ID: 458843
Sample Name:
SWIFT_MT103.exe
Cookbook: default.jbs
Time: 19:41:37
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

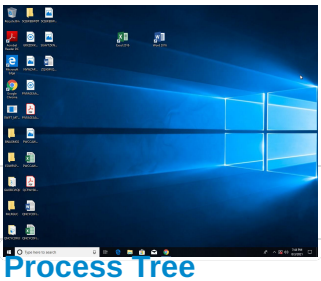
Windows Analysis Report SWIFT_MT103.exe

Overview

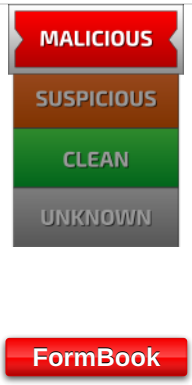
General Information

Sample Name:	SWIFT_MT103.exe
Analysis ID:	458843
MD5:	b54e7fb4262c31a.
SHA1:	060dbdd923a63f4.
SHA256:	6c282c90bf6e722..
Tags:	exe null
Infos:	

Most interesting Screenshot:



Detection



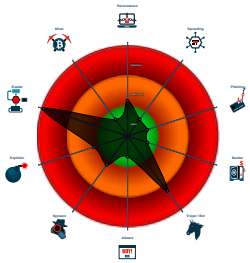
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- SWIFT_MT103.exe (PID: 720 cmdline: 'C:\Users\user\Desktop\SWIFT_MT103.exe' MD5: B54E7FB4262C31A414B6DBCB49A5D800)
  - RegSvcs.exe (PID: 6056 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
    - explorer.exe (PID: 3388 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - rundll32.exe (PID: 5040 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - cmd.exe (PID: 4960 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.bodymoisturizer.online/q4kr/"
  ],
  "decoy": [
    "realmodapk.com",
    "hanoharuka.com",
    "shivalikspiritualproducts.com",
    "womenshealthclinincagra.com",
    "racketpark.com",
    "startuporig.com",
    "azkachinas.com",
    "klanblog.com",
    "linuxradio.tools",
    "siteoficial-liquida.com",
    "glsbuyer.com",
    "bestdeez.com",
    "teens2cash.com",
    "valleyviewconstruct.com",
    "myfortniteskins.com",
    "cambecare.com",
    "csec2011.com",
    "idookap.com",
    "warmwallsrecords.com",
    "smartmirror.one",
    "alertreels.com",
    "oiop.online",
    "61cratoslot.com",
    "hispanicassoclv.com",
    "pennyforyourprep.com",
    "fayansistanbul.com",
    "superbartendergigs.club",
    "herr-nourimann.com",
    "oatkc.net",
    "romahony.com",
    "sportcrea.com",
    "crystalnieblas.com",
    "lcmet.com",
    "nwaymyatthu-mm.com",
    "edsufferen.club",
    "apispotlight.com",
    "shadowcatrecording.com",
    "capwisefin.com",
    "themesinsider.com",
    "kadrisells.com",
    "db-82.com",
    "rentyoursubmarine.com",
    "rin-ronshop.com",
    "donzfamilia.com",
    "loyalcollegeofart.com",
    "socialize.site",
    "shadesailstructure.com",
    "smcenterbiz.com",
    "zcdonghua.com",
    "1420radiolider.com",
    "ckenpo.com",
    "trucksitasa.com",
    "getthistle.com",
    "usvisanicaragua.com",
    "josiemaxwrites.com",
    "dehaagennutraceuticals.com",
    "noiaapp.com",
    "blinbins.com",
    "getreitive.com",
    "turmericbar.com",
    "manifestwealthrightnow.com",
    "garagekuhn.com",
    "longviewfinancialadvisor.com",
    "hallworthcapital.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.357804367.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.357804367.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000002.357804367.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.301061394.0000000003A29000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.301061394.0000000003A29000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x81bb8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x81f52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x147548:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1478e2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8dc65:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1535f5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x8d751:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1530e1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x8dd67:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1536f7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x8dedf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x15386f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8296a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1482fa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x8c9cc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x15235c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x836e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x149072:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x92d57:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1586e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x93dfa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
11.2.RegSvcs.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
11.2.RegSvcs.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158c9:$sqlite3step: 68 34 1C 7B E1 • 0x159dc:$sqlite3step: 68 34 1C 7B E1 • 0x158f8:$sqlite3text: 68 38 2A 90 C5 • 0x15a1d:$sqlite3text: 68 38 2A 90 C5 • 0x1590b:$sqlite3blob: 68 53 D8 7F 8C • 0x15a33:$sqlite3blob: 68 53 D8 7F 8C
11.2.RegSvcs.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
11.2.RegSvcs.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Suspicious Rundll32 Without Any CommandLine Params

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

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)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

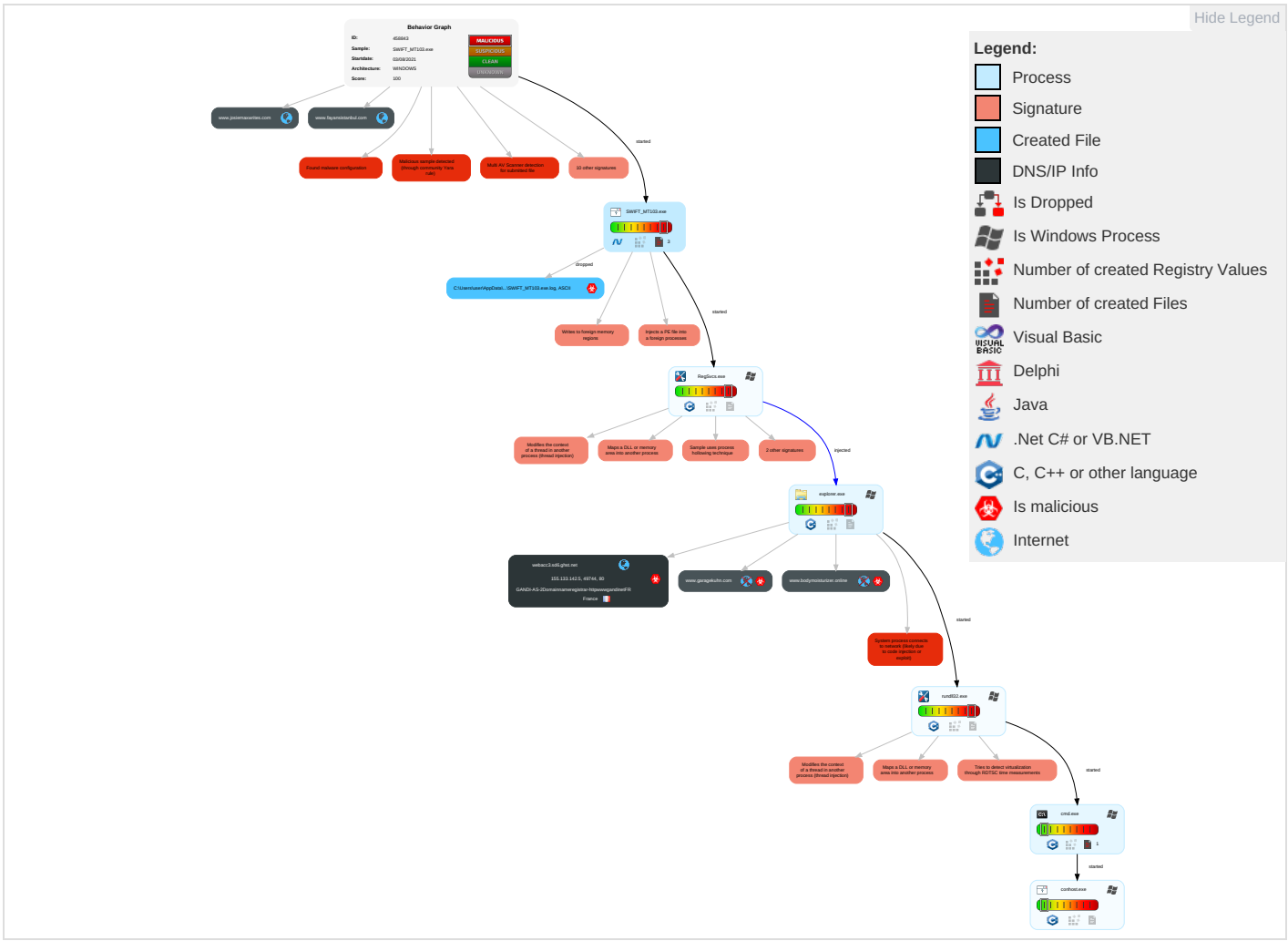
Remote Access Functionality:

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	Shared Modules 1	Path Interception	Process Injection 7 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop (Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 7 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

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
SWIFT_MT103.exe	37%	Metadefender		Browse
SWIFT_MT103.exe	79%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
SWIFT_MT103.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/D	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cno	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/_	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://www.fontbureau.comasv	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://https://www.fayansistanbul.com/q4kr/?4h_4=eOXhpEoLIa7YYnf6/8HRqFDyW	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/M	0%	URL Reputation	safe	
http://www.fontbureau.comR.TTFr	0%	Avira URL Cloud	safe	
http://www.fontbureau.comV	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/r	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/D	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.fontbureau.comi	0%	Avira URL Cloud	safe	
www.bodymoisturizer.online/q4kr/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/o4	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/h	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/vnoi	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/_	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.josiemaxwrites.com	199.34.228.67	true	false		unknown
webacc3.sd6.ghst.net	155.133.142.5	true	true		unknown
www.fayansistanbul.com	172.67.130.233	true	false		unknown
www.bodymoisturizer.online	unknown	unknown	true		unknown
www.garagekuhn.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation

Name	Malicious	Antivirus Detection	Reputation
www.bodymoisturizer.online/q4kr/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
155.133.142.5	webacc3.sd6.ghst.net	France		203476	GANDI-AS-2Domainnameregistrar-httpwwwgandinetFR	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458843
Start date:	03.08.2021
Start time:	19:41:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SWIFT_MT103.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@4/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 59.9% (good quality ratio 54.3%) • Quality average: 72.6% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
155.133.142.5	Payment_Advice000987.exe	Get hash	malicious	Browse	• www.garagekuhn.com/q4kr/?zJEPD=4hMXovbxmz&-ZalKtr=CWCBar0ajh7IOPyGoiQ+OSxuK1fv7pOEcpev3lNBz5ExpQMJFIwPX0r3WtdZztc5D/uY
	PI.exe	Get hash	malicious	Browse	• www.garagekuhn.com/q4kr/?p6A=CWCBar0ajh7IOPyGoiQ+OSxuK1fv7pOEcpev3lNBz5ExpQMJFIwPX0r3WtdZztc5D/uY&UDK0fp=0FQt7
	Payment_Advice.exe	Get hash	malicious	Browse	• www.garagekuhn.com/q4kr/?QtRl=CWCBar0ajh7IOPyGoiQ+OSxuK1fv7pOEcpev3lNBz5ExpQMJFIwPX0r3WtdZztc5D/uY&w2MLb=6lux

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
webacc3.sd6.ghst.net	Payment_Advice000987.exe	Get hash	malicious	Browse	• 155.133.142.5
	PI.exe	Get hash	malicious	Browse	• 155.133.142.5
	payment_copy.exe	Get hash	malicious	Browse	• 155.133.142.5
	000987654345XASD.exe	Get hash	malicious	Browse	• 155.133.142.5
	Payment_Advice.exe	Get hash	malicious	Browse	• 155.133.142.5
www.fayansistanbul.com	Payment_Advice.exe	Get hash	malicious	Browse	• 104.21.3.157
	PI_OIUYT0987654456.exe	Get hash	malicious	Browse	• 172.67.130.233
www.josiemaxwrites.com	MX-M502N_201145.exe	Get hash	malicious	Browse	• 199.34.228.67
	PI_OIUYT0987654456.exe	Get hash	malicious	Browse	• 199.34.228.67
	000987654345XASD.exe	Get hash	malicious	Browse	• 199.34.228.67

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GANDI-AS-2Domainnameregistrar-httpwwwgandinetFR	Payment_Advice000987.exe	Get hash	malicious	Browse	• 155.133.142.5
	GYrZTFjj6s.exe	Get hash	malicious	Browse	• 155.133.130.88
	ZU3hkQYpMr.exe	Get hash	malicious	Browse	• 155.133.130.88
	5DmHH1SVTr.exe	Get hash	malicious	Browse	• 155.133.130.88
	PI.exe	Get hash	malicious	Browse	• 155.133.142.5
	fS5DVkL6jm.exe	Get hash	malicious	Browse	• 155.133.138.10
	VSP-88D-Neo1-F YX20210315086 KSAI21061536.xlsx	Get hash	malicious	Browse	• 155.133.138.10
	a8eC6O6okf.exe	Get hash	malicious	Browse	• 155.133.138.10
	Payment_Advice.exe	Get hash	malicious	Browse	• 155.133.142.5
	$RAULIU9.exe	Get hash	malicious	Browse	• 155.133.142.13
	h8lD4SWL35.exe	Get hash	malicious	Browse	• 155.133.132.7
	iWlLtgXNf8.xls	Get hash	malicious	Browse	• 155.133.132.7
	iWlLtgXNf8.xls	Get hash	malicious	Browse	• 155.133.132.7

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	iWlLtgXNf8.xls	Get hash	malicious	Browse	• 155.133.132.7
	BL_SHIPMENT CI509808730.exe	Get hash	malicious	Browse	• 155.133.138.3
	tS9P6wPz9x.exe	Get hash	malicious	Browse	• 155.133.142.13
	ransomware.exe	Get hash	malicious	Browse	• 155.133.142.13
	ransomware.exe	Get hash	malicious	Browse	• 155.133.142.13
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 155.133.142.13
	6VEoBuy32f.xls	Get hash	malicious	Browse	• 155.133.132.7

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SWIFT_MT103.exe.log

Process:	C:\Users\user\Desktop\SWIFT_MT103.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.823048609176136
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	SWIFT_MT103.exe
File size:	735744
MD5:	b54e7fb4262c31a414b6dbcb49a5d800
SHA1:	060dbdd923a63f4c782afe0d252bbc2e2585d255
SHA256:	6c282c90bf6e72212f3c2038601a503d9e9e36bb417687fc8b16362fe854fa3d

General

SHA512:	efe8474e2a54f76634c812a87a64c664da9e5c1fe1f6d08a95176ef7dd0d8cdd3f1e9ed49cea07885b2ebda0edcdf7e6cc494dbae109d9e5bd6fb408e0698bbf
SSDEEP:	12288:VqnBrep+gczyhNSvRbBQHR4qz91hI0zSaNsvz+yuWDVId21NaI+E8tyvXkXRbWHu:VqlYX8Y9KpuYu4mTFORYwcX/b
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..0.....O... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b4f92
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:	0x9CA2CF99 [Thu Apr 10 16:34:33 2053 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	0xb2fb8	0xb3000	False	0.902687456355	data	7.83042762199	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x5c4	0x600	False	0.42578125	data	4.13458372963	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb8000	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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 19:44:15.753284931 CEST	192.168.2.3	8.8.8.8	0x484	Standard query (0)	www.garagekuhn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:44:26.308141947 CEST	192.168.2.3	8.8.8.8	0xb6d9	Standard query (0)	www.bodymoisturizer.online	A (IP address)	IN (0x0001)
Aug 3, 2021 19:44:31.371221066 CEST	192.168.2.3	8.8.8.8	0x25ee	Standard query (0)	www.fayansistanbul.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:44:36.466392994 CEST	192.168.2.3	8.8.8.8	0x4620	Standard query (0)	www.josiemaxwrites.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 19:44:15.898096085 CEST	8.8.8.8	192.168.2.3	0x484	No error (0)	www.garagekuhn.com	webacc3.sd6.ghst.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:44:15.898096085 CEST	8.8.8.8	192.168.2.3	0x484	No error (0)	webacc3.sd6.ghst.net		155.133.142.5	A (IP address)	IN (0x0001)
Aug 3, 2021 19:44:26.348918915 CEST	8.8.8.8	192.168.2.3	0xb6d9	Name error (3)	www.bodymoisturizer.online	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 19:44:31.408288956 CEST	8.8.8.8	192.168.2.3	0x25ee	No error (0)	www.fayansistanbul.com		172.67.130.233	A (IP address)	IN (0x0001)
Aug 3, 2021 19:44:31.408288956 CEST	8.8.8.8	192.168.2.3	0x25ee	No error (0)	www.fayansistanbul.com		104.21.3.157	A (IP address)	IN (0x0001)
Aug 3, 2021 19:44:36.622869968 CEST	8.8.8.8	192.168.2.3	0x4620	No error (0)	www.josiemaxwrites.com		199.34.228.67	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.garagekuhn.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49744	155.133.142.5	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:44:15.948903084 CEST	6542	OUT	GET /q4kr/?h6=Vpi8s2sp00E&4h_4=CWCBar0ajh7IOPyGoiQ+OSxuK1fv7pOEcpev3lNBz5ExpQMJFlwPX0r3WtdZztc5D/uY HTTP/1.1 Host: www.garagekuhn.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 19:44:15.985829115 CEST	6542	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 03 Aug 2021 17:44:15 GMT Server: Varnish Location: https://www.garagekuhn.com/q4kr/?h6=Vpi8s2sp00E&4h_4=CWCBar0ajh7IOPyGoiQ+OSxuK1fv7pOEcpev3lNBz5ExpQMJFlwPX0r3WtdZztc5D/uY Content-Length: 0 Connection: close

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SWIFT_MT103.exe PID: 720 Parent PID: 5676

General

Start time:	19:42:26
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\SWIFT_MT103.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SWIFT_MT103.exe'
Imagebase:	0x690000
File size:	735744 bytes
MD5 hash:	B54E7FB4262C31A414B6DBCB49A5D800
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: 00000000.00000002.301061394.0000000003A29000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.301061394.0000000003A29000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.301061394.0000000003A29000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 6056 Parent PID: 720

General

Start time:	19:43:08
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb70000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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.00000002.357804367.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.357804367.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.357804367.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.358391118.0000000001100000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.358391118.0000000001100000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.358391118.0000000001100000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.358413416.0000000001130000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.358413416.0000000001130000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.358413416.0000000001130000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3388 Parent PID: 6056

General

Start time:	19:43:10
Start date:	03/08/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5040 Parent PID: 3388

General

Start time:	19:43:37
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0x180000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.465035906.0000000000250000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.465035906.0000000000250000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.465035906.0000000000250000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.467645501.0000000004190000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.467645501.0000000004190000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.467645501.0000000004190000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.467412388.00000000029C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.467412388.00000000029C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.467412388.00000000029C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 4960 Parent PID: 5040

General

Start time:	19:43:42
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5428 Parent PID: 4960

General

Start time:	19:43:42
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis