ID: 383831
Sample Name: 8sxgohtHjM.exe
Cookbook: default.jbs
Time: 10:46:51
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

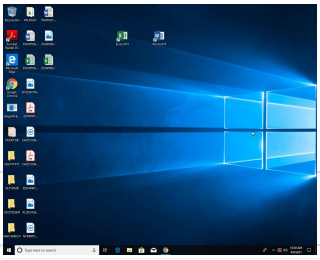
Analysis Report 8sxgohtHjM.exe

Overview

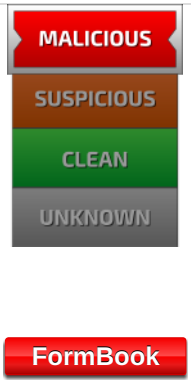
General Information

Sample Name:	8sxgohtHjM.exe
Analysis ID:	383831
MD5:	d381b0a2268051..
SHA1:	7c580bde96219d..
SHA256:	da51c0642c1d22..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

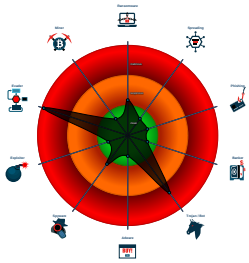


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- 8sxgohtHjM.exe (PID: 6752 cmdline: 'C:\Users\user\Desktop\8sxgohtHjM.exe' MD5: D381B0A2268051AA83B031DDC87EE7DF)
  - 8sxgohtHjM.exe (PID: 7100 cmdline: C:\Users\user\Desktop\8sxgohtHjM.exe MD5: D381B0A2268051AA83B031DDC87EE7DF)
  - 8sxgohtHjM.exe (PID: 7108 cmdline: C:\Users\user\Desktop\8sxgohtHjM.exe MD5: D381B0A2268051AA83B031DDC87EE7DF)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - NETSTAT.EXE (PID: 6656 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.paintersdistrictcouncil.com/vu9b/"
  ],
  "decoy": [
    "longdoggy.net",
    "gylvs.com",
    "evonnemccray.com",
    "nicemoneymaker.com",
    "baby-schutzen.com",
    "xgahovzm.icu",
    "psdcompany.com",
    "makeupjunkiewholesale.com",
    "vz357.com",
    "carshownet.com",
    "forneyus.com",
    "nfoptic.com",
    "lampacosmetiques.com",
    "newmandu.com",
    "localupdate.net",
    "theartofmajur1.com",
    "bancosecurity.website",
    "cabinhealthy.com",
    "tiprent.com",
    "lloydwellsandassociates.com",
    "cekaventure.com",
    "nahomredda.com",
    "transitionmonster.com",
    "apiquet.com",
    "covidbizdisaster.com",
    "darrelbrodkemd.com",
    "sproutsocialleads.com",
    "curtex.info",
    "wsilhavy.net",
    "regaltire.net",
    "sellbulkweed.com",
    "trumedenroll.com",
    "pone2.com",
    "jedinomad.net",
    "sleekandshinebeauty.com",
    "sango-style.com",
    "bjshuangtai.net",
    "shopasadesigns.com",
    "siloamtree.com",
    "happilyeverhughes.net",
    "hayalpresst.com",
    "wfdrc.icu",
    "astronumerolan.com",
    "pvplearing.net",
    "moyoujf.com",
    "bestwishesforyou.online",
    "3erkala.xyz",
    "calificatucasa.com",
    "cuple.info",
    "k-acad.com",
    "iesco.net",
    "investmentresourcesaz.com",
    "4018398.com",
    "cbluedotpanowdbuy.com",
    "llllll0.com",
    "plainsteelforsale.com",
    "abarrotesflorita.com",
    "tunemovie.website",
    "dfendglobal.com",
    "drvincewoodonline.com",
    "support-applela.com",
    "unclejoeandkamala2020.com",
    "frrin.com",
    "pennsylvaniapot.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.520943854.0000000003540000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000010.00000002.520943854.0000000003540000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000010.00000002.520943854.0000000003540000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.311088720.0000000000D00000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.311088720.0000000000D00000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

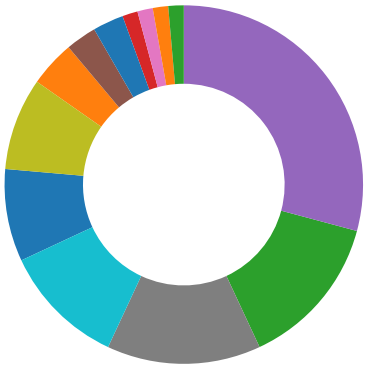
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.8sxgohtHjM.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.8sxgohtHjM.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.8sxgohtHjM.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
4.2.8sxgohtHjM.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.8sxgohtHjM.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

Uses netstat to query active network connections and open ports

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

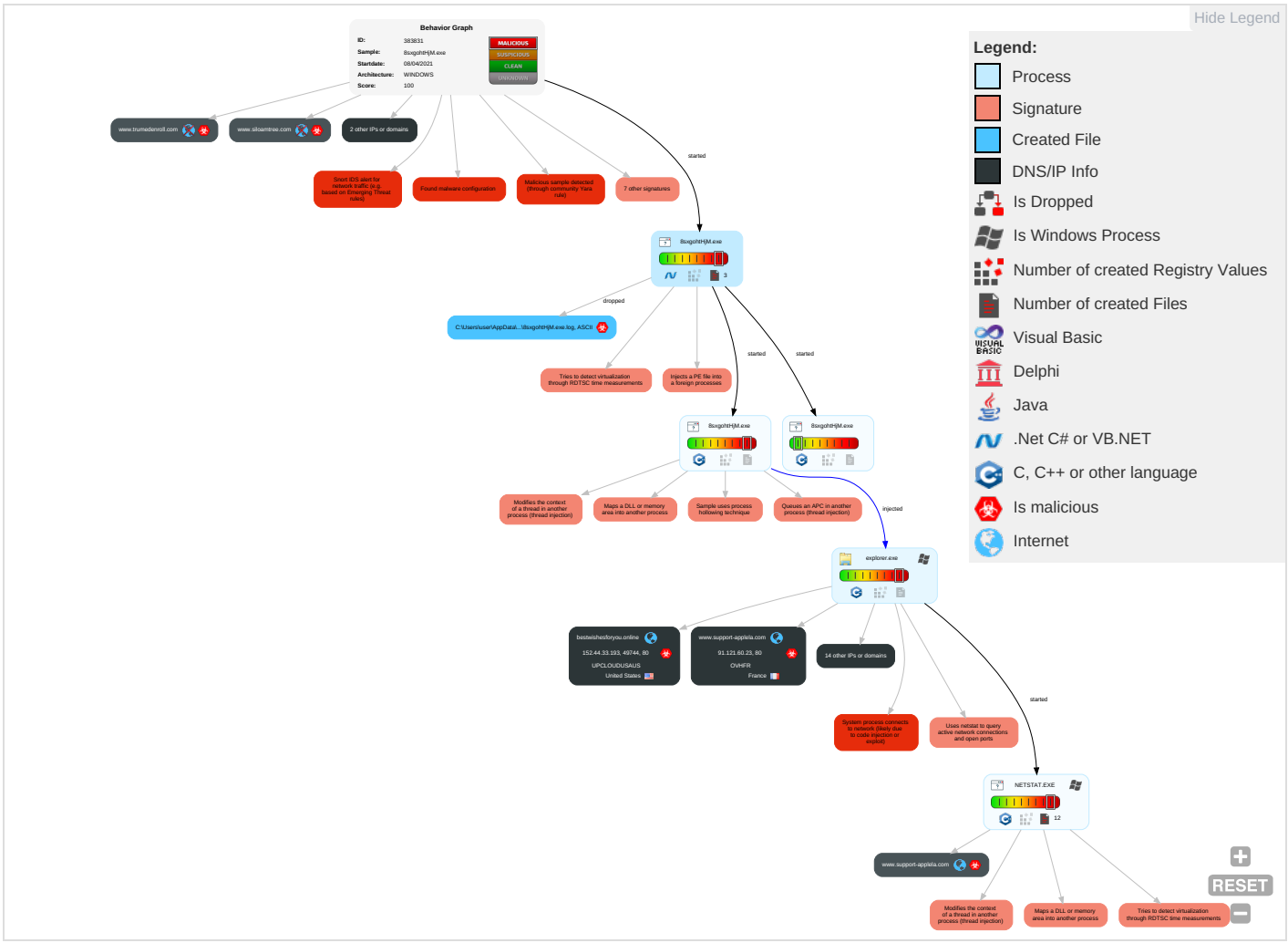
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	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)	Process Injection 6 1 2	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	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Network Connections Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

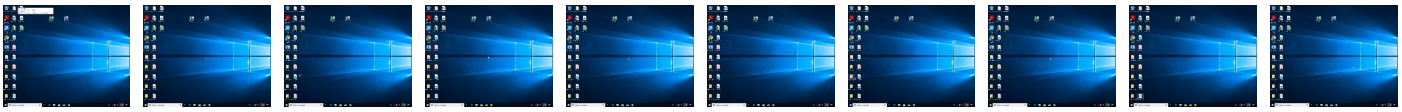
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
8sxgohtHjM.exe	35%	Virustotal		Browse
8sxgohtHjM.exe	33%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
8sxgohtHjM.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.8sxgohtHjM.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.bestwishesforyou.online/vu9b/?uZQL2=D48x&0pn=Ucm1yDKmPu3sqYnPT23C7jNgC5pC+S3WITJgysPBW6tpfdLYpWyQ+yZVED0YNT4HHiqT	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.unclejoeandkamala2020.com/vu9b/?0pn=ZRZicPUHGdpu447/ToshtXbk+LjFT6TcRbqWThirrcjgIxqMd1CJhqCrqkTzpGUGM9/e&uZQL2=D48x	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.nfoptic.com/vu9b/?0pn=TnflO2yLdbi4Ns0f55IiNebWCRsDsubrkj3vpv5xkUkHd7zC3bp6KG+yVlLNRE0xHemI&uZQL2=D48x	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.pone2.com/vu9b/?uZQL2=D48x&0pn=4FRBZlZfmJP1ouB3qG1kZTmIcoiAlBFvqheXtdlBznGFOOcTf1arb+p8J++3khlBMjQo	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.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	
www.paintersdistrictcouncil.com/vu9b/	0%	Avira URL Cloud	safe	
http://www.support-applela.com/vu9b/?0pn=31nFjjjg4oAcb4MokEe	100%	Avira URL Cloud	phishing	
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.nahomredda.com/vu9b/?uZQL2=D48x&0pn=epJyvIJN9Oil2pb9nHYNHIQUuRpQuBcV3xjjobJny1KcYNO6WcXhtFEWRhmWC8oG0KHq	0%	Avira URL Cloud	safe	
http://www.siloamtree.com/vu9b/?uZQL2=D48x&0pn=XOyfHYtLU1lLdZnaXZe4OvPQMiRanaHMlAIcsSmWFWkLxOIqqTB9rasY28K6kY36/QRI	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	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.newmandu.com/?fp=teRCGBRWnsMyQPYBLQzITP%2FRZhRM%2BzRVkHY6lKODoxW9UBFBZ%2BAUTjJBDU4IosgaQp	0%	Avira URL Cloud	safe	
http://www.newmandu.com/vu9b/?0pn=gvDMKnL2DiygUqkLOW8equ0SBtiZsQsp9RF77GdE0oWtaZL2dcC9ipMcSo2LbyxlKRwH&uZQL2=D48x	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	3.13.255.157	true	false		high
trumedenroll.com	184.168.131.241	true	true		unknown
cname.landingi.com	108.128.238.226	true	false		high
www.newmandu.com	208.91.197.91	true	true		unknown
nfoptic.com	34.102.136.180	true	false		unknown
www.support-applela.com	91.121.60.23	true	true		unknown
siloamtree.com	34.102.136.180	true	false		unknown
unclejoeandkamala2020.com	34.102.136.180	true	false		unknown
bestwishesforyou.online	152.44.33.193	true	true		unknown
www.pvplearing.net	unknown	unknown	true		unknown
www.siloamtree.com	unknown	unknown	true		unknown
www.paintersdistrictcouncil.com	unknown	unknown	true		unknown
www.bancosecurity.website	unknown	unknown	true		unknown
www.bestwishesforyou.online	unknown	unknown	true		unknown
www.pone2.com	unknown	unknown	true		unknown
www.trumedenroll.com	unknown	unknown	true		unknown
www.evonnemccray.com	unknown	unknown	true		unknown
www.nfoptic.com	unknown	unknown	true		unknown
www.unclejoeandkamala2020.com	unknown	unknown	true		unknown
www.nahomredda.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.bestwishesforyou.online/vu9b/?uZQL2=D48x&0pn=Ucm1yDKmPu3sqYnPT23C7jNgC5pC+S3WITJgysPBW6tpfdLYpWyQ+yZVED0YNT4HHiqT	true	• Avira URL Cloud: safe	unknown
http://www.unclejoeandkamala2020.com/vu9b/?0pn=ZRZicPUHGdpu447/ToshtXbk+LjFT6TcRbqWThirrcjgIxqMd1CJhqCrqkTzpGUGM9/e&uZQL2=D48x	false	• Avira URL Cloud: safe	unknown
http://www.nfoptic.com/vu9b/?0pn=TnflO2yLdbi4Ns0f55IiNebWCRsDsubrkj3vpv5xkUkHd7zC3bp6KG+yVlLNRE0xHemI&uZQL2=D48x	false	• Avira URL Cloud: safe	unknown
http://www.pone2.com/vu9b/?uZQL2=D48x&0pn=4FRBZlZfmJP1ouB3qG1kZTmIcoiAlBFvqheXtdlBznGFOOcTf1arb+p8J++3khIBMjQo	true	• Avira URL Cloud: safe	unknown
www.paintersdistrictcouncil.com/vu9b/	true	• Avira URL Cloud: safe	low
http://www.nahomredda.com/vu9b/?uZQL2=D48x&0pn=epJyvIJN9OiI2pb9nHYNHIQUuRpQuBcV3xjjobJny1KcYNO6WcXhtFEWRhmWC8oG0KHq	true	• Avira URL Cloud: safe	unknown
http://www.siloamtree.com/vu9b/?uZQL2=D48x&0pn=XOyfHYtLU1lLdZnaXZe4OvPQMiRanaHMlAIcsSmWFWkLxOIqqTB9rasY28K6kY36/QRI	false	• Avira URL Cloud: safe	unknown
http://www.newmandu.com/vu9b/?0pn=gvDMKnL2DiygUqkLOW8equ0SBtiZsQsp9RF77GdE0oWtaZL2dcC9ipMcSo2LbyxlKRwH&uZQL2=D48x	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

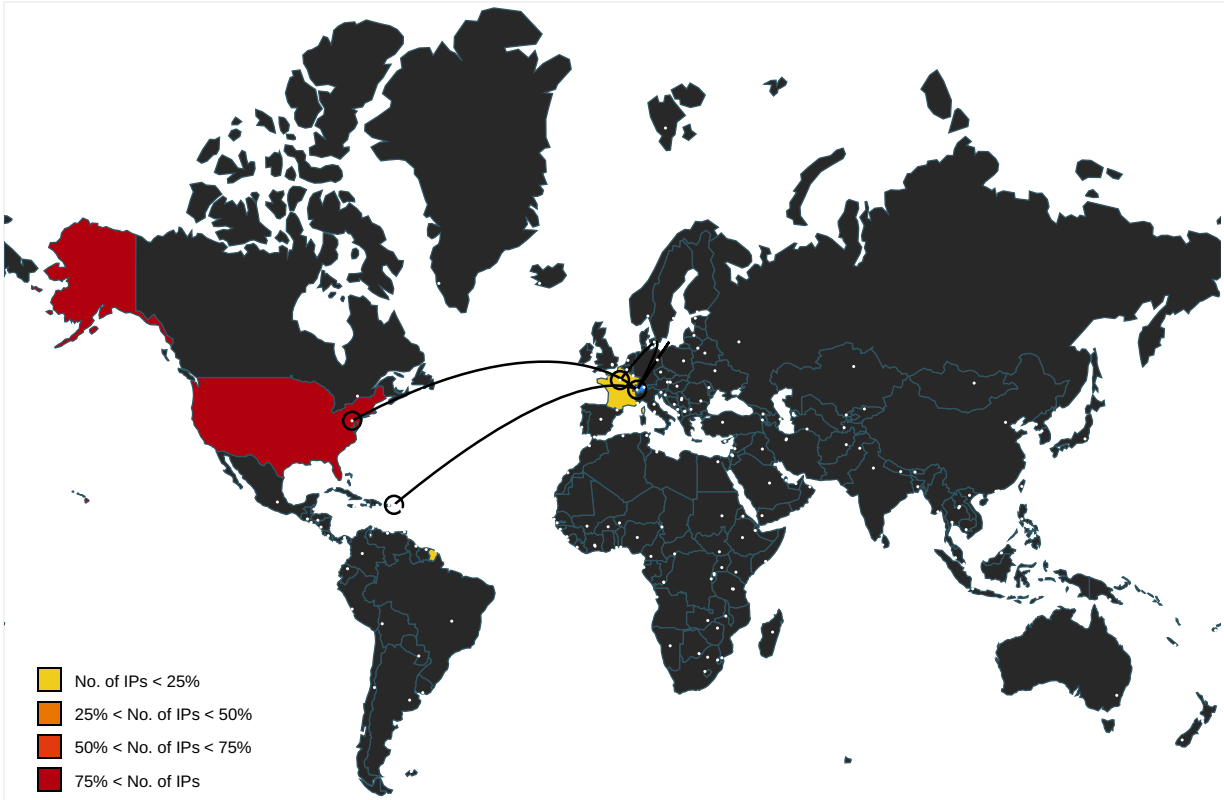
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false		high
http://https://www.gnu.org/licenses/	8sxgohtHjM.exe	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	8sxgohtHjM.exe, 00000000.00000002.270751775.000000000271E000.00000004.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	8sxgohtHjM.exe, 00000000.00000002.270742230.0000000002713000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.support-applela.com/vu9b/?0pn=31nFjjjg4oAcb4MokEe	NETSTAT.EXE, 00000010.00000002.521546345.00000000036FA000.00000004.00000020.sdmp	true	• Avira URL Cloud: phishing	unknown
http://www.jiyu-kobo.co.jp/	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.gnu.org	8sxgohtHjM.exe	false		high
http://www.fontbureau.com/designers8	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fonts.com	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	8sxgohtHjM.exe, 00000000.00000002.270731871.0000000002701000.00000004.00000001.sdmp, 8sxgohtHjM.exe, 00000000.00000002.270751775.000000000271E000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	8sxgohtHjM.exe, 00000000.00000002.274767057.0000000005840000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.294908014.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.newmandu.com/?fp=teRCGBRWnsMyQPYBLQzITP%2FRZhRM%2BzRVkHY6lKODoxW9UBFBZ%2BAUTjJBDU4IosgaQp	NETSTAT.EXE, 00000010.00000002.522730869.00000000041A2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.128.238.226	cname.landingi.com	United States		16509	AMAZON-02US	false
208.91.197.91	www.newmandu.com	Virgin Islands (BRITISH)		40034	CONFLUENCE-NETWORK-INCVG	true
34.102.136.180	nfoptic.com	United States		15169	GOOGLEUS	false
91.121.60.23	www.support-applela.com	France		16276	OVHFR	true
3.13.255.157	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
152.44.33.193	bestwishesforyou.online	United States		25697	UPCLOUDUSAUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383831
Start date:	08.04.2021
Start time:	10:46:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8sxgohtHjM.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:	26
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@6/1@14/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10.1% (good quality ratio 9%) • Quality average: 71.2% • Quality standard deviation: 32.8%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.139.144, 40.88.32.150, 52.147.198.201, 104.42.151.234, 95.100.54.203, 104.43.193.48, 20.50.102.62, 23.10.249.26, 23.10.249.43, 20.54.26.129, 20.82.210.154 • Excluded domains from analysis (whitelisted): fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:48:09	API Interceptor	1x Sleep call for process: 8sxgohtHjM.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
108.128.238.226	Product list.xlsx	Get hash	malicious	Browse	• www.nahomredda.com/vu9b/?-ZltiVX8=epJyvIJI9JiM25XxlHYNHIQUuRpQuBcV3x7z0YVm2VKdY8i8RMGt7B8USEKAGss1/JaaiQ==&RfR4I=JR-06F20O6g
	WaybillDoc_6848889025.xlsx	Get hash	malicious	Browse	• www.sharonrebucas.com/zn7/?Onm8=SDduXp1o7dE71Da9+0V04Ztckfd fPP4tr6m4xYquXCp64QmrI4GriJ50Xm5wysiJ8nfb8g==&MtApfP=GPB8rNApHF1D
208.91.197.91	PRC-20-518 ORIGINAL.xlsx	Get hash	malicious	Browse	• www.chitrakaah.com/g050/?MBN0yn=gh6gYfQCrnQBnQvKqXR1BBdq6I0/ia6nXcyoJzz4U03ljs0U8DV8qCnN3+fv2J4IGdTu1A==&2dht=XHE0Qdm
	ORIGINAL SHIPPING DOCUMENTSPDF.exe	Get hash	malicious	Browse	• www.rajeshpaul.com/qqeq/?D8IxB=7nSpJtUpafTlT6&eb=my9HLCyGyTUI7ijeZNMt9rsHqU3anFReddNHkecDwv0iZCMXfCC6FueMusiXp9GGW0pUqn5axA==
	PO#7689.zip.exe	Get hash	malicious	Browse	• www.greenlightsmokables.com/md5/?Jzu4_4C=zHBqlneB+dU0jWTqKpl7P0UhTg+HlH4MpY8JEipF1WP+CJ4l7o5pEqU4RJVuKm5urAdq&NrThfj=D48x
	products order pdf.exe	Get hash	malicious	Browse	• www.tudeladirecto.com/nt8e/?wTX=EFNpsN9xNb-Dd&n4p=d5sTnujAaLwCHAV7Hkod4AGONRw1Ceya8p7QHyuAjU2hemaQC5CnvhOz2MROTqxwdpcV

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	7Q5Er1TObp.exe	Get hash	malicious	Browse	• www.newmandu.com/vu9b/?FTjl4F=gvDMKnL2DiygUqkLOW8equ0SBtiZsQsp9RF77GdE0oWtaZL2dcC9ipMcSo2LbyxlKRwH&vRDtx=khL0M89p_R8hBZa
	New Purchase Order.exe	Get hash	malicious	Browse	• www.fairview.global/noi6/?Ktklc=djQtGmR2ozp5r2jxyahjtN1TJLTs4NvNMxVFhpbWlLclFF8JTFJQ/pXyn76jflCi7GGZ&lzul=z8o4n2BhWV
	Bombermania.exe	Get hash	malicious	Browse	• live.interballs.com/reporting_server/
	Bombermania.exe	Get hash	malicious	Browse	• live.interballs.com/reporting_server/
	2021_03_16.exe	Get hash	malicious	Browse	• www.ltc-gold.com/2bg/?lnud=/i/lb+Dffob7lMQ5ivcx1VEzEzf2K5SYmZpCl/xPFCYFxY/A/vBZb7BF8LsLTj5bzBQKXYQmxg==&1bm=3fedQNQ0wlQl0H
	orii11.exe	Get hash	malicious	Browse	• www.fotoincasa.com/mdi/?8pp=r1iONhcrP0pbpGclQVhVGgc+Q37F54QKHkqxX6oGe/sLqU52wzsf7IojbzpCHshmMIC4&sZCx=1bYdfPf8ef5pjPm
	bnb.exe	Get hash	malicious	Browse	• www.fotoincasa.com/mdi/?Jh=r1iONhcrP0pbpGclQVhVGgc+Q37F54QKHkqxX6oGe/sLqU52wzsf7IojbzpoYcRmIKK4&njl0d=Rzuls4
	Purchase Order.exe	Get hash	malicious	Browse	• www.fairview.global/noi6/?rXOp32I=djQtGmR2ozp5r2jxyahjtN1TJLTs4NvNMxVFhpbWlLclFF8JTFJQ/pXyn76JA4yi/EOZ&Bd4Dh=CX6p

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO_98276300.exe	Get hash	malicious	Browse	• www.ojavedа.com/ame8/?8p=TUdynzXewDV4R6hcP/TtpIkDjP+ZRmt16Hw3snKWLRaKzibVm3POi5J75QFaIAfkEyg3&Cb=hN98bjZH
	DHL_receipt.exe	Get hash	malicious	Browse	• www.greenlightsmokable.com/s8gq/?GVTl=CdTDr&CtxLR=GcXO2lQJXedQXP0VXXtwOzFelwMaLaizNNb08pvp0e1v1F0rbo8J5l47qDnDSsA31Tvl
	QUOTATION00187612.exe	Get hash	malicious	Browse	• www.gamingmag.online/nsk/?5juH1Lw=DnZ6smjvmKtwuwAXRixl0xHJiuXjV7QbSQXcUxw83NwxPjQzvt78aHwZY7I20FYugkDr&kxl0dL=nDH8a8R86Pb8o
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• www.pathwaysnorman.com/idir/?jFNhC=QcfpPsZsTQkbfi9dIqkstDiu8gpji7zGKQT9CcYXB17rdgdInICGKPMkjk7u0mNGiAFDxGC1Zg==&PlHT0=_6g89p5H3xehg
	DHL Document. PDF.exe	Get hash	malicious	Browse	• www.xpressteamironing.com/d8ak/?Szr0s4=GfmXTYq2Yn2AckQWwnE6BBibtFv31Qjt2UWEfiHUUpW9PpEAUCSsafVf838QtlI0BZoH7o+vNw==&QL3=uTyTqJdh5XE07
	INV.xlsx	Get hash	malicious	Browse	• www.h-v-biz.com/c8so/?cf=hsMrMOU/4wmWTnQK7BegBqlrTsujOywA7VbOlqdg4Ej/UmxkJ2Rbh4V4PlD+e7xk19hcsA==&nH4xu=erRXJfgPJ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6tivtkKtQx.exe	Get hash	malicious	Browse	• www.h-v-biz.com/c8so/?BZL0RN=hsMrMOU643mST3cG5BegBqlrTsujOywA7VDeUpBh8kj+UXdiOmAX38t6MDDBZrJv3dJ61wwARA==&3fPHK=w8O8gTXxNJq
	k5K4BcM1b5.exe	Get hash	malicious	Browse	• www.athleteshive.com/gqx2/?NBtLW=kdwz49ReWeybRPZJolgC7QJtxuB/meiNTkYp+nGTjDB+7BQCfNz2YW0PX4LStuRlOVbvsJZwJw==&tTxX=Apm0n4
91.121.60.23	yQh96Jd6TZ.exe	Get hash	malicious	Browse	
	Product list.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	vbc.exe	Get hash	malicious	Browse	• 3.13.255.157
	Order Inquiry.exe	Get hash	malicious	Browse	• 3.14.206.30
	PaymentAdvice.exe	Get hash	malicious	Browse	• 3.14.206.30
	BL01345678053567.exe	Get hash	malicious	Browse	• 3.14.206.30
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 3.14.206.30
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 3.13.255.157
	shipping documents.exe	Get hash	malicious	Browse	• 3.14.206.30
	BL836477488575.exe	Get hash	malicious	Browse	• 3.13.255.157
	Certrificate Confirmation.exe	Get hash	malicious	Browse	• 3.14.206.30
	TT COPY.exe	Get hash	malicious	Browse	• 3.14.206.30
	PaymentInvoice.exe	Get hash	malicious	Browse	• 3.13.255.157
	Swift 76498,pdf.exe	Get hash	malicious	Browse	• 3.14.206.30
	swift_76567643.exe	Get hash	malicious	Browse	• 52.15.160.167
	BL COPY.exe	Get hash	malicious	Browse	• 52.15.160.167
	MV WAF PASSION.exe	Get hash	malicious	Browse	• 3.131.252.17
	CUFUYO.exe	Get hash	malicious	Browse	• 52.15.160.167
	IMG_963394832387043.jpg.exe	Get hash	malicious	Browse	• 52.15.160.167
	TNUiVpymgH.exe	Get hash	malicious	Browse	• 3.131.252.17
	NEW ORDER.exe	Get hash	malicious	Browse	• 52.15.160.167
	Lista de nuevos pedidos.exe	Get hash	malicious	Browse	• 52.15.160.167
cname.landingi.com	yQh96Jd6TZ.exe	Get hash	malicious	Browse	• 54.77.19.84
	Paymonth invoice.exe	Get hash	malicious	Browse	• 54.77.19.84
	Product list.xlsx	Get hash	malicious	Browse	• 108.128.238.226
	WaybillDoc_6848889025.xlsx	Get hash	malicious	Browse	• 108.128.238.226
	quotation.exe	Get hash	malicious	Browse	• 52.212.68.12
	qpFvMReV7S.exe	Get hash	malicious	Browse	• 108.128.238.226
	900821.exe	Get hash	malicious	Browse	• 52.208.196.199
www.support-applela.com	yQh96Jd6TZ.exe	Get hash	malicious	Browse	• 91.121.60.23
	Product list.xlsx	Get hash	malicious	Browse	• 91.121.60.23
www.newmandu.com	7Q5Er1TObp.exe	Get hash	malicious	Browse	• 208.91.197.91

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CONFLUENCE-NETWORK-INCVG	PO7321.exe	Get hash	malicious	Browse	• 208.91.197.39
	PRC-20-518 ORIGINAL.xlsx	Get hash	malicious	Browse	• 208.91.197.39
	Lista e porosive te blerjes.exe	Get hash	malicious	Browse	• 209.99.64.33

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BL836477488575.exe	Get hash	malicious	Browse	• 204.11.56.48
	BL84995005038483.exe	Get hash	malicious	Browse	• 204.11.56.48
	DHL Shipping Documents.exe	Get hash	malicious	Browse	• 208.91.197.27
	Formbook.exe	Get hash	malicious	Browse	• 204.11.56.48
	ORIGINAL SHIPPING DOCUMENTSPDF.exe	Get hash	malicious	Browse	• 208.91.197.91
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• 208.91.197.27
	bank details.exe	Get hash	malicious	Browse	• 208.91.197.27
	PO#7689.zip.exe	Get hash	malicious	Browse	• 208.91.197.91
	ORDER_PDF.exe	Get hash	malicious	Browse	• 209.99.64.18
	deIt7iuD1y.exe	Get hash	malicious	Browse	• 204.11.56.48
	Bista_094924,ppdf.exe	Get hash	malicious	Browse	• 208.91.197.27
	PO_RFQ007899_PDF.exe	Get hash	malicious	Browse	• 209.99.64.55
	PaymentInvoice.exe	Get hash	malicious	Browse	• 208.91.197.39
	products order pdf.exe	Get hash	malicious	Browse	• 208.91.197.91
	ZGNbR8E726.exe	Get hash	malicious	Browse	• 204.11.56.48
	MV Sky Marine.xlsx	Get hash	malicious	Browse	• 204.11.56.48
	DH7v8T4xFa.exe	Get hash	malicious	Browse	• 208.91.197.27
OVHFR	C7SRTTLgsn.exe	Get hash	malicious	Browse	• 54.36.27.31
	ApuE9QrdQxe7Um6.exe	Get hash	malicious	Browse	• 66.70.204.222
	YReGeOs683XKMn4.exe	Get hash	malicious	Browse	• 51.195.53.221
	LCSXS44U22.exe	Get hash	malicious	Browse	• 54.36.27.31
	Ewkoo9igCN.dll	Get hash	malicious	Browse	• 51.91.76.89
	49Bvnq7iFK.dll	Get hash	malicious	Browse	• 51.91.76.89
	OtOXfybCmW.dll	Get hash	malicious	Browse	• 51.91.76.89
	Ewkoo9igCN.dll	Get hash	malicious	Browse	• 51.91.76.89
	W3aLwWHvWB.dll	Get hash	malicious	Browse	• 51.91.76.89
	IJh1SAcSNP.dll	Get hash	malicious	Browse	• 51.91.76.89
	OtOXfybCmW.dll	Get hash	malicious	Browse	• 51.91.76.89
	afC9TbiOWl.dll	Get hash	malicious	Browse	• 51.91.76.89
	wABiemJeyB.dll	Get hash	malicious	Browse	• 51.91.76.89
	l316Yh2noM.dll	Get hash	malicious	Browse	• 51.91.76.89
	W3aLwWHvWB.dll	Get hash	malicious	Browse	• 51.91.76.89
	IJh1SAcSNP.dll	Get hash	malicious	Browse	• 51.91.76.89
	afC9TbiOWl.dll	Get hash	malicious	Browse	• 51.91.76.89
	9iJMZNQTad.dll	Get hash	malicious	Browse	• 51.91.76.89
	wABiemJeyB.dll	Get hash	malicious	Browse	• 51.91.76.89
	r4fUczb42h.dll	Get hash	malicious	Browse	• 51.91.76.89
AMAZON-02US	eQLPRPErea.exe	Get hash	malicious	Browse	• 13.248.216.40
	vbc.exe	Get hash	malicious	Browse	• 3.13.255.157
	o2KKHvtb3c.exe	Get hash	malicious	Browse	• 18.218.104.192
	Order Inquiry.exe	Get hash	malicious	Browse	• 3.14.206.30
	6IGbftBsBg.exe	Get hash	malicious	Browse	• 104.192.141.1
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 52.218.213.96
	PaymentAdvice.exe	Get hash	malicious	Browse	• 3.14.206.30
	ikoAlmKWvI.exe	Get hash	malicious	Browse	• 104.192.141.1
	BL01345678053567.exe	Get hash	malicious	Browse	• 3.14.206.30
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	Statement of Account.xlsx	Get hash	malicious	Browse	• 15.165.26.252
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 52.217.8.51
	bmws51TeIm.exe	Get hash	malicious	Browse	• 3.141.177.1
	Receipt779G0D675432.html	Get hash	malicious	Browse	• 52.219.97.138
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 52.51.245.167
	Documents_460000622_1464906353.xls	Get hash	malicious	Browse	• 52.12.4.186
	comprobante de pago bancario.exe	Get hash	malicious	Browse	• 44.227.76.166
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 3.13.255.157
	shipping documents.exe	Get hash	malicious	Browse	• 3.14.206.30

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8sxgohtHjM.exe.log	
Process:	C:\Users\user\Desktop\8sxgohtHjM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.785317811577518
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	8sxgohtHjM.exe
File size:	585728
MD5:	d381b0a2268051aa83b031ddc87ee7df
SHA1:	7c580bde96219de369ad1503d62703e77c4c3fa6
SHA256:	da51c0642c1d22815991ec7f4da9f27206352ee2c5419d29af09cb69688b0b47
SHA512:	d06241c1a89819b9961cdaf1be2f30af6e44cbca51d702d87a9c3d57453242d5f688119726a6d87e4ece8bff7e8eb91706a18181443a86665ddeb44323aaa4e5
SSDEEP:	12288:YM7OsIVW7F3vllYIk9gkZsTSr6cTbjoN9xr249psBX:1OsAOlilVk9r6uwiX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...VDn`.....P.....~.... .....@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x49037e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x606E4456 [Wed Apr 7 23:46:30 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x90328	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x92000	0x800	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x94000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x8e384	0x8e400	False	0.882462379174	data	7.7978615602	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x92000	0x800	0x800	False	0.3447265625	data	3.53195008008	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x94000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x92090	0x3d4	data		
RT_MANIFEST	0x92474	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	AssemblyTitleAttribute.exe
FileVersion	1.0.0.0
CompanyName	BobbleSoft
LegalTrademarks	
Comments	Converts one textual format to another.
ProductName	Format Converter
ProductVersion	1.0.0.0
FileDescription	Format Converter
OriginalFilename	AssemblyTitleAttribute.exe

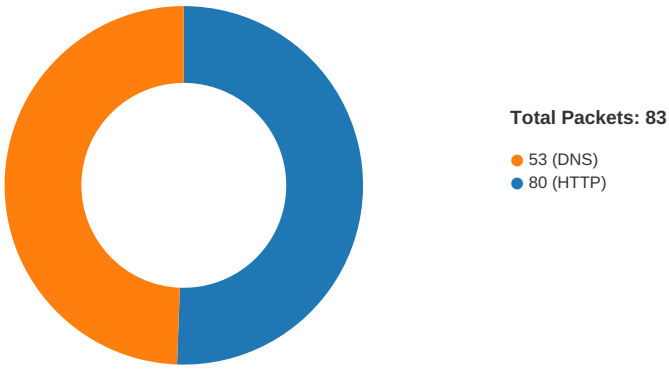
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-10:48:49.840874	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.3	108.128.238.226
04/08/21-10:48:49.840874	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.3	108.128.238.226

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-10:48:49.840874	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.3	108.128.238.226
04/08/21-10:49:05.183074	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49737	34.102.136.180	192.168.2.3
04/08/21-10:49:57.294074	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.3	208.91.197.91
04/08/21-10:49:57.294074	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.3	208.91.197.91
04/08/21-10:49:57.294074	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.3	208.91.197.91
04/08/21-10:50:08.043181	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49745	34.102.136.180	192.168.2.3
04/08/21-10:50:13.109870	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49746	80	192.168.2.3	34.102.136.180
04/08/21-10:50:13.109870	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49746	80	192.168.2.3	34.102.136.180
04/08/21-10:50:13.109870	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49746	80	192.168.2.3	34.102.136.180
04/08/21-10:50:13.227869	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49746	34.102.136.180	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:48:49.800071955 CEST	49727	80	192.168.2.3	108.128.238.226
Apr 8, 2021 10:48:49.840373993 CEST	80	49727	108.128.238.226	192.168.2.3
Apr 8, 2021 10:48:49.840626955 CEST	49727	80	192.168.2.3	108.128.238.226
Apr 8, 2021 10:48:49.840873957 CEST	49727	80	192.168.2.3	108.128.238.226
Apr 8, 2021 10:48:49.881361008 CEST	80	49727	108.128.238.226	192.168.2.3
Apr 8, 2021 10:48:49.881459951 CEST	80	49727	108.128.238.226	192.168.2.3
Apr 8, 2021 10:48:49.881586075 CEST	49727	80	192.168.2.3	108.128.238.226
Apr 8, 2021 10:48:49.881968021 CEST	49727	80	192.168.2.3	108.128.238.226
Apr 8, 2021 10:48:49.921756983 CEST	80	49727	108.128.238.226	192.168.2.3
Apr 8, 2021 10:49:04.986361027 CEST	49737	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:49:04.998783112 CEST	80	49737	34.102.136.180	192.168.2.3
Apr 8, 2021 10:49:04.998888016 CEST	49737	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:49:04.999016047 CEST	49737	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:49:05.011384964 CEST	80	49737	34.102.136.180	192.168.2.3
Apr 8, 2021 10:49:05.183073997 CEST	80	49737	34.102.136.180	192.168.2.3
Apr 8, 2021 10:49:05.183109045 CEST	80	49737	34.102.136.180	192.168.2.3
Apr 8, 2021 10:49:05.183301926 CEST	49737	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:49:05.183351040 CEST	49737	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:49:05.196171045 CEST	80	49737	34.102.136.180	192.168.2.3
Apr 8, 2021 10:49:25.580018044 CEST	49738	80	192.168.2.3	91.121.60.23
Apr 8, 2021 10:49:28.581443071 CEST	49738	80	192.168.2.3	91.121.60.23
Apr 8, 2021 10:49:34.581850052 CEST	49738	80	192.168.2.3	91.121.60.23
Apr 8, 2021 10:49:48.670568943 CEST	49741	80	192.168.2.3	91.121.60.23

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:49:51.677001953 CEST	49741	80	192.168.2.3	91.121.60.23
Apr 8, 2021 10:49:51.767041922 CEST	49742	80	192.168.2.3	3.13.255.157
Apr 8, 2021 10:49:51.877587080 CEST	80	49742	3.13.255.157	192.168.2.3
Apr 8, 2021 10:49:51.877728939 CEST	49742	80	192.168.2.3	3.13.255.157
Apr 8, 2021 10:49:51.877827883 CEST	49742	80	192.168.2.3	3.13.255.157
Apr 8, 2021 10:49:51.988086939 CEST	80	49742	3.13.255.157	192.168.2.3
Apr 8, 2021 10:49:51.988156080 CEST	80	49742	3.13.255.157	192.168.2.3
Apr 8, 2021 10:49:51.988187075 CEST	80	49742	3.13.255.157	192.168.2.3
Apr 8, 2021 10:49:51.988426924 CEST	49742	80	192.168.2.3	3.13.255.157
Apr 8, 2021 10:49:51.988699913 CEST	49742	80	192.168.2.3	3.13.255.157
Apr 8, 2021 10:49:52.099188089 CEST	80	49742	3.13.255.157	192.168.2.3
Apr 8, 2021 10:49:57.147592068 CEST	49743	80	192.168.2.3	208.91.197.91
Apr 8, 2021 10:49:57.293652058 CEST	80	49743	208.91.197.91	192.168.2.3
Apr 8, 2021 10:49:57.293806076 CEST	49743	80	192.168.2.3	208.91.197.91
Apr 8, 2021 10:49:57.294074059 CEST	49743	80	192.168.2.3	208.91.197.91
Apr 8, 2021 10:49:57.440273046 CEST	80	49743	208.91.197.91	192.168.2.3
Apr 8, 2021 10:49:57.479624987 CEST	80	49743	208.91.197.91	192.168.2.3
Apr 8, 2021 10:49:57.479655981 CEST	80	49743	208.91.197.91	192.168.2.3
Apr 8, 2021 10:49:57.479671001 CEST	80	49743	208.91.197.91	192.168.2.3
Apr 8, 2021 10:49:57.479830980 CEST	49743	80	192.168.2.3	208.91.197.91
Apr 8, 2021 10:49:57.480165005 CEST	49743	80	192.168.2.3	208.91.197.91
Apr 8, 2021 10:49:57.514394045 CEST	80	49743	208.91.197.91	192.168.2.3
Apr 8, 2021 10:49:57.514514923 CEST	49743	80	192.168.2.3	208.91.197.91
Apr 8, 2021 10:49:57.626471996 CEST	80	49743	208.91.197.91	192.168.2.3
Apr 8, 2021 10:49:57.693111897 CEST	49741	80	192.168.2.3	91.121.60.23
Apr 8, 2021 10:50:02.625783920 CEST	49744	80	192.168.2.3	152.44.33.193
Apr 8, 2021 10:50:02.736835957 CEST	80	49744	152.44.33.193	192.168.2.3
Apr 8, 2021 10:50:02.737078905 CEST	49744	80	192.168.2.3	152.44.33.193
Apr 8, 2021 10:50:02.737376928 CEST	49744	80	192.168.2.3	152.44.33.193
Apr 8, 2021 10:50:02.848086119 CEST	80	49744	152.44.33.193	192.168.2.3
Apr 8, 2021 10:50:02.848124027 CEST	80	49744	152.44.33.193	192.168.2.3
Apr 8, 2021 10:50:02.848407984 CEST	80	49744	152.44.33.193	192.168.2.3
Apr 8, 2021 10:50:02.848552942 CEST	49744	80	192.168.2.3	152.44.33.193
Apr 8, 2021 10:50:02.848601103 CEST	49744	80	192.168.2.3	152.44.33.193
Apr 8, 2021 10:50:02.959345102 CEST	80	49744	152.44.33.193	192.168.2.3
Apr 8, 2021 10:50:07.914855003 CEST	49745	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:50:07.927746058 CEST	80	49745	34.102.136.180	192.168.2.3
Apr 8, 2021 10:50:07.927865982 CEST	49745	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:50:07.928015947 CEST	49745	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:50:07.940891981 CEST	80	49745	34.102.136.180	192.168.2.3
Apr 8, 2021 10:50:08.043180943 CEST	80	49745	34.102.136.180	192.168.2.3
Apr 8, 2021 10:50:08.043205023 CEST	80	49745	34.102.136.180	192.168.2.3
Apr 8, 2021 10:50:08.043450117 CEST	49745	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:50:08.043561935 CEST	49745	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:50:08.056231022 CEST	80	49745	34.102.136.180	192.168.2.3
Apr 8, 2021 10:50:13.097506046 CEST	49746	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:50:13.109659910 CEST	80	49746	34.102.136.180	192.168.2.3
Apr 8, 2021 10:50:13.109781027 CEST	49746	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:50:13.109869957 CEST	49746	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:50:13.122262001 CEST	80	49746	34.102.136.180	192.168.2.3
Apr 8, 2021 10:50:13.227869034 CEST	80	49746	34.102.136.180	192.168.2.3
Apr 8, 2021 10:50:13.227902889 CEST	80	49746	34.102.136.180	192.168.2.3
Apr 8, 2021 10:50:13.228168011 CEST	49746	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:50:13.228198051 CEST	49746	80	192.168.2.3	34.102.136.180
Apr 8, 2021 10:50:13.241094112 CEST	80	49746	34.102.136.180	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:47:43.767472982 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:47:43.780256987 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 8, 2021 10:47:44.549355984 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:47:44.562393904 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 10:47:45.390475035 CEST	64938	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:47:45.403153896 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 10:47:46.167490959 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:47:46.180757999 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 8, 2021 10:47:47.192456007 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:47:47.205771923 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:02.979878902 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:02.992888927 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:06.020994902 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:06.033951044 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:09.686635971 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:09.704866886 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:11.232563972 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:11.245111942 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:12.179533958 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:12.192090034 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:13.244406939 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:13.256509066 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:14.543807983 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:14.557054996 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:15.705270052 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:15.717885971 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:16.424599886 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:16.439021111 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:23.047386885 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:23.059376955 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:26.042622089 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:26.056108952 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:27.773591995 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:27.786364079 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:28.509497881 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:28.521418095 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:29.507829905 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:29.521481037 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:31.422092915 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:31.435568094 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:32.741475105 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:32.754563093 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:45.363080978 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:45.375853062 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:49.768059015 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:49.792867899 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:54.115600109 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:54.141582966 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 10:48:59.911103010 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:48:59.928137064 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 10:49:00.875983953 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:49:00.893342018 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 10:49:03.917886972 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:49:03.935990095 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 10:49:04.962331057 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:49:04.985348940 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 10:49:10.193857908 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:49:10.225215912 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 10:49:15.242029905 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:49:15.273442030 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 10:49:20.325412035 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:49:20.389976025 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 8, 2021 10:49:25.399233103 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:49:25.577531099 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 8, 2021 10:49:36.198688030 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:49:36.211636066 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 8, 2021 10:49:38.135968924 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:49:38.162513971 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 10:49:48.474037886 CEST	61946	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:49:48.640762091 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 8, 2021 10:49:51.644726038 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:49:51.765275002 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 10:49:56.999083042 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:49:57.145478964 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 8, 2021 10:50:02.496042013 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:50:02.623742104 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 8, 2021 10:50:07.879797935 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:50:07.913424969 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 8, 2021 10:50:13.057121038 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:50:13.096925020 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 8, 2021 10:50:18.242928028 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:50:18.266840935 CEST	53	58784	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 10:48:49.768059015 CEST	192.168.2.3	8.8.8.8	0x49da	Standard query (0)	www.nahomredda.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:48:59.911103010 CEST	192.168.2.3	8.8.8.8	0x2c82	Standard query (0)	www.paintersdistrictcouncil.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:04.962331057 CEST	192.168.2.3	8.8.8.8	0x5440	Standard query (0)	www.nfoptic.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:10.193857908 CEST	192.168.2.3	8.8.8.8	0xabbb	Standard query (0)	www.pvplearing.net	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:15.242029905 CEST	192.168.2.3	8.8.8.8	0x367c	Standard query (0)	www.bancosecurity.website	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:20.325412035 CEST	192.168.2.3	8.8.8.8	0x7b39	Standard query (0)	www.evonnemccray.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:25.399233103 CEST	192.168.2.3	8.8.8.8	0x7f30	Standard query (0)	www.support-applela.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:48.474037886 CEST	192.168.2.3	8.8.8.8	0x4a0b	Standard query (0)	www.support-applela.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:51.644726038 CEST	192.168.2.3	8.8.8.8	0x61ca	Standard query (0)	www.pone2.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:56.999083042 CEST	192.168.2.3	8.8.8.8	0x2107	Standard query (0)	www.newmandu.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:02.496042013 CEST	192.168.2.3	8.8.8.8	0x5799	Standard query (0)	www.bestwishesforyou.online	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:07.879797935 CEST	192.168.2.3	8.8.8.8	0xe5d5	Standard query (0)	www.unclejoeandkamala2020.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:13.057121038 CEST	192.168.2.3	8.8.8.8	0x7e01	Standard query (0)	www.siloamtree.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:18.242928028 CEST	192.168.2.3	8.8.8.8	0x271c	Standard query (0)	www.trumedenroll.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 10:48:49.792867899 CEST	8.8.8.8	192.168.2.3	0x49da	No error (0)	www.nahomredda.com	cname.landingi.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:48:49.792867899 CEST	8.8.8.8	192.168.2.3	0x49da	No error (0)	cname.landingi.com		108.128.238.226	A (IP address)	IN (0x0001)
Apr 8, 2021 10:48:49.792867899 CEST	8.8.8.8	192.168.2.3	0x49da	No error (0)	cname.landingi.com		54.77.19.84	A (IP address)	IN (0x0001)
Apr 8, 2021 10:48:49.792867899 CEST	8.8.8.8	192.168.2.3	0x49da	No error (0)	cname.landingi.com		52.212.68.12	A (IP address)	IN (0x0001)
Apr 8, 2021 10:48:59.928137064 CEST	8.8.8.8	192.168.2.3	0x2c82	Name error (3)	www.paintersdistrictcouncil.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:04.985348940 CEST	8.8.8.8	192.168.2.3	0x5440	No error (0)	www.nfoptic.com	nfoptic.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:49:04.985348940 CEST	8.8.8.8	192.168.2.3	0x5440	No error (0)	nfoptic.com		34.102.136.180	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 10:49:10.225215912 CEST	8.8.8.8	192.168.2.3	0xabbb	Name error (3)	www.pvpleering.net	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:15.273442030 CEST	8.8.8.8	192.168.2.3	0x367c	Name error (3)	www.bancosecurity.website	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:20.389976025 CEST	8.8.8.8	192.168.2.3	0x7b39	Name error (3)	www.evonnemccray.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:25.577531099 CEST	8.8.8.8	192.168.2.3	0x7f30	No error (0)	www.support-applela.com		91.121.60.23	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:48.640762091 CEST	8.8.8.8	192.168.2.3	0x4a0b	No error (0)	www.support-applela.com		91.121.60.23	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:51.765275002 CEST	8.8.8.8	192.168.2.3	0x61ca	No error (0)	www.pone2.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:49:51.765275002 CEST	8.8.8.8	192.168.2.3	0x61ca	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.13.255.157	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:51.765275002 CEST	8.8.8.8	192.168.2.3	0x61ca	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.14.206.30	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:51.765275002 CEST	8.8.8.8	192.168.2.3	0x61ca	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		52.15.160.167	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:57.145478964 CEST	8.8.8.8	192.168.2.3	0x2107	No error (0)	www.newmandu.com		208.91.197.91	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:02.623742104 CEST	8.8.8.8	192.168.2.3	0x5799	No error (0)	www.bestwishesforyou.online	bestwishesforyou.online		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:50:02.623742104 CEST	8.8.8.8	192.168.2.3	0x5799	No error (0)	bestwishesforyou.online		152.44.33.193	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:07.913424969 CEST	8.8.8.8	192.168.2.3	0xe5d5	No error (0)	www.unclejoeandkamala2020.com	unclejoeandkamala2020.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:50:07.913424969 CEST	8.8.8.8	192.168.2.3	0xe5d5	No error (0)	unclejoeandkamala2020.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:13.096925020 CEST	8.8.8.8	192.168.2.3	0x7e01	No error (0)	www.siloamtree.com	siloamtree.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:50:13.096925020 CEST	8.8.8.8	192.168.2.3	0x7e01	No error (0)	siloamtree.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:18.266840935 CEST	8.8.8.8	192.168.2.3	0x271c	No error (0)	www.trumedenroll.com	trumedenroll.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:50:18.266840935 CEST	8.8.8.8	192.168.2.3	0x271c	No error (0)	trumedenroll.com		184.168.131.241	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.nahomredda.com
- www.nfoptic.com
- www.pone2.com
- www.newmandu.com
- www.bestwishesforyou.online
- www.unclejoeandkamala2020.com
- www.siloamtree.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49727	108.128.238.226	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:48:49.840873957 CEST	1432	OUT	GET /vu9b/?uZQL2=D48x&0pn=epJyvIJN9OiI2pb9nHYNHIQUuRpQuBcV3xjjobJny1KcYNO6WcXhtFEWRhmWC8oG0KHq HTTP/1.1 Host: www.nahomredda.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:48:49.881361008 CEST	1432	IN	HTTP/1.1 301 Moved Permanently content-length: 0 location: https://www.nahomredda.com/vu9b/?uZQL2=D48x&0pn=epJyvIJN9OiI2pb9nHYNHIQUuRpQuBcV3xjjobJny1KcYNO6WcXhtFEWRhmWC8oG0KHq connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49737	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:04.999016047 CEST	4118	OUT	GET /vu9b/?0pn=TnflO2yLdbi4Ns0f55IiNebWCRsDsubrkj3vpv5xkUkHd7zC3bp6KG+yVlLNRE0xHemI&uZQL2=D48x HTTP/1.1 Host: www.nfoptic.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:49:05.183073997 CEST	4118	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 08:49:05 GMT Content-Type: text/html Content-Length: 275 ETag: "606abe80-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49742	3.13.255.157	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:51.877827883 CEST	5738	OUT	GET /vu9b/?uZQL2=D48x&0pn=4FRBZlZfmJP1ouB3qG1kZTmIcoiAlBFvqheXtdIBznGFOOcTf1arb+p8J++3khIBMjQo HTTP/1.1 Host: www.pone2.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:49:51.988156080 CEST	5739	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 08:49:51 GMT Content-Type: text/html Content-Length: 153 Connection: close Server: nginx/1.16.1 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 2f 31 2e 31 36 2e 31 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/1.16.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49743	208.91.197.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:57.294074059 CEST	5739	OUT	GET /vu9b/?0pn=gvDMKnL2DiygUqkLOW8equ0SBtiZsQsp9RF77GdE0oWtaZL2dcC9ipMcSo2LbyxlKRwH&uZQL2=D48x HTTP/1.1 Host: www.newmandu.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:49:57.479624987 CEST	5741	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 08:49:57 GMT Server: Apache Set-Cookie: vsid=928vr3654173974123123; expires=Tue, 07-Apr-2026 08:49:57 GMT; Max-Age=157680000; path=/; domain=www.newmandu.com; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_BkrQvPC8sk24uvc+Nn9tqdRZgLCRUlnQZz65 yc0bqXefVa5ctkyyuEEjbRhEn+bFORz0PyYM6ecDwqWw1JjvNg== Content-Length: 2512 Keep-Alive: timeout=5, max=127 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 2d 2d 0d 0a 09 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 65 77 6d 61 6e 64 75 2e 63 6f 6d 2f 3f 66 70 3d 74 65 52 43 47 42 52 57 6e 73 4d 79 51 50 59 42 4c 51 7a 49 54 50 25 32 46 52 5a 68 52 4d 25 32 42 7a 52 56 6b 48 59 36 6c 4b 4f 44 6f 78 57 39 55 42 46 42 5a 25 32 42 41 55 54 6a 4a 42 44 55 34 49 6f 73 67 61 51 70 5a 78 44 4b 68 70 34 65 59 54 64 75 30 6a 78 48 32 6d 71 50 4a 51 42 69 56 39 31 68 66 70 38 4c 75 48 50 77 6a 7a 37 6d 57 37 56 4f 6b 67 6e 30 54 38 52 73 31 68 72 6f 44 63 4a 43 68 33 69 77 4c 70 6d 58 44 6d 50 4d 73 6b 43 50 39 36 58 6b 6a 6d 64 41 62 45 54 65 34 56 79 30 4f 71 41 49 77 5a 79 4d 7a 4c 57 7a 30 25 33 44 26 70 72 76 74 6f 66 3d 4f 25 32 42 35 56 4e 25 32 42 44 49 25 32 42 68 38 70 38 54 7a 50 72 5a 6d 48 61 56 33 70 41 44 4c 72 65 67 76 37 33 56 5a 38 5a 41 38 6d 53 43 63 25 33 44 26 70 6f 72 75 3d 68 75 6c 4f 30 54 52 6f 6a 68 78 55 4f 48 79 51 42 6a 75 59 42 44 6c 43 31 42 6c 74 38 4e 46 69 70 30 66 75 5a 42 51 4a 48 4a 43 67 67 4e 4e 62 67 4a 76 30 44 41 36 33 79 67 74 46 75 59 75 69 41 6b 6c 75 71 6d 43 4d 4e 64 66 72 46 42 78 43 34 43 34 66 45 46 62 68 72 43 52 37 37 56 33 4d 67 4b 68 79 71 41 74 6c 6b 4f 45 35 6d 36 66 32 76 71 68 42 78 6f 37 6e 38 68 44 32 47 34 62 50 39 5a 45 67 55 59 51 57 65 79 31 6a 6b 6d 50 45 55 67 49 4a 38 74 6b 65 41 32 53 6c 56 25 32 46 49 35 58 25 32 42 6e 44 43 42 45 67 48 6c 6b 62 79 64 4b 52 65 59 76 50 46 6e 25 32 46 57 4f 47 59 52 64 58 64 74 26 63 69 66 72 3d 31 26 30 70 6e 3d 67 76 44 4d 4b 6e 4c 32 44 69 79 67 55 71 6b 4c 4f 57 38 65 71 75 30 53 42 74 69 5a 73 51 73 70 39 52 46 37 37 47 64 45 30 6f 67 74 61 5a 4c 32 64 63 43 39 69 70 4d 63 53 6f 32 4c 62 79 78 6c 4b 52 77 48 26 75 5a 51 4c 32 3d 44 34 38 78 22 3b 0d 0a 09 2f 2a 0d 0a 2d 2d 3e 0d 0a 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4b 58 37 34 69 78 70 7a 56 79 58 62 4a 70 72 63 4c 66 62 48 34 70 73 50 34 2b 4c 32 65 6e 74 71 72 69 30 6c 7a 68 36 70 6b 41 61 58 4c 50 49 63 63 6c 76 36 44 51 42 65 4a 4a 6a 47 46 57 72 42 49 46 36 51 4d 79 46 77 58 54 35 43 43 52 79 6a 53 32 70 65 6e 45 43 41 77 45 41 41 51 3d 3d 5f 42 6b 72 51 76 50 43 38 73 6b 32 34 75 76 63 Data Ascii: ...top.location="http://www.newmandu.com/?fp=teRCGBRWnsMyQPYBLQzITP%2FRZhRM%2BzRVkHY6lKO DoxW9UBFBZ%2BAUTjJBDU4IosgaQpZxDKhp4eYTdu0jxH2mqPJQBiV91hfp8LuHPwjz7mW7VOkgn0T8Rs1hroDcJCh 3iwLpmXDmPMskCP96XkjmdAbETe4Vy0OqAlwZyMzLWz0%3D&prvtof=O%2B5VN%2BDI%2Bh8p8TzPrZmHaV3pADLre gv73VZ8ZA8mSCc%3D&poru=hulO0TRojhxUOHyQBjuYBDlC1Blt8NFip0fuZBQJHJCggNNbgJv0DA63ygtFuYuiAkl uqmCMNdfrFBxC4C4fEFbhrCR77V3MgKhyqAtlkOE5m6f2vqhBxo7n8hD2G4bP9ZEgUYQWey1jkmPEUgIJ8tkeA2SlV %2FI5X%2BnDCBEgHlkbydKReYvPFn%2FWOGYRdXdt&cifr=1&0pn=gvDMKnL2DiygUqkLOW8equ0SBtiZsQsp9RF77 GdE0oWtaZL2dcC9ipMcSo2LbyxlKRwH&uZQL2=D48x";/*--><html data-adblockkey="MFwwDQYJKoZIhvcNAQ EBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkAaXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5 CCRyjS2penECAwEAAQ==_BkrQvPC8sk24uvc

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49744	152.44.33.193	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:50:02.737376928 CEST	5744	OUT	GET /vu9b/?uZQL2=D48x&0pn=Ucm1yDKmPu3sqYnPT23C7jNgC5pC+S3WITJgysPBW6tpfdLYpWyQ+yZVED0YNT4HHiqT HTTP/1.1 Host: www.bestwishesforyou.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:50:02.848124027 CEST	5745	IN	HTTP/1.1 301 Moved Permanently Connection: close Content-Type: text/html Content-Length: 707 Date: Thu, 08 Apr 2021 08:49:59 GMT Location: https://www.bestwishesforyou.online/vu9b/?uZQL2=D48x&0pn=Ucm1yDKmPu3sqYnPT23C7jNgC5pC+S3WITJgysPBW6tpfdLYpWyQ+yZVED0YNT4HHiqT Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49745	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:50:07.928015947 CEST	5746	OUT	GET /vu9b/?0pn=ZRZicPUHGdpu447/ToshtXbk+LjFT6TcRbqWThirrcjgIxqMd1CJhqCrqkTzpGUGM9/e&uZQL2=D48x HTTP/1.1 Host: www.unclejoeandkamala2020.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:50:08.043180943 CEST	5747	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 08:50:07 GMT Content-Type: text/html Content-Length: 275 ETag: "6061898c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49746	34.102.136.180	80	C:\Windows\explorer.exe

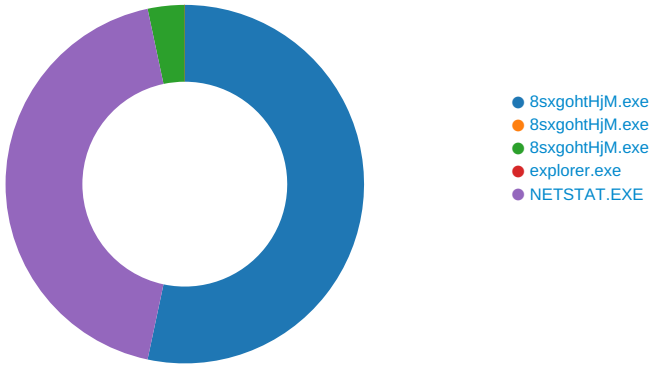
Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:50:13.109869957 CEST	5748	OUT	GET /vu9b/?uZQL2=D48x&0pn=XOyfHYtLU1lLdZnaXZe4OvPQMiRanaHMlAlcsSmWFWkLxOIqqTB9rasY28K6kY36/QRI HTTP/1.1 Host: www.siloamtree.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:50:13.227869034 CEST	5748	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 08:50:13 GMT Content-Type: text/html Content-Length: 275 ETag: "6063a886-113" 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: 8sxgohtHjM.exe PID: 6752 Parent PID: 5548

General

Start time:	10:48:02
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\8sxgohtHjM.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\8sxgohtHjM.exe'
Imagebase:	0x3b0000
File size:	585728 bytes
MD5 hash:	D381B0A2268051AA83B031DDC87EE7DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.270742230.0000000002713000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.271249729.00000000037C5000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.271249729.00000000037C5000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.271249729.00000000037C5000.00000004.00000001.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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF0CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF0CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8sxgohtHjM.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E21C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8sxgohtHjM.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E21C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD51B4F	ReadFile

Analysis Process: 8sxgohtHjM.exe PID: 7100 Parent PID: 6752

General

Start time:	10:48:10
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\8sxgohtHjM.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\8sxgohtHjM.exe
Imagebase:	0x2c0000
File size:	585728 bytes
MD5 hash:	D381B0A2268051AA83B031DDC87EE7DF
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 8sxgohtHjM.exe PID: 7108 Parent PID: 6752

General

Start time:	10:48:11
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\8sxgohtHjM.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\8sxgohtHjM.exe
Imagebase:	0x6e0000
File size:	585728 bytes
MD5 hash:	D381B0A2268051AA83B031DDC87EE7DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.311088720.0000000000D00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.311088720.0000000000D00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.311088720.0000000000D00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.310623101.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.310623101.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.310623101.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.311156911.0000000001030000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.311156911.0000000001030000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.311156911.0000000001030000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

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

Analysis Process: explorer.exe PID: 3388 Parent PID: 7108

General

Start time:	10:48:13
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes

MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: NETSTAT.EXE PID: 6656 Parent PID: 3388

General

Start time:	10:48:27
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0x1060000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.520943854.0000000003540000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.520943854.0000000003540000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.520943854.0000000003540000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.521004557.0000000003570000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.521004557.0000000003570000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.521004557.0000000003570000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.518608127.0000000000FD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.518608127.0000000000FD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.518608127.0000000000FD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	FE899E	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	FE899E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	FE899E	HttpSendRequestA
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	FE899E	HttpSendRequestA
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	FE899E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	FE899E	HttpSendRequestA
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	FE899E	HttpSendRequestA
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	FE899E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	FE899E	HttpSendRequestA
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	FE899E	HttpSendRequestA
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	FE899E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	FE899E	HttpSendRequestA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	FE82A7	NtReadFile

Disassembly

Code Analysis