ID: 433143
Sample Name: INVOICE.exe
Cookbook: default.jbs
Time: 11:36:19
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

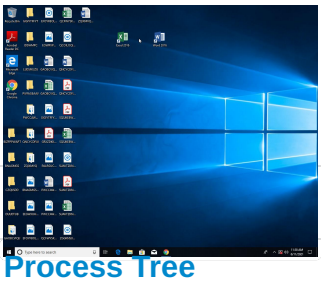
Analysis Report INVOICE.exe

Overview

General Information

Sample Name:	INVOICE.exe
Analysis ID:	433143
MD5:	98901aff995d926..
SHA1:	6dac1968c4a9ae..
SHA256:	fb6e849cd3af7e8..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

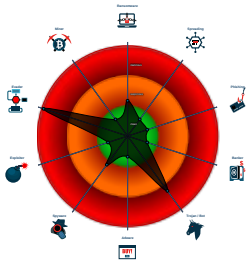
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- 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…
- Executable has a suspicious name (…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- INVOICE.exe (PID: 6440 cmdline: 'C:\Users\user\Desktop\INVOICE.exe' MD5: 98901AFF995D92677CF637B241AE9A9B)
  - INVOICE.exe (PID: 6476 cmdline: 'C:\Users\user\Desktop\INVOICE.exe' MD5: 98901AFF995D92677CF637B241AE9A9B)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - systray.exe (PID: 2148 cmdline: C:\Windows\SysWOW64\systray.exe MD5: 1373D481BE4C8A6E5F5030D2FB0A0C68)
      - cmd.exe (PID: 2100 cmdline: /c del 'C:\Users\user\Desktop\INVOICE.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.gicc-fx.com/uer0/"
  ],
  "decoy": [
    "bonds101.com",
    "lyotrust.com",
    "can-amchainseurope.com",
    "mysoulcure.com",
    "hometownsmut.com",
    "cxpzhy.site",
    "hjklrmn.xyz",
    "bsdminingservice.com",
    "mockpacket.com",
    "standwithkam.com",
    "yxbdj.com",
    "soulseedz.com",
    "whxldjt.com",
    "ruayhunhangseng.com",
    "benefitcrystal.info",
    "rahalake.com",
    "cryptnex.com",
    "comicslighthouse.com",
    "ridenwithbiden.net",
    "samsunbilsem.com",
    "homestorestoragemanhattan.com",
    "33-today.club",
    "laurajimore.com",
    "wellnesswithshami.com",
    "palmyra-beaute.com",
    "ringerpinger.com",
    "cpf3life.com",
    "medusaantalya.com",
    "meganmccalla.com",
    "xn--2qux23coval6o.net",
    "icheaplivemall.com",
    "theseekers5thdimension.com",
    "hydrogenfunding.com",
    "calphad.cloud",
    "amazingdiapercakes.com",
    "11gongli.com",
    "bhuyanit.com",
    "16263937888.com",
    "crowgangrecords.com",
    "ytub.xyz",
    "virtual-ledlight.com",
    "dollysusmitha.com",
    "istanbulkonyasofrasi.com",
    "phonetomouth.com",
    "tiendasred.com",
    "destemidovapes.com",
    "quinnmonroe.com",
    "internationaldatingapps.com",
    "aib-confirm.com",
    "rentthemansion.com",
    "musicmysoul.com",
    "alpinesocks.net",
    "8425sentinaechasedrive.com",
    "danielabigalli.com",
    "atlasresearchus.com",
    "rossinkmobilenotary.com",
    "mynevve.com",
    "alfacapital.fund",
    "jumtix.xyz",
    "rr-program.com",
    "trumpoutnowhat.com",
    "motorworld.rentals",
    "condoproinsurance.com",
    "quantumkca.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000001.201178753.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000001.201178753.0000000000400000.00000040.00020000.sdmp	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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000001.201178753.0000000000400000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.275287960.00000000006F0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.275287960.00000000006F0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.INVOICE.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.INVOICE.exe.400000.0.raw.unpack	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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.INVOICE.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
1.1.INVOICE.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.INVOICE.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- Executable has a suspicious name (potential lure to open the executable)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- Detected unpacking (changes PE section rights)

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

Stealing of Sensitive Information:

Yara detected FormBook

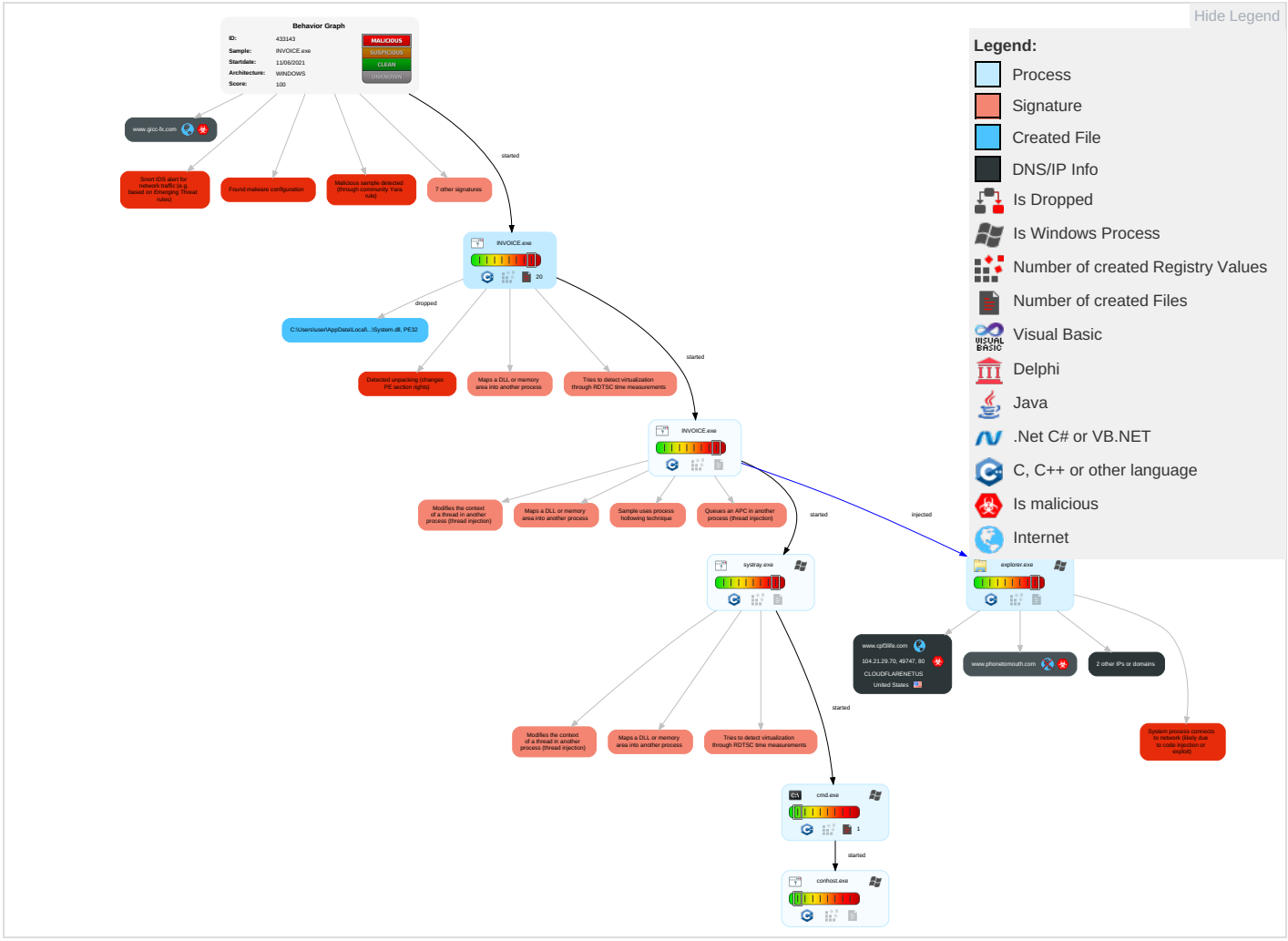
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 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	Obfuscated Files or Information 2	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

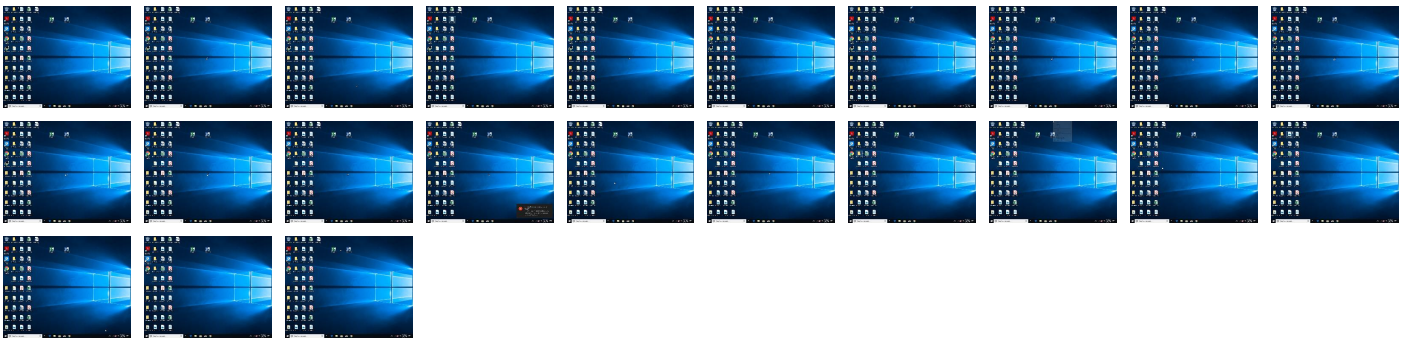
Behavior Graph



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
INVOICE.exe	66%	ReversingLabs	Win32.Trojan.Emotet	
INVOICE.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsj9221.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsj9221.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.INVOICE.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
0.2.INVOICE.exe.9990000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.INVOICE.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.INVOICE.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.systray.exe.4ccf834.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.INVOICE.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
0.0.INVOICE.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
8.2.systray.exe.ac3748.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

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.cpf3life.com/uer0/?cT=IWphFoHV4jp5oknFMScIxRoUR2WJRPQs/XYBCw5pT/o6GbblNl6C3qYdj4q6OTOtoDPc&0rjL0=00GhNj0PalVPThz	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://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.phonetomouth.com/uer0/?0rjL0=00GhNj0PalVPThz&cT=mzn46ufhhzCxwm8qeMWDu5BECFFcgbpMb+xr4Y5+z9rgY/t3xuFClMCjGCpTywHehpEI	0%	Avira URL Cloud	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.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	
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.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.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.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.urwpp.deDPlease	0%	URL Reputation	safe	
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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
www.gicc-fx.com/uer0/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.cpf3life.com	104.21.29.70	true	true		unknown
www.gicc-fx.com	198.252.100.204	true	true		unknown
phonetomouth.com	34.102.136.180	true	false		unknown
www.phonetomouth.com	unknown	unknown	true		unknown
www.dollysusmitha.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.cpf3life.com/uer0/?cT=lWphFoHV4jp5oknFMScIxRoUR2WJRPQs/XYBCw5pT/o6GbblNl6C3qYdj4q6OTOtoDPc&0rjL0=00GhNj0PalVPThz	true	• Avira URL Cloud: safe	unknown
http://www.phonetomouth.com/uer0/?0rjL0=00GhNj0PalVPThz&cT=mzn46ufhhzCxwm8qeMWDu5BECFFcgbpMb+xr4Y5+z9rgY/t3xuFClMCjGCpTywHehpEI	false	• Avira URL Cloud: safe	unknown
www.gicc-fx.com/uer0/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.29.70	www.cpf3life.com	United States		13335	CLOUDFLARENETUS	true
34.102.136.180	phonetomouth.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433143
Start date:	11.06.2021
Start time:	11:36:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INVOICE.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:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/4@4/2
EGA Information:	Failed

HDC Information:	• Successful, ratio: 30.8% (good quality ratio 28.9%) • Quality average: 78.1% • Quality standard deviation: 28%
HCA Information:	• Successful, ratio: 89% • 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

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Request Quotation.exe	Get hash	malicious	Browse	• 104.21.19.200
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 172.67.169.41
	Shipment Invoice & Consignment Notification.exe	Get hash	malicious	Browse	• 172.67.188.154
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 172.67.169.41
	w4X8dxtGi6.exe	Get hash	malicious	Browse	• 172.67.163.99
	St3aq2ELIJ.exe	Get hash	malicious	Browse	• 104.21.2.30
	KY4cmAI0jU.exe	Get hash	malicious	Browse	• 172.67.206.33
	w1iSiwLXiV.exe	Get hash	malicious	Browse	• 172.67.188.154
	TKeRmCuiit.exe	Get hash	malicious	Browse	• 172.67.188.154
	c71fd2gJus.exe	Get hash	malicious	Browse	• 172.67.222.38
	BrBsL8sBvm.exe	Get hash	malicious	Browse	• 172.67.188.69
	New Order PO2193570O1.doc	Get hash	malicious	Browse	• 162.159.134.233
	Proforma Invoice.exe	Get hash	malicious	Browse	• 172.67.188.154
	00010200390_0192021.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Payment Advice.pdf.doc	Get hash	malicious	Browse	• 104.21.19.200
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	bL6FwQU4K5.exe	Get hash	malicious	Browse	• 172.67.163.99
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 104.21.62.88
	crt9O3URua.exe	Get hash	malicious	Browse	• 172.67.38.66
	fuoAl0V94I.exe	Get hash	malicious	Browse	• 172.67.162.27

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsj9221.tmp\System.dll	Shipment Invoice & Consignment Notification.exe	Get hash	malicious	Browse	
	KY4cmAI0jU.exe	Get hash	malicious	Browse	
	5t2CmTUhKc.exe	Get hash	malicious	Browse	
	8qdfmqz1PN.exe	Get hash	malicious	Browse	
	New Order PO2193570O1.doc	Get hash	malicious	Browse	
	L2.xlsx	Get hash	malicious	Browse	
	Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.xlsx	Get hash	malicious	Browse	
	New Order PO2193570O1.pdf.exe	Get hash	malicious	Browse	
	2320900000000.exe	Get hash	malicious	Browse	
	CshpH9OSkc.exe	Get hash	malicious	Browse	
	5SXTKXCnqS.exe	Get hash	malicious	Browse	
	i6xFULh8J5.exe	Get hash	malicious	Browse	
	AWB00028487364 -000487449287.doc	Get hash	malicious	Browse	
	090049000009000.exe	Get hash	malicious	Browse	
	dYy3yfSkwY.exe	Get hash	malicious	Browse	
	PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx	Get hash	malicious	Browse	
	Purchase Order Price List 061021.xlsx	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	UGGJ4NnzFz.exe	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\jxl61c12gqlj1w2	
Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	data
Category:	dropped
Size (bytes):	186368
Entropy (8bit):	**7.999073326465555**
Encrypted:	**true**
SSDEEP:	3072:zeJR8AqtAiPJCcwSkW24wzwEV/SyhAJdPAanMl535y6iMSy2TZOcoREojDx9Syda:zeX8m2Ccwx9brJSymPbnMl535iyUOpL2
MD5:	EABF5B1834E87B0207D0DC3130F37357
SHA1:	C0B6A3BD8A5598EBAE0180E03DFA5208BAC7B8CC
SHA-256:	58575C8E3AD256B66DC397F4721A0BD6E1BE2A80322B868591835394C53D0595
SHA-512:	9D0F02D820ADED3AD52DDEBFBD8CAB10F3A9B45EAAECCDA5872B34439A328ED772B0F9B5878DF312D80326FBF6AB3ACC8E449AF3D9F76523918717EE14E4D402
Malicious:	false
Reputation:	low
Preview:	.!..!P.(.....F[.A03.W...?J.N.....F2.L..Pp.&..O%9....yg.a...:D.....P.[k...w..g....iK".Q..r..lw".3U.c.=;....[..w..G...L.(...v....F...5|..F.....A...P...u...B...o..z....1.S.Ll...9.$,Ns.$Fp.....<I.I>.F#..K.3X.N_..d.#.._...O../...q.....qy..b..s..u/...*?...".[x..E6..E...T.s.*..x.E../A.{+...!..D.\...U.U.dV.....y8w6.._`G.Tp8.K.9.=.}.L...Gb.8.F.t....4..S.\.....~!*@..y.T..;.[..."`.kp..\.....A0U1a4'.=.....10..U..(.3...?..Pz....<s.F..pF.....N..Cl.....D/n..W#.(..x...IO.u..8...'e.?Pj.]U..}..C....O.9M...+.%?..rQ"X..33\S.:..).%.'....H.?.....,>.-.....<.....w-..".Qt..Q.,...-B..?.j(.}.Wf)>.....'.....2...2e.n....U.t.L...+t...b..dZ..=i&.z4.%.v.#'.1.....R4..,@%.Q.....o !&4.5.F..D[.....V....\.....B,.77a...s.....:..i+}..."....l...uE..9.L..OI@..y/.....DW7..v."..Tr....nl `./...=.... .y6.(L.W.v...Z....].%.Y..0.'.r.8G.....MG..8s{..p....Q}.tR@.....x.._]D..'V.$I...^.....v.Q...X.?p...Me..m.0.N.h..G.P...G..#....x...X..C..^Icy.

C:\Users\user\AppData\Local\Temp\nfqccgctc	
Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	data
Category:	dropped
Size (bytes):	56625
Entropy (8bit):	4.977281164917555
Encrypted:	false
SSDEEP:	1536:vpfNMGP6XAbV3hcW3/NFikDoq6/hWMlGXEWfBJwNAv:vPMGCwbFhhNFnorJWEGyNQ
MD5:	BD19C858192D97E9604FACD096F21BAB
SHA1:	20BE0E18245A58AFE0CF734670FE56E5FEE8650B
SHA-256:	B62F6C39FAFAEEC5573AC373180FEDD001FD05D876035EFB56A6AD49DEACC280
SHA-512:	49B5259F56056CC933D091AAC6024C0428AE70328F8A10150D80973F4BAE3862D5C9736EA45BD8E4D72979E7E756D77CA223BEEE11ABAA3056A90171B66F4218
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\nfqccgctc	
Preview:	U.....L.....M.....N.....O.....P.....Q.....R.....S.../.T.....U.....V.....W.....X.....Y.....Z../.[...F.\.../.].....^.....`.....a...8.b.....c.....d.....e.....f.....g...S.h.....i.....j.....k.....l.....m.....n.....o.....p.....q...+.r...8.s.....t...S.u.....v.....w.....x.....y.....z...+.{.....|.....}.....~.....+.....+.....S.....S..... .....'.....K.....B.....\.....\.....\.....8.....K.....K.....K..... .....'.....B.....\... ..\.....\.....8.....

C:\Users\user\AppData\Local\Temp\nsj9220.tmp	
Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	data
Category:	dropped
Size (bytes):	279242
Entropy (8bit):	7.450736154071571
Encrypted:	false
SSDEEP:	6144:fYeX8m2Ccwx9brJSymPbnMl535iyUOpLmyD2S8dCwbFhjFnMI7ypt:AN9y5AhPe5pjUcd/8dCQhxMI2z
MD5:	8FF52CDF1885512EB8681CC3FF94FA64
SHA1:	12684292C1E37F8609B321E29F44E2E0C07B0B5E
SHA-256:	588996F8F600844C43C8BB51A443B1E6046CB02DFA69CD19D62D63B8F51A5EAC
SHA-512:	044614F6ADA0F03CC1DC021F6602DF069F4D7DB6F464AF513ECCA8C50DC224CD7205C1A91E5FDB85AE1CA09B78D94682B9BBDD3A651F0F3CCF8169348567F(2
Malicious:	false
Reputation:	low
Preview:	._.....,.....xH.....^.....q_..... .....J.....j.....b..... ....

C:\Users\user\AppData\Local\Temp\nsj9221.tmp\System.dll	
Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Shipment Invoice & Consignment Notification.exe, Detection: malicious, Browse • Filename: KY4cmAI0jU.exe, Detection: malicious, Browse • Filename: 5t2CmTUhKc.exe, Detection: malicious, Browse • Filename: 8qdfmqz1PN.exe, Detection: malicious, Browse • Filename: New Order PO2193570O1.doc, Detection: malicious, Browse • Filename: L2.xlsx, Detection: malicious, Browse • Filename: Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx, Detection: malicious, Browse • Filename: New Order PO2193570O1.pdf.exe, Detection: malicious, Browse • Filename: 2320900000000.exe, Detection: malicious, Browse • Filename: CshpH9OSkc.exe, Detection: malicious, Browse • Filename: 5SXTKXCnqS.exe, Detection: malicious, Browse • Filename: i6xFULh8J5.exe, Detection: malicious, Browse • Filename: AWB00028487364 -000487449287.doc, Detection: malicious, Browse • Filename: 090049000009000.exe, Detection: malicious, Browse • Filename: dYy3yfSkwY.exe, Detection: malicious, Browse • Filename: PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx, Detection: malicious, Browse • Filename: Purchase Order Price List 061021.xlsx, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: UGGJ4NnzFz.exe, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.92520264057843
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	INVOICE.exe
File size:	246224
MD5:	98901aff995d92677cf637b241ae9a9b
SHA1:	6dac1968c4a9ae4bf26f7fd38efb721fcf7d05dc
SHA256:	fb6e849cd3af7e8b0c8143397e62a595a42abbfbbac81f2cdd0b2cb4d18ea543
SHA512:	e969e941f176c67d1be598ac56882048fb2fc401e5a582b9f2314f09738d6b8768522ba5f67d8c80c260f1169ac103b8972084611a23ea9467c513f03ca9d883
SSDEEP:	6144:Ds9q5ND7xrAX/6ccjpGYZ/T12D2TLV47VVgLP3CATNTLzcocuk:ySD9rAXCccjN/T1TRXbtcuk
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40323c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4B1AE3C6 [Sat Dec 5 22:50:46 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a5a	0x5c00	False	0.660453464674	data	6.41769823686	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.4453125	data	5.18162709925	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x9000	0x1af98	0x400	False	0.55859375	data	4.70902740305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x9e0	0xa00	False	0.45625	data	4.51012867721	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/11/21-11:38:41.596097	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	104.21.29.70
06/11/21-11:38:41.596097	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	104.21.29.70
06/11/21-11:38:41.596097	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	104.21.29.70
06/11/21-11:39:01.004425	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49750	34.102.136.180	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 11:38:18.626332998 CEST	192.168.2.3	8.8.8.8	0x8b6	Standard query (0)	www.dollysusmitha.com	A (IP address)	IN (0x0001)
Jun 11, 2021 11:38:41.481421947 CEST	192.168.2.3	8.8.8.8	0xce40	Standard query (0)	www.cpf3life.com	A (IP address)	IN (0x0001)
Jun 11, 2021 11:39:00.753635883 CEST	192.168.2.3	8.8.8.8	0xf502	Standard query (0)	www.phonetomouth.com	A (IP address)	IN (0x0001)
Jun 11, 2021 11:39:23.180476904 CEST	192.168.2.3	8.8.8.8	0xaefa	Standard query (0)	www.gicc-fx.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 11:38:18.689140081 CEST	8.8.8.8	192.168.2.3	0x8b6	No error (0)	www.dollysusmitha.com	www.dollysusmitha.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 11:38:41.552371025 CEST	8.8.8.8	192.168.2.3	0xce40	No error (0)	www.cpf3life.com		104.21.29.70	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 11:38:41.552371025 CEST	8.8.8.8	192.168.2.3	0xce40	No error (0)	www.cpf3life.com		172.67.148.145	A (IP address)	IN (0x0001)
Jun 11, 2021 11:39:00.815494061 CEST	8.8.8.8	192.168.2.3	0xf502	No error (0)	www.phonetomouth.com	phonetomouth.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 11:39:00.815494061 CEST	8.8.8.8	192.168.2.3	0xf502	No error (0)	phonetomouth.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 11, 2021 11:39:23.242651939 CEST	8.8.8.8	192.168.2.3	0xaefa	No error (0)	www.gicc-fx.com		198.252.100.204	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.cpf3life.com
- www.phonetomouth.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49747	104.21.29.70	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 11:38:41.596096992 CEST	5863	OUT	GET /uer0/?cT=IWphFoHV4jp5oknFMSclxRoUR2WJRPQs/XYBCw5pT/o6GbblNl6C3qYdj4q6OTOtoDPc&0rjL0=00GhNj0PalVPThz HTTP/1.1 Host: www.cpf3life.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49750	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 11:39:00.861119986 CEST	5905	OUT	GET /uer0/?0rjL0=00GhNj0PalVPThz&cT=mzn46ufhhzCxwm8qeMWDu5BECFFcgbpMb+xr4Y5+z9rgY/t3xuFClMCjGCpTywHehpEI HTTP/1.1 Host: www.phonetomouth.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 11:39:01.004425049 CEST	5905	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 11 Jun 2021 09:39:00 GMT Content-Type: text/html Content-Length: 275 ETag: "60c03ab8-113" 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

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: INVOICE.exe PID: 6440 Parent PID: 5804

General

Start time:	11:37:03
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\INVOICE.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INVOICE.exe'
Imagebase:	0x400000
File size:	246224 bytes
MD5 hash:	98901AFF995D92677CF637B241AE9A9B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.204139591.0000000009990000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.204139591.0000000009990000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.204139591.0000000009990000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: INVOICE.exe PID: 6476 Parent PID: 6440

General

Start time:	11:37:04
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\INVOICE.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INVOICE.exe'
Imagebase:	0x400000
File size:	246224 bytes
MD5 hash:	98901AFF995D92677CF637B241AE9A9B
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: 00000001.00000001.201178753.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.201178753.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.201178753.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.275287960.00000000006F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.275287960.00000000006F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.275287960.00000000006F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.274983977.0000000000590000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.274983977.0000000000590000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.274983977.0000000000590000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.273615422.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.273615422.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.273615422.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3388 Parent PID: 6476

General

Start time:	11:37:08
Start date:	11/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
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: systray.exe PID: 2148 Parent PID: 6476

General

Start time:	11:37:39
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\systray.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\systray.exe
Imagebase:	0xc50000
File size:	9728 bytes
MD5 hash:	1373D481BE4C8A6E5F5030D2FB0A0C68
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: 00000008.00000002.461491283.0000000000A50000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.461491283.0000000000A50000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.461491283.0000000000A50000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.460557300.00000000005B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.460557300.00000000005B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.460557300.00000000005B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.461394658.0000000000A20000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.461394658.0000000000A20000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.461394658.0000000000A20000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2100 Parent PID: 2148

General

Start time:	11:37:41
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\INVOICE.exe'
Imagebase:	0x10b0000
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: 4968 Parent PID: 2100

General

Start time:	11:37:42
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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