ID: 458773
Sample Name: V5cfxBHd71.exe
Cookbook: default.jbs
Time: 18:23:43
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

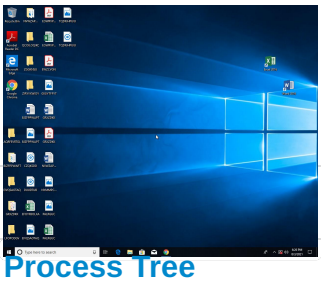
Windows Analysis Report V5cfxBHd71.exe

Overview

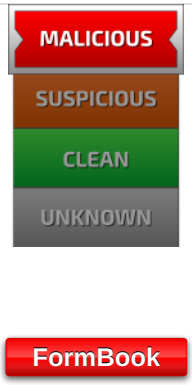
General Information

Sample Name:	V5cfxBHd71.exe
Analysis ID:	458773
MD5:	182170393a1acd..
SHA1:	e2b2d6405b359d..
SHA256:	71ec0c91aeec50…
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

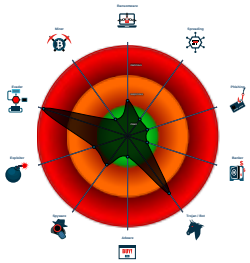


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- V5cfxBHd71.exe (PID: 5700 cmdline: 'C:\Users\user\Desktop\V5cfxBHd71.exe' MD5: 182170393A1ACD19744575F00562384F)
  - V5cfxBHd71.exe (PID: 6092 cmdline: C:\Users\user\Desktop\V5cfxBHd71.exe MD5: 182170393A1ACD19744575F00562384F)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - msdt.exe (PID: 3332 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
      - cmd.exe (PID: 340 cmdline: /c del 'C:\Users\user\Desktop\V5cfxBHd71.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 1496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.adultpeace.com/p2io/"
  ],
  "decoy": [
    "essentiallyourscandles.com",
    "cleanxcare.com",
    "bigplatesmallwallet.com",
    "iotcloud.technology",
    "dmgt4m2g8y2uh.net",
    "malcorinmobiliaria.com",
    "thriveglucose.com",
    "fuhaitongxin.com",
    "magetu.info",
    "pyithuhluttaw.net",
    "myfavbutik.com",
    "xzklrhy.com",
    "anewdistraction.com",
    "mercuryaid.net",
    "thesoulrevitalist.com",
    "swayam-moj.com",
    "liminaltechnology.com",
    "lucytime.com",
    "alfenas.info",
    "carmelodesign.com",
    "newmopeds.com",
    "cyrilgraze.com",
    "ruhexuangou.com",
    "trendbold.com",
    "centergolosinas.com",
    "leonardocarrillo.com",
    "advancedaccessapplications.com",
    "aideliveryrobot.com",
    "defenestration.world",
    "zgcbw.net",
    "shopihy.com",
    "3cheer.com",
    "untylservice.com",
    "totally-seo.com",
    "cmannouncements.com",
    "tpcgzwlpyggm.mobi",
    "hfjxhs.com",
    "balloon-artists.com",
    "vectoroutlines.com",
    "boogerstv.com",
    "procircleacademy.com",
    "tricqr.com",
    "hazard-protection.com",
    "buylocalclub.info",
    "m678.xyz",
    "hiddenwholesale.com",
    "ololmychartlogin.com",
    "redudiban.com",
    "brunoecatarina.com",
    "69-1hn7uc.net",
    "zmzcrossrt.xyz",
    "dreamcashbuyers.com",
    "yunlimall.com",
    "jonathan-mandt.com",
    "painhut.com",
    "pandemisorgugirisi-tr.com",
    "sonderbach.net",
    "kce0728com.net",
    "austinpavingcompany.com",
    "biztekno.com",
    "rodriggi.com",
    "micheldrake.com",
    "foxwaybrasil.com",
    "a3i7ufz4pt3.net"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.352974421.0000000000B00000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.352974421.0000000000B0 0000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.352974421.0000000000B0 0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.353232950.0000000000F40000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.353232950.0000000000F40000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.V5cfxBHd71.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.V5cfxBHd71.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.V5cfxBHd71.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
4.2.V5cfxBHd71.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.V5cfxBHd71.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

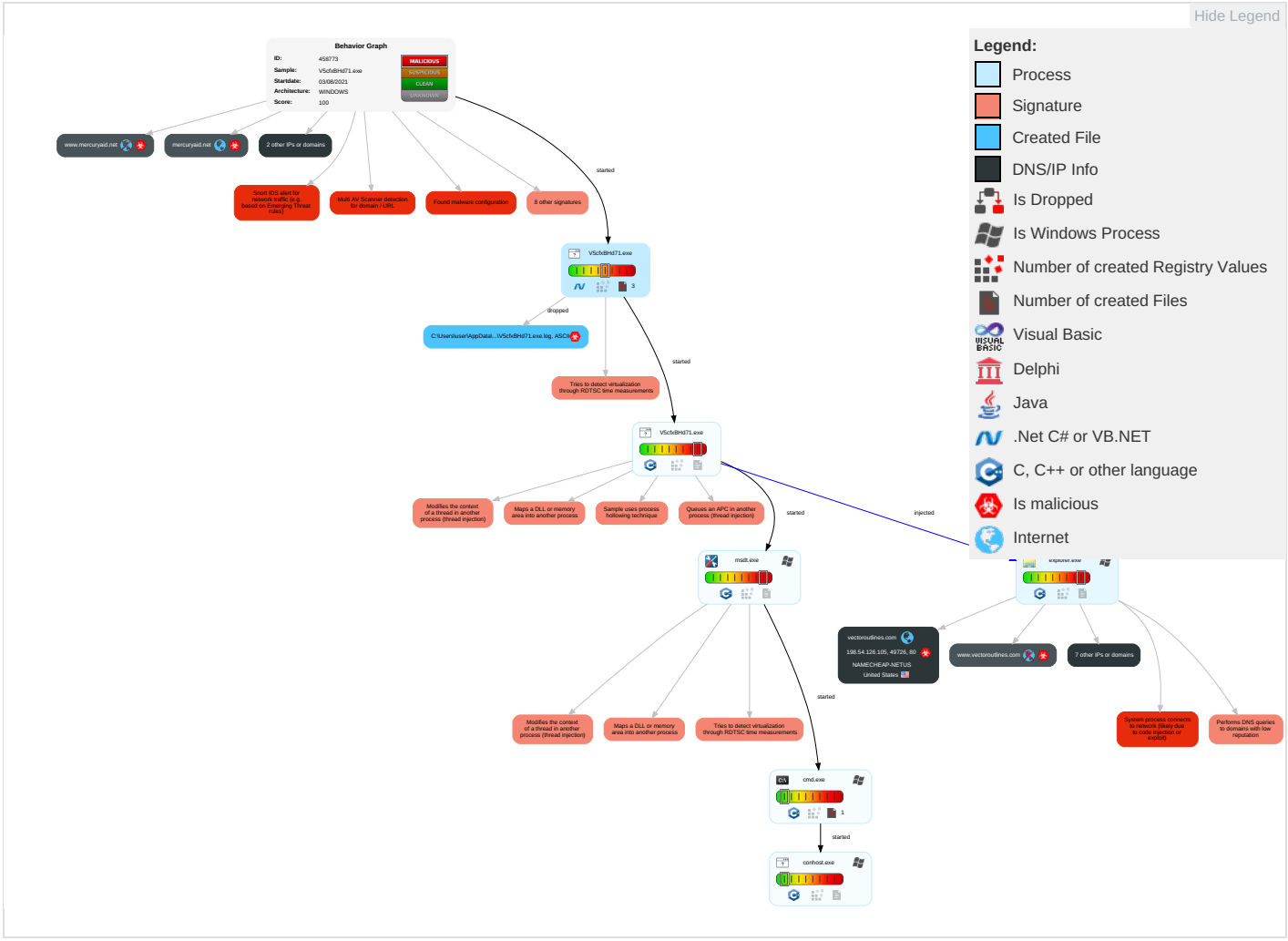
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 3	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Timestomp 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
V5cfxBHd71.exe	29%	Virustotal		Browse
V5cfxBHd71.exe	30%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
V5cfxBHd71.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.V5cfxBHd71.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.hazard-protection.com	2%	Virustotal		Browse
3cheer.com	2%	Virustotal		Browse
www.leonardocarrillo.com	1%	Virustotal		Browse
vectoroutlines.com	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.tiro.comFI	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFQ	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/9	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/:	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcom:	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
www.adultpeace.com/p2io/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.fontbureau.comF5	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ch	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/f	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF:	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comR.TTF	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/help5	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://www.fontbureau.comdy	0%	Avira URL Cloud	safe	
http://www.fontbureau.co	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/C	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmo	0%	Avira URL Cloud	safe	
http://www.fontbureau.comueTFC	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.urwpp.debI	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/y	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.boogerstv.com/p2io/?BJ=fW2NkW2j278wyrs6d/m+egXTc5dWq8qtohQAL+tQrXSmfdetyJ3HBVVg7jRLyNqpfuRL&b2Ml9=0txtgJLXY6ULB	100%	Avira URL Cloud	malware	
http://www.fontbureau.com.TTF5	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comalsFC	0%	Avira URL Cloud	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/f	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/nly	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	
http://www.vectoroutlines.com/p2io/?BJ=RfOK6jKhDkXNwKgMe5LTyAppaXreGCTFlz0prsbY2047Xu3Gxs4GQwDY2/SnNVlkbHQV&b2Ml9=0txtgJLXY6ULB	100%	Avira URL Cloud	malware	
http://www.jiyu-kobo.co.jp/tion	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.hazard-protection.com	148.59.128.71	true	false	• 2%, Virustotal, Browse	unknown
3cheer.com	34.102.136.180	true	false	• 2%, Virustotal, Browse	unknown
parkingpage.namecheap.com	198.54.117.218	true	false		high
www.leonardocarrillo.com	172.107.55.6	true	false	• 1%, Virustotal, Browse	unknown
vectoroutlines.com	198.54.126.105	true	true	• 6%, Virustotal, Browse	unknown
mercuryaid.net	223.29.234.230	true	true		unknown
www.tpcgzwlpyggm.mobi	unknown	unknown	true		unknown
www.boogerstv.com	unknown	unknown	true		unknown
www.m678.xyz	unknown	unknown	true		unknown
www.kce0728com.net	unknown	unknown	true		unknown
www.mercuryaid.net	unknown	unknown	true		unknown
www.vectoroutlines.com	unknown	unknown	true		unknown
www.3cheer.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.adultpeace.com/p2io/	true	• URL Reputation: safe	low
http://www.boogerstv.com/p2io/?BJ=fW2NkW2j278wyrs6d/m+egXTc5dWq8qtohQAL+tQrXSmfdetyJ3HBVVg7jRLyNqpfuRL&b2Ml9=0txtgJLXY6ULB	true	• Avira URL Cloud: malware	unknown
http://www.vectoroutlines.com/p2io/?BJ=RfOK6jKhDkXNwKgMe5LTyAppaXreGCTFIz0prsbY2047Xu3Gxs4GQwDY2/SnNVlkbHQV&b2Ml9=0txtgJLXY6ULB	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.117.218	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
34.102.136.180	3cheer.com	United States		15169	GOOGLEUS	false
198.54.126.105	vectoroutlines.com	United States		22612	NAMECHEAP-NETUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458773
Start date:	03.08.2021
Start time:	18:23:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	V5cfxBHd71.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:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/1@9/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27.2% (good quality ratio 23.3%) • Quality average: 69.2% • Quality standard deviation: 34.6%
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

Simulations

Behavior and APIs

Time	Type	Description
18:24:46	API Interceptor	1x Sleep call for process: V5cfxBHd71.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.117.218	TNT Shipping doc.exe	Get hash	malicious	Browse	• www.zawajalgos.com/m8uk/?XV=MTy09FK0DZb&xJB4=nPIao3MtkZZfKB1sMK+jBa6jiFKBTthlCTc/qxHBcyQb4+aqEw0YIfO52cL0KqdOdHaJ
	Dimensions and sizes for valves quotation.exe	Get hash	malicious	Browse	• www.ukuleleintensive.com/gbwy/?k6Ad=hPDdBc6xjVVVKqTpS12Zj2KWY/xbJiOaJ1g8o8RJGjNB7GfntMGyz7zUvwO+2i9W7Ket&Vv_d=PrNDGXc
	PI for the order 20210407DTR001.pdf.gz.exe	Get hash	malicious	Browse	• www.synth.pizza/3b4e/?QBZxT=7nopdd9xcT&a8q=1PeMpVR0bS4CVM3zcs5suMbyrMp2Y/RA6dgrMfA7ZoqktSfsEthxMaqEH9TPZZD2gzi2JG1zGQ==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	242jQP4mQP.exe	Get hash	malicious	Browse	• www.galvinsky.digital/dy8g/?S8tT3n=K+H2wjnk8RqujiMAF6k6lUq9+zoJ+xpADfX0uiRvrYfx+zwl829klMm2N7W/QIPtbcnmYyz+UQ==&8p=SN6XYPXXpfCx
	eTWZtFRRMJ.exe	Get hash	malicious	Browse	• www.boogerstv.com/p2io/?X48P0=fW2NkW2j278wyrs6d/m+egXTc5dWq8qtohQAL+tQrXSmfdetyJ3HBVVg7gxb9s6RBL4M&NJ=6lvHNFHx
	ekeson and sons.exe	Get hash	malicious	Browse	• www.activedevon.xyz/eo5u/?3flLi=3fixF&WDH4Z=gO4K5mHcn2QPYGRvxafNe+5p9r0cfSpdBn55FnpuS2mPyHUUFTjtXKJi1XneNJcm9Y4m6sLWag==
	Payment receipt MT103.exe	Get hash	malicious	Browse	• www.blockchain-365.com/n86i/?3fDpH=scV3eC5LnrxmdTaZDMUbfdarjWOrUI17K3tFUIp30YFf7UyQTMB90CuHfsBJQ1LJ+yqs&Vjo=1bT0vz7
	cy.exe	Get hash	malicious	Browse	• www.fundheros.com/zrmt/?6lux=9Kp3w7DCYJwNU8WsE17OQw23x7mujlthWWaTZWOKl7Ig6Bz27x2cp62T+P49v/mmqthg&Klh8a=p2JDfHUh1
	j5rXLljONk.exe	Get hash	malicious	Browse	• www.g-cleanpartners.in/dlc/distribution.php?pub=mixinte
	Ohki Blower Skid Base Enquiry 052521.exe	Get hash	malicious	Browse	• www.locply.com/un8c/?5j9=NGTfkvtaSdon4EkoI3ozpRr9bmxMgy9gsF1pztjoLp+4u8wBsb/6oXmWjnwO4OIYUp5f&vR=Ltxx
	New order 301534.pdf.exe	Get hash	malicious	Browse	• www.yamagym.com/sbqi/?ZjR=A9FpVWg2dAPyDanCbkAal5xn8XynSE6PITFa1NeTTcon3r6OOg1WhLKe7RzZoujgxIl9KDseIA==&ndnddT=ot9xbpDpf8H4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Ciikfddtznhxmtqufdujkifxwmwhrfjkcl_Signed_.exe	Get hash	malicious	Browse	• www.f3g.found/qd8i/?Qp=iKdGhUQd0gzURvlm3Jt41em8p9uaSRabaJyAAib1YADWOisPkV2HIhSGGZPUNHkrRq2K&xPWH_=LVz4vpXpDf7DLZ
	Wire Payment Of $35,276.70.exe	Get hash	malicious	Browse	• www.locply.com/un8c/?q48=GbqltxjpVhB0It&Bzu=NGTfkvtaSdon4EkoI3ozpRr9bmxMgy9gsF1pztjoLp+4u8wBsb/6oXmWjn8OreEbN55J1SAp8g==
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• www.challance.design/uoe8/?V2=LhqpTfJ8&rDHpw=fYbYSxt3Qhcb551a7rNTvuoixibj8olf9Mxoep0JAE6bsM5dZYso9WmxDlWOvfueGt5G
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• www.playx.finance/qjnt/?BZz=lIM0X6&h48x=1Vbp9If7QMpbnqc0ueS3EHoyDdmNKH7SkWmwpG2wK8nHe9QxMxQiDr/Rv9rAbZu592D3MQ==
	z5Wqivscwd.exe	Get hash	malicious	Browse	• www.rascontractingllc.com/f0sg/?EzrtFB=4hL05l3xNH1L&9rQPJl=VL61RGYCRIinPGEMi+ZAGnHYp8XZVvRzeWAN7Ibk9LNon96r6atV/Ask5zouKtgOTJp7
	AL-IEDAHINV.No09876543.exe	Get hash	malicious	Browse	• www.sandybottomsflipflops.com/uv34/?gjKTUx=6lchmDL0&rnKTobm=/y2QUNCyd1bGxdPjEN+TG3wvArtE+ieT5j9LKQh68qSP5982epgdol7eXG9G+2GrVPAT
	24032130395451.pdf .exe	Get hash	malicious	Browse	• www.partum.life/uabu/?ojqD-Z=KdrhxNh8&9r4Hc=Z0zf2dbKX6YlEzcl0VbwASPt08RzMP75iVffTsKn6GzwBBbR2IjFiCH6cCoBJQjqXWja

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Ac5RA9R99F.exe	Get hash	malicious	Browse	• www.abundancewithmelissaharvey.com/evpn/?CZa4=UnLa0x8cdATkkSAlrLSX44s3EHgIYFf2NLcg8KhuRo/6FK7nrIMQsSkng9ZA6ahsodQ1&CPWhW=C8eHk
	SA-NQAW12n-NC9W03-pdf.exe	Get hash	malicious	Browse	• www.switcheo.finance/uwec/?GFQl9jnp=3cOH6CffnF8zA2vO0DHvKlrvSwO+w2vUbH/s+qgAJjYXXQ/ohIL0shsdTQ14Zv3dTuQV&Rl4=YVFTx4yh

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.hazard-protection.com	ZQGMiyaTir.exe	Get hash	malicious	Browse	• 148.59.128.71
	eHTLcWfhgv.exe	Get hash	malicious	Browse	• 148.59.128.71
	UOMp9cDcqZ.exe	Get hash	malicious	Browse	• 148.59.128.71
	qXDtb88hht.exe	Get hash	malicious	Browse	• 148.59.128.71
	17jLieeOPx.exe	Get hash	malicious	Browse	• 148.59.128.71
	KWX1rM9GB0.exe	Get hash	malicious	Browse	• 148.59.128.71
	Contract MAY2021.xlsx	Get hash	malicious	Browse	• 148.59.128.71
	k7AgZOwF4S.exe	Get hash	malicious	Browse	• 148.59.128.71
	o52k2obPCG.exe	Get hash	malicious	Browse	• 148.59.128.71
	uNttFPI36y.exe	Get hash	malicious	Browse	• 148.59.128.71
	1ucvVfbHnD.exe	Get hash	malicious	Browse	• 148.59.128.71
	pumYguna1i.exe	Get hash	malicious	Browse	• 148.59.128.71
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 148.59.128.71
	g0g865fQ2S.exe	Get hash	malicious	Browse	• 148.59.128.71
	mar2403.xlsx	Get hash	malicious	Browse	• 148.59.128.71
parkingpage.namecheap.com	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 198.54.117.216
	Payment For Invoice 321-1005703.exe	Get hash	malicious	Browse	• 198.54.117.212
	Medical Equipment Order 2021.PDF.exe	Get hash	malicious	Browse	• 198.54.117.210
	YfDl.dll	Get hash	malicious	Browse	• 198.54.117.210
	d9UdQnXQ86ld31G.exe	Get hash	malicious	Browse	• 198.54.117.212
	k0INCz463k.exe	Get hash	malicious	Browse	• 198.54.117.210
	PO-829ARTS-PI 2021-7-17.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	Inv_7623980.exe	Get hash	malicious	Browse	• 198.54.117.215
	direction.dll	Get hash	malicious	Browse	• 198.54.117.218
	Purchase Order.exe	Get hash	malicious	Browse	• 198.54.117.215
	PYY74882220#.exe	Get hash	malicious	Browse	• 198.54.117.215
	cZj7V8FfFk.exe	Get hash	malicious	Browse	• 198.54.117.218
	Order Signed PEARLTECH contract and PO.exe	Get hash	malicious	Browse	• 198.54.117.210
	Payment_invoice.exe	Get hash	malicious	Browse	• 198.54.117.212
	INVOICE.exe	Get hash	malicious	Browse	• 198.54.117.211
	Order.exe	Get hash	malicious	Browse	• 198.54.117.215
	SMdWrQW0nH.exe	Get hash	malicious	Browse	• 198.54.117.218
	4326_PDF.exe	Get hash	malicious	Browse	• 198.54.117.216
	LPY15536W4.exe	Get hash	malicious	Browse	• 198.54.117.211
	u5xgJUljfI.exe	Get hash	malicious	Browse	• 198.54.117.210

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 198.54.117.216
	scan_2021_567812097854317907854.exe	Get hash	malicious	Browse	• 199.188.201.82

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SGKCM20217566748_Federighi Turkiye Oferta Term#U00e9k.exe	Get hash	malicious	Browse	• 192.64.119.222
	bYrKwcFL8m.exe	Get hash	malicious	Browse	• 198.54.122.60
	Our Company Account Details-08-2021.xlsx	Get hash	malicious	Browse	• 198.54.122.60
	Payment For Invoice 321-1005703.exe	Get hash	malicious	Browse	• 198.54.117.212
	Medical Equipment Order 2021.PDF.exe	Get hash	malicious	Browse	• 198.54.117.216
	YfDl.dll	Get hash	malicious	Browse	• 162.255.119.73
	sstein@cptech.com_94994965Application.HTM	Get hash	malicious	Browse	• 162.213.253.39
	d9UdQnXQ86ld31G.exe	Get hash	malicious	Browse	• 198.54.117.212
	Vt03edQseah3iHM.exe	Get hash	malicious	Browse	• 68.65.123.125
	INVOICE & PACKING LIST FOR SEA SHIPMENT.EXE	Get hash	malicious	Browse	• 199.188.200.123
	MIN56KgzBN.exe	Get hash	malicious	Browse	• 63.250.33.126
	xA8Yyl9vEB.exe	Get hash	malicious	Browse	• 198.54.122.60
	xVg4so8mq9.exe	Get hash	malicious	Browse	• 198.54.122.60
	REVISED PO 26663S.doc	Get hash	malicious	Browse	• 198.54.122.60
	order PT Macropharma.pdf.doc	Get hash	malicious	Browse	• 198.54.122.60
	Purchase Order No. PHS-01521-22..doc	Get hash	malicious	Browse	• 198.54.122.60
	Blackcatjsc inquiry.doc	Get hash	malicious	Browse	• 198.54.122.60
	1M3InhCdS7.exe	Get hash	malicious	Browse	• 198.54.122.60

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\V5cfxBHd71.exe.log

Process:	C:\Users\user\Desktop\V5cfxBHd71.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	unknown
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):	7.395625597721572

General

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:	V5cfxBHd71.exe
File size:	793600
MD5:	182170393a1acd19744575f00562384f
SHA1:	e2b2d6405b359d78ba965b54e9cc6b38e223fd97
SHA256:	71ec0c91aeec5071da283d23bceb39800e9ad6c133bb6aef99d1302f47a4ada3
SHA512:	92e122d0edf30c0ad285b79e344795b90682a6ad4d8a9b6fd6003d4c2bfcaed8b2ce599caed8b55e1fdb6a2474f22236661a1780063521eea4d084afeb522f3a
SSDEEP:	12288:Eo4rGVHDwXyWU6/RRtaD8xI5eFYECvT+5wMpTxcujI80v42iN:EobBitaII5eFYkm6TxcujZx1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....M.....P.....1... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c31f2
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:	0xF0944DD6 [Mon Nov 25 20:51:34 2097 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc11f8	0xc1200	False	0.778078226133	data	7.40347651298	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x5f4	0x600	False	0.434244791667	data	4.20291982241	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc6000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-18:26:15.542488	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49726	80	192.168.2.5	198.54.126.105
08/03/21-18:26:15.542488	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49726	80	192.168.2.5	198.54.126.105
08/03/21-18:26:15.542488	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49726	80	192.168.2.5	198.54.126.105
08/03/21-18:26:20.797106	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49729	80	192.168.2.5	34.102.136.180
08/03/21-18:26:20.797106	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49729	80	192.168.2.5	34.102.136.180
08/03/21-18:26:20.797106	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49729	80	192.168.2.5	34.102.136.180
08/03/21-18:26:20.911098	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49729	34.102.136.180	192.168.2.5
08/03/21-18:26:53.982804	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.5	223.29.234.230
08/03/21-18:26:53.982804	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.5	223.29.234.230
08/03/21-18:26:53.982804	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.5	223.29.234.230

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 18:26:09.839133978 CEST	192.168.2.5	8.8.8.8	0x4a65	Standard query (0)	www.tpcgzwlpyggm.mobi	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:15.319434881 CEST	192.168.2.5	8.8.8.8	0x3184	Standard query (0)	www.vectoroutlines.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:20.726124048 CEST	192.168.2.5	8.8.8.8	0x5822	Standard query (0)	www.3cheer.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:25.950511932 CEST	192.168.2.5	8.8.8.8	0xa8fc	Standard query (0)	www.m678.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:31.351497889 CEST	192.168.2.5	8.8.8.8	0x3b41	Standard query (0)	www.kce0728com.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:37.261212111 CEST	192.168.2.5	8.8.8.8	0x746e	Standard query (0)	www.boogerstv.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:42.740745068 CEST	192.168.2.5	8.8.8.8	0x49f2	Standard query (0)	www.leonardocarrillo.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:48.287003040 CEST	192.168.2.5	8.8.8.8	0xb99d	Standard query (0)	www.hazard-protection.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:53.710860014 CEST	192.168.2.5	8.8.8.8	0xfef8	Standard query (0)	www.mercuryaid.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:26:10.303777933 CEST	8.8.8.8	192.168.2.5	0x4a65	Name error (3)	www.tpcgzwlpyggm.mobi	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:26:15.370718956 CEST	8.8.8.8	192.168.2.5	0x3184	No error (0)	www.vectoroutlines.com	vectoroutlines.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:26:15.370718956 CEST	8.8.8.8	192.168.2.5	0x3184	No error (0)	vectoroutlines.com		198.54.126.105	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:20.778676987 CEST	8.8.8.8	192.168.2.5	0x5822	No error (0)	www.3cheer.com	3cheer.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:26:20.778676987 CEST	8.8.8.8	192.168.2.5	0x5822	No error (0)	3cheer.com		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:26.333971977 CEST	8.8.8.8	192.168.2.5	0xa8fc	Name error (3)	www.m678.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:31.864424944 CEST	8.8.8.8	192.168.2.5	0x3b41	Server failure (2)	www.kce0728com.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:37.297532082 CEST	8.8.8.8	192.168.2.5	0x746e	No error (0)	www.boogerstv.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:26:37.297532082 CEST	8.8.8.8	192.168.2.5	0x746e	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:37.297532082 CEST	8.8.8.8	192.168.2.5	0x746e	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:37.297532082 CEST	8.8.8.8	192.168.2.5	0x746e	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:37.297532082 CEST	8.8.8.8	192.168.2.5	0x746e	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:37.297532082 CEST	8.8.8.8	192.168.2.5	0x746e	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:37.297532082 CEST	8.8.8.8	192.168.2.5	0x746e	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:37.297532082 CEST	8.8.8.8	192.168.2.5	0x746e	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:42.924705029 CEST	8.8.8.8	192.168.2.5	0x49f2	No error (0)	www.leonardocarrillo.com		172.107.55.6	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:48.414810896 CEST	8.8.8.8	192.168.2.5	0xb99d	No error (0)	www.hazard-protection.com		148.59.128.71	A (IP address)	IN (0x0001)
Aug 3, 2021 18:26:53.749840975 CEST	8.8.8.8	192.168.2.5	0xfef8	No error (0)	www.mercuryaid.net	mercuryaid.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:26:53.749840975 CEST	8.8.8.8	192.168.2.5	0xfef8	No error (0)	mercuryaid.net		223.29.234.230	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.vectoroutlines.com
- www.3cheer.com
- www.boogerstv.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49726	198.54.126.105	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:26:15.542488098 CEST	4735	OUT	GET /p2io/?BJ=RfOK6jKhDkXNwKgMe5LTyAppaXreGCTFIz0prsbY2047Xu3Gxs4GQwDY2/SnNVlkbHQV&b2Ml9=0txtgJLXY6ULB HTTP/1.1 Host: www.vectoroutlines.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 18:26:15.712918043 CEST	4736	IN	HTTP/1.1 301 Moved Permanently content-type: text/html content-length: 707 date: Tue, 03 Aug 2021 16:26:15 GMT server: LiteSpeed location: https://www.vectoroutlines.com/p2io/?BJ=RfOK6jKhDkXNwKgMe5LTyAppaXreGCTFIz0prsbY2047Xu3Gxs4GQwDY2/SnNVlkbHQV&b2Ml9=0txtgJLXY6ULB x-turbo-charged-by: LiteSpeed 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 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49729	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:26:20.797106028 CEST	4754	OUT	GET /p2io/?BJ=hDwxgnCxHqZG/nBf9NFToL98ekU0apx9FaMqifAGLuP7v/j66cUXhxpzlnLclYHrbOLF&b2Ml9=0txtgJLXY6ULB HTTP/1.1 Host: www.3cheer.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 18:26:20.911098003 CEST	4755	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 16:26:20 GMT Content-Type: text/html Content-Length: 275 ETag: "6104831f-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	192.168.2.5	49730	198.54.117.218	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:26:37.492023945 CEST	4756	OUT	GET /p2io/?BJ=fW2NkW2j278wyrs6d/m+egXTc5dWq8qtohQAL+tQrXSmfdetyJ3HBVVg7jRLyNqpfuRL&b2Ml9=0 txtgJLXY6ULB HTTP/1.1 Host: www.boogerstv.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: V5cfxBHd71.exe PID: 5700 Parent PID: 5636

General

Start time:	18:24:35
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\V5cfxBHd71.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\V5cfxBHd71.exe'
Imagebase:	0xea0000
File size:	793600 bytes
MD5 hash:	182170393A1ACD19744575F00562384F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.258210431.000000000335B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.258699660.00000000041D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.258699660.00000000041D9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.258699660.00000000041D9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: V5cfxBHd71.exe PID: 6092 Parent PID: 5700

General

Start time:	18:24:47
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\V5cfxBHd71.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\V5cfxBHd71.exe
Imagebase:	0x4d0000
File size:	793600 bytes
MD5 hash:	182170393A1ACD19744575F00562384F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.352974421.0000000000B00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.352974421.0000000000B00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.352974421.0000000000B00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.353232950.0000000000F40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.353232950.0000000000F40000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.353232950.0000000000F40000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.352380368.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.352380368.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.352380368.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 6092

General

Start time:	18:24:49
Start date:	03/08/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: msdt.exe PID: 3332 Parent PID: 6092

General

Start time:	18:25:31
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0x1290000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
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: 00000011.00000002.497388587.0000000000A40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.497388587.0000000000A40000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.497388587.0000000000A40000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.500475231.0000000000E90000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.500475231.0000000000E90000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.500475231.0000000000E90000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.499943855.0000000000E60000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.499943855.0000000000E60000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.499943855.0000000000E60000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 340 Parent PID: 3332

General

Start time:	18:25:33
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\V5cfxBHd71.exe'
Imagebase:	0x150000
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: 1496 Parent PID: 340

General

Start time:	18:25:34
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis