JoeSandbox Cloud BASIC

ID: 528767
Sample Name: HSBC_SWIFT-20-11-2021.exe
Cookbook: default.jbs
Time: 18:47:51
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

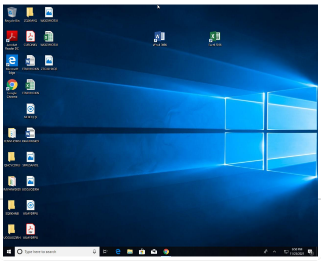
Table of Contents

Windows Analysis Report HSBC_SWIFT-20-11-2021.exe

Overview

General Information

Sample Name:	HSBC_SWIFT-20-11-2021.exe
Analysis ID:	528767
MD5:	3e9bddcd8ede94..
SHA1:	27723f2fb360a30..
SHA256:	4518c17e858eaa..
Tags:	exe Formbook HSBC
Infos:	
Most interesting Screenshot:	



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

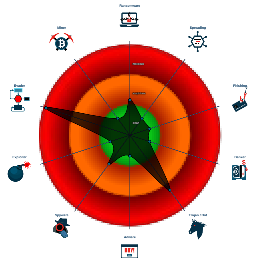
FormBook

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

Signatures

- Found malware configuration
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicious Add Tas…
- Self deletion via cmd delete
- .NET source code contains potentia…
- Sigma detected: Powershell Defende…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- HSBC_SWIFT-20-11-2021.exe (PID: 7156 cmdline: "C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe" MD5: 3E9BDDCD8EDE94BEB73D43D4D3446FE7)
  - powershell.exe (PID: 5828 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4708 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5576 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\RdffGefdbLSx.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4532 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4528 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\RdffGefdbLSx" /XML "C:\Users\user\AppData\Local\Temp\tmp4EB8.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - HSBC_SWIFT-20-11-2021.exe (PID: 6020 cmdline: C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe MD5: 3E9BDDCD8EDE94BEB73D43D4D3446FE7)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 1972 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 5868 cmdline: /c del "C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3184 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - explorer.exe (PID: 3120 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.164661.com/ntfs/"
  ],
  "decoy": [
    "cast-host.com",
    "sheenwoman.com",
    "cateringpairs.com",
    "butikgamis.com",
    "esd66.com",
    "beautystaze.com",
    "findavetnearme.com",
    "lyketigers.com",
    "nesboutiqe.com",
    "jadeutil.com",
    "survivalfresh.com",
    "realestatebramlett.com",
    "glorynap.com",
    "awards.institute",
    "huangtapps.com",
    "beyondwithyou.com",
    "cryptocustomerhelp.com",
    "plataformasoma.net",
    "lstpark.com",
    "noalareelecionindefinida.com",
    "supersconti.xyz",
    "emotors-invoice.com",
    "adamelsouk.com",
    "pellondo.com",
    "itstimewashington.com",
    "ss9n.xyz",
    "wecuxs.com",
    "wonderfulwithyou.com",
    "livetvnews24.com",
    "humanblessings.com",
    "soins-sophro.website",
    "pailuanshizhi.com",
    "balanzasdeplataformaperu.com",
    "wingboxonline.com",
    "importexportjessi.com",
    "revenberggmemergencyupgrade.com",
    "comicvan.com",
    "docomoaj.xyz",
    "accelerate6.com",
    "englishforbreakfast.com",
    "braapboxclub.com",
    "damana-vetements.com",
    "corinnewehby.com",
    "tonesify.com",
    "growversa.com",
    "cemetrasbeautyboutique.com",
    "newbalancecore.xyz",
    "cqguipu.com",
    "vdcasinolinkegit.club",
    "sednayachts.com",
    "alinatargetpro.com",
    "pawcomart.com",
    "aisle5.store",
    "dayinburgas.com",
    "c2batxpvme9ey3poams7369.com",
    "everythingby-b.com",
    "laliinparfumeri.com",
    "ntwapedi.com",
    "mrbubblesftlauderdale.com",
    "averiansmom.com",
    "ipelle.com",
    "waiting-game.com",
    "online-security.support",
    "hartfortlife.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.475690715.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.475690715.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.475690715.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000014.00000002.625088628.0000000003610000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000014.00000002.625088628.0000000003610000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.0.HSBC_SWIFT-20-11-2021.exe.400000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.0.HSBC_SWIFT-20-11-2021.exe.400000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
8.0.HSBC_SWIFT-20-11-2021.exe.400000.4.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cc9:$sqlite3step: 68 34 1C 7B E1 • 0x15ddc:$sqlite3step: 68 34 1C 7B E1 • 0x15cf8:$sqlite3text: 68 38 2A 90 C5 • 0x15e1d:$sqlite3text: 68 38 2A 90 C5 • 0x15d0b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e33:$sqlite3blob: 68 53 D8 7F 8C
8.0.HSBC_SWIFT-20-11-2021.exe.400000.6.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.0.HSBC_SWIFT-20-11-2021.exe.400000.6.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 17 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Possible Applocker Bypass

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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)

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected FormBook

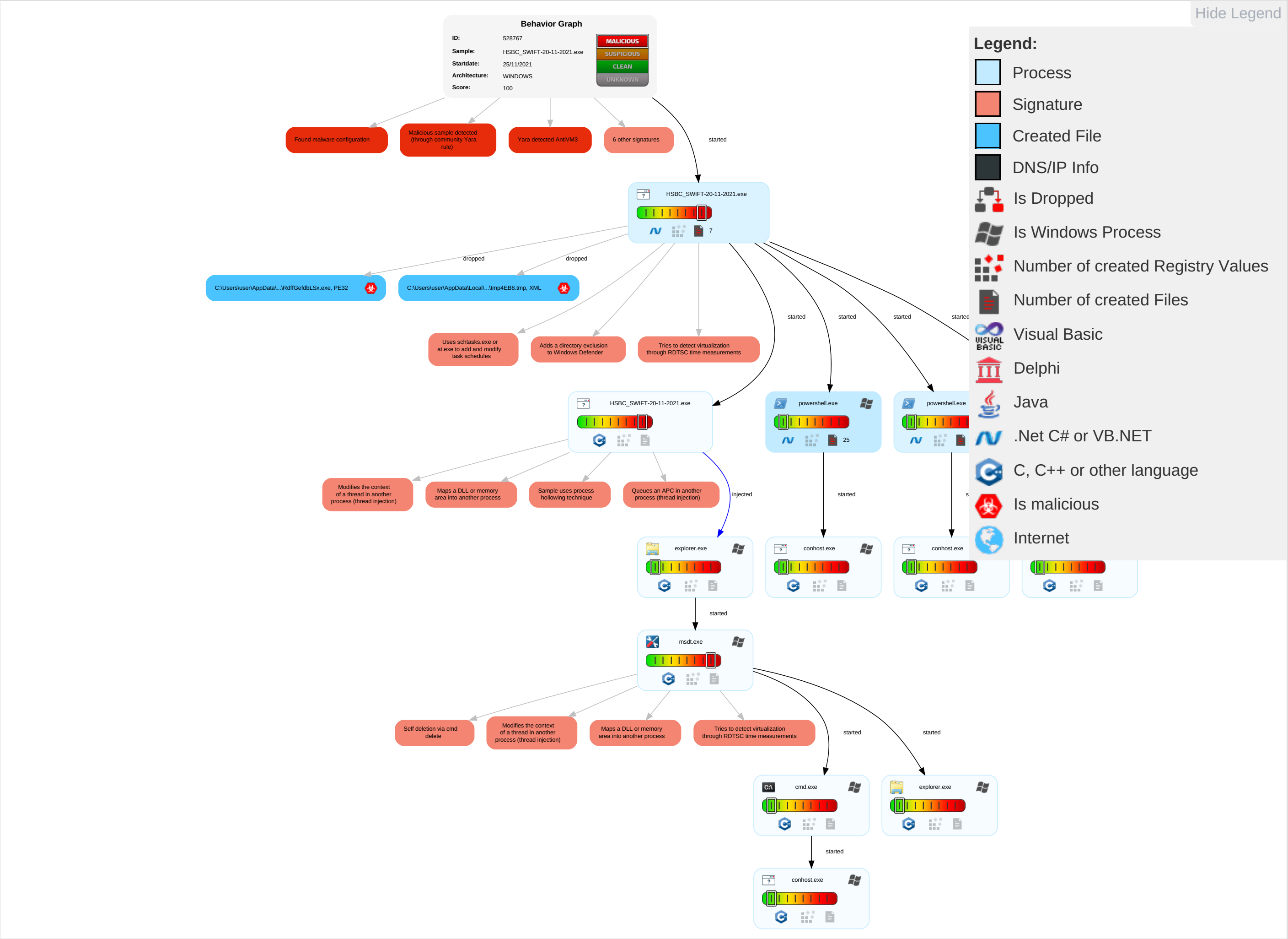
Remote Access Functionality:

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	Scheduled Task/Job 1	Process Injection 4 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 2 4 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS Redirect P Calls/SMS
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 4 1 2	NTDS	Virtualization/Sandbox Evasion 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi- Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

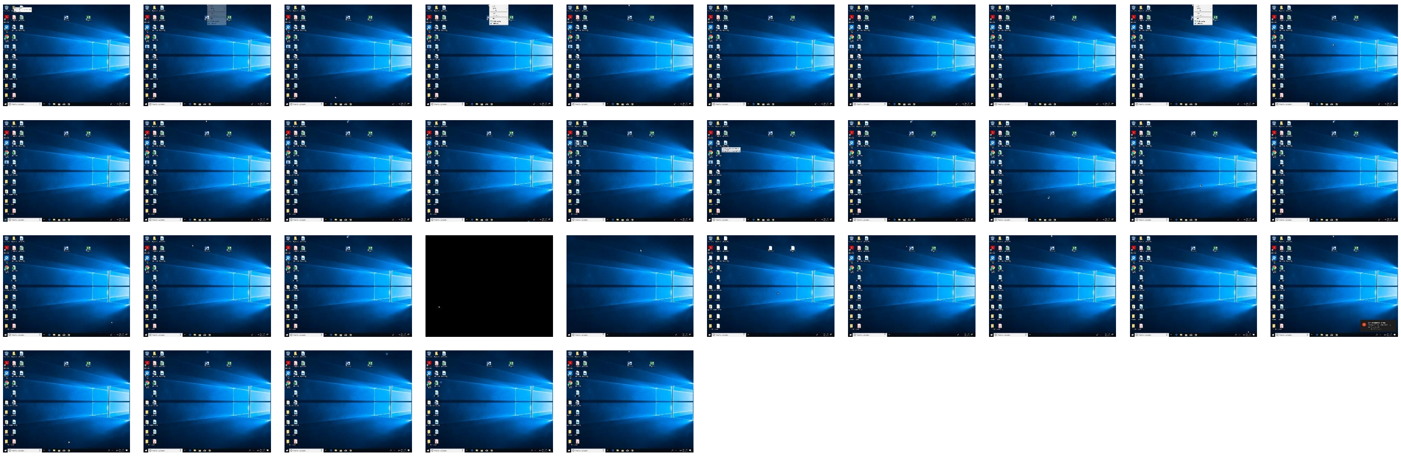
Behavior Graph


Hide Legend
Behavior Graph
ID: 528767
Sample: HSBC_SWIFT-20-11-2021.exe
Startdate: 25/11/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Malicious sample detected (through community Yara rule)
Yara detected AntiVM3
6 other signatures
started
HSBC_SWIFT-20-11-2021.exe
7
dropped
dropped
C:\Users\user\AppData\...\RdffGefdbLSx.exe, PE32
C:\Users\user\AppData\Local\...\tmp4EB8.tmp, XML
Uses schtasks.exe or at.exe to add and modify task schedules
Adds a directory exclusion to Windows Defender
Tries to detect virtualization through RDTSC time measurements
started
started
started
started
HSBC_SWIFT-20-11-2021.exe
powershell.exe
25
powershell.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
started
explorer.exe
conhost.exe
conhost.exe
started
msdt.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
started
cmd.exe
explorer.exe
started
conhost.exe
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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.HSBC_SWIFT-20-11-2021.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.HSBC_SWIFT-20-11-2021.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.HSBC_SWIFT-20-11-2021.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.HSBC_SWIFT-20-11-2021.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.164661.com/ntfs/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.164661.com/ntfs/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528767
Start date:	25.11.2021
Start time:	18:47:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HSBC_SWIFT-20-11-2021.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:	34
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@17/12@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20% (good quality ratio 18.2%) • Quality average: 73.8% • Quality standard deviation: 31%
HCA Information:	• Successful, ratio: 98% • 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
18:48:50	API Interceptor	80x Sleep call for process: HSBC_SWIFT-20-11-2021.exe modified
18:48:57	API Interceptor	72x Sleep call for process: powershell.exe modified
18:50:16	API Interceptor	140x Sleep call for process: explorer.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_SWIFT-20-11-2021.exe.log	
Process:	C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntIxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
Malicious:	false
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

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	modified
Size (bytes):	29232
Entropy (8bit):	1.7174925014010742

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db	
Encrypted:	false
SSDEEP:	96:4Xn/EwkcovPYCckGbZQYNAY+DcExux/H2ZPzgf:0kbvrc3N3LEy/z
MD5:	9CEA85F54A98B49F9713D46001D44B3F
SHA1:	655BFE94A738ADF4510A0F07DBB76AC343E09A22
SHA-256:	B365CE9FE495AF8D436049A93F34CA1A8363439C0D8EB45EB46921519A4A0458
SHA-512:	4E30DAC95FDC5601121BBD5A02E2DCA67852E36700E56A972EBDF14872AA41B0E23BFBB96198B7C2A04D5E2275509599EB57E148716C9C57F9101A58C50E532
Malicious:	false
Preview:	..0 IMMM ....z...........4... ................................QR...D... ....T..z.....Q. ....R..T.g.5 ....:..e.;6. ....j...b...;K..0... ....+${..a?0................o...

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22276
Entropy (8bit):	5.603205624926295
Encrypted:	false
SSDEEP:	384:utCDLj1Bi1EIUkl+RMSBKnwjultI+77Y9gtSJ3xeT1MaXZlbAV7EvDWhmRZBDI+W:n41E3k14KwClthftc8C+fwAvfVM
MD5:	8022AC6DB8E130F172B0B1DFD81A75BD
SHA1:	8A5CF5649B9ABDCB791D0E79EE914A25A41E458E
SHA-256:	697F49E4F30B68C3B95A7B87338203A034077667D314430DEDCF9A95B74BD80D
SHA-512:	22AFC211C14434E845E5CF81AB29583604A511C1BDE49866B37A1F57FC9DAE9A84A67397D846B2268F0FC6E9D88EEF5931FE4200F62BA72828B3E72ED2E981D
Malicious:	false
Preview:	@...e...........y.......h.\...........B...F..........@..........H...............<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD...............fZve...F.....x.)........System.Managemen t.Automation4...............[...{a.C..%6..h.........System.Core.0..............G-.o...A...4B..........System..4................Zg5..:O..g..q..........System.Xml..L..............7.....J@......~...... .#.Microsoft.Management.Infrastructure.8...............'....L..}...........System.Numerics.@...............Lo...QN......<Q........System.DirectoryServices<................H..QN.Y.f....... .....System.Management...4...................].D.E.....#.......System.Data.H................. ....H..m)aUu.........Microsoft.PowerShell.Security...<.................~.[L.D.Z.>..m.........Sy stem.Transactions.<................):gK..G...$.1.q........System.ConfigurationP................/.C..J..%...].......%.Microsoft.PowerShell.Commands.Utility...D.................-.D.F.<;.nt.1 ....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_04xvx3ge.imm.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_5azzze0s.akj.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_dpdt4pua.1fr.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_nt4teizv.av4.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp4EB8.tmp	
Process:	C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1611
Entropy (8bit):	5.116240184745884
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtLk+xvn:cgea6YrFdOFzOzN33ODOiDdKrsuTgyv
MD5:	774E84F6AC7E66BE600BBDC7957155AC
SHA1:	1A752B132A55F7BB5287A10AAE4F104E825845F3
SHA-256:	72AAD5A5B5425BA55BAB6210181C959F71F5D9B5C205A74398D369A3D2CF8BDB
SHA-512:	6F82A8DF85B62DA11D3E26DF1BE3AE49B9E4B41FFEA11C1D6229C47D62D3D9815289CCDC02643AD75446468F9BC1E4729A6AC6A21A94730FFE61CBC4208609 7
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailab

C:\Users\user\AppData\Roaming\RdffGefdbLSx.exe	
Process:	C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	438272
Entropy (8bit):	7.8432109795537235
Encrypted:	false
SSDEEP:	12288:lH41U0XdLgxmfz9aWuIazPy03IYwr3EQZpdoyWQHzKQMixBFm:lHYU0uEr9aWTyNBwjppd1WQTAi1
MD5:	3E9BDDCD8EDE94BEB73D43D4D3446FE7
SHA1:	27723F2FB360A300DF95C22FD1D8353A5D940455
SHA-256:	4518C17E858EAAE9A38CDF5953BD7D0CAD3C3FD5FA2B9A5B84E0CAD5E8ECFC5E

C:\Users\user\AppData\Roaming\RdffGefdbLSx.exe

SHA-512:	81FFD8D361C6809E41819F9074E7EE84E8E8ED4BD744D8C87270E26CA405BF613EA9C29247C71ED50E057B5F39BB05CBBACD78433A37426BA02EFA7063366D B
Malicious:	**true**
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L...5G.a.............0............j.... ....@.. ....@....................................O.. ....H...........text........ ....`.rsrc...............................@..@.reloc........ ......................@..B................L.......H........e..Xv.............................................................{ ...*..{!...*..{"...*..{#...*..($.....} .....}!.....}"......}#...*....0..s........u........f.,`(%....{ ....{ ...o&. ..,H('....{!....{!...o(...,0()....{"....{"...o*...,.(+....{#....{#...o,...+..+..*..0..b....... .@d)UU.Z(%....{ ...o-...X)UU.Z('....{!...o....X)UU.Z()....{"...o/...X)UU.Z(+....{#...o0...X*...0...........r... p......%..{ ......%q.........-.&.+.......o1....%..{!......%q.........-.&.+.....

C:\Users\user\AppData\Roaming\RdffGefdbLSx.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20211125\PowerShell_transcript.921702.IDbll8EJ.20211125184857.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5827
Entropy (8bit):	5.374058040185106
Encrypted:	false
SSDEEP:	96:BZhTLVNgtqDo1ZmZ1TLVNgtqDo1ZPT57jZgTLVNgtqDo1Z+KrrnZo:ubjl
MD5:	05DB53C96F655EBF6EF4CAE8E1DBEFC3
SHA1:	B72A74AE311C15631AB3AAB1E0234BE99589ACEB
SHA-256:	A56C0763BF6000D191FC20B20569FA5C41FCA4F18B22CC1BC5A6F70C7BA94965
SHA-512:	D271C3801CF15FC23B4756C2484F1D2AA692E7B82496A3FE5858F8DA58686E79F732C4E94AB6B9B042F9101C1D404D1A9B63F8557326FBDDFA84DA59382D7944
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20211125184859..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 921702 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\RdffGefdbLSx.exe..Process ID: 5576..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********************..**********************..Command start time: 20211125184859..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\RdffGefdbLSx.exe..**********************..Windows PowerShell transcript start..Start time: 20211125185229..Username: computer\user..RunAs User: D

C:\Users\user\Documents\20211125\PowerShell_transcript.921702.K2IUYCHw.20211125184856.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5831
Entropy (8bit):	5.396138733203896
Encrypted:	false
SSDEEP:	96:BZjTLVNGyqDo1ZCkZCTLVNGyqDo1ZmecWjZxTLVNGyqDo1ZDDGGuZB:X
MD5:	FE22AF4958E2ED64F3F431ECC096159B
SHA1:	A2FC81D82CBCC50F8917A6A7ED8AF55E881FF7C1
SHA-256:	32B36EC0073F167F8E8415BC0E858272709C6F3D9ACECF8E71E1EB6730A9CF1B
SHA-512:	6E52400245BD4F75AEA9E916E5937ACE0E70AA8C717AFED07EA7049A36394234704D20BCE7102389327F707153FE96A816BBE0A04BA3070032305A150DE1D7E4
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20211125184857..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 921702 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe..Process ID: 5828..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********************..**********************..Command start time: 20211125184857..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe..**********************..Windows PowerShell transcript start..Start time: 20211125185336..Username: computer\user..RunAs User:

