themssterofssuepnse.rest/0oqq/polb=tYchV8	100%	Avira URL Cloud	malware	
http://www.ketoibabal.cyou/0oqq/qt9TW=60_ljPJoqo6d2	0%	Avira URL Cloud	safe	
http://www.landlotto.ru/0oqq/?lCHyvj5=zVtcFUb2erpe1riHNV8x4uTJHdjXeMKlBrPOkTLBlxKebXbCPRW4F79HIT/4WhPpl+5XC4kkcR4ywvq/sd7+lksDMuqQ2YrnfA==&qt9TW=60_ljPJoqo6d2	100%	Avira URL Cloud	malware	
http://www.hudsonandbailey.uk/0oqq/?lCHyvj5=8lDg7smsrRHQ2qUpjxtX5vXhip5hsKbS8bjyUsS5uXhQwZhytHa5U2zriYWyog0tbgqTaVuvH+VyL3+e5fQfLE/J79Vj0e1H5A==&qt9TW=60_ljPJoqo6d2	100%	Avira URL Cloud	malware	
http://www.virginhairweave.co.uk	0%	Avira URL Cloud	safe	
http://www.virginhairweave.co.uk/0oqq/?qt9TW=60_ljPJoqo6d2&ICHyvj5=uTgIqe0UraKbEL8bVan9urdYcpPucjhGk2sL3YY9ls8dblQwqoiZoebTO/nXMXVf1qLfWs/b3Kzx4hfR3b8+tPCCgrVHYEBTbA==	0%	Avira URL Cloud	safe	
http://www.allison2patrick.online/0oqq/?qt9TW=60_ljPJoqo6d2&ICHyvj5=+kFy7HAJLaaTMVi2uF0rU22efsuYGHBQaVugoRnSwIkO/2Cyn5VxSDOnkUbRzJjMahwif1zr/P1d/M6VqUD0f3xgTygnYxnqlA==	100%	Avira URL Cloud	malware	
http://www.themssterofssuepnse.rest/0oqq/qt9TW=60_ljPJoqo6d2	100%	Avira URL Cloud	malware	
http://www.g2fm.co.uk	0%	Avira URL Cloud	safe	
http://www.landlotto.ru	100%	Avira URL Cloud	malware	
http://www.hudsonandbailey.uk/0oqq/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dirdikyepedia.com	5.181.216.141	true	true	• 9%, Virustotal, Browse	unknown
allison2patrick.online	62.4.21.190	true	true	• 6%, Virustotal, Browse	unknown
www.gorwly.top	192.64.116.162	true	true	• 3%, Virustotal, Browse	unknown
glb-mobility.com	88.99.217.197	true	true	• 3%, Virustotal, Browse	unknown
www.hudsonandbailey.uk	199.59.243.223	true	true		unknown
www.virginhairweave.co.uk	198.58.118.167	true	true		unknown
www.g2fm.co.uk	213.171.195.105	true	true		unknown
www.landlotto.ru	109.70.26.37	true	true		unknown
www.karlscurry.co.uk	217.160.0.249	true	true		unknown
www.ty23vip.com	162.209.159.142	true	true		unknown
fanversewallet.com	203.245.24.47	true	true		unknown
www.mynichemarket.co.uk	185.151.30.181	true	true		unknown
www.themssterofssuepnse.rest	unknown	unknown	true		unknown
www.glb-mobility.com	unknown	unknown	true		unknown
www.fanversewallet.com	unknown	unknown	true		unknown
www.ketoibabal.cyou	unknown	unknown	true		unknown
www.allison2patrick.online	unknown	unknown	true		unknown
www.brennmansoluciones.com	unknown	unknown	true		unknown
www.dirdikyepedia.com	unknown	unknown	true		unknown
www.thelastwill.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.g2fm.co.uk/0oqq/?lCHyvj5=mrIlldvmtur7mkt/rPLDu6zCaW7pq/FSfCj+/pKGfo5WkxwIgZbXON4VpSp8r5ryJHF0PKr2dhp3lAxH7D3LGu58YX7EcXy0Ow==&qt9TW=60_ljPJoqo6d2	true	• Avira URL Cloud: safe	unknown
http://www.fanversewallet.com/0oqq/?qt9TW=60_ljPJoqo6d2&lCHyvj5=Yikzj9CFq5vqEc2vNlbzxihd8s3DrMcGxuzxagcCy5X6CzTVIy/a14lT5vlHy5RQ1Z7Px0aDVF6+DD/SwGM+3qMYWad3MBh6/g==	true	• Avira URL Cloud: malware	unknown
http://www.karlscurry.co.uk/0oqq/	true	• Avira URL Cloud: safe	unknown
http://www.karlscurry.co.uk/0oqq/?lCHyvj5=/wt4JY4W3l+DpUlEm50j75nj98dXbWC1Jam/Xyx5jEHfTH+E1ePLpr1g8eshFzfVb4/25r9KS6bvXq1NrjcG6ioEuox+na//qA==&qt9TW=60_ljPJoqo6d2	true	• Avira URL Cloud: safe	unknown
http://www.dirdikyepedia.com/0oqq/?qt9TW=60_ljPJoqo6d2&lCHyvj5=PRQC41TmcI9bvUwILfW251fDqJjDWsuIERfzYnlMN4HgHjqryKViH0BFVe/NE6lVKE81tYv052d7aHxIDF6KpDCDELCE9pYayA==	true	• Avira URL Cloud: malware	unknown
http://www.mynichemarket.co.uk/0oqq/	true	• Avira URL Cloud: safe	unknown
http://www.glb-mobility.com/0oqq/?lCHyvj5=L0mSdT0ooJoC+WTAff+ZGzvWM+chwjv3Dy0WIeNakQkmi/ixITEkKFHCL0Q8UzGKK5QpSY+AVQ3lyxgaFTuxUTcmK0rro2dEnw==&qt9TW=60_ljPJoqo6d2	true	• Avira URL Cloud: safe	unknown
http://www.allison2patrick.online/0oqq/	true	• Avira URL Cloud: malware	unknown
http://www.glb-mobility.com/0oqq/	true	• Avira URL Cloud: safe	unknown
http://www.g2fm.co.uk/0oqq/	true	• Avira URL Cloud: safe	unknown
http://www.fanversewallet.com/0oqq/	true	• Avira URL Cloud: malware	unknown
http://www.landlotto.ru/0oqq/	true	• Avira URL Cloud: malware	unknown
http://www.dirdikyepedia.com/0oqq/	true	• Avira URL Cloud: malware	unknown
http://www.gorwly.top/0oqq/	true	• Avira URL Cloud: malware	unknown
http://www.mynichemarket.co.uk/0oqq/?qt9TW=60_ljPJoqo6d2&lCHyvj5=bPiAqCboB3xuuR9jBd2d5kx4kdlhaJ3zm41TCptSu6l9zHYblFc2aOuFx07ZodW9tNkBHFGkWniHGpAg445zXTdag0fAcLuZfA==	true	• Avira URL Cloud: safe	unknown
http://www.virginhairweave.co.uk/0oqq/	true	• Avira URL Cloud: safe	unknown
http://www.landlotto.ru/0oqq/?lCHyvj5=zVtcFUb2erpe1riHNV8x4uTJHdjXeMKlBrPOkTLBlxKebXbCPRW4F79HIT/4WhPpl+5XC4kkcR4ywvq/sd7+lksDMuqQ2YrnfA==&qt9TW=60_ljPJoqo6d2	true	• Avira URL Cloud: malware	unknown
http://www.hudsonandbailey.uk/0oqq/?lCHyvj5=8lDg7smsrRHQ2qUpjxtX5vXhip5hsKbS8bjyUsS5uXhQwZhytHa5U2zriYWyog0tbgqTaVuvH+VyL3+e5fQfLE/J79Vj0e1H5A==&qt9TW=60_ljPJoqo6d2	true	• Avira URL Cloud: malware	unknown
http://www.virginhairweave.co.uk/0oqq/?qt9TW=60_ljPJoqo6d2&lCHyvj5=uTgIqe0UraKbEL8bVan9urdYcpPucjhGk2sL3YY9ls8dblQwqoiZoebTO/nXMXVf1qLfWs/b3Kzx4hfR3b8+tPCCgrVHYEBTbA==	true	• Avira URL Cloud: safe	unknown
http://www.allison2patrick.online/0oqq/?qt9TW=60_ljPJoqo6d2&lCHyvj5=+kFy7HAJLaaTMVi2uF0rU22efsuYGHBQaVugoRnSwlkO/2Cyn5VxSDOnkUbRzJjMahwif1zr/P1d/M6VqUD0f3xgTygnYxnqIA==	true	• Avira URL Cloud: malware	unknown
http://www.hudsonandbailey.uk/0oqq/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	rundll32.exe, 0000000D.00000002.778376326.000000000310F000.00000004.00000020.00020000.00000000.sdmp, 81EFaKSJ3.13.dr	false		high
http://https://www.nic.ru/catalog/mail/on-domain/?ipartner=6666&adv_id=click_mail&utm_source=stpg_all&utm_m	rundll32.exe, 0000000D.00000002.781664990.00000000074F0000.00000004.00000800.00020000.00000000.sdmp, rundll32.exe, 0000000D.00000002.781120791.0000000005E14000.00000004.10000000.00040000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	81EFaKSJ3.13.dr	false		high
http://www.ty23vip.com/0oqq/	explorer.exe, 00000003.00000003.670569523.000000000F527000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fanversewallet.com/0oqq/qt9TW=60_ljPJoqo6d2	explorer.exe, 00000003.00000003.473077921.000000000F51E000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.475275139.000000000F527000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ketoibabal.cyou/0oqq/	explorer.exe, 00000003.00000002.79152454 6.000000000F52A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.473077921.000000000F51E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.475275139.000000 000F527000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.670569523.000000000F527000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.nic.ru/catalog/ssl/	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://https://www.nic.ru/catalog/sites/sitebuilder/	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://https://www.nic.ru/catalog/domains/ru/	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://nic.ru/images/w8/win8transp.png	rundll32.exe, 0000000D.00000002.78112079 1.0000000005E14000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://www.hudsonandbailey.uk	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ty23vip.com/0oqq/qt9TW=60_ljPJoqo6d2	explorer.exe, 00000003.00000003.47307792 1.000000000F51E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.475275139.000000000F527000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.glb-mobility.com	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.00000000054A8000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://nic.ru/	rundll32.exe, 0000000D.00000002.78112079 1.0000000005E14000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://https://www.nic.ru/catalog/domains/	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://www.thelastwill.net/0oqq/	explorer.exe, 00000003.00000003.47307792 1.000000000F51E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.475275139.000000000F527000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.670569523.000000 000F527000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.nic.ru/whois/?searchWord=LANDLOTTO.RU&ipartner=6666&adv_id=whois_info&utm_source=stpg_al	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://www.thelastwill.net/0oqq/qt9TW=60_ljPJoqo6d2	explorer.exe, 00000003.00000003.47307792 1.000000000F51E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.475275139.000000000F527000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.670569523.000000 000F527000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gorwly.top/0oqq/qt9TW=60_ljPJoqo6d2	explorer.exe, 00000003.00000003.47307792 1.000000000F51E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.475275139.000000000F527000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/normalize/5.0.0/normalize.min.css	rundll32.exe, 0000000D.00000002.78112079 1.0000000005FA6000.00000004.10000000.000 40000.00000000.sdmp	false		high

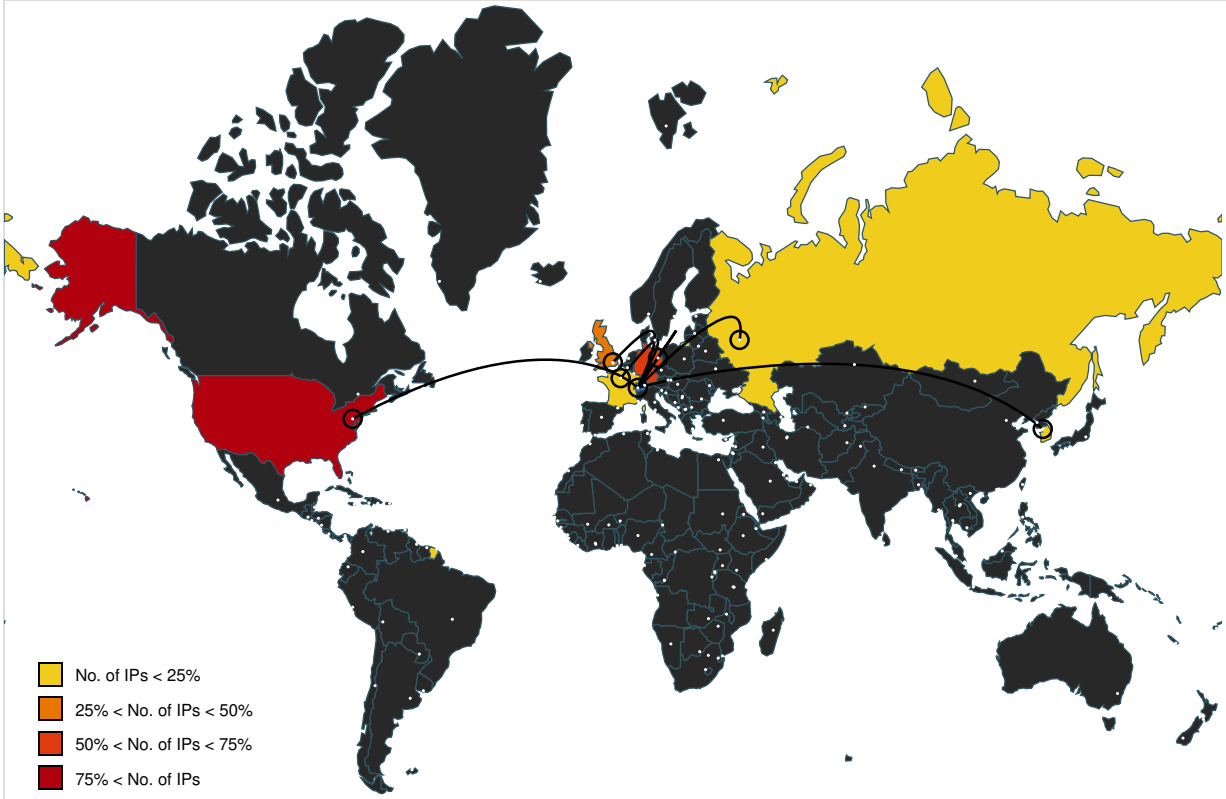
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.brennmansoluciones.com	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.nic.ru/catalog/mail/on-domain/	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://www.karlscurry.co.uk	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.nic.ru/product/mail/forward/?ipartner=6666&adv_id=click_mail_forward&utm_source=stpg_all	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://https://www.nic.ru/help/statusnaya-stranica_4785.html?ipartner=6666&adv_id=faq&utm_source=stpg_all&u	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://www.thelastwill.net	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.nic.ru/catalog/domains/rf/	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://www.thebang.sbs	explorer.exe, 00000003.00000002.79152454 6.000000000F52A000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.nic.ru/auction/	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://www.sexopornoxx.store/0oqq/	explorer.exe, 00000003.00000002.79152454 6.000000000F52A000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.ty23vip.com	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	81EFaKSJ3.13.dr	false		high
http://https://www.nic.ru/catalog/hosting/dedicated/	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://www.nic.ru/catalog/sites/sitebuilder/?ipartner=6666&adv_id=click_sitebuild&utm_source=stpg_a	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	OUTSTANDING_PAYMENT.exe	false		high
http://https://www.nic.ru/catalog/domains/com/	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://https://tiao2022.vip:12306/?u=	rundll32.exe, 0000000D.00000002.78112079 1.000000000645C000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.nic.ru/product/for-domain-use/web-forwarding/?ipartner=6666&adv_id=click_domain_forward&	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	rundll32.exe, 0000000D.00000002.77837632 6.000000000310F000.00000004.00000020.000 20000.00000000.sdmp, 81EFaKSJ3.13.dr	false		high
http://www.gorwly.top	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.mynichemarket.co.uk	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.themssterofssuepnse.rest	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.fanversewallet.com	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.nic.ru/opensearch.xml	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://storage.nic.ru/ru/images/png/1.rc-logo-og.png	rundll32.exe, 0000000D.00000002.78112079 1.0000000005E14000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://www.brennmansoluciones.com/0oqq/qt9TW=60_ljPJoqo6d2	explorer.exe, 00000003.00000002.79152454 6.000000000F52A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.473077921.000000000F51E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.475275139.000000 000F527000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.670569523.000000000F527000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.karlscurry.co.uk/0oqq/qt9TW=60_ljPJoqo6d2	explorer.exe, 00000003.00000003.47307792 1.000000000F51E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.475275139.000000000F527000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.670569523.000000 000F527000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.leewanyam.com/0oqq/polb=tYchV8	explorer.exe, 00000003.00000002.79152454 6.000000000F52A000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.allison2patrick.online	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.brennmansoluciones.com/0oqq/polb=tYchV8	explorer.exe, 00000003.00000002.79152454 6.000000000F52A000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.glb-mobility.com/0oqq/qt9TW=60_ljPJoqo6d2	explorer.exe, 00000003.00000003.47307792 1.000000000F51E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.475275139.000000000F527000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.brennmansoluciones.com/0oqq/	explorer.exe, 00000003.00000002.79152454 6.000000000F52A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.473077921.000000000F51E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.475275139.000000 000F527000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.670569523.000000000F527000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com?fr=crmas_sfpf	rundll32.exe, 0000000D.00000002.77837632 6.000000000310F000.00000004.00000020.000 20000.00000000.sdmp, 81EFaKSJ3.13.dr	false		high
http://https://www.fasthosts.co.uk/domain-names/search/?domain=$	rundll32.exe, 0000000D.00000002.78112079 1.0000000005AF0000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.themssterofssuepnse.rest/0oqq/	explorer.exe, 00000003.00000002.79152454 6.000000000F52A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.473077921.000000000F51E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.475275139.000000 000F527000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.670569523.000000000F527000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.leewanyam.com/0oqq/	explorer.exe, 00000003.00000002.79152454 6.000000000F52A000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.landlotto.ru/0oqq/qt9TW=60_ljPJoqo6d2	explorer.exe, 00000003.00000003.47307792 1.000000000F51E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.475275139.000000000F527000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://fasthosts.co.uk/	rundll32.exe, 0000000D.00000002.78112079 1.0000000005AF0000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ketoibabal.cyou	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.nic.ru/catalog/hosting/shared/	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://www.mynichemarket.co.uk/0oqq/qt9TW=60_ljPJoqo6d2	explorer.exe, 00000003.00000003.47307792 1.000000000F51E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.475275139.000000000F527000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.fasthosts.co.uk/get-online?utm_source=domainparking&utm_medium=referral&utm_campaign=fh_	rundll32.exe, 0000000D.00000002.78112079 1.0000000005AF0000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.themssterofssuepnse.rest/0oqq/poIb=tYchV8	explorer.exe, 00000003.00000002.79152454 6.000000000F52A000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.nic.ru/cata	rundll32.exe, 0000000D.00000002.78112079 1.0000000005E14000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://www.ketoibabal.cyou/0oqq/qt9TW=60_ljPJoqo6d2	explorer.exe, 00000003.00000002.79152454 6.000000000F52A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.473077921.000000000F51E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.475275139.000000 000F527000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.670569523.000000000F527000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.nic.ru/catalog/hosting/shared/?ipartner=6666&adv_id=click_vh&utm_source=stpg_all&utm_med	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://www.landlotto.ru	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	rundll32.exe, 0000000D.00000002.77837632 6.000000000310F000.00000004.00000020.000 20000.00000000.sdmp, 81EFaKSJ3.13.dr	false		high
http://https://www.nic.ru?ipartner=6666&adv_id=logo&utm_source=stpg_all&utm_medium=link&utm_campaign=logo	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://www.virginhairweave.co.uk	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.litespeedtech.com/error-page	rundll32.exe, 0000000D.00000002.78112079 1.000000000595E000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	rundll32.exe, 0000000D.00000002.77837632 6.000000000310F000.00000004.00000020.000 20000.00000000.sdmp, 81EFaKSJ3.13.dr	false		high
http://https://www.nic.ru/catalog/hosting/cms/?ipartner=6666&adv_id=click_cmsh&utm_source=stpg_all&utm_medi	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://www.themssterofssuepnse.rest/0oqq/qt9TW=60_ljPJoqo6d2	explorer.exe, 00000003.00000002.79152454 6.000000000F52A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.473077921.000000000F51E000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.475275139.000000 000F527000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.670569523.000000000F527000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://ac.ecosia.org/autocomplete?q=	81EFaKSJ3.13.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	rundll32.exe, 0000000D.00000002.77837632 6.000000000310F000.00000004.00000020.000 20000.00000000.sdmp, 81EFaKSJ3.13.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.nic.ru/catalog/hosting/vds-vps/	rundll32.exe, 0000000D.00000002.78166499 0.00000000074F0000.00000004.00000800.000 20000.00000000.sdmp, rundll32.exe, 00000 00D.00000002.781120791.0000000005E14000. 00000004.10000000.00040000.00000000.sdmp	false		high
http://www.g2fm.co.uk	explorer.exe, 00000003.00000003.67056952 3.000000000F527000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.70.26.37	www.landlotto.ru	Russian Federation		48287	RU-CENTERRU	true
88.99.217.197	glb-mobility.com	Germany		24940	HETZNER-ASDE	true
217.160.0.249	www.karlscurry.co.uk	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
162.209.159.142	www.ty23vip.com	United States		40065	CNSERVERSUS	true
192.64.116.162	www.gorwly.top	United States		22612	NAMECHEAP-NETUS	true
199.59.243.223	www.hudsonandbailey.uk	United States		395082	BODIS-NJUS	true
5.181.216.141	dirdikyepedia.com	Germany		59637	ASRSINETRU	true
62.4.21.190	allison2patrick.online	France		12876	OnlineSASFR	true
185.151.30.181	www.mynichemarket.co.uk	United Kingdom		48254	TWENTYIGB	true
203.245.24.47	fanversewallet.com	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
198.58.118.167	www.virginhairweave.co.uk	United States		63949	LINODE-APLinodeLLCUS	true
213.171.195.105	www.g2fm.co.uk	United Kingdom		8560	ONEANDONE-ASBrauerstrasse48DE	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830322
Start date and time:	2023-03-20 09:06:45 +01:00

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 10s
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:	18
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:	OUTSTANDING_PAYMENT.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/5@26/12
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 33.6% (good quality ratio 32.5%) • Quality average: 81% • Quality standard deviation: 24.3%
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 • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:07:58	API Interceptor	1873x 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\81EFaKSJ3

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\bpgvtpbkoxw.z

Process:	C:\Users\user\Desktop\OUTSTANDING_PAYMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	6222
Entropy (8bit):	7.133693106224874
Encrypted:	false
SSDEEP:	96:Farc6oYwg/DrYu8k2XO5oSwQCahg5GwYTfOdaFxrsyGli1GReZw7zmzuZP0ed:FarcRYkhX1S1CapwYmaFmyGIDCzzSL
MD5:	933BE16F654BB3BC251347110454FB49
SHA1:	A4580CC4A1D3AC955D648A9C34BBD27B5C48F9AE
SHA-256:	5252B99D4CEB221CF6F0440F0F2430F7A76D1B6EAC6AB2997FB21828400B502E
SHA-512:	845B3DA4F3AA844508AC7B0CE86253A2E588C994308D29EFB5385034CF38C413258820CB0C7C938F04E7B447549FE24076CD1EA327957AD70D200748BAAC942
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\nsmF14F.tmp

Process:	C:\Users\user\Desktop\OUTSTANDING_PAYMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	288752
Entropy (8bit):	7.703024922742189
Encrypted:	false

SSDEEP:	6144:7iDso57TQE/u3+8fgnGdzNrja8LI57EUHyTZ5CslO2br0xp1I:7iDsO7Myi+3nGdRa8Lyw57lO2brm
MD5:	B770DC09825AC013742565DF7C5B0DF5
SHA1:	8B0F5C52ABE0EB2310371254F051F63DD2841AF6
SHA-256:	4A205CB23069324967DFE9615F25B7D8118D779979BFE22A8E366B02180AB140
SHA-512:	87B160CBAFC2D042000A201802FAF88F5674C498624A9802D98BC0AF6B4386E8A54110ABB1CA769654259091C35511898A50CC82E759B02EEF32CB4D20BDA22A
Malicious:	false
Reputation:	low
Preview:	.-.....,.....s...p.....,.....-.....*..... .....G.....%...j.....C..... ....

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

Process:	C:\Users\user\Desktop\OUTSTANDING_PAYMENT.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	59904
Entropy (8bit):	6.225922782264242
Encrypted:	false
SSDEEP:	768:Rpbnyq696YM4+FJV/dRuDh96ir6VhAkAXuabEoK3r412IGXM5x8dsr:RpbRrYSJV/ToZr6VhhAXj7GnI15is
MD5:	41C9E29A7ED3640682A0003BE2DF4D93
SHA1:	E22976256F765E9B526728A2890D2A59FD535636
SHA-256:	FE949C62767413F53307655AE55EFAD92454EAF28DC874F4650DDD74C79A7050
SHA-512:	FC22103EB32998D76A3207EA789011E7633E3B7838DAD274C41930908E19F74905C101D9FABA58A3B8295248A94F38EF4932248DFCFD84D2A24D160335E8C48A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 51%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1... ...6.....<...$...Rich.....PE..L...?..d..... ....`.....@.....0.....@.....d..... .....text..... ..`. rdata...!.....".....@..@.data....,.....@....reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\tmjcdbgtyam.ggz

Process:	C:\Users\user\Desktop\OUTSTANDING_PAYMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	210904
Entropy (8bit):	**7.998936663875696**
Encrypted:	**true**
SSDEEP:	6144:OiDso57TQE/u3+8fgnGdzNrja8LI57EUHyTZ5CslO2l:OiDsO7Myi+3nGdRa8Lyw57lO2l
MD5:	9E7E609FCC35E2BF40522D621CB62D4F
SHA1:	17E126ADA88229FE6C42E2DAFEE0080C6643F345
SHA-256:	0DD2596D144CACBA46ECD058E5CE2F13D27414313D8D33DADBDC455F3358B09A
SHA-512:	68BEB80FE38D860FAAB5F40398B0EFC91A60A33946AE5D9A259007B35FF0F87D7C6DBD7EED662F0B21954F7656F1860D0029EE828A2EC8D062DF5D896F84BB42
Malicious:	false
Reputation:	low
Preview:	....._0.a.!..@...7.?\n...8I~JK.O.|...@.W.>..=..{..*X.....J..AWE...N>..J..6.Z..I..]S=7....k!.n...K..Z...1'.z 4h.....Y.....>bt@iReh.u..c..k.QY...}...9....>..62I.K.../b.....M..s.K9.....I I5k.g..J_.....Y..o._\.....[....I.+.8....{..g..V..J...._0....t.k.4.~.....$>=<.r.O..=.@..>E.=..{./*X.....J...(.....h.....`B\.e....1.zN..J....mrX.....G....&x..v.FC.....o...?/.#..x..{.3h.-.! .....5...=t"....r...b.....M..+(t.K9..Z..O.ml/}r..J_.....&:/.U..f.....[.,.....+.....{.mg..Q....._0.a..t.k.4...)...$>=D.K.O.|...@.W.>..=..{..*X.....J...(.....h.....`B\.e....1.zN..J....mrX.....G.. ..&x..v.FC.....o...?/.#..x..{.3h.-.!.....5...=t"....r...b.....M..s.K9.N...O+ml/.....J_.....&:/.o..\.....[.,.....+.....{.mg..Q....._0.a..t.k.4...)...$>=D.K.O.|...@.W.>..=..{..*X.....J...(.....h.... .`B\.e....1.zN..J....mrX.....G....&x..v.FC.....o...?/.#..x..{.3h.-.!.....5...=t"....r...b.....M..s.K9.N...O+ml/.....J_.....&:/.o..\.....[

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.886295753349112

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:	OUTSTANDING_PAYMENT.exe
File size:	297210
MD5:	4832e17c1f6841aee2e1984a429ed946
SHA1:	d7ad36c7bee5cb39aa5b77944ced8a716a8af545
SHA256:	d0ac15eeb53f64ad6f399ead8724f38344daf243332f03790598c6716a04f162
SHA512:	f7dbb5749ad23b13d001c55be2ba6e4b8deab56d0687804c8a61bddb98b723bd1a244c32507bb16b9544e092d7bf5a37480d6ff34944752dfe464d30ada7244e
SSDEEP:	6144:qYa6cFVIKVgBgM6rpFh/U8KAg9gxt03ZaHJ1XoF5KOJeeqN3rj:qYa3fWg3TK8KRg4pCUGj
TLSH:	615402D19350D1E6E8A706F00C35EA2712BF7E3D54705E4A3B9E71A97E73192822EE03
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:	517959587979b110

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
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

Instruction
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 00007FB070C04CCAh
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 00007FB070C04C9Ah
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	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0x4510	.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	0x4510	0x4600	False	0.4218191964285714	data	5.130936129573036	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b238	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216, resolution 3779 x 3779 px/m	English	United States
RT_ICON	0x3d7e0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096, resolution 3779 x 3779 px/m	English	United States
RT_ICON	0x3e888	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024, resolution 3779 x 3779 px/m	English	United States
RT_DIALOG	0x3ecf0	0x100	data	English	United States
RT_DIALOG	0x3edf0	0x11c	data	English	United States
RT_DIALOG	0x3ef10	0x60	data	English	United States
RT_GROUP_ICON	0x3ef70	0x30	data	English	United States
RT_VERSION	0x3efa0	0x22c	data	English	United States
RT_MANIFEST	0x3f1d0	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

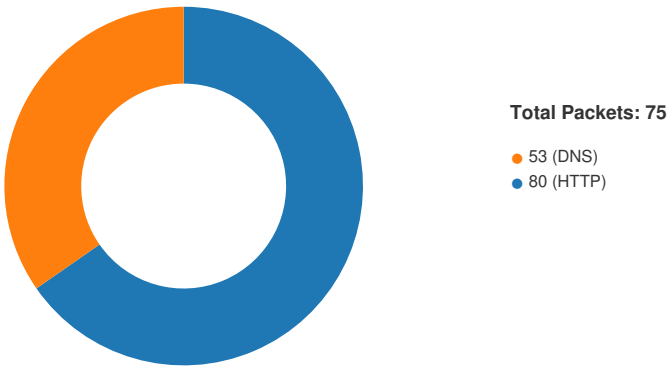
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3185.151.30.18 149711802031453 03/20/23-09:09:32.876293	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49711	80	192.168.2.3	185.151.30.181
192.168.2.3192.64.116.16 249717802031449 03/20/23-09:09:54.051496	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.3	192.64.116.162
192.168.2.35.181.216.141 49705802031449 03/20/23-09:09:09.878629	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49705	80	192.168.2.3	5.181.216.141
192.168.2.3192.64.116.16 249717802031412 03/20/23-09:09:54.051496	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.3	192.64.116.162
192.168.2.35.181.216.141 49705802031453 03/20/23-09:09:09.878629	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49705	80	192.168.2.3	5.181.216.141
192.168.2.3192.64.116.16 249717802031453 03/20/23-09:09:54.051496	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.3	192.64.116.162
192.168.2.3185.151.30.18 149711802031449 03/20/23-09:09:32.876293	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49711	80	192.168.2.3	185.151.30.181
192.168.2.38.8.8.8511395 32023883 03/20/23-09:09:48.362224	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	51139	53	192.168.2.3	8.8.8.8
192.168.2.35.181.216.141 49705802031412 03/20/23-09:09:09.878629	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49705	80	192.168.2.3	5.181.216.141
192.168.2.3185.151.30.18 149711802031412 03/20/23-09:09:32.876293	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49711	80	192.168.2.3	185.151.30.181

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:08:23.239229918 CET	49698	80	192.168.2.3	199.59.243.223
Mar 20, 2023 09:08:23.258771896 CET	80	49698	199.59.243.223	192.168.2.3
Mar 20, 2023 09:08:23.258922100 CET	49698	80	192.168.2.3	199.59.243.223
Mar 20, 2023 09:08:23.259864092 CET	49698	80	192.168.2.3	199.59.243.223
Mar 20, 2023 09:08:23.280504942 CET	80	49698	199.59.243.223	192.168.2.3
Mar 20, 2023 09:08:23.462835073 CET	80	49698	199.59.243.223	192.168.2.3
Mar 20, 2023 09:08:23.466599941 CET	80	49698	199.59.243.223	192.168.2.3
Mar 20, 2023 09:08:23.466635942 CET	80	49698	199.59.243.223	192.168.2.3
Mar 20, 2023 09:08:23.466769934 CET	49698	80	192.168.2.3	199.59.243.223
Mar 20, 2023 09:08:23.466814995 CET	49698	80	192.168.2.3	199.59.243.223
Mar 20, 2023 09:08:23.466965914 CET	49698	80	192.168.2.3	199.59.243.223
Mar 20, 2023 09:08:23.476100922 CET	80	49698	199.59.243.223	192.168.2.3
Mar 20, 2023 09:08:23.476188898 CET	49698	80	192.168.2.3	199.59.243.223
Mar 20, 2023 09:08:23.486416101 CET	80	49698	199.59.243.223	192.168.2.3
Mar 20, 2023 09:08:33.718719006 CET	49700	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:33.860883951 CET	80	49700	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:33.861018896 CET	49700	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:33.861186028 CET	49700	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:34.004131079 CET	80	49700	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:34.004220963 CET	80	49700	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:34.004365921 CET	49700	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:35.370201111 CET	49700	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:36.387404919 CET	49701	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:36.529535055 CET	80	49701	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:36.529732943 CET	49701	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:36.530070066 CET	49701	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:36.673634052 CET	80	49701	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:36.673666954 CET	80	49701	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:36.678245068 CET	80	49701	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:36.678307056 CET	80	49701	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:36.678327084 CET	80	49701	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:36.678345919 CET	80	49701	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:36.678364992 CET	80	49701	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:36.678384066 CET	80	49701	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:36.678401947 CET	80	49701	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:36.678421021 CET	80	49701	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:36.678453922 CET	80	49701	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:36.678473949 CET	80	49701	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:36.678502083 CET	49701	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:36.678550959 CET	49701	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:38.041094065 CET	49701	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:39.057307005 CET	49702	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:39.198124886 CET	80	49702	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:39.198402882 CET	49702	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:39.198573112 CET	49702	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:39.338808060 CET	80	49702	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:39.338846922 CET	80	49702	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:39.338994026 CET	49702	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:39.339560032 CET	49702	80	192.168.2.3	198.58.118.167
Mar 20, 2023 09:08:39.479263067 CET	80	49702	198.58.118.167	192.168.2.3
Mar 20, 2023 09:08:52.197664976 CET	49703	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:08:55.183217049 CET	49703	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:08:55.350596905 CET	80	49703	5.181.216.141	192.168.2.3
Mar 20, 2023 09:08:55.350929976 CET	49703	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:08:55.351131916 CET	49703	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:08:55.518073082 CET	80	49703	5.181.216.141	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:08:55.518115997 CET	80	49703	5.181.216.141	192.168.2.3
Mar 20, 2023 09:08:55.518137932 CET	80	49703	5.181.216.141	192.168.2.3
Mar 20, 2023 09:08:55.518275976 CET	49703	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:08:55.518762112 CET	80	49703	5.181.216.141	192.168.2.3
Mar 20, 2023 09:08:55.518836021 CET	49703	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:08:56.855484962 CET	49703	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:08:57.871778011 CET	49704	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:08:58.037409067 CET	80	49704	5.181.216.141	192.168.2.3
Mar 20, 2023 09:08:58.037661076 CET	49704	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:08:58.038130045 CET	49704	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:08:58.202923059 CET	80	49704	5.181.216.141	192.168.2.3
Mar 20, 2023 09:08:58.202984095 CET	80	49704	5.181.216.141	192.168.2.3
Mar 20, 2023 09:08:58.203006983 CET	80	49704	5.181.216.141	192.168.2.3
Mar 20, 2023 09:08:58.203119993 CET	49704	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:08:58.203399897 CET	80	49704	5.181.216.141	192.168.2.3
Mar 20, 2023 09:08:58.203422070 CET	80	49704	5.181.216.141	192.168.2.3
Mar 20, 2023 09:08:58.203469038 CET	49704	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:08:58.367841005 CET	80	49704	5.181.216.141	192.168.2.3
Mar 20, 2023 09:08:58.367882967 CET	80	49704	5.181.216.141	192.168.2.3
Mar 20, 2023 09:09:00.559386015 CET	49705	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:09:03.558839083 CET	49705	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:09:09.716959000 CET	49705	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:09:09.878328085 CET	80	49705	5.181.216.141	192.168.2.3
Mar 20, 2023 09:09:09.878494024 CET	49705	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:09:09.878628969 CET	49705	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:09:10.038577080 CET	80	49705	5.181.216.141	192.168.2.3
Mar 20, 2023 09:09:10.038641930 CET	80	49705	5.181.216.141	192.168.2.3
Mar 20, 2023 09:09:10.038702965 CET	80	49705	5.181.216.141	192.168.2.3
Mar 20, 2023 09:09:10.038727999 CET	80	49705	5.181.216.141	192.168.2.3
Mar 20, 2023 09:09:10.038892031 CET	49705	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:09:10.038979053 CET	49705	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:09:10.039194107 CET	49705	80	192.168.2.3	5.181.216.141
Mar 20, 2023 09:09:10.199062109 CET	80	49705	5.181.216.141	192.168.2.3
Mar 20, 2023 09:09:15.096410036 CET	49706	80	192.168.2.3	213.171.195.105
Mar 20, 2023 09:09:15.129733086 CET	80	49706	213.171.195.105	192.168.2.3
Mar 20, 2023 09:09:15.129988909 CET	49706	80	192.168.2.3	213.171.195.105
Mar 20, 2023 09:09:15.130350113 CET	49706	80	192.168.2.3	213.171.195.105
Mar 20, 2023 09:09:15.164252996 CET	80	49706	213.171.195.105	192.168.2.3
Mar 20, 2023 09:09:15.164403915 CET	80	49706	213.171.195.105	192.168.2.3
Mar 20, 2023 09:09:15.164463043 CET	80	49706	213.171.195.105	192.168.2.3
Mar 20, 2023 09:09:15.164660931 CET	49706	80	192.168.2.3	213.171.195.105
Mar 20, 2023 09:09:16.639620066 CET	49706	80	192.168.2.3	213.171.195.105
Mar 20, 2023 09:09:17.654774904 CET	49707	80	192.168.2.3	213.171.195.105
Mar 20, 2023 09:09:17.688360929 CET	80	49707	213.171.195.105	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:08:18.059130907 CET	61787	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:08:18.108978987 CET	53	61787	8.8.8.8	192.168.2.3
Mar 20, 2023 09:08:23.120605946 CET	58921	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:08:23.235593081 CET	53	58921	8.8.8.8	192.168.2.3
Mar 20, 2023 09:08:33.538893938 CET	49977	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:08:33.677284002 CET	53	49977	8.8.8.8	192.168.2.3
Mar 20, 2023 09:08:44.356928110 CET	57840	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:08:44.618321896 CET	53	57840	8.8.8.8	192.168.2.3
Mar 20, 2023 09:08:45.622361898 CET	57990	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:08:45.811009884 CET	53	57990	8.8.8.8	192.168.2.3
Mar 20, 2023 09:08:46.827991962 CET	52387	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:08:46.985388994 CET	53	52387	8.8.8.8	192.168.2.3
Mar 20, 2023 09:08:52.008558989 CET	56924	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:08:52.196227074 CET	53	56924	8.8.8.8	192.168.2.3
Mar 20, 2023 09:09:15.063662052 CET	60625	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:09:15.094926119 CET	53	60625	8.8.8.8	192.168.2.3
Mar 20, 2023 09:09:27.620827913 CET	49302	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:09:27.751117945 CET	53	49302	8.8.8.8	192.168.2.3
Mar 20, 2023 09:09:38.002252102 CET	53975	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:09:38.020363092 CET	53	53975	8.8.8.8	192.168.2.3
Mar 20, 2023 09:09:48.362224102 CET	51139	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:09:48.472723007 CET	53	51139	8.8.8.8	192.168.2.3
Mar 20, 2023 09:10:00.005140066 CET	52955	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:10:00.160120964 CET	53	52955	8.8.8.8	192.168.2.3
Mar 20, 2023 09:10:01.176269054 CET	60582	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:10:01.385709047 CET	53	60582	8.8.8.8	192.168.2.3
Mar 20, 2023 09:10:02.394485950 CET	57134	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:10:02.523490906 CET	53	57134	8.8.8.8	192.168.2.3
Mar 20, 2023 09:10:07.544554949 CET	62050	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:10:07.567246914 CET	53	62050	8.8.8.8	192.168.2.3
Mar 20, 2023 09:10:08.603447914 CET	56042	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:10:08.626447916 CET	53	56042	8.8.8.8	192.168.2.3
Mar 20, 2023 09:10:09.648912907 CET	59636	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:10:09.669090033 CET	53	59636	8.8.8.8	192.168.2.3
Mar 20, 2023 09:10:14.745964050 CET	55638	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:10:14.768513918 CET	53	55638	8.8.8.8	192.168.2.3
Mar 20, 2023 09:10:25.792670965 CET	57704	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:10:25.829457998 CET	53	57704	8.8.8.8	192.168.2.3
Mar 20, 2023 09:10:36.036226034 CET	65320	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:10:36.065522909 CET	53	65320	8.8.8.8	192.168.2.3
Mar 20, 2023 09:10:46.233026028 CET	60767	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:10:46.512599945 CET	53	60767	8.8.8.8	192.168.2.3
Mar 20, 2023 09:10:58.079703093 CET	65107	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:10:58.134869099 CET	53	65107	8.8.8.8	192.168.2.3
Mar 20, 2023 09:11:10.968102932 CET	53848	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:11:11.017399073 CET	53	53848	8.8.8.8	192.168.2.3
Mar 20, 2023 09:11:37.019893885 CET	57571	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:11:37.163110971 CET	53	57571	8.8.8.8	192.168.2.3
Mar 20, 2023 09:11:38.184684038 CET	58691	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:11:38.328841925 CET	53	58691	8.8.8.8	192.168.2.3
Mar 20, 2023 09:11:39.347182989 CET	53305	53	192.168.2.3	8.8.8.8
Mar 20, 2023 09:11:39.494823933 CET	53	53305	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 09:08:18.059130907 CET	192.168.2.3	8.8.8.8	0x7c1d	Standard query (0)	www.themsterofssuepnse.rest	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:23.120605946 CET	192.168.2.3	8.8.8.8	0xa01d	Standard query (0)	www.hudsonandbailey.uk	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:33.538893938 CET	192.168.2.3	8.8.8.8	0xd7a5	Standard query (0)	www.virginhairweave.co.uk	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:44.356928110 CET	192.168.2.3	8.8.8.8	0x34e3	Standard query (0)	www.brennmansolucioneses.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:45.622361898 CET	192.168.2.3	8.8.8.8	0x388c	Standard query (0)	www.brennmansolucioneses.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:46.827991962 CET	192.168.2.3	8.8.8.8	0xb63f	Standard query (0)	www.brennmansolucioneses.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 09:08:52.008558989 CET	192.168.2.3	8.8.8.8	0x96dc	Standard query (0)	www.dirdikyepedia.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:09:15.063662052 CET	192.168.2.3	8.8.8.8	0xc039	Standard query (0)	www.g2fm.co.uk	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:09:27.620827913 CET	192.168.2.3	8.8.8.8	0x468d	Standard query (0)	www.mynichemarket.co.uk	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:09:38.002252102 CET	192.168.2.3	8.8.8.8	0x2560	Standard query (0)	www.landlotto.ru	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:09:48.362224102 CET	192.168.2.3	8.8.8.8	0xc976	Standard query (0)	www.gorwly.top	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:00.005140066 CET	192.168.2.3	8.8.8.8	0x627d	Standard query (0)	www.ketoibabal.cyou	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:01.176269054 CET	192.168.2.3	8.8.8.8	0xbe46	Standard query (0)	www.ketoibabal.cyou	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:02.394485950 CET	192.168.2.3	8.8.8.8	0x1805	Standard query (0)	www.ketoibabal.cyou	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:07.544554949 CET	192.168.2.3	8.8.8.8	0x1492	Standard query (0)	www.thelastwill.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:08.603447914 CET	192.168.2.3	8.8.8.8	0x442d	Standard query (0)	www.thelastwill.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:09.648912907 CET	192.168.2.3	8.8.8.8	0x46d1	Standard query (0)	www.thelastwill.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:14.745964050 CET	192.168.2.3	8.8.8.8	0x87cc	Standard query (0)	www.ty23vip.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:25.792670965 CET	192.168.2.3	8.8.8.8	0xc5ab	Standard query (0)	www.allison2patrick.online	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:36.036226034 CET	192.168.2.3	8.8.8.8	0x5df2	Standard query (0)	www.glb-mobility.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:46.233026028 CET	192.168.2.3	8.8.8.8	0x9aa8	Standard query (0)	www.fanversewallet.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:58.079703093 CET	192.168.2.3	8.8.8.8	0x8e22	Standard query (0)	www.karlscurry.co.uk	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:10.968102932 CET	192.168.2.3	8.8.8.8	0xd22	Standard query (0)	www.themssterofssuepnse.rest	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:37.019893885 CET	192.168.2.3	8.8.8.8	0x528	Standard query (0)	www.brennmansolucionees.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:38.184684038 CET	192.168.2.3	8.8.8.8	0xacb9	Standard query (0)	www.brennmansolucionees.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:39.347182989 CET	192.168.2.3	8.8.8.8	0x43ad	Standard query (0)	www.brennmansolucionees.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 09:08:18.108978987 CET	8.8.8.8	192.168.2.3	0x7c1d	Server failure (2)	www.themssterofssuepnse.rest	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:23.235593081 CET	8.8.8.8	192.168.2.3	0xa01d	No error (0)	www.hudsonandbailey.uk		199.59.243.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:33.677284002 CET	8.8.8.8	192.168.2.3	0xd7a5	No error (0)	www.virginhairweave.co.uk		198.58.118.167	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:33.677284002 CET	8.8.8.8	192.168.2.3	0xd7a5	No error (0)	www.virginhairweave.co.uk		45.33.18.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:33.677284002 CET	8.8.8.8	192.168.2.3	0xd7a5	No error (0)	www.virginhairweave.co.uk		45.79.19.196	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:33.677284002 CET	8.8.8.8	192.168.2.3	0xd7a5	No error (0)	www.virginhairweave.co.uk		96.126.123.244	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:33.677284002 CET	8.8.8.8	192.168.2.3	0xd7a5	No error (0)	www.virginhairweave.co.uk		45.33.20.235	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 09:08:33.677284002 CET	8.8.8.8	192.168.2.3	0xd7a5	No error (0)	www.virginhairweave.co.uk		173.255.194.134	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:33.677284002 CET	8.8.8.8	192.168.2.3	0xd7a5	No error (0)	www.virginhairweave.co.uk		45.56.79.23	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:33.677284002 CET	8.8.8.8	192.168.2.3	0xd7a5	No error (0)	www.virginhairweave.co.uk		45.33.2.79	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:33.677284002 CET	8.8.8.8	192.168.2.3	0xd7a5	No error (0)	www.virginhairweave.co.uk		72.14.185.43	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:33.677284002 CET	8.8.8.8	192.168.2.3	0xd7a5	No error (0)	www.virginhairweave.co.uk		45.33.30.197	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:33.677284002 CET	8.8.8.8	192.168.2.3	0xd7a5	No error (0)	www.virginhairweave.co.uk		72.14.178.174	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:33.677284002 CET	8.8.8.8	192.168.2.3	0xd7a5	No error (0)	www.virginhairweave.co.uk		45.33.23.183	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:44.618321896 CET	8.8.8.8	192.168.2.3	0x34e3	Server failure (2)	www.brennmansolucioneses.com	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:45.811009884 CET	8.8.8.8	192.168.2.3	0x388c	Server failure (2)	www.brennmansolucioneses.com	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:46.985388994 CET	8.8.8.8	192.168.2.3	0xb63f	Server failure (2)	www.brennmansolucioneses.com	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:08:52.196227074 CET	8.8.8.8	192.168.2.3	0x96dc	No error (0)	www.dirdikyepedia.com	dirdikyepedia.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:08:52.196227074 CET	8.8.8.8	192.168.2.3	0x96dc	No error (0)	dirdikyepedia.com		5.181.216.141	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:09:15.094926119 CET	8.8.8.8	192.168.2.3	0xc039	No error (0)	www.g2fm.co.uk		213.171.195.105	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:09:27.751117945 CET	8.8.8.8	192.168.2.3	0x468d	No error (0)	www.mynichemarket.co.uk		185.151.30.181	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:09:38.020363092 CET	8.8.8.8	192.168.2.3	0x2560	No error (0)	www.landlotto.ru		109.70.26.37	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:09:38.020363092 CET	8.8.8.8	192.168.2.3	0x2560	No error (0)	www.landlotto.ru		194.85.61.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:09:48.472723007 CET	8.8.8.8	192.168.2.3	0xc976	No error (0)	www.gorwly.top		192.64.116.162	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:00.160120964 CET	8.8.8.8	192.168.2.3	0x627d	Server failure (2)	www.ketoibabal.cyou	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:01.385709047 CET	8.8.8.8	192.168.2.3	0xbe46	Server failure (2)	www.ketoibabal.cyou	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:02.523490906 CET	8.8.8.8	192.168.2.3	0x1805	Server failure (2)	www.ketoibabal.cyou	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:07.567246914 CET	8.8.8.8	192.168.2.3	0x1492	Refused (5)	www.thelastwill.net	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:08.626447916 CET	8.8.8.8	192.168.2.3	0x442d	Refused (5)	www.thelastwill.net	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:09.669090033 CET	8.8.8.8	192.168.2.3	0x46d1	Refused (5)	www.thelastwill.net	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:14.768513918 CET	8.8.8.8	192.168.2.3	0x87cc	No error (0)	www.ty23vip.com		162.209.159.142	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:25.829457998 CET	8.8.8.8	192.168.2.3	0xc5ab	No error (0)	www.allison2patrick.online	allison2patrick.online		CNAME (Canonical name)	IN (0x0001)	false

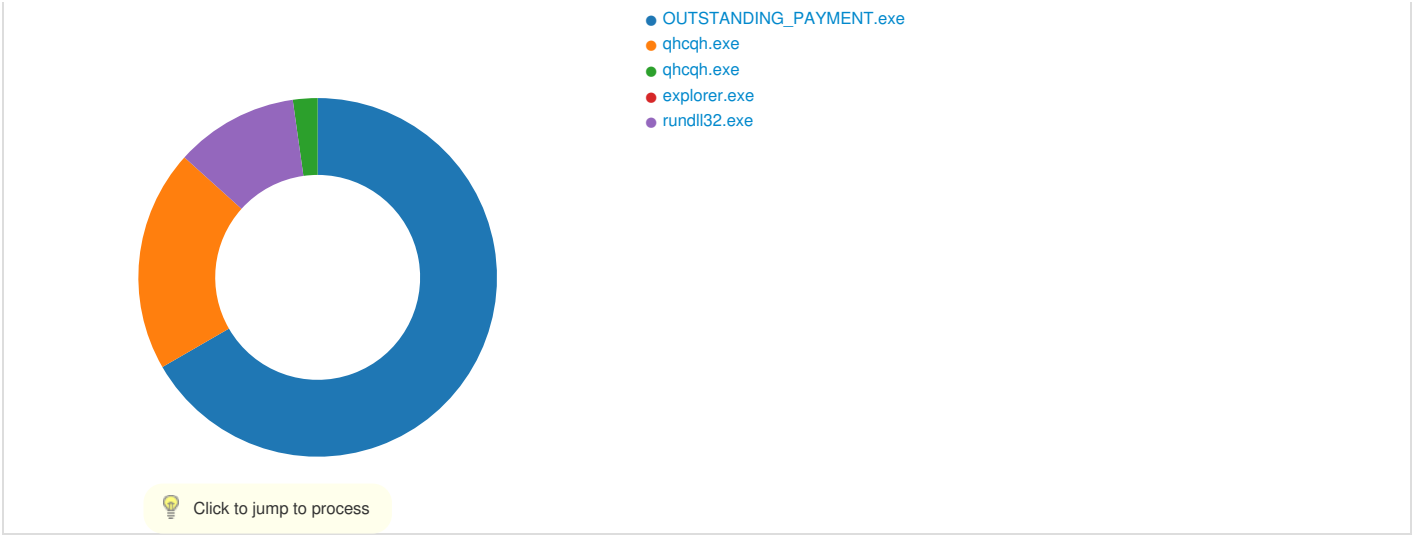
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 09:10:25.829457998 CET	8.8.8.8	192.168.2.3	0xc5ab	No error (0)	allison2patrick.online		62.4.21.190	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:36.065522909 CET	8.8.8.8	192.168.2.3	0x5df2	No error (0)	www.glb-mobility.com	glb-mobility.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:10:36.065522909 CET	8.8.8.8	192.168.2.3	0x5df2	No error (0)	glb-mobility.com		88.99.217.197	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:46.512599945 CET	8.8.8.8	192.168.2.3	0x9aa8	No error (0)	www.fanversewallet.com	fanversewallet.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:10:46.512599945 CET	8.8.8.8	192.168.2.3	0x9aa8	No error (0)	fanversewallet.com		203.245.24.47	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:58.134869099 CET	8.8.8.8	192.168.2.3	0x8e22	No error (0)	www.karlscurry.co.uk		217.160.0.249	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:11.017399073 CET	8.8.8.8	192.168.2.3	0xd22	Server failure (2)	www.themssterofssuepnse.rest	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:37.163110971 CET	8.8.8.8	192.168.2.3	0x528	Server failure (2)	www.brennmansolucioneses.com	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:38.328841925 CET	8.8.8.8	192.168.2.3	0xacb9	Server failure (2)	www.brennmansolucioneses.com	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:39.494823933 CET	8.8.8.8	192.168.2.3	0x43ad	Server failure (2)	www.brennmansolucioneses.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.hudsonandbailey.uk
- www.virginhairweave.co.uk
- www.dirdikyepedia.com
- www.g2fm.co.uk
- www.mynichemarket.co.uk
- www.landlotto.ru
- www.gorwly.top
- www.allison2patrick.online
- www.glb-mobility.com
- www.fanversewallet.com
- www.karlscurry.co.uk

Statistics

Behavior



System Behavior

Analysis Process: OUTSTANDING_PAYMENT.exe PID: 4224, Parent PID: 3452

General

Target ID:	0
Start time:	09:07:40
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\OUTSTANDING_PAYMENT.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\OUTSTANDING_PAYMENT.exe
Imagebase:	0x400000
File size:	297210 bytes
MD5 hash:	4832E17C1F6841AEE2E1984A429ED946
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: qhcqh.exe PID: 5156, Parent PID: 4224

General

Target ID:	1
Start time:	09:07:41
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\qhcqh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\qhcqh.exe" C:\Users\user\AppData\Local\Temp\bpgvtpbkoxw.z
Imagebase:	0xc50000
File size:	59904 bytes
MD5 hash:	41C9E29A7ED3640682A0003BE2DF4D93
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 51%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bpgvtpbkoxw.z	unknown	4096	success or wait	1	C5508D	ReadFile
C:\Users\user\AppData\Local\Temp\bpgvtpbkoxw.z	unknown	4096	success or wait	1	C5508D	ReadFile
C:\Users\user\AppData\Local\Temp\tmjcdbgtyam.ggz	unknown	189952	success or wait	1	27F3368	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	27F398F	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	27F398F	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	27F398F	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	27F398F	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	27F398F	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	27F398F	ReadFile

Analysis Process: qhcqh.exe PID: **5124**, Parent PID: **5156**

General

Target ID:	2
Start time:	09:07:41
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\qhcqh.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\qhcqh.exe
Imagebase:	0xc50000
File size:	59904 bytes
MD5 hash:	41C9E29A7ED3640682A0003BE2DF4D93
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: 00000002.00000002.303713415.0000000000F30000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.303713415.0000000000F30000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.303713415.0000000000F30000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.303334914.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.303334914.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.303334914.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.303576938.0000000000DB0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.303576938.0000000000DB0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.303576938.0000000000DB0000.00000040.10000000.00040000.00000000.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	41E70A	NtReadFile

Analysis Process: explorer.exe PID: **3452**, Parent PID: **5124**

General

Target ID:	3
Start time:	09:07:47
Start date:	20/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69fe90000
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: rundll32.exe PID: **4948**, Parent PID: **3452**

General

Target ID:	13
Start time:	09:08:02
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0xe30000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 0000000D.00000002.777131854.0000000000C40000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.777131854.0000000000C40000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.777131854.0000000000C40000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 0000000D.00000002.778084369.0000000002FA0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.778084369.0000000002FA0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.778084369.0000000002FA0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 0000000D.00000002.777503905.0000000000E00000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.777503905.0000000000E00000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.777503905.0000000000E00000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	high

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\qhcqh.exe	success or wait	1	C5C957	NtDeleteFile
C:\Users\user\AppData\Local\Temp\81EFaKSJ3	object name not found	1	C5C957	NtDeleteFile
C:\Users\user\AppData\Local\Temp\81EFaKSJ3	sharing violation	1	C5C957	NtDeleteFile
C:\Users\user\AppData\Local\Temp\81EFaKSJ3	sharing violation	1	C5C957	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	C5C927	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