ID: 242362
Sample Name: swift_7974.exe
Cookbook: default.jbs
Time: 18:33:50
Date: 30/06/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

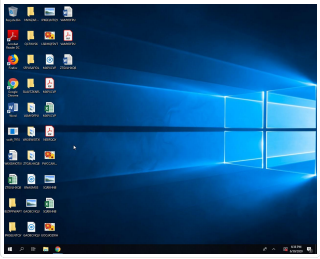
Analysis Report swift_7974.exe

Overview

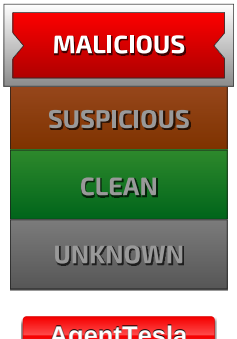
General Information

Sample Name:	swift_7974.exe
MD5:	475e1f8a737a113.
SHA1:	15b9a691f4490c3.
SHA256:	0310713073d73d..

Most interesting Screenshot:



Detection

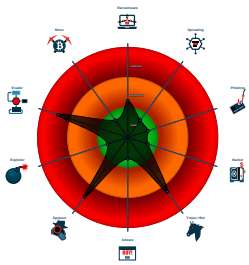


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- .NET source code contains potential …
- Injects a PE file into a foreign proces…
- Queries sensitive BIOS Information (…
- Queries sensitive network adapter inf…
- Tries to harvest and steal Putty / Win…
- Tries to harvest and steal browser inf…
- Tries to harvest and steal ftp login cr…

Classification



Startup

- **System is w10x64**
- swift_7974.exe (PID: 4028 cmdline: 'C:\Users\user\Desktop\swift_7974.exe' MD5: 475E1F8A737A1137A0935909184F8824)
  - schtasks.exe (PID: 1336 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\iupISfIFOx' /XML 'C:\Users\user\AppData\Local\Temp\tmp1E19.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - swift_7974.exe (PID: 5288 cmdline: C:\Users\user\Desktop\swift_7974.exe MD5: 475E1F8A737A1137A0935909184F8824)
  - swift_7974.exe (PID: 3688 cmdline: C:\Users\user\Desktop\swift_7974.exe MD5: 475E1F8A737A1137A0935909184F8824)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.1197046321.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.809000099.000000000381 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.1199051636.0000000002D 10000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.1199051636.0000000002D 10000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Process Memory Space: swift_7974.exe PID: 4028	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 2 entries

Unpacked PEs

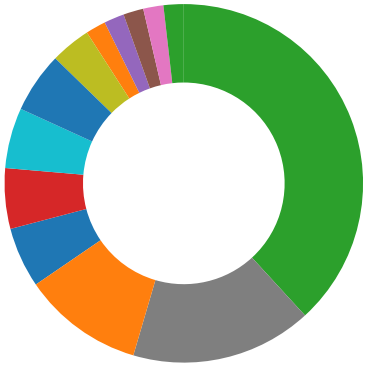
Source	Rule	Description	Author	Strings
5.2.swift_7974.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

System Summary:

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:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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)

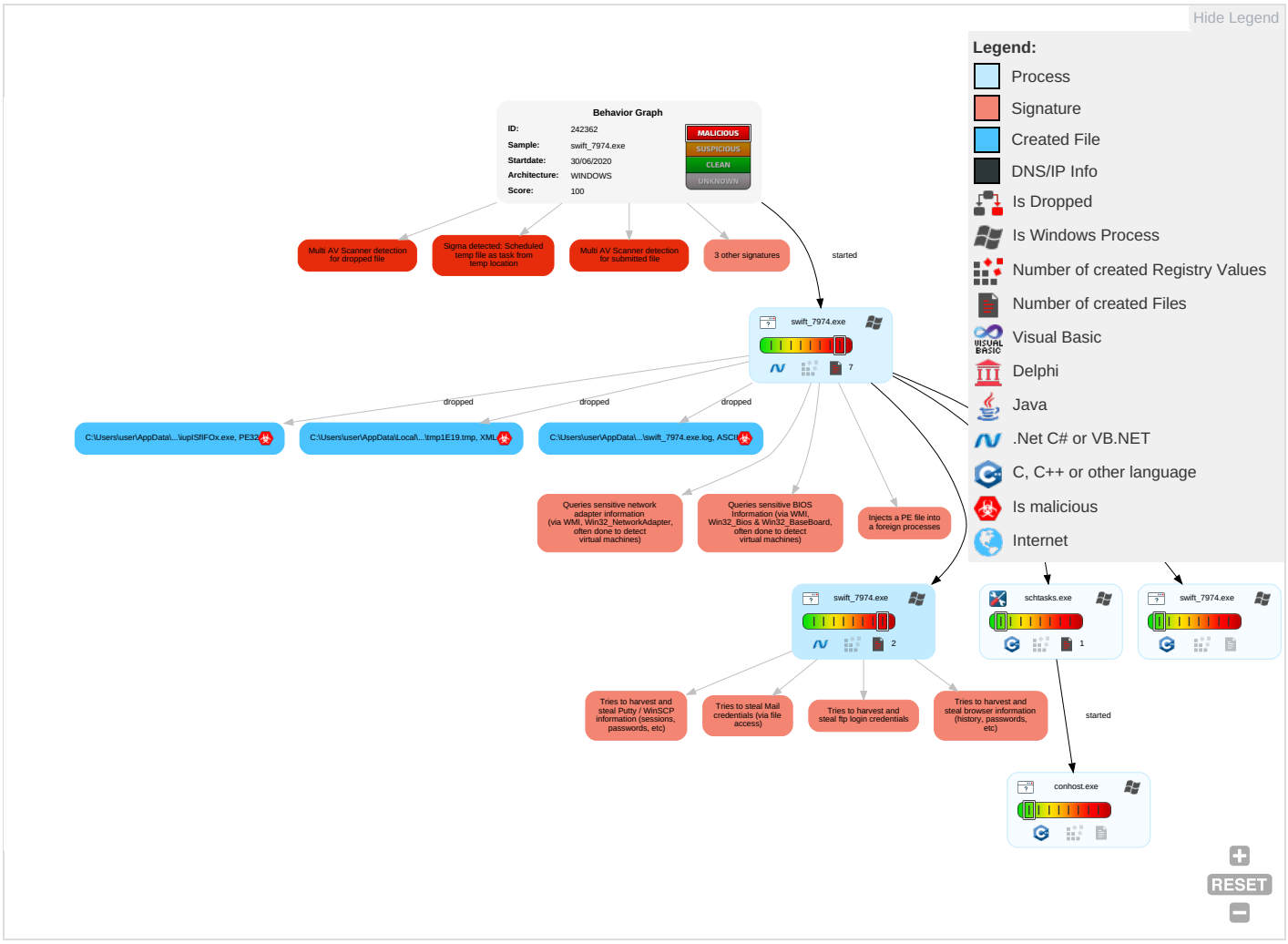
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Cont
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task 1	Process Injection 1 1 2	Masquerading 1	Credential Dumping 2	Virtualization/Sandbox Evasion 1 3	Application Deployment Software	Email Collection 1	Data Encrypted 1	Standard Cryptogra Protocol
Replication Through Removable Media	Scheduled Task 1	Port Monitors	Scheduled Task 1	Software Packing 1 3	Credentials in Registry 1	Process Discovery 2	Remote Services	Data from Local System 2	Exfiltration Over Other Network Medium	Fallback Channels
External Remote Services	Windows Management Instrumentation	Accessibility Features	Path Interception	Disabling Security Tools 1	Input Capture	Application Window Discovery 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Custom Cryptogra Protocol
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Virtualization/Sandbox Evasion 1 3	Credentials in Files	Account Discovery 1	Logon Scripts	Input Capture	Data Encrypted	Multiband Communi
Exploit Public-Facing Application	Command-Line Interface	Shortcut Modification	File System Permissions Weakness	Process Injection 1 1 2	Account Manipulation	System Owner/User Discovery 1	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptogra Protocol
Spearphishing Link	Graphical User Interface	Modify Existing Service	New Service	Obfuscated Files or Information 2	Brute Force	Security Software Discovery 2 1 1	Third-party Software	Screen Capture	Data Transfer Size Limits	Commonly Used Port
Spearphishing Attachment	Scripting	Path Interception	Scheduled Task	Software Packing	Two-Factor Authentication Interception	File and Directory Discovery 1	Pass the Hash	Email Collection	Exfiltration Over Command and Control Channel	Uncommo Used Port
Spearphishing via Service	Third-party Software	Logon Scripts	Process Injection	Indicator Blocking	Bash History	System Information Discovery 1 1 4	Remote Desktop Protocol	Clipboard Data	Exfiltration Over Alternative Protocol	Standard Applicatio Layer Pro

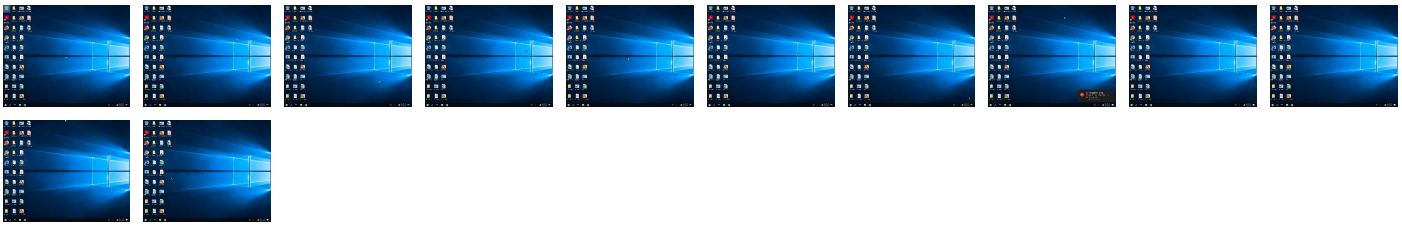
Behavior Graph



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_7974.exe	17%	Virustotal		Browse
swift_7974.exe	19%	ReversingLabs	ByteCode-MSIL.Trojan.Genkryptik	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\iupISfIFOx.exe	17%	Virustotal		Browse
C:\Users\user\AppData\Roaming\iupISfIFOx.exe	19%	ReversingLabs	ByteCode-MSIL.Trojan.Genkryptik	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.swift_7974.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	Virustotal		Browse
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://fontfabrik.com	0%	Virustotal		Browse
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	Virustotal		Browse
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	1%	Virustotal		Browse
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	Virustotal		Browse
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.tiro.com	0%	Virustotal		Browse
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	Virustotal		Browse
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	Virustotal		Browse
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	Virustotal		Browse
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	Virustotal		Browse
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	Virustotal		Browse
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe	low
http://www.apache.org/licenses/LICENSE-2.0	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false		high
http://fontfabrik.com	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe	low
http://www.founder.com.cn/cn	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe	low
http://www.founder.com.cn/cn/bThe	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false	• 1%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe	low
http://www.tiro.com	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe	low
http://www.goodfont.co.kr	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe	low
http://www.zhongyicts.com.cn	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	swift_7974.exe, 00000000.00000002.808171948.0000000002810000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe	low
http://www.carterandcone.coml	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	swift_7974.exe, 00000000.00000002.812905478.0000000005866000.00000002.00000001.sdmp	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	242362
Start date:	30.06.2020
Start time:	18:33:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	swift_7974.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	11
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.spyw.evad.winEXE@8/4@0/0
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 0.5% (good quality ratio 0.4%) • Quality average: 62.6% • Quality standard deviation: 42.5%

HCA Information:	• Successful, ratio: 99% • 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): dllhost.exe, WMIADAP.exe, MusNotifyIcon.exe, UsoClient.exe • Execution Graph export aborted for target swift_7974.exe, PID 5288 because there are no executed function • 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.

Simulations

Behavior and APIs

Time	Type	Description
18:34:20	API Interceptor	716x Sleep call for process: swift_7974.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\swift_7974.exe.log

Process:	C:\Users\user\Desktop\swift_7974.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	1216
Entropy (8bit):	5.35517900119921
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\swift_7974.exe.log	
MD5:	B5216C0AB1D432F8BAA1F92213439982
SHA1:	74B5D7346BB9887D2629A24D54D872C39A6C3C31
SHA-256:	A6E8891AE40BB81379EDDA1C02484AAB48B65A1463B4854876FC4813FB4A28FD
SHA-512:	619AF102721CD51072CA0665C497DE8DA5ED28F1B3F0562FF15BA586732C74BA279D29FC2BD82D48C91ADD026C8ECADCE1301A1C128EB8BD62ABD2BEFB1C0 2CE
Malicious:	**true**
Reputation:	moderate, 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\84b9171c43be8428a7ceaf253e5d7738\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\2da4cf2bb9a8f8a554da96d83ee20d39\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\d88a90d2c98cca1a9d491dfeb73352be\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\4d91b386e64bacbfdf3b2db1

C:\Users\user\AppData\Local\Temp\tmp1E19.tmp	
Process:	C:\Users\user\Desktop\swift_7974.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Size (bytes):	1622
Entropy (8bit):	5.152145390200903
Encrypted:	false
MD5:	DBDD4216A660097327660BBC726E5B12
SHA1:	8CD65F53FF5E55E6CFA59C7D2DE5AC375A4B7AF7
SHA-256:	16DC57EBE815B150CEDE2222B821F3324EC3E0906A9DF00F191391C5ACF8CC9D
SHA-512:	C88763B1BB6E11ACB3240128824F68304702F89121D97A37ABD2F52934247F196EB11D0FD734C3F313F0D7F6DDB3FC1CE1CE2672CD2E1F1AFF61CCA88A4F227
Malicious:	**true**
Reputation:	low
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>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\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\iupISfIFOx.exe	
Process:	C:\Users\user\Desktop\swift_7974.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Size (bytes):	496128
Entropy (8bit):	7.594171800602376
Encrypted:	false
MD5:	475E1F8A737A1137A0935909184F8824
SHA1:	15B9A691F4490C3C562E8BF5639F999C4CF95313
SHA-256:	0310713073D73DA7A45FF957B3FDBA84D8D6DA70A91A8404C66561007D505D08
SHA-512:	1FF39B6BDE5AE30072B43D9E9D32CE2256508656ECA5DC7FCCB0C0058F102371E9F5CA1EA3FB3B2EBE74F4AADA43C62220CCA2873DD6549EFFBE5DEB4B873 0FE
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 17%, Browse • Antivirus: ReversingLabs, Detection: 19%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^.....0.....F.... .....@.. ....@.....O..... ....H.....text...L.... ..... .`.rsrc.....@..@.reloc..... .....@..B.....(.....H.....|.....f...d.....{....*".}....*".(....*...}.....(.....(.....{.....(....o.....{.....(....o.....*^..}.....(.....(....*...0..._.....(.. .....(.....o.....,)....t.....o....r...p(.....,..o.....+..(....o....(.....+...*..0.....(....o....o ....+..*....0..:.....(.....(.....o.....,r...p.+....t....o!....+..*....0..:.....(.....(.....o..... ...,r...p.+....t....o"....+..*...0..:....

C:\Users\user\AppData\Roaming\iupISfIFOx.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\swift_7974.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false

C:\Users\user\AppData\Roaming\iupISfIFOx.exe:Zone.Identifier	
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.594171800602376
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • 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% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	swift_7974.exe
File size:	496128
MD5:	475e1f8a737a1137a0935909184f8824
SHA1:	15b9a691f4490c3c562e8bf5639f999c4cf95313
SHA256:	0310713073d73da7a45ff957b3fdba84d8d6da70a91a8404c66561007d505d08
SHA512:	1ff39b6bde5ae30072b43d9e9d32ce2256508656eca5dc7fccb0c0058f102371e9f5ca1ea3fb3b2ebe74f4aada43c62220cca2873dd6549effbe5deb4b8730fe
SSDEEP:	6144:RJb+RQ3tB+rXRXJh5PjutOqK+H7o8L8s+FO8eJz8X9Tl3lfNwlpNG3O5b/rQuUko:/tkPco+MNF39DlVVT/rtUkk
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^.....0.....F.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47a546
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:	0x5EFADC98 [Tue Jun 30 06:32:56 2020 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

Instruction
jmp dword ptr [00402000h]

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7a4f4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7c000	0x680	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7e000	0xc	.reloc
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7854c	0x78600	False	0.783452589564	data	7.61010132234	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7c000	0x680	0x800	False	0.36572265625	data	3.62451970509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x7c090	0x3ee	data		
RT_MANIFEST	0x7c490	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2005-2018 Piriform Ltd
Assembly Version	1.32.0.5
InternalName	QxfboEprjJ.exe
FileVersion	1.32.0.5
CompanyName	Piriform Ltd
LegalTrademarks	
Comments	Speccy is the place to start if you need to know whats inside your PC.
ProductName	Speccy
ProductVersion	1.32.0.5
FileDescription	Speccy
OriginalFilename	QxfboEprjJ.exe

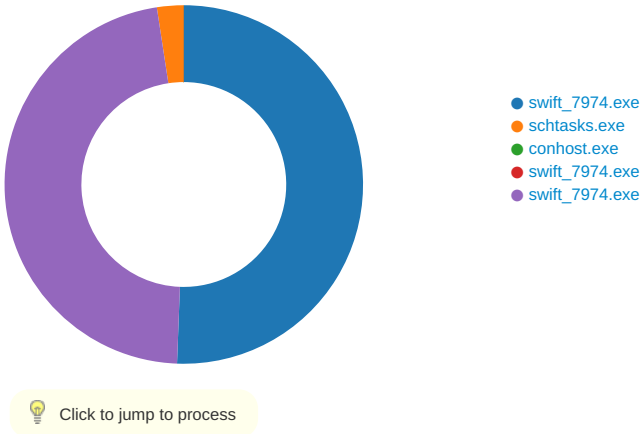
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: swift_7974.exe PID: 4028 Parent PID: 5316

General

Start time:	18:34:15
Start date:	30/06/2020
Path:	C:\Users\user\Desktop\swift_7974.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\swift_7974.exe'
Imagebase:	0x4a0000
File size:	496128 bytes
MD5 hash:	475E1F8A737A1137A0935909184F8824
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.809000099.0000000003819000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D27A9F6	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D27A9F6	unknown
C:\Users\user\AppData\Roaming\iupISfIFOx.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C12DD66	CopyFileW
C:\Users\user\AppData\Roaming\iupISfIFOx.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C12DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp1E19.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C127038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\swift_7974.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D5ECA8D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1E19.tmp	success or wait	1	6C126A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\iupISfIFOx.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 98 dc fa 5e 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 86 07 00 00 0a 00 00 00 00 00 00 46 a5 07 00 00 20 00 00 00 c0 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......^.......... ....0............F.... ....@.. ....@................	success or wait	4	6C12DD66	CopyFileW
C:\Users\user\AppData\Roaming\ iupISfIFOx.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C12DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp1E19.tmp	unknown	1622	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 47 55 43 43 49 2d 50 43 5c 47 75 63 63 69 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>..	success or wait	1	6C121B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\swift_7974.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	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_v4.0.3	success or wait	1	6D5ECC07	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D223625	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\5e7364da399b604ae01baff696551080\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D18EE1E	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D22A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D22A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D22A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6D22A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D22A974	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\84b9171c43be8428a7ceaf253e5d7738\System.ni.dll.aux	unknown	620	success or wait	1	6D18EE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\d88a90d2c98cca1a9d491dfeb73352be\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D18EE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\2da4cf2bb9a8f8a554da96d83ee20d39\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D18EE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4d91b386e64bacbfdf3b2db16155386b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D18EE1E	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	2	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C121B4F	ReadFile

Analysis Process: schtasks.exe PID: 1336 Parent PID: 4028

General

Start time:	18:34:23
Start date:	30/06/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\iupISfIFOx' /XML 'C:\Users\user\AppData\Local\Temp\tmp1E19.tmp'
Imagebase:	0xf00000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1E19.tmp	unknown	2	success or wait	1	F0AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1E19.tmp	unknown	1623	success or wait	1	F0ABD9	ReadFile

Analysis Process: conhost.exe PID: 5300 Parent PID: 1336

General

Start time:	18:34:24
Start date:	30/06/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7d5a10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: swift_7974.exe PID: 5288 Parent PID: 4028

General

Start time:	18:34:24
Start date:	30/06/2020
Path:	C:\Users\user\Desktop\swift_7974.exe
Wow64 process (32bit):	false

Commandline:	C:\Users\user\Desktop\swift_7974.exe
Imagebase:	0x140000
File size:	496128 bytes
MD5 hash:	475E1F8A737A1137A0935909184F8824
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: swift_7974.exe PID: 3688 Parent PID: 4028

General

Start time:	18:34:25
Start date:	30/06/2020
Path:	C:\Users\user\Desktop\swift_7974.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\swift_7974.exe
Imagebase:	0x9e0000
File size:	496128 bytes
MD5 hash:	475E1F8A737A1137A0935909184F8824
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.1197046321.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.1199051636.0000000002D10000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.1199051636.0000000002D10000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D27A9F6	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D27A9F6	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D223625	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\5e7364da399b604ae01baff696551080\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D18EE1E	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D22A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D22A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D22A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6D22A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D22A974	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	2	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	6D223625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D223625	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\84b917 1c43be8428a7ceaf253e5d7738\System.ni.dll.aux	unknown	620	success or wait	1	6D18EE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\2 da4cf2bb9a8f8a554da96d83ee20d39\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D18EE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manage ment\75bcfbe3b1bae498cf18ca849d4fa253\System.Management.ni.dll.aux	unknown	764	success or wait	1	6D18EE1E	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	18432	success or wait	1	6C121B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\d88a90d2c98cca1a9d491dfeb73352be\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D18EE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4d 91b386e64bacbfdf3b2db16155386b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D18EE1E	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C121B4F	ReadFile

Disassembly

Code Analysis