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8432109795537235
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_SWIFT-20-11-2021.exe
File size:	438272
MD5:	3e9bddcd8ede94beb73d43d4d3446fe7
SHA1:	27723f2fb360a300df95c22fd1d8353a5d940455
SHA256:	4518c17e858eaae9a38cdf5953bd7d0cad3c3fd5fa2b9a5b84e0cad5e8ecfc5e
SHA512:	81ffd8d361c6809e41819f9074e7ee84e8e8ed4bd744d8c87270e26ca405bf613ea9c29247c71ed50e057b5f39bb05cbbacd78433a37426ba02efa7063366dab
SSDEEP:	12288:lH41U0XdLgxmfz9aWuIazPy03IYwr3EQZpdoyWQHzKQMixBFm:lHYU0uEr9aWTyNBwjppd1WQTAi1
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...5G.a.............0............j.... ....@.. ....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46c56a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619F4735 [Thu Nov 25 08:20:05 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	0x6a580	0x6a600	False	0.881970200499	data	7.85580215694	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6e000	0x5f4	0x600	False	0.440104166667	data	4.21799031052	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x70000	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

No network behavior found

Code Manipulations

Statistics

Behavior

💡 Click to jump to process

System Behavior

Analysis Process: HSBC_SWIFT-20-11-2021.exe PID: 7156 Parent PID: 6088

General

Start time:	18:48:48
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe"
Imagebase:	0xc00000
File size:	438272 bytes
MD5 hash:	3E9BDDCD8EDE94BEB73D43D4D3446FE7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.384226199.0000000002FC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.384803178.0000000003FCD000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.384803178.0000000003FCD000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.384803178.0000000003FCD000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.385092750.0000000004232000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.385092750.0000000004232000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.385092750.0000000004232000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.384521083.000000000314D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 5828 Parent PID: 7156

General

Start time:	18:48:54
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 4708 Parent PID: 5828

General

Start time:	18:48:55
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: powershell.exe PID: 5576 Parent PID: 7156

General

Start time:	18:48:55
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\RdffGefdbLSx.exe
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 4532 Parent PID: 5576

General

Start time:	18:48:56
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: schtasks.exe PID: 4528 Parent PID: 7156

General

Start time:	18:48:56
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\RdffGefdbLSx" /XML "C:\Users\user\AppData\Local\Temp\tmp4EB8.tmp
Imagebase:	0x9d0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6496 Parent PID: 4528

General

Start time:	18:48:59
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: HSBC_SWIFT-20-11-2021.exe PID: 6020 Parent PID: 7156

General

Start time:	18:49:01
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe
Imagebase:	0xea0000
File size:	438272 bytes
MD5 hash:	3E9BDDCD8EDE94BEB73D43D4D3446FE7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.475690715.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.475690715.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.475690715.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.380797387.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.380797387.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.380797387.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.476496897.00000000017D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.476496897.00000000017D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.476496897.00000000017D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.381918997.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.381918997.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.381918997.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.476370956.0000000001590000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.476370956.0000000001590000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.476370956.0000000001590000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 6020

General

Start time:	18:49:08
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
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: 0000000A.00000000.412407613.0000000007682000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.412407613.0000000007682000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.412407613.0000000007682000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.432842993.0000000007682000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.432842993.0000000007682000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.432842993.0000000007682000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: msdt.exe PID: 1972 Parent PID: 3440

General

Start time:	18:49:47
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xf60000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
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: 00000014.00000002.625088628.0000000003610000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.625088628.0000000003610000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.625088628.0000000003610000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.622812715.0000000000E30000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.622812715.0000000000E30000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.622812715.0000000000E30000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.624991985.00000000035E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.624991985.00000000035E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.624991985.00000000035E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

Analysis Process: cmd.exe PID: 5868 Parent PID: 1972

General

Start time:	18:49:52

Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\HSBC_SWIFT-20-11-2021.exe"
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3184 Parent PID: 5868

General

Start time:	18:49:53
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3120 Parent PID: 568

General

Start time:	18:50:15
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer.exe
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal