ID: 385257
Sample Name: SWIFT Payment Advise 39 430-25.exe
Cookbook: default.jbs
Time: 09:05:53
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report SWIFT Payment Advise 39 430-25.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 4
Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
HIPS / PFW / Operating System Protection Evasion: 5
Stealing of Sensitive Information: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted IPs 9
Public 9
General Information 9
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 13
Data Directories 14
Sections 14
Resources 14
Imports 14

Version Infos 15
Network Behavior 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 17
DNS Queries 18
DNS Answers 18
HTTPS Packets 18
Code Manipulations 19
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: SWIFT Payment Advise 39 430-25.exe PID: 5960 Parent PID: 5704 19
General 19
Registry Activities 20
Key Created 20
Key Value Created 20
Analysis Process: ieinstal.exe PID: 6896 Parent PID: 5960 20
General 20
File Activities 20
File Created 20
File Deleted 21
File Written 21
File Read 21
Disassembly 21
Code Analysis 21

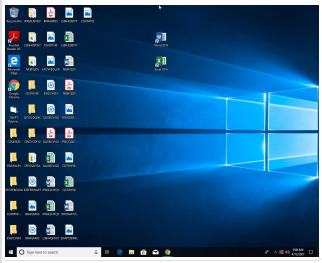
Analysis Report SWIFT Payment Advise 39 430-25.exe

Overview

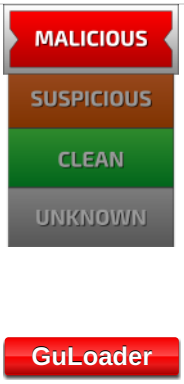
General Information

Sample Name:	SWIFT Payment Advise 39 430-25.exe
Analysis ID:	385257
MD5:	758028b3f6c4288.
SHA1:	f23458e2f4b1ec7..
SHA256:	7e2f0e6ba024408.
Tags:	GuLoader
Infos:	

Most interesting Screenshot:



Detection



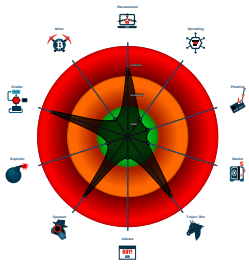
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Executable has a suspicious name (…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- SWIFT Payment Advise 39 430-25.exe (PID: 5960 cmdline: 'C:\Users\user\Desktop\SWIFT Payment Advise 39 430-25.exe' MD5: 758028B3F6C428890BF423F4BF61493F)
  - ieinstal.exe (PID: 6896 cmdline: 'C:\Users\user\Desktop\SWIFT Payment Advise 39 430-25.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1dZX_cFlErs_ZNtLRip3fHBXb5WHo03u0"
}
```

Yara Overview

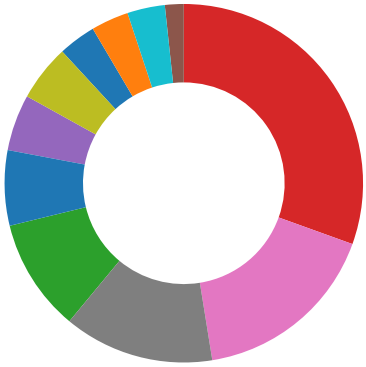
Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.497022856.000000000323 2000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: SWIFT Payment Advise 39 430-25.exe PID: 5960	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: ieinstal.exe PID: 6896	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

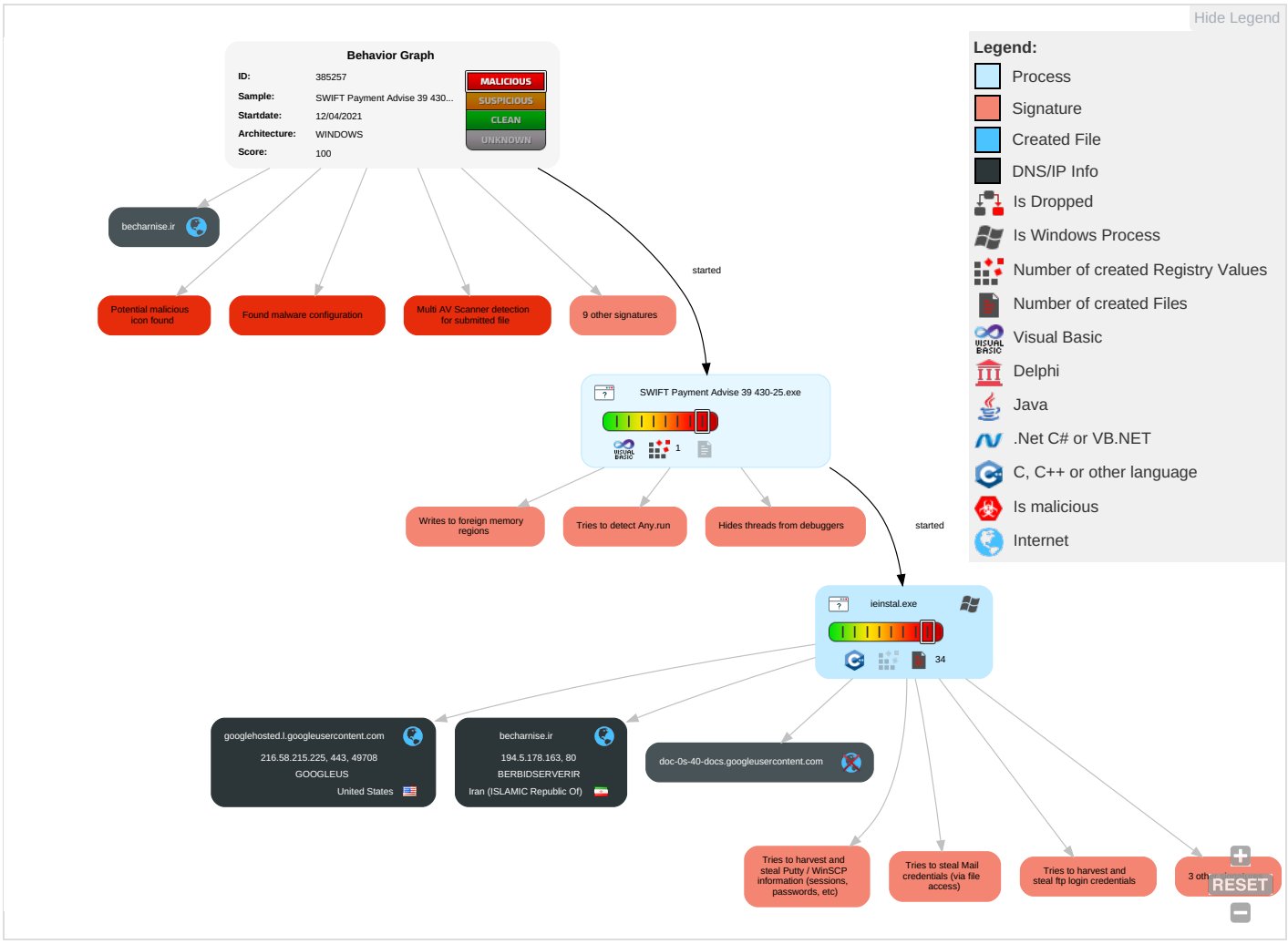
Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 6 2 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesd Insecur Networl Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 3	Credentials in Registry 1	Virtualization/Sandbox Evasion 2 3	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 2 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service

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 Payment Advise 39 430-25.exe	27%	ReversingLabs	Win32.Trojan.Graftor	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
becharnise.ir	194.5.178.163	true	false		unknown
googlehosted.l.googleusercontent.com	216.58.215.225	true	false		high
doc-0s-40-docs.googleusercontent.com	unknown	unknown	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.215.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
194.5.178.163	becharnise.ir	Iran (ISLAMIC Republic Of)		200406	BERBIDSERVERIR	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385257
Start date:	12.04.2021
Start time:	09:05:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SWIFT Payment Advise 39 430-25.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:	22

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.rans.troj.spyw.evad.winEXE@3/2@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.7% (good quality ratio 3.4%) • Quality average: 50.8% • Quality standard deviation: 17.3%
HCA Information:	• Successful, ratio: 69% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 92.122.145.220, 184.30.24.56, 13.88.21.125, 13.64.90.137, 8.241.121.254, 8.253.204.120, 67.27.158.126, 8.248.131.254, 8.253.207.120, 216.58.215.238, 20.82.210.154, 104.43.139.144, 168.61.161.212, 92.122.213.194, 92.122.213.247, 20.50.102.62, 104.43.193.48, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, drive.google.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/385257/sample/SWIFT Payment Advise 39 430-25.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.178.163	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• becharnise.ir/fb19/fre.php
	Required.exe	Get hash	malicious	Browse	• fleximexi.ir/ari/Panel/fre.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
becharnise.ir	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 194.5.178.163
	SMYXumaA91.exe	Get hash	malicious	Browse	• 195.211.44.113
	4xxwII41mG.exe	Get hash	malicious	Browse	• 195.211.44.113
	SPARE PARTS drawing.xlsx	Get hash	malicious	Browse	• 195.211.44.113
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 195.211.44.113
	SOA#0850.exe	Get hash	malicious	Browse	• 194.147.142.237
	RfqHongJ.exe	Get hash	malicious	Browse	• 194.147.142.237
	Remittance slip.exe	Get hash	malicious	Browse	• 194.147.142.237
	_ShipDoc_CI_PL_HBL_.xlsx	Get hash	malicious	Browse	• 194.147.142.237
	r2HXquFlQa.exe	Get hash	malicious	Browse	• 194.147.142.237
	NyBozyKqtT.exe	Get hash	malicious	Browse	• 194.147.142.237
	WdJ1OsBhHk.exe	Get hash	malicious	Browse	• 194.147.142.237
	FTdoFIURU7.exe	Get hash	malicious	Browse	• 194.147.142.237
	VSLS PARTICULARS.xlsx	Get hash	malicious	Browse	• 194.147.142.237
	VSL_MT LOYALTY_pdf.exe	Get hash	malicious	Browse	• 194.147.142.237
	SecuriteInfo.com.W32.AIDetect.malware2.3511.exe	Get hash	malicious	Browse	• 194.147.142.237
	aH3bqPMEP2.exe	Get hash	malicious	Browse	• 185.208.180.121
	SecuriteInfo.com.W32.AIDetect.malware1.6066.exe	Get hash	malicious	Browse	• 185.208.180.121
	INV 0898764_pdf.exe	Get hash	malicious	Browse	• 185.208.180.121
	VSL_MT LOYALTY.xlsx	Get hash	malicious	Browse	• 185.208.180.121

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BERBIDSERVERIR	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 194.5.178.163
	Required.exe	Get hash	malicious	Browse	• 194.5.178.163

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	malevolo.ps1	Get hash	malicious	Browse	• 216.58.215.225
	shipping document.exe	Get hash	malicious	Browse	• 216.58.215.225
	Statement-ID261179932209970.vbs	Get hash	malicious	Browse	• 216.58.215.225
	Alexandra38.docx	Get hash	malicious	Browse	• 216.58.215.225
	rRobw1VVRP.exe	Get hash	malicious	Browse	• 216.58.215.225
	Tmd7W7qwQw.dll	Get hash	malicious	Browse	• 216.58.215.225
	SecuriteInfo.com.Trojan.Agent.FFIJ.17175.exe	Get hash	malicious	Browse	• 216.58.215.225
	documents-351331057.xlsm	Get hash	malicious	Browse	• 216.58.215.225
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 216.58.215.225
	mail_6512365134_7863_202104108.html	Get hash	malicious	Browse	• 216.58.215.225
	Copia bancaria de swift.exe	Get hash	malicious	Browse	• 216.58.215.225
	SecuriteInfo.com.Trojan.GenericKD.36659493.29456.exe	Get hash	malicious	Browse	• 216.58.215.225
	SecuriteInfo.com.Trojan.Siggen12.64197.30705.exe	Get hash	malicious	Browse	• 216.58.215.225
	#Ud83d#Udcde973.htm	Get hash	malicious	Browse	• 216.58.215.225
	3vQD6TIYA1.exe	Get hash	malicious	Browse	• 216.58.215.225
	SOLICITUD DE PRESUPUESTO 08-04-2021#U00b7pdf.exe	Get hash	malicious	Browse	• 216.58.215.225
	XN123gfQJQ.exe	Get hash	malicious	Browse	• 216.58.215.225
	documento.xlsb	Get hash	malicious	Browse	• 216.58.215.225
	securedmessage.htm	Get hash	malicious	Browse	• 216.58.215.225

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.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\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\eb42b1a5c308fc11edf1ddbdd25c8486_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	data
Category:	dropped
Size (bytes):	450
Entropy (8bit):	0.95853443959644
Encrypted:	false
SSDEEP:	3:/lvlLFlvlLFlvlLFlvlLFlvlp:LVVV3
MD5:	4C69543CC021AEC1EFB640FDF5DD2F16
SHA1:	347AA81846DD5797E1A6A85D9B1CAF9E3BF36EFF
SHA-256:	91B97E7BCC50DDC0792D5CEF438D56895955F29D5121994CE0A43E78D23CBD7E
SHA-512:	09627F4C8875300AD045B011B66A91D374581A65DEAA75FE1F95C2322BE747EE17893C5F27433B52BD7CE90412D0C08C5980F6BEB2907027F2142BFDAAABCB3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\eb42b1a5c308fc11edf1ddbdd25c8486_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Preview:	.....user.....user.....user..... .....user.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.224475355355028
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SWIFT Payment Advise 39 430-25.exe
File size:	90112
MD5:	758028b3f6c428890bf423f4bf61493f
SHA1:	f23458e2f4b1ec7b1b626892878fbc8a81bcc8d6
SHA256:	7e2f0e6ba024408d3b889101de8ab48b3592b465e7a33c95c4fbcb5a4c912fb7
SHA512:	edec88afa520fcf43119a293810b1e2eaf2ff6c8d4c860c2d2862686d8b3bafff5e76bfd5b733b60f98532209caeaa3d324cc04078959f646239cb0e3120280d
SSDEEP:	768:+M3sZY/kPxOwOJu9LydptAQe9Pjm1j+BDMlf4tgTQx5dauPDJO1SiSjwvJ:BsZY/kZOwhtydtehuj+BOfs5Od
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6...W...W...W...K...W...u...W...q...W..Rich.W.....PE..L...&..P.....0...`.....`.....@....@

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401460
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x50F6E326 [Wed Jan 16 17:28:06 2013 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	281390d21b787569ccc2303fd6dad5ce

Entrypoint Preview

Instruction
push 00401650h

Instruction
call 00007F8C549F1C73h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add al, dl
mov ah, ch
pop ds
sbb ebx, dword ptr [ebx]
mov edi, 8BCA814Ch

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x13474	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x19000	0x9d4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x238	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x118	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x12948	0x13000	False	0.413522820724	data	5.69403723922	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x14000	0x45d8	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x19000	0x9d4	0x1000	False	0.178466796875	data	2.13575147568	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x198a4	0x130	data		
RT_ICON	0x195bc	0x2e8	data		
RT_ICON	0x19494	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x19464	0x30	data		
RT_VERSION	0x19150	0x314	data		

Imports

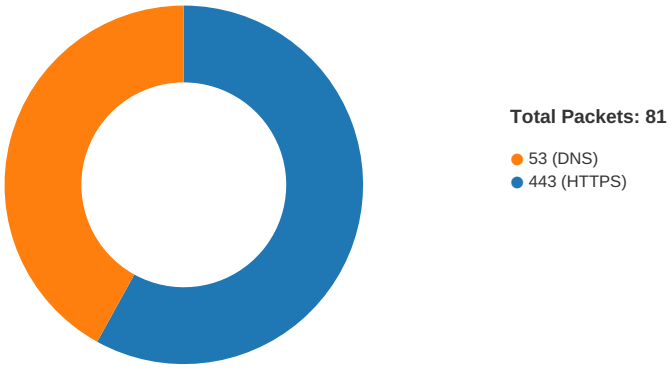
DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaAryMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaVarForInit, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarDup, __vbaStrToAnsi, __vbaFpI4, _CIatan, __vbaCastObj, __vbaStrMove, _allmul, _CItan, __vbaVarForNext, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Freak Class
InternalName	Plateaued1
FileVersion	1.00
CompanyName	Freak Class
LegalTrademarks	Freak Class
Comments	Freak Class
ProductName	Freak Class
ProductVersion	1.00
FileDescription	Freak Class
OriginalFilename	Plateaued1.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:07:48.598371983 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:48.643932104 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:48.644054890 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:48.645006895 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:48.690490007 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:48.703102112 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:48.703159094 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:48.703186989 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:48.703210115 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:48.703232050 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:48.703274012 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:48.717717886 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:48.763536930 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:48.763689995 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:48.764540911 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:48.814651966 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.009479046 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.009500027 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.009517908 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.009535074 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.009551048 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.009659052 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.009728909 CEST	49708	443	192.168.2.7	216.58.215.225

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:07:49.012581110 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.012599945 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.012690067 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.012713909 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.015794992 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.015815973 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.015875101 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.015896082 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.018996954 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.019026995 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.019085884 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.019109011 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.022227049 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.022248030 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.022308111 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.022341967 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.024789095 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.024808884 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.024858952 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.024892092 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.055063009 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.055089951 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.055161953 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.056919098 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.056942940 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.056982040 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.057019949 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.060045958 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.060075045 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.060106993 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.060146093 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.063033104 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.063064098 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.063123941 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.063155890 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.066437960 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.066462994 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.066499949 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.066641092 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.069379091 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.069436073 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.069468021 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.069503069 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.072921991 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.072949886 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.072988033 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.073013067 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.075773954 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.075797081 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.075867891 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.075896978 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.078938007 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.078963995 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.079004049 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.079030991 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.082005978 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.082027912 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.082108974 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.085016966 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.085052013 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.085094929 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.085115910 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.087999105 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.088020086 CEST	443	49708	216.58.215.225	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:07:49.088079929 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.088099957 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.090986013 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.091017962 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.091087103 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.091118097 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.094185114 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.094208956 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.094254971 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.094276905 CEST	49708	443	192.168.2.7	216.58.215.225
Apr 12, 2021 09:07:49.097011089 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.097044945 CEST	443	49708	216.58.215.225	192.168.2.7
Apr 12, 2021 09:07:49.097079039 CEST	49708	443	192.168.2.7	216.58.215.225

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:06:36.242970943 CEST	61242	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:06:36.291995049 CEST	53	61242	8.8.8.8	192.168.2.7
Apr 12, 2021 09:06:38.411036968 CEST	58562	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:06:38.469515085 CEST	53	58562	8.8.8.8	192.168.2.7
Apr 12, 2021 09:07:01.964020967 CEST	56590	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:07:02.029580116 CEST	53	56590	8.8.8.8	192.168.2.7
Apr 12, 2021 09:07:07.087543011 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:07:07.136581898 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 12, 2021 09:07:12.467433929 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:07:12.518182993 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 12, 2021 09:07:29.937313080 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:07:29.988806009 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 12, 2021 09:07:31.541711092 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:07:31.590414047 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 12, 2021 09:07:47.708326101 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:07:47.773395061 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 12, 2021 09:07:48.300764084 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:07:48.349626064 CEST	53	54640	8.8.8.8	192.168.2.7
Apr 12, 2021 09:07:48.514470100 CEST	58739	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:07:48.592413902 CEST	53	58739	8.8.8.8	192.168.2.7
Apr 12, 2021 09:07:50.652332067 CEST	60338	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:07:50.994090080 CEST	53	60338	8.8.8.8	192.168.2.7
Apr 12, 2021 09:07:53.984365940 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:07:54.035808086 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 12, 2021 09:07:55.852821112 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:07:55.901554108 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 12, 2021 09:07:56.777328968 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:07:56.826278925 CEST	53	54329	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:01.756891966 CEST	58052	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:01.815680027 CEST	53	58052	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:07.905358076 CEST	54008	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:07.954016924 CEST	53	54008	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:12.613359928 CEST	59451	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:12.672434092 CEST	53	59451	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:21.194430113 CEST	52914	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:21.245867968 CEST	53	52914	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:34.574978113 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:34.635107994 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:35.324676037 CEST	52816	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:35.373492002 CEST	53	52816	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:40.045149088 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:40.113033056 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:40.921453953 CEST	54230	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:40.970021009 CEST	53	54230	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:45.084790945 CEST	54911	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:45.133462906 CEST	53	54911	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:46.929852962 CEST	49958	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:08:46.982414007 CEST	53	49958	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:48.553877115 CEST	50860	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:48.602652073 CEST	53	50860	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:50.361248970 CEST	50452	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:50.418330908 CEST	53	50452	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:52.272304058 CEST	59730	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:52.362983942 CEST	53	59730	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:52.822804928 CEST	59310	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:52.885870934 CEST	53	59310	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:53.434803009 CEST	51919	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:53.495085955 CEST	53	51919	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:54.140201092 CEST	64296	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:54.250591040 CEST	53	64296	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:54.717360973 CEST	56680	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:54.779048920 CEST	53	56680	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:55.310853004 CEST	58820	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:55.369240046 CEST	53	58820	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:55.726608992 CEST	60983	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:55.789849043 CEST	53	60983	8.8.8.8	192.168.2.7
Apr 12, 2021 09:08:55.855614901 CEST	49247	53	192.168.2.7	8.8.8.8
Apr 12, 2021 09:08:55.912578106 CEST	53	49247	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 09:07:48.514470100 CEST	192.168.2.7	8.8.8.8	0x5053	Standard query (0)	doc-0s-40-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:07:50.652332067 CEST	192.168.2.7	8.8.8.8	0x39ce	Standard query (0)	becharnise.ir	A (IP address)	IN (0x0001)
Apr 12, 2021 09:08:12.613359928 CEST	192.168.2.7	8.8.8.8	0x4347	Standard query (0)	becharnise.ir	A (IP address)	IN (0x0001)
Apr 12, 2021 09:08:34.574978113 CEST	192.168.2.7	8.8.8.8	0xe771	Standard query (0)	becharnise.ir	A (IP address)	IN (0x0001)
Apr 12, 2021 09:08:55.726608992 CEST	192.168.2.7	8.8.8.8	0x5a76	Standard query (0)	becharnise.ir	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 09:07:48.592413902 CEST	8.8.8.8	192.168.2.7	0x5053	No error (0)	doc-0s-40-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:07:48.592413902 CEST	8.8.8.8	192.168.2.7	0x5053	No error (0)	googlehosted.l.googleusercontent.com		216.58.215.225	A (IP address)	IN (0x0001)
Apr 12, 2021 09:07:50.994090080 CEST	8.8.8.8	192.168.2.7	0x39ce	No error (0)	becharnise.ir		194.5.178.163	A (IP address)	IN (0x0001)
Apr 12, 2021 09:08:12.672434092 CEST	8.8.8.8	192.168.2.7	0x4347	No error (0)	becharnise.ir		194.5.178.163	A (IP address)	IN (0x0001)
Apr 12, 2021 09:08:34.635107994 CEST	8.8.8.8	192.168.2.7	0xe771	No error (0)	becharnise.ir		194.5.178.163	A (IP address)	IN (0x0001)
Apr 12, 2021 09:08:55.789849043 CEST	8.8.8.8	192.168.2.7	0x5a76	No error (0)	becharnise.ir		194.5.178.163	A (IP address)	IN (0x0001)

HTTPS Packets

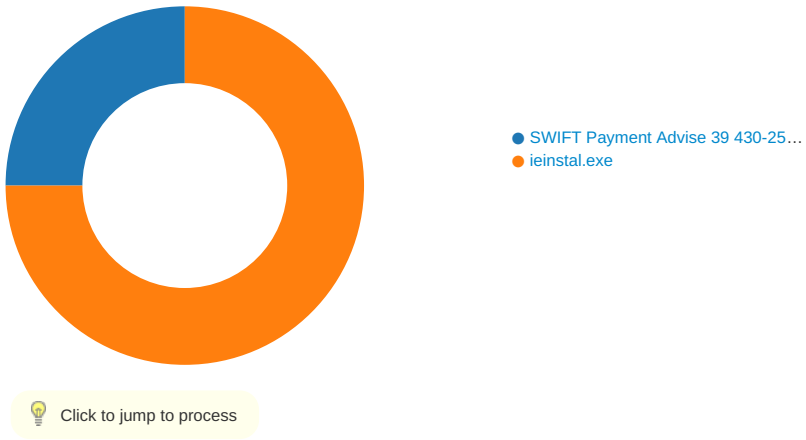
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 12, 2021 09:07:48.703210115 CEST	216.58.215.225	443	192.168.2.7	49708	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:32:57 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:32:56 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SWIFT Payment Advise 39 430-25.exe PID: 5960 Parent PID: 5704

General

Start time:	09:06:42
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\SWIFT Payment Advise 39 430-25.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SWIFT Payment Advise 39 430-25.exe'
Imagebase:	0x400000
File size:	90112 bytes
MD5 hash:	758028B3F6C428890BF423F4BF61493F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\PRAGUE	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\PRAGUE\ANTIKLDERNE	success or wait	1	660E2872	RegCreateKeyW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\PRAGUE\ANTIKLDERNE	Defileret4	unicode	MS Sans Serif	success or wait	1	660E2183	RegSetValueExW

Analysis Process: ieinstal.exe PID: 6896 Parent PID: 5960

General

Start time:	09:07:27
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SWIFT Payment Advise 39 430-25.exe'
Imagebase:	0xc70000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 0000000B.00000002.497022856.0000000003232000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3234100	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3234100	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3234100	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3234100	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3234100	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3234100	InternetOpenUrlA
C:\Users\user\AppData\Roaming\C79A3B	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	403C8D	CreateDirectoryW
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4042FB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	success or wait	1	403C1F	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	unknown	1	31	1	success or wait	1	404336	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	40415C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	40415C	ReadFile

Disassembly

Code Analysis