ID: 458848
Sample Name:
New_1007572_021.exe
Cookbook: default.jbs
Time: 19:47:24
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

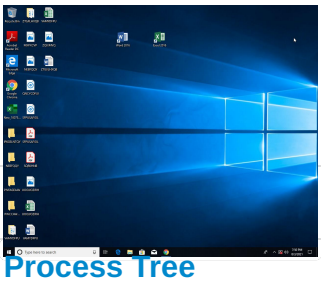
Windows Analysis Report New_1007572_021.exe

Overview

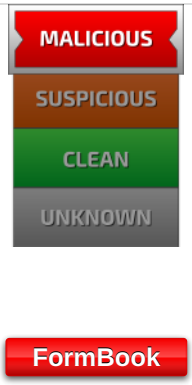
General Information

Sample Name:	New_1007572_021.exe
Analysis ID:	458848
MD5:	41137fd61b9cc0d..
SHA1:	15d023fd6d344cb.
SHA256:	b04306fa8223c20.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

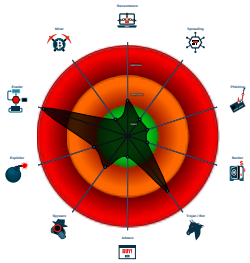


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for dropped file
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- New_1007572_021.exe (PID: 6688 cmdline: 'C:\Users\user\Desktop\New_1007572_021.exe' MD5: 41137FD61B9CC0D92225C91660A5902C)
  - New_1007572_021.exe (PID: 6280 cmdline: C:\Users\user\AppData\Local\Temp\New_1007572_021.exe MD5: 41137FD61B9CC0D92225C91660A5902C)
    - FB_5908.tmp.exe (PID: 6340 cmdline: 'C:\Users\user\AppData\Local\Temp\FB_5908.tmp.exe' MD5: 74BAFB3E707C7B0C63938AC200F99C7F)
    - FB_5E87.tmp.exe (PID: 6344 cmdline: 'C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe' MD5: 48ECE2CA39A9EAE7FCED7418CF071D46)
      - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - cscript.exe (PID: 6000 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
          - cmd.exe (PID: 6872 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 6756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.domoexpra.club/cg53/"
  ],
  "decoy": [
    "sugarlushcosmetic.com",
    "a2net.info",
    "ximakaya.com",
    "thevochick.com",
    "khafto.com",
    "zsgpbgsbh.icu",
    "psm-gen.com",
    "jhxhotei.com",
    "7991899.com",
    "nda.today",
    "fourseasonsvanlines.com",
    "splediferous.info",
    "thesqlgoth.com",
    "newpathequine.com",
    "advan.digital",
    "skamanderboats.com",
    "thejnit.com",
    "pardusarms.net",
    "mevasoluciones.com",
    "biggdoggSn2.com",
    "anogirl.com",
    "xinyisanreqi.com",
    "2mothertruckers.net",
    "phongvevic.com",
    "atmosphere.rent",
    "amabie-net.com",
    "stocksp24.com",
    "starseedbeing.com",
    "icreditmalaysia.com",
    "inochinokagayaki.net",
    "christianbooktrailer.com",
    "gidrot.com",
    "junglecli.com",
    "greenportcivic.com",
    "beyondparenting101.com",
    "tracisolomon.xyz",
    "healinghandssalem.com",
    "hackersincgolf.com",
    "goselling.solutions",
    "cumuluspharma.com",
    "ramblecollections.com",
    "mac-marine.com",
    "likeit21.com",
    "gdlejing.com",
    "si600.net",
    "greenhearthome.com",
    "tourps.com",
    "lvyi19.com",
    "frequent420.com",
    "goodteattirerebates.com",
    "melanie-gore.com",
    "comfsresidential.com",
    "vrgkk.com",
    "losmaestrosencarpinteria.com",
    "nikhitaindustries.com",
    "fresgolens.online",
    "xpj777.life",
    "zerkalo-mr-bit-casino.com",
    "thorsensgrinding.com",
    "ronniethemole.com",
    "poundlove.com",
    "joansv.com",
    "finneyplace.com",
    "dakotacntr.com"
  ]
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.926228324.0000000004F0F000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000013.00000002.926228324.0000000004F0F000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xa11c:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xa386:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15ea9:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15995:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15fab:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x16123:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xad9e:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x14c10:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xba97:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1bd1b:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1cd1e:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000013.00000002.926228324.0000000004F0F000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18c3d:$sqlite3step: 68 34 1C 7B E1 • 0x18d50:$sqlite3step: 68 34 1C 7B E1 • 0x18c6c:$sqlite3text: 68 38 2A 90 C5 • 0x18d91:$sqlite3text: 68 38 2A 90 C5 • 0x18c7f:$sqlite3blob: 68 53 D8 7F 8C • 0x18da7:$sqlite3blob: 68 53 D8 7F 8C
00000013.00000002.925005416.0000000000278000.00000004.00000020.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000013.00000002.925005416.0000000000278000.00000004.00000020.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xa040:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xa2aa:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15dcd:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x158b9:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15ecf:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x16047:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xacc2:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x14b34:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb9bb:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1bc3f:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1cc42:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.New_1007572_021.exe.3eb8b30.6.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0.2.New_1007572_021.exe.3eb8b30.6.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xe5c0:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xe82a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1a34d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x19e39:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1a44f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1a5c7:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xf242:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x190b4:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xff3b:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x201bf:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x211c2:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.New_1007572_021.exe.3eb8b30.6.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1d0e1:$sqlite3step: 68 34 1C 7B E1 • 0x1d1f4:$sqlite3step: 68 34 1C 7B E1 • 0x1d110:$sqlite3text: 68 38 2A 90 C5 • 0x1d235:$sqlite3text: 68 38 2A 90 C5 • 0x1d123:$sqlite3blob: 68 53 D8 7F 8C • 0x1d24b:$sqlite3blob: 68 53 D8 7F 8C
10.2.FB_5E87.tmp.exe.1080000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.FB_5E87.tmp.exe.1080000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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:

Modifies the prolog of user mode functions (user mode inline hooks)

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

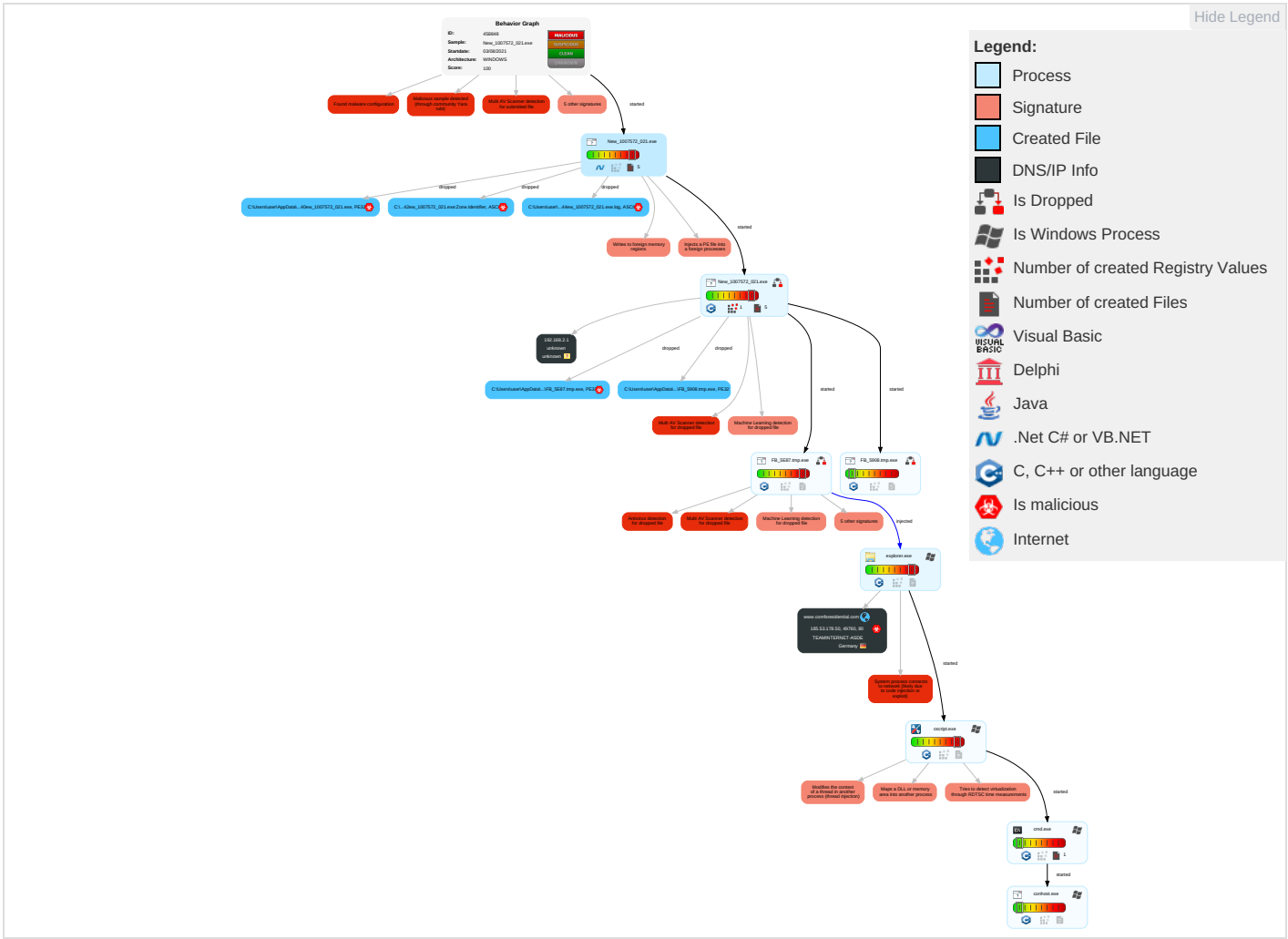
Yara detected FormBook

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 7 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	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	Process Injection 7 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

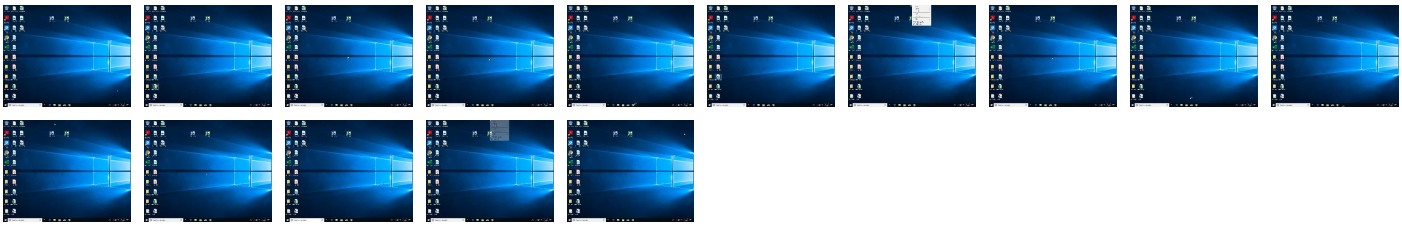
Behavior Graph



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
New_1007572_021.exe	28%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
New_1007572_021.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\New_1007572_021.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\FB_5908.tmp.exe	5%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\FB_5908.tmp.exe	2%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe	49%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe	86%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\user\AppData\Local\Temp\New_1007572_021.exe	28%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.New_1007572_021.exe.2d49d5c.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.New_1007572_021.exe.3eb8b30.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
10.2.FB_5E87.tmp.exe.1080000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.1.FB_5E87.tmp.exe.1080000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.0.FB_5E87.tmp.exe.1080000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.New_1007572_021.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.New_1007572_021.exe.3bc9930.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.come.comE	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.comfsresidential.com/cg53/?y48=RnXd-dV8&04VdoL_=jL4gYOGdbdGLgCuh81HWgUyhq6g08d9KQ1n+auYX12/KRBTZXwpphFOeP1KBAJVgFN6h	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.comfsresidential.com	185.53.178.50	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.comfsresidential.com/cg53/?y48=RnXd-dV8&04VdoL_=jL4gYOGdbdGLgCuh81HWgUyhq6g08d9KQ1n+auYX12/KRBTZXwpphFOeP1KBAJVgFN6h	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.53.178.50	www.comfsresidential.com	Germany		61969	TEAMINTERNET-ASDE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458848
Start date:	03.08.2021
Start time:	19:47:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New_1007572_021.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:	22
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@11/5@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 61.7% (good quality ratio 54.7%) • Quality average: 69.1% • Quality standard deviation: 33.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.53.178.50	http://www.fgoogle.at	Get hash	malicious	Browse	• www.fgoogle.at/favicon.ico

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TEAMINTERNET-ASDE	rL3Wx4zKD4.exe	Get hash	malicious	Browse	• 185.53.177.53
	Medical Equipment Order 2021.PDF.exe	Get hash	malicious	Browse	• 185.53.179.90
	d9UdQnXQ86ld31G.exe	Get hash	malicious	Browse	• 185.53.177.11
	YKqDUg3NxSA9bwZ.exe	Get hash	malicious	Browse	• 185.53.178.11
	dl145cKtrs.exe	Get hash	malicious	Browse	• 185.53.178.12
	PO 3457773.exe	Get hash	malicious	Browse	• 185.53.177.14
	PO#JFUB0002 FOR NEW ORDER.exe	Get hash	malicious	Browse	• 185.53.177.53
	Confirma PI#4042021 INVOICE.exe	Get hash	malicious	Browse	• 185.53.177.53
	RFQ-2176 NEW PROJECT QUOTATION MAY.exe	Get hash	malicious	Browse	• 185.53.177.11
	WXs8v9QuE7.exe	Get hash	malicious	Browse	• 185.53.177.12
	KBzeB23bE1.exe	Get hash	malicious	Browse	• 185.53.177.13
	xnuE49NGol.exe	Get hash	malicious	Browse	• 185.53.177.11
	aVzUZCHkko.exe	Get hash	malicious	Browse	• 185.53.177.11
	PO#310521.PDF.exe	Get hash	malicious	Browse	• 185.53.178.10
	Scanned Specification Catalogue 7464.exe	Get hash	malicious	Browse	• 185.53.177.52
	Ciikfddtznhxmtqufdujkifxwmwhrfjkcl_Signed_.exe	Get hash	malicious	Browse	• 185.53.178.53
	$RAULIU9.exe	Get hash	malicious	Browse	• 185.53.177.31
	350969bc_by_Libranalysis.exe	Get hash	malicious	Browse	• 185.53.177.53
	GLqbDRKePPp16Zr.exe	Get hash	malicious	Browse	• 185.53.177.12
	sample3.exe	Get hash	malicious	Browse	• 185.53.177.12

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\FB_5908.tmp.exe	IMG_105_13_676_571.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.DownloaderNET.151.21045.exe	Get hash	malicious	Browse	
	4-1.doc	Get hash	malicious	Browse	
	Order Inqury-93-23-20.doc	Get hash	malicious	Browse	
	IMG_7189012.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.45131634.12155.exe	Get hash	malicious	Browse	
	77.doc	Get hash	malicious	Browse	
	qlvti.exe	Get hash	malicious	Browse	
	RFQ-220818.xls	Get hash	malicious	Browse	
	RFQ-220818.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New_1007572_021.exe.log

Process:	C:\Users\user\Desktop\New_1007572_021.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New_1007572_021.exe.log	
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	**true**
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..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

C:\Users\user\AppData\Local\Temp\FB_5908.tmp.exe	
Process:	C:\Users\user\AppData\Local\Temp\New_1007572_021.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	1.7089931293899303
Encrypted:	false
SSDEEP:	24:7U6Id6l1iWyyyyyyyytrUUUUUUUUUgro:oO
MD5:	74BAFB3E707C7B0C63938AC200F99C7F
SHA1:	10C5506337845ED9BF25C73D2506F9C15AB8E608
SHA-256:	129450BA06AD589CF6846A455A5B6B5F55E164EE4906E409EB692AB465269689
SHA-512:	5B24DC5ACD14F812658E832B587B60695FB16954FCA006C2C3A7382EF0EC65C3BD1AAF699425C49FF3CCEEF16869E75DD6F00EC189B9F673F08F7E1B80CF778
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 2%
Joe Sandbox View:	• Filename: IMG_105_13_676_571.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.DownloaderNET.151.21045.exe, Detection: malicious, Browse • Filename: 4-1.doc, Detection: malicious, Browse • Filename: Order Inqury-93-23-20.doc, Detection: malicious, Browse • Filename: IMG_7189012.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.GenericKD.45131634.12155.exe, Detection: malicious, Browse • Filename: 77.doc, Detection: malicious, Browse • Filename: qlvti.exe, Detection: malicious, Browse • Filename: RFQ-220818.xls, Detection: malicious, Browse • Filename: RFQ-220818.xls, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZI.....@.....Win32 Program!..$.....!.L.!`...GoLink, GoAsm www.GoDevTool.com.PE..L....y.>.....@.....0.....C..... ..... .....code..... ..`.rsrc..... .....@..@.....

C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe	
Process:	C:\Users\user\AppData\Local\Temp\New_1007572_021.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	186368
Entropy (8bit):	7.314572114292142
Encrypted:	false
SSDEEP:	3072:4dqYxe9j7g+D8OwXoopyPS5O1lFqRKMhZ6L7Ne61PCbyl2:4kXh8OIoYyq5ILqRKMo7cFN
MD5:	48ECE2CA39A9EAE7FCED7418CF071D46
SHA1:	7570995CBF699088A8F208015CB2C92BE5BC837A
SHA-256:	4119B29BC938578D5D243DB714D0619228D37C10CCAA52925F9E81A410720D59
SHA-512:	E897FDED4B643054796E410CADCC348C1215C934FE70F5407E36E9F10E59E2B10B7EDCBB99D746709AEF8FF498D98D848ADA90FB477EA732A128EE138ED0FDB
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe, Author: JPCERT/CC Incident Response Group

C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe	
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 86%
Preview:	MZER.....X.....<.....(.....!..L.!This program cannot be run in DOS mode....$.....f..f..f.....f.....f.....f.Rich.f.....PE..L.....N..... .....@.....@.....text..... ..`..... ....

C:\Users\user\AppData\Local\Temp\New_1007572_021.exe	
Process:	C:\Users\user\Desktop\New_1007572_021.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	455168
Entropy (8bit):	7.937198220453206
Encrypted:	false
SSDEEP:	12288:bHOWiWyFfGU94mxuYfv/PT9WK+dG7VWfQTB:bHQ4mF7ZBMfwB
MD5:	41137FD61B9CC0D92225C91660A5902C
SHA1:	15D023FD6D344CB18243469A3EE01FEA6BB189AF
SHA-256:	B04306FA8223C20A1ABAAA6AEB5CABB2A83DC04337BEB2ACFD47784B34B682BC
SHA-512:	E32EE01FD957EE49F6BFCEFF4BC58B8B695111EF7416F8487398CBFAFD16B2EEAE0B79C41A8071075FD4E09D584CB642393F9E1655A5D70AB3135ADDD2E7EC BA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...ms).....0.....J..... .....@.. .....`..... ..@.....@...K.....F.....@..... ..... ..H.....text..... ..... ..`.rsrc....F.....H.....@..@.rel oc.....@.....@..B.....p.....H.....<..,.....,...i..,\.....0..>.....(.... ....~...:....&8....8.....E.....8.....(....8....*...s....o....*.0..}.....8m..... .E....[.....8V....{....(....8....8....8.....(... ....~c...9....&8....{....9.... ....~2...:....&8....*.:....8.....0.....8.....E.....n.....8.....(....8.....(....8'.....s....(.... ....~K...9....&8..... ....s....(.... ....~t...:....&8y....r...p(....8.....(....8.....

C:\Users\user\AppData\Local\Temp\New_1007572_021.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\New_1007572_021.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.937198220453206
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	New_1007572_021.exe
File size:	455168
MD5:	41137fd61b9cc0d92225c91660a5902c
SHA1:	15d023fd6d344cb18243469a3ee01fea6bb189af

General

SHA256:	b04306fa8223c20a1abaaa6aeb5cabb2a83dc04337beb2acfd47784b34b682bc
SHA512:	e32ee01fd957ee49f6bfceff4bc58b8b695111ef7416f8487398cbfafd16b2eeae0b79c41a8071075fd4e09d584cb642393f9e1655a5d70ab3135addd2e7ecba
SSDEEP:	12288:bHOWiWyFfGU94mxuYfv/PT9WK+dG7VWfQTB:bHQ4mF7ZBMfwB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...ms).....0.....J..... .....@.. .....`.....@.....

File Icon

Icon Hash:	888c9abc8c8ad8d8

Static PE Info

General

Entrypoint:	0x46c58e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xDF29736D [Sun Aug 22 17:54:53 2088 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	0x6a594	0x6a600	False	0.982139578437	data	7.98710710749	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6e000	0x46f4	0x4800	False	0.181206597222	data	4.45766439274	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x74000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-19:50:15.399423	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49760	185.53.178.50	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 19:50:15.298187971 CEST	192.168.2.4	8.8.8.8	0x6317	Standard query (0)	www.comfsresidential.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 19:50:15.339657068 CEST	8.8.8.8	192.168.2.4	0x6317	No error (0)	www.comfsresidential.com		185.53.178.50	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.comfsresidential.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49760	185.53.178.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:50:15.382633924 CEST	6717	OUT	GET /cg53/?y48=RnXd-dV8&04VdoL_=jL4gYOGdbdGLgCuh81HWgUyhq6g08d9KQ1n+auYX12/KRBTZXwpphFOeP1KBAJVgFN6h HTTP/1.1 Host: www.comfsresidential.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 19:50:15.399422884 CEST	6717	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 03 Aug 2021 17:50:15 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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 33 20 46 6f 72 62 69 64 64 65 6e 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 6e 67 69 6e 78 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 Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: New_1007572_021.exe PID: 6688 Parent PID: 5932

General

Start time:	19:48:16
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\New_1007572_021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New_1007572_021.exe'
Imagebase:	0x800000
File size:	455168 bytes
MD5 hash:	41137FD61B9CC0D92225C91660A5902C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.739038576.0000000003BCD000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.739038576.0000000003BCD000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.739038576.0000000003BCD000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.739831969.0000000003EBC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.739831969.0000000003EBC000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.739831969.0000000003EBC000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.739343756.0000000003D06000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.739343756.0000000003D06000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.739343756.0000000003D06000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: New_1007572_021.exe PID: 6280 Parent PID: 6688

General

Start time:	19:48:53
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Local\Temp\New_1007572_021.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\New_1007572_021.exe
Imagebase:	0xb50000
File size:	455168 bytes
MD5 hash:	41137FD61B9CC0D92225C91660A5902C
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: 00000008.00000002.740535210.0000000000404000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.740535210.0000000000404000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.740535210.0000000000404000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 28%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Registry Activities

Show Windows behavior

Key Value Created

Key Value Modified

Analysis Process: FB_5908.tmp.exe PID: 6340 Parent PID: 6280

General

Start time:	19:48:55
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Local\Temp\FB_5908.tmp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\FB_5908.tmp.exe'
Imagebase:	0x400000
File size:	3072 bytes
MD5 hash:	74BAFB3E707C7B0C63938AC200F99C7F
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 5%, Metadefender, Browse • Detection: 2%, ReversingLabs
Reputation:	moderate

Analysis Process: FB_5E87.tmp.exe PID: 6344 Parent PID: 6280

General

Start time:	19:48:55
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe'
Imagebase:	0x1080000
File size:	186368 bytes
MD5 hash:	48ECE2CA39A9EAE7FCED7418CF071D46
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: 0000000A.00000002.821727953.0000000001081000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.821727953.0000000001081000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.821727953.0000000001081000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.821846658.00000000012B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.821846658.00000000012B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.821846658.00000000012B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.821488799.0000000000E10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.821488799.0000000000E10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.821488799.0000000000E10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.740219963.0000000001081000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.740219963.0000000001081000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.740219963.0000000001081000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 49%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6344

General

Start time:	19:48:57
Start date:	03/08/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cscript.exe PID: 6000 Parent PID: 3424

General

Start time:	19:49:31
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0xe0000
File size:	143360 bytes
MD5 hash:	00D3041E47F99E48DD5FFFEDF60F6304
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: 00000013.00000002.926228324.0000000004F0F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.926228324.0000000004F0F000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.926228324.0000000004F0F000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.925005416.0000000000278000.00000004.00000020.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.925005416.0000000000278000.00000004.00000020.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.925005416.0000000000278000.00000004.00000020.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.925127682.0000000000490000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.925127682.0000000000490000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.925127682.0000000000490000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.926114786.0000000004BA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.926114786.0000000004BA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.926114786.0000000004BA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.925530735.00000000031B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.925530735.00000000031B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.925530735.00000000031B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6872 Parent PID: 6000

General

Start time:	19:49:34
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\FB_5E87.tmp.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6756 Parent PID: 6872

General

Start time:	19:49:35
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis