ID: 502374
Sample Name: Fu94e0b1TR
Cookbook: default.jbs
Time: 20:56:10
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

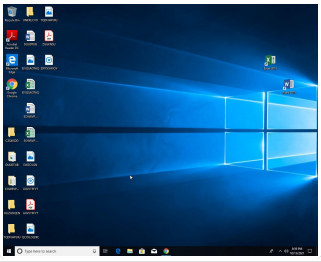
Windows Analysis Report Fu94e0b1TR

Overview

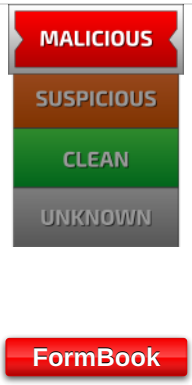
General Information

Sample Name:	Fu94e0b1TR (renamed file extension from none to exe)
Analysis ID:	502374
MD5:	6429aa83e4bc08..
SHA1:	0ead59881f05428.
SHA256:	96c57ae661562e..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

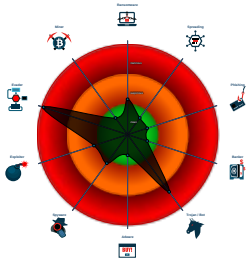


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Uses netstat to query active network…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Self deletion via cmd delete
- .NET source code contains potentia…
- Queues an APC in another process …
- Tries to detect virtualization through…

Classification



Process Tree

- **System is w10x64**
- Fu94e0b1TR.exe (PID: 4628 cmdline: 'C:\Users\user\Desktop\Fu94e0b1TR.exe' MD5: 6429AA83E4BC083B4F0B3F44B0D7950F)
  - Fu94e0b1TR.exe (PID: 4840 cmdline: C:\Users\user\Desktop\Fu94e0b1TR.exe MD5: 6429AA83E4BC083B4F0B3F44B0D7950F)
  - Fu94e0b1TR.exe (PID: 2848 cmdline: C:\Users\user\Desktop\Fu94e0b1TR.exe MD5: 6429AA83E4BC083B4F0B3F44B0D7950F)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - NETSTAT.EXE (PID: 3204 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
        - cmd.exe (PID: 1844 cmdline: /c del 'C:\Users\user\Desktop\Fu94e0b1TR.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.fis.photos/ef6c/"
  ],
  "decoy": [
    "gicaredocs.com",
    "govusergroup.com",
    "conversationspit.com",
    "brondairy.com",
    "rjtherealest.com",
    "xn--9m1bq8wgkag3rjvb.com",
    "mylori.net",
    "softandcute.store",
    "ahljsm.com",
    "shacksolid.com",
    "weekendmusecollection.com",
    "gaminghallarna.net",
    "pgonline111.online",
    "44mpt.xyz",
    "ambrandt.com",
    "eddytattoo.com",
    "blendeqes.com",
    "upinmyfeels.com",
    "lacucinadesign.com",
    "docomoau.xyz",
    "xn--90armbk7e.online",
    "xzq585858.net",
    "kidzgovroom.com",
    "lhznqyl.press",
    "publicationsplace.com",
    "jakante.com",
    "csspadding.com",
    "test-testjisdnsec.store",
    "lafabriqueabeilleassurances.com",
    "clf010.com",
    "buybabysnuggle.com",
    "uzmdrmustafaalperaykanat.com",
    "levanttradegroup.com",
    "arcflorals.com",
    "kinglot2499.com",
    "freekagyans.com",
    "region10group.gmbh",
    "yeyelm744.com",
    "thehomedesigncentre.com",
    "vngc.xyz",
    "szesdkj.com",
    "charlottewright.online",
    "planetgreennetwork.com",
    "pacifica7.com",
    "analogueadapt.com",
    "sensorypantry.com",
    "narbaal.com",
    "restaurant-utopia.xyz",
    "golnay.com",
    "szyyglass.com",
    "redelirevearyseuiop.xyz",
    "goldsteelconstruction.com",
    "discovercotswoldcottages.com",
    "geniuseven.net",
    "apricitee.com",
    "stopmoshenik.online",
    "ya2gh.com",
    "instatechnovelz.com",
    "dbe648.com",
    "seifjuban.com",
    "conquershirts.store",
    "totalcovidtravel.com",
    "pamperotrabajo.com",
    "satellitphonestore.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.370028583.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.370028583.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.370028583.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16aa9:$sqlite3step: 68 34 1C 7B E1 • 0x16bbc:$sqlite3step: 68 34 1C 7B E1 • 0x16ad8:$sqlite3text: 68 38 2A 90 C5 • 0x16bfd:$sqlite3text: 68 38 2A 90 C5 • 0x16aeb:$sqlite3blob: 68 53 D8 7F 8C • 0x16c13:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.277178151.0000000002B11000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000012.00000002.513567456.0000000000A20000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.Fu94e0b1TR.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.Fu94e0b1TR.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.Fu94e0b1TR.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ca9:$sqlite3step: 68 34 1C 7B E1 • 0x15dbc:$sqlite3step: 68 34 1C 7B E1 • 0x15cd8:$sqlite3text: 68 38 2A 90 C5 • 0x15dfd:$sqlite3text: 68 38 2A 90 C5 • 0x15ceb:$sqlite3blob: 68 53 D8 7F 8C • 0x15e13:$sqlite3blob: 68 53 D8 7F 8C
6.2.Fu94e0b1TR.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.Fu94e0b1TR.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$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 • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 8 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Yara detected FormBook

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- System process connects to network (likely due to code injection or exploit)
- Uses netstat to query active network connections and open ports
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

- Self deletion via cmd delete

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)
- Sample uses process hollowing technique
- Maps a DLL or memory area into another process
- Queues an APC in another process (thread injection)
- Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

- Yara detected FormBook

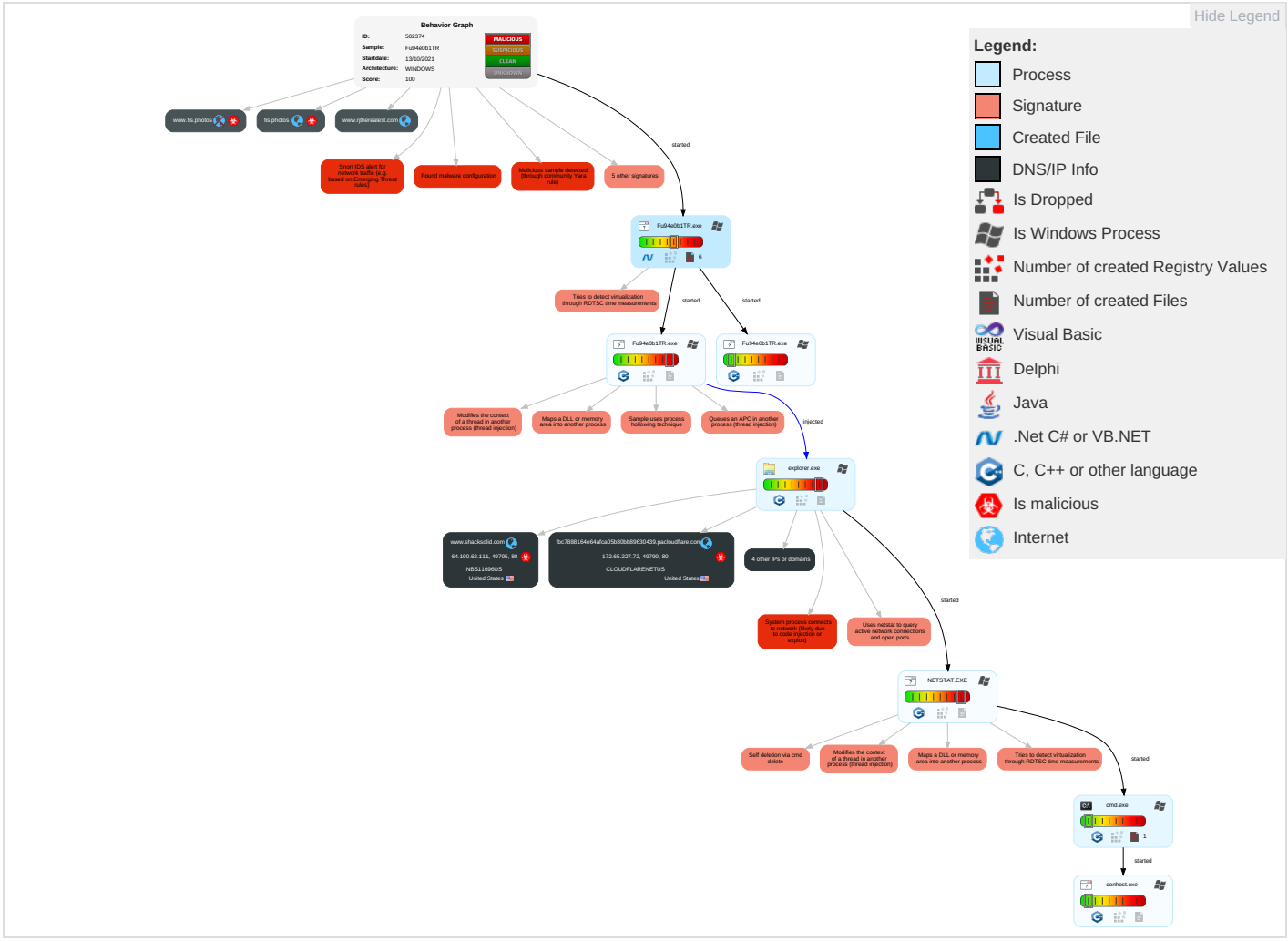
Remote Access Functionality:

- 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 o Insecure Network Communicat
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 Redirect Phc 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 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Network Connections 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	Software Packing 1 3	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

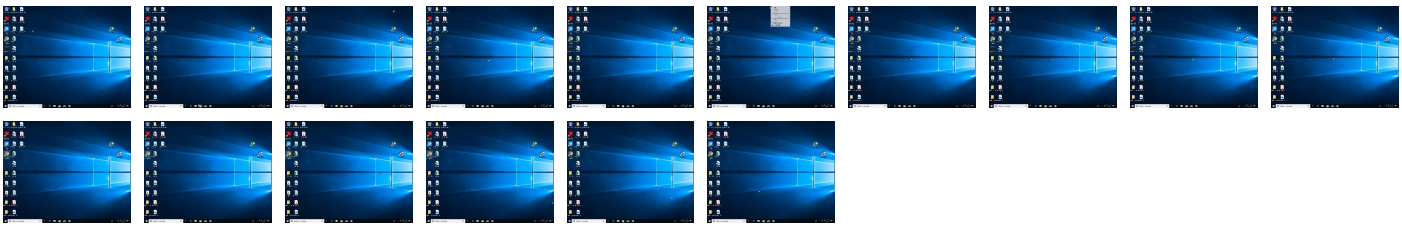
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.Fu94e0b1TR.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://flow.page/rjdarealest/ef6c/?BJB=7nO80D&yrTlglv8=yyRuLH34I	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmNormaldk	0%	Avira URL Cloud	safe	
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comdito	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comalicu	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/D	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	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	
www.fis.photos/ef6c/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/7	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ch	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.apricitee.com/ef6c/?BJB=7nO80D&yrTlglv8=KSHN/72DEJPyd/OuGOIXNFBSZoOhZSSqcZP1Rqc2bg8KEPsXLZdPsQK+HlsXn3Jp1PaC	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.fontbureau.com7	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comD	0%	Avira URL Cloud	safe	
http://www.fontbureau.comR.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comtuta	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmS	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/k	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/nt	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//lpk	0%	Avira URL Cloud	safe	
http://www.tiro.coma-e	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0ro	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/D	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.urwpp.deMT	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.shacksolid.com/ef6c/?yrTlglv8=JeohSOzXiZYIapiQlSWyFy7AWxQU0a2IMxMIOt5NBtSaZYcWimwRehmIZ/KtlrBMaY3r&BJB=7nO80D	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/denQ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/y	0%	URL Reputation	safe	
http://www.fontbureau.comk	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ms	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/v	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/nly	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFk	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fbc7888164e64afca05b80bb89630439.pacloudflare.com	172.65.227.72	true	true		unknown
www.rjtherealest.com	74.208.236.145	true	false		unknown
www.shacksolid.com	64.190.62.111	true	true		unknown
fis.photos	192.0.78.24	true	true		unknown
www.apricitee.com	unknown	unknown	true		unknown
www.fis.photos	unknown	unknown	true		unknown
www.instatechnovelz.com	unknown	unknown	true		unknown
www.brondairy.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.fis.photos/ef6c/	true	• Avira URL Cloud: safe	low
http://www.apricitee.com/ef6c/?BJB=7nO80D&yrTlglv8=KSHN/72DEJPyd/OuGOIXNFBSZoOhZSSqcZP1Rqc2bg8KEPsXLZdPsQK+HlsXn3Jp1PaC	true	• Avira URL Cloud: safe	unknown
http://www.shacksolid.com/ef6c/?yrTlglv8=JeohSOzXiZYIapiQlSWyFy7AWxQU0a2IMxMIOt5NBtSaZYcWimwRehmIZ/KtlrBMaY3r&BJB=7nO80D	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.190.62.111	www.shacksolid.com	United States		11696	NBS11696US	true
172.65.227.72	fbc7888164e64afca05b80bb89630439.pacloudflare.com	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502374
Start date:	13.10.2021
Start time:	20:56:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Fu94e0b1TR (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:	27
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@9/1@6/2
EGA Information:	Failed

HDC Information:	• Successful, ratio: 8% (good quality ratio 7%) • Quality average: 72.9% • Quality standard deviation: 33%
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
20:57:21	API Interceptor	1x Sleep call for process: Fu94e0b1TR.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
64.190.62.111	divpCHa0h7.exe	Get hash	malicious	Browse	• www.mambacustomboats.com/fqiq/?ZvEd=oM7C4s4K9Ux9NUwG97tedYlymorHgm5Kv3Umj1Gnv/i5ubiDMWU/+XDfdu3U3Pyuil7R&z0DH=f0Dtar1PYnAdDzS
	wDzceoRPhB.exe	Get hash	malicious	Browse	• www.artoidmode.com/ed9s/?2d64u=GZS0ntMXED7DC&j6A=OS1OG2uUyb/VuVpwb7VagzR+sXqT97Ebu6qajULP6tWiYdo/lZowWla7DoFCis6BwYQ7
	wO4j83Z0nB.exe	Get hash	malicious	Browse	• www.eaglelures.com/shjn/?4huPeB=fLPs2Pf5YsyIrReC5+nyeXhjuGvcKd4ZNbc7bYo7WcEYvq7qfTlOwt6z9eiotXX8oFy5NaIH5g==&8pll=h2M80lLH_NRh4lTP
	RNIpSzBRVC.exe	Get hash	malicious	Browse	• www.shacksolid.com/ef6c/?l6phLTh=JeohSOzXiZYIapiQlSWyFy7AWxQU0a2IMxMIOt5NBtSaZYcWimwRehmlZ/Gtb7NPDI39K9qB3Q==&UL=5j0Ll4TXePsH7TFp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL_DELIVERY_ADDRESS_CONFIRMATION.xlsx	Get hash	malicious	Browse	• www.eaglelures.com/shjn/?lL=fLPs2Pf8YryMrBSO7+nyeXhjuGvcKd4ZNbErHb06S8EZvbXsYD0CmpCx+4iXqHv3qlafUg==&NRX4i6=BxoHnNf8mX1
	Swift Copy.exe	Get hash	malicious	Browse	• www.margotandmontague.com/eods/?i8kt=rS6FBqWeadRIrUjRXVGDKJCXOrHmePLNijFl/Z5Z+nBb3zS+3MyVFNG7lwq4S2nmAYRT&1bRLa=YfFxl
	p83BktbXwe.exe	Get hash	malicious	Browse	• www.shacksolid.com/ef6c/?TN6=m6pTon&YFQLD6=JeohSOzXiZYIapiQlSWyFy7AWxQU0a2IMxMIOt5NBtSaZYcWimwRehmlZ/GUEKtMNer6K9qGkg==
	HUuKj0kt3z.exe	Get hash	malicious	Browse	• www.shacksolid.com/ef6c/?p4R4=PhjHKdH0&M0=JeohSOzXiZYIapiQlSWyFy7AWxQU0a2IMxMIOt5NBtSaZYcWimwRehmlZ8q9HKR0E9es
	ibelNHDA0l.exe	Get hash	malicious	Browse	• www.shacksolid.com/ef6c/?-ZUt=d0G0Yn1hWXrx&6liX3=JeohSOzXiZYIapiQlSWyFy7AWxQU0a2IMxMIOt5NBtSaZYcWimwRehmlZ/KtIrBMaY3r
	SOA.exe	Get hash	malicious	Browse	• www.margotandmontague.com/eods/?t2J=i48Hk&0488qv=rS6FBqWeadRIrUjRXVGDKJCXOrHmePLNijFl/Z5Z+nBb3zS+3MyVFNG7lwq4S2nmAYRT
	JFE6tQehuD.exe	Get hash	malicious	Browse	• www.metaju.com/hp6s/?3fi4-=oTVRl9Ml+OPXCj4hXV9OE5wFzXP9r5xGefeVUpAp//OvItILtz2iowizXiJv4RVplgLV&nHe8qD=uT4P8xNpn2xLT

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	qFghuPTDuw.exe	Get hash	malicious	Browse	• www.espressence.com/heth/?ZL3DB4=k0ADkxu0U9bB5vfcGnx5Bs1sio5yDITUm4QVk28VSMP15iSTcA+z80qdnmNkqg687zJ8t5HzaA==&j48D=mDHPtfePwBFdPz
	DUE PAYMENT.exe	Get hash	malicious	Browse	• www.arroundworld.com/b2c0/?2dpPwJP=HgvD120OCtIy2y4XcSYLXMqfh1iHIXLo+sJztNYgJy1E5kFWd+L461vXk/S7HsBG78Yt&uN9=3fPH4rk8fd4xHD
	DUE INVOICES.exe	Get hash	malicious	Browse	• www.cleanerstoday.com/b6cu/?BT=2dhhnfvPB6f8zBxp&R2MD6=s6p0OZd7QyF8NlKcRKg3d1Mhcu09NMFJH4/6pKf9s+pgPcRhCY/sfApJlg4NsLKExf7o
	04_extracted.exe	Get hash	malicious	Browse	• www.floving.com/n64d/?Cp=DP82qm31la64DOOKpdUd06m34NWm8oWBFGOqGRtoZCrcCLyfaO//8P4OrMWD8005mMFK&z8t=Xnpl7Zy8MJQL
	Order.exe	Get hash	malicious	Browse	• www.delights.info/k8b5/?wHzl=n58VdqdNqp0SKyCVZWhsMzftZSLJsGdR5bs0KFZ5CUW42r4DzaRBfIPAFoSHs1TqGO6s&-ZC=m6APvNqxt
	Statement of Account.exe	Get hash	malicious	Browse	• www.cleanerstoday.com/b6cu/?1bxdQ0YH=s6p0OZd7QyF8NlKcRKg3d1Mhcu09NMFJH4/6pKf9s+pgPcRhCY/sfApJljYdjqa8v6Sv&m0DD=bT0pMNUhtf28
	USD INV#1191189.exe	Get hash	malicious	Browse	• www.cleanerstoday.com/b6cu/?R2Mx=s6p0OZd7QyF8NlKcRKg3d1Mhcu09NMFJH4/6pKf9s+pgPcRhCY/sfApJljY38aq8r4av&gJBp9R=4hx40FuPFpNXarZP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NEW_PO_QUOTE_88987_PDF.exe	Get hash	malicious	Browse	• www.itbling.com/snaa/?Rv=HoB7UN9NeUtFFxU706ZiB/yN8phSIrDDzxMV/Ji+4+dNDKz34ah20hb+VYbC7wDWP/ld&p2J=vZw8NdKxk8f
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• www.nge.xyz/mo8t/?zxlpi=o1c4mJ3VAZ0Opt29tYk9ZJ1L/8ohiIP72w8Hsb8darVa0q91TqSigaAH0fmvs0SBq4qZcQ==&LR=w4UxT2yx30FHEXz

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fbc7888164e64afca05b80bb89630439.pa cloudflare.com	RNIpSzBRVC.exe	Get hash	malicious	Browse	• 172.65.227.72
	1taaCpMNKr.exe	Get hash	malicious	Browse	• 172.65.227.72
	qZfsUMa6Jh.exe	Get hash	malicious	Browse	• 172.65.227.72
	HUuKj0kt3z.exe	Get hash	malicious	Browse	• 172.65.227.72
	pdrAizaO1R.exe	Get hash	malicious	Browse	• 172.65.227.72
	$$$.exe	Get hash	malicious	Browse	• 172.65.227.72
	sample catalog_2021.exe	Get hash	malicious	Browse	• 172.65.227.72
	Transfer application.exe	Get hash	malicious	Browse	• 172.65.227.72
	CTM ARRANGEMENT.exe	Get hash	malicious	Browse	• 172.65.227.72
	Proforma Invoice & Bank Swift Copy.exe	Get hash	malicious	Browse	• 172.65.227.72
	USU(1).exe	Get hash	malicious	Browse	• 172.65.227.72
	PO#EIMG_501_367_089.exe	Get hash	malicious	Browse	• 172.65.227.72
	RFQ_AP65425652_032421 v#U00e1#U00ba#U00a5n #U00c4#U2018#U00e1#U00bb ,pdf.exe	Get hash	malicious	Browse	• 172.65.227.72
	Request for Quotation RFQ GC-0016862.PDF.exe	Get hash	malicious	Browse	• 172.65.227.72
	hEtfBNCsR8.rtf	Get hash	malicious	Browse	• 172.65.227.72
www.shacksolid.com	RNIpSzBRVC.exe	Get hash	malicious	Browse	• 64.190.62.111
	p83BktbXwe.exe	Get hash	malicious	Browse	• 64.190.62.111
	HUuKj0kt3z.exe	Get hash	malicious	Browse	• 64.190.62.111
	ibelNHDA0l.exe	Get hash	malicious	Browse	• 64.190.62.111
www.rjtherealest.com	0n1pEFuGKC.exe	Get hash	malicious	Browse	• 74.208.236.145
	4ZfdpLEQn1.exe	Get hash	malicious	Browse	• 74.208.236.145

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NBS11696US	divpCHa0h7.exe	Get hash	malicious	Browse	• 64.190.62.111
	wDzceoRPhB.exe	Get hash	malicious	Browse	• 64.190.62.111
	wO4j83Z0nB.exe	Get hash	malicious	Browse	• 64.190.62.111
	RNIpSzBRVC.exe	Get hash	malicious	Browse	• 64.190.62.111
	DHL_DELIVERY_ADDRESS_CONFIRMATION.xlsx	Get hash	malicious	Browse	• 64.190.62.111
	Swift Copy.exe	Get hash	malicious	Browse	• 64.190.62.111
	p83BktbXwe.exe	Get hash	malicious	Browse	• 64.190.62.111
	HUuKj0kt3z.exe	Get hash	malicious	Browse	• 64.190.62.111
	ibelNHDA0l.exe	Get hash	malicious	Browse	• 64.190.62.111
	SOA.exe	Get hash	malicious	Browse	• 64.190.62.111
	JFE6tQehuD.exe	Get hash	malicious	Browse	• 64.190.62.111
	qFghuPTDuw.exe	Get hash	malicious	Browse	• 64.190.62.111
	DUE PAYMENT.exe	Get hash	malicious	Browse	• 64.190.62.111
	x86_64	Get hash	malicious	Browse	• 209.87.95.109
	DUE INVOICES.exe	Get hash	malicious	Browse	• 64.190.62.111
	04_extracted.exe	Get hash	malicious	Browse	• 64.190.62.111
	Order.exe	Get hash	malicious	Browse	• 64.190.62.111

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Statement of Account.exe	Get hash	malicious	Browse	• 64.190.62.111
	USD INV#1191189.exe	Get hash	malicious	Browse	• 64.190.62.111
	NEW_PO_QUOTE_88987_PDF.exe	Get hash	malicious	Browse	• 64.190.62.111
CLOUDFLARENETUS	qbrMYaTNrE.exe	Get hash	malicious	Browse	• 104.21.26.237
	M12s7KNFDg.exe	Get hash	malicious	Browse	• 172.67.168.153
	farcry6_repack.exe	Get hash	malicious	Browse	• 162.159.130.233
	Original Shipment Doc Ref 2853801324189923,PDF.exe	Get hash	malicious	Browse	• 162.159.134.233
	Gsdqz.dll	Get hash	malicious	Browse	• 104.26.6.139
	4tOOUNDwaW.exe	Get hash	malicious	Browse	• 172.67.168.153
	7ofFMoirr5.exe	Get hash	malicious	Browse	• 104.21.26.237
	HUTWMrDhov.dll	Get hash	malicious	Browse	• 104.26.7.139
	2u2u8wnrrW.exe	Get hash	malicious	Browse	• 172.67.216.2
	z8FnqbFMkV.exe	Get hash	malicious	Browse	• 172.67.168.153
	divpCHa0h7.exe	Get hash	malicious	Browse	• 23.227.38.74
	M1YceQ237E.dll	Get hash	malicious	Browse	• 104.20.185.68
	BF2042.exe	Get hash	malicious	Browse	• 162.159.134.233
	SecuriteInfo.com.W32.AIDetect.malware1.10225.exe	Get hash	malicious	Browse	• 104.21.26.237
	5y4jNIVnk2.exe	Get hash	malicious	Browse	• 104.21.26.237
	vlF8tRNmtw.exe	Get hash	malicious	Browse	• 172.67.173.58
	FTdhc25gn8.exe	Get hash	malicious	Browse	• 162.159.130.233
	Paymentslip 10132021.xlsx	Get hash	malicious	Browse	• 172.67.188.154
	UZlg2Sq2pQ.exe	Get hash	malicious	Browse	• 104.21.17.130
	Revised_Purchase_Order.htm	Get hash	malicious	Browse	• 172.67.219.206

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Fu94e0b1TR.exe.log	
Process:	C:\Users\user\Desktop\Fu94e0b1TR.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.348115897127242
Encrypted:	false
SSDEEP:	24:MLUE4KJXE4qpE4Ks2E1qE4qpAE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4x88:MIHKtH2HKXE1qHmAHKzvRYHKhQnoPtH2
MD5:	832D6A22CE7798D72609B9C21B4AF152
SHA1:	B086DE927BFEE6039F5555CE53C397D1E59B4CA4
SHA-256:	9E5EE72EF293C66406AF155572BF3B0CF9DA09CC1F60ED6524AAFD65553CE551
SHA-512:	A1A70F76B98C2478830AE737B4F12507D859365F046C5A415E1EBE3D87FFD2B64663A31E1E5142F7C3A7FE9A6A9CB8C143C2E16E94C3DD6041D1CCABEDDD2C21
Malicious:	false
Reputation:	moderate, 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..2,"System.Deployment, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.47098319943845
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:	Fu94e0b1TR.exe
File size:	474112
MD5:	6429aa83e4bc083b4f0b3f44b0d7950f
SHA1:	0ead59881f054284f611accb61451ed1ffc818fc
SHA256:	96c57ae661562e958e01bb0b490c09a0a51bb367931620223174963de88bdfcb
SHA512:	186383701c591db2c011c8ae24920759c10880068dd217e32110ae54b9c7f0863b7fb04e893f601a234742deb5838a22820dc8835ba9198d66b7bb297d502f9b
SSDEEP:	6144:zMkhBsNolyfnZle9UX08PF85KQ4O1LkyUCZ2e12XZ0bp2Qo7lYB:oSBblyfnZlW+08+5KQpyy52nZ0vo7a
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....fa.....0..... .....@.. .....@.....

File Icon

Icon Hash:	c4b28ed696aa92c0

Static PE Info

General

Entrypoint:	0x45c99e
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:	0x6166A519 [Wed Oct 13 09:21:29 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	0x5a9a4	0x5aa00	False	0.880191271552	data	7.77320879492	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x5e000	0x18c94	0x18e00	False	0.1953125	data	5.07036789646	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	0x78000	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
10/13/21-20:59:09.555144	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49795	80	192.168.2.5	64.190.62.111
10/13/21-20:59:09.555144	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49795	80	192.168.2.5	64.190.62.111
10/13/21-20:59:09.555144	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49795	80	192.168.2.5	64.190.62.111
10/13/21-20:59:19.990837	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49797	80	192.168.2.5	192.0.78.24
10/13/21-20:59:19.990837	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49797	80	192.168.2.5	192.0.78.24
10/13/21-20:59:19.990837	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49797	80	192.168.2.5	192.0.78.24

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 20:58:54.008306980 CEST	192.168.2.5	8.8.8.8	0x3f12	Standard query (0)	www.apricitee.com	A (IP address)	IN (0x0001)
Oct 13, 2021 20:58:59.395916939 CEST	192.168.2.5	8.8.8.8	0xc785	Standard query (0)	www.instatechnovelz.com	A (IP address)	IN (0x0001)
Oct 13, 2021 20:59:04.443331003 CEST	192.168.2.5	8.8.8.8	0xcda9	Standard query (0)	www.brondairy.com	A (IP address)	IN (0x0001)
Oct 13, 2021 20:59:09.501405954 CEST	192.168.2.5	8.8.8.8	0x377a	Standard query (0)	www.shacksolid.com	A (IP address)	IN (0x0001)
Oct 13, 2021 20:59:14.611547947 CEST	192.168.2.5	8.8.8.8	0x698b	Standard query (0)	www.rjtherealest.com	A (IP address)	IN (0x0001)
Oct 13, 2021 20:59:19.956043005 CEST	192.168.2.5	8.8.8.8	0x449d	Standard query (0)	www.fis.photos	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 20:58:54.033735037 CEST	8.8.8.8	192.168.2.5	0x3f12	No error (0)	www.apricitee.com	vip.shoplazza.store		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 20:58:54.033735037 CEST	8.8.8.8	192.168.2.5	0x3f12	No error (0)	vip.shoplazza.store	fbc7888164e64afca05b80bb89630439.pacloudflare.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 20:58:54.033735037 CEST	8.8.8.8	192.168.2.5	0x3f12	No error (0)	fbc7888164e64afca05b80bb89630439.pacloudflare.com		172.65.227.72	A (IP address)	IN (0x0001)
Oct 13, 2021 20:58:59.421633959 CEST	8.8.8.8	192.168.2.5	0xc785	Name error (3)	www.instatechnovelz.com	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 20:59:04.465982914 CEST	8.8.8.8	192.168.2.5	0xcda9	Name error (3)	www.brondairy.com	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 20:59:09.534939051 CEST	8.8.8.8	192.168.2.5	0x377a	No error (0)	www.shacksolid.com		64.190.62.111	A (IP address)	IN (0x0001)
Oct 13, 2021 20:59:14.630974054 CEST	8.8.8.8	192.168.2.5	0x698b	No error (0)	www.rjtherealest.com		74.208.236.145	A (IP address)	IN (0x0001)
Oct 13, 2021 20:59:19.974540949 CEST	8.8.8.8	192.168.2.5	0x449d	No error (0)	www.fis.photos	fis.photos		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 20:59:19.974540949 CEST	8.8.8.8	192.168.2.5	0x449d	No error (0)	fis.photos		192.0.78.24	A (IP address)	IN (0x0001)
Oct 13, 2021 20:59:19.974540949 CEST	8.8.8.8	192.168.2.5	0x449d	No error (0)	fis.photos		192.0.78.25	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.apricitee.com
- www.shacksolid.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49790	172.65.227.72	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 20:58:54.065588951 CEST	6908	OUT	GET /ef6c/?BJB=7nO80D&yrTlglv8=KSHN/72DEJPyd/OuGOIXNFBSZoOhZSSqcZP1Rqc2bg8KEPsXLZdPsQK+HlsXn3Jp1PaC HTTP/1.1 Host: www.apricitee.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 20:58:54.380971909 CEST	6909	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=utf-8 Location: https://www.apricitee.com/ef6c/?BJB=7nO80D&yrTlglv8=KSHN/72DEJPyd/OuGOIXNFBSZoOhZSSqcZP1Rqc2bg8KEPsXLZdPsQK+HlsXn3Jp1PaC Strict-Transport-Security: max-age=315360000; includeSubdomains X-Content-Type-Options: nosniff X-Download-Options: noopen X-Xss-Protection: 1; mode=block Date: Wed, 13 Oct 2021 18:58:54 GMT Content-Length: 159 Connection: close Data Raw: 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 61 70 72 69 63 69 74 65 65 2e 63 6f 6d 2f 65 66 36 63 2f 3f 42 4a 42 3d 37 6e 4f 38 30 44 26 61 6d 70 3b 79 72 54 6c 67 6c 76 38 3d 4b 53 48 4e 2f 37 32 44 45 4a 50 79 64 2f 4f 75 47 4f 49 58 4e 46 42 53 5a 6f 4f 68 5a 53 53 71 63 5a 50 31 52 71 63 32 62 67 38 4b 45 50 73 58 4c 5a 64 50 73 51 4b 2b 48 6c 73 58 6e 33 4a 70 31 50 61 43 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 61 3e 2e 0a 0a Data Ascii: Moved Permanently.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49795	64.190.62.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 20:59:09.555144072 CEST	6931	OUT	GET /ef6c/?yrTlglv8=JeohSOzXiZYIapiQlSWyFy7AWxQU0a2IMxMIOt5NBtSaZYcWimwRehmIZ/KtlrBMaY3r&BJB=7nO80D HTTP/1.1 Host: www.shacksolid.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 20:59:09.598285913 CEST	6932	IN	HTTP/1.1 302 Found date: Wed, 13 Oct 2021 18:59:09 GMT content-type: text/html; charset=UTF-8 content-length: 0 x-adblock-key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhxb9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_D3MXYL1dze6qe7cOwJ2xLuV/g0A+RCNznrrC7wxtyCM8qdSMYKIxkg1u6Sue7w2UedwCteHB8MdfRzHrGBDLoQ== expires: Mon, 26 Jul 1997 05:00:00 GMT cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 pragma: no-cache last-modified: Wed, 13 Oct 2021 18:59:09 GMT location: https://sedo.com/search/details/?partnerid=324561&language=e&domain=shacksolid.com&origin=sales_lander_1&utm_medium=Parking&utm_campaign=offerpage x-cache-miss-from: parking-f666569bc-whw7l server: NginX connection: close

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Fu94e0b1TR.exe PID: 4628 Parent PID: 6048

General

Start time:	20:57:09
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\Fu94e0b1TR.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Fu94e0b1TR.exe'
Imagebase:	0x6d0000
File size:	474112 bytes
MD5 hash:	6429AA83E4BC083B4F0B3F44B0D7950F
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: 00000000.00000002.277178151.0000000002B11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.282740924.0000000003B19000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.282740924.0000000003B19000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.282740924.0000000003B19000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Fu94e0b1TR.exe PID: 4840 Parent PID: 4628

General

Start time:	20:57:22
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\Fu94e0b1TR.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Fu94e0b1TR.exe
Imagebase:	0x350000
File size:	474112 bytes
MD5 hash:	6429AA83E4BC083B4F0B3F44B0D7950F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Fu94e0b1TR.exe PID: 2848 Parent PID: 4628

General

Start time:	20:57:23
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\Fu94e0b1TR.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Fu94e0b1TR.exe
Imagebase:	0x610000
File size:	474112 bytes
MD5 hash:	6429AA83E4BC083B4F0B3F44B0D7950F
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: 00000006.00000002.370028583.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.370028583.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.370028583.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.371224121.0000000000F20000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.371224121.0000000000F20000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.371224121.0000000000F20000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.371120002.0000000000CF0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.371120002.0000000000CF0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.371120002.0000000000CF0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 2848

General

Start time:	20:57:25
Start date:	13/10/2021
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
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.333414635.000000000FAD6000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.333414635.000000000FAD6000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.333414635.000000000FAD6000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.311554346.000000000FAD6000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.311554346.000000000FAD6000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.311554346.000000000FAD6000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: NETSTAT.EXE PID: 3204 Parent PID: 3472

General

Start time:	20:58:05
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0xb70000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
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: 00000012.00000002.513567456.0000000000A20000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.513567456.0000000000A20000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.513567456.0000000000A20000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.513760624.0000000000A50000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.513760624.0000000000A50000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.513760624.0000000000A50000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.512579124.00000000003C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.512579124.00000000003C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.512579124.00000000003C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1844 Parent PID: 3204

General

Start time:	20:58:09
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Fu94e0b1TR.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: 4308 Parent PID: 1844

General

Start time:	20:58:10
Start date:	13/10/2021
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