ID: 680490
Sample Name: SWIFT TRANSFER.exe
Cookbook: default.jbs
Time: 17:35:08
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

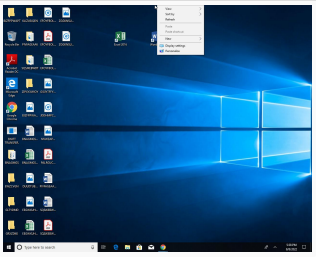
Windows Analysis Report

SWIFT TRANSFER.exe

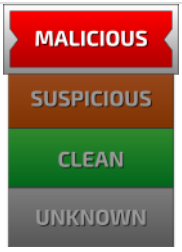
Overview

General Information

Sample Name:	SWIFT TRANSFER.exe
Analysis ID:	680490
MD5:	735ee862055fcb..
SHA1:	a4438d8649da60.
SHA256:	b496205d5045c9..
Tags:	agenttesla exe
Infos:	



Detection



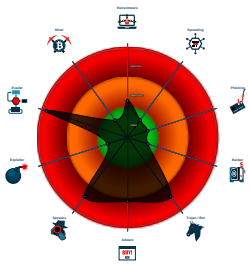
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- SWIFT TRANSFER.exe (PID: 5952 cmdline: "C:\Users\user\Desktop\SWIFT TRANSFER.exe" MD5: 735EE862055FCBCC574B73B1695AF599)
  - SWIFT TRANSFER.exe (PID: 5752 cmdline: C:\Users\user\Desktop\SWIFT TRANSFER.exe MD5: 735EE862055FCBCC574B73B1695AF599)
    - WerFault.exe (PID: 1228 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5752 -s 1700 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "marketing9@activandalucia.com",
  "Password": "iyke123456789@$",
  "Host": "mail.activandalucia.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.271754334.0000000002B22000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000000.266929046.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.266929046.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000000.266929046.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x304fe:$a13: get_DnsResolver • 0x2ecef:$a20: get_LastAccessed • 0x30e7c:$a27: set_InternalServerPort • 0x311a1:$a30: set_GuidMasterKey • 0x2edf6:$a33: get_Clipboard • 0x2ee04:$a34: get_Keyboard • 0x30119:$a35: get_ShiftKeyDown • 0x3012a:$a36: get_AltKeyDown • 0x2ee11:$a37: get_Password • 0x2f8b5:$a38: get_PasswordHash • 0x308fe:$a39: get_DefaultCredentials
00000000.00000002.270173185.00000000028D3000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.SWIFT TRANSFER.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.SWIFT TRANSFER.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.0.SWIFT TRANSFER.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32fce:$s10: logins • 0x32a35:$s11: credential • 0x2eff6:$g1: get_Clipboard • 0x2f004:$g2: get_Keyboard • 0x2f011:$g3: get_Password • 0x30309:$g4: get_CtrlKeyDown • 0x30319:$g5: get_ShiftKeyDown • 0x3032a:$g6: get_AltKeyDown
4.0.SWIFT TRANSFER.exe.400000.0.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x306fe:$a13: get_DnsResolver • 0x2eeef:$a20: get_LastAccessed • 0x3107c:$a27: set_InternalServerPort • 0x313a1:$a30: set_GuidMasterKey • 0x2eff6:$a33: get_Clipboard • 0x2f004:$a34: get_Keyboard • 0x30319:$a35: get_ShiftKeyDown • 0x3032a:$a36: get_AltKeyDown • 0x2f011:$a37: get_Password • 0x2fab5:$a38: get_PasswordHash • 0x30afe:$a39: get_DefaultCredentials
0.2.SWIFT TRANSFER.exe.3a04e80.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 22 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 185.162.171.75

Timestamp:	192.168.2.3185.162.171.75497445872851779 08/08/22-17:36:37.122597
SID:	2851779
Source Port:	49744
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 185.162.171.75

Timestamp:	192.168.2.3185.162.171.75497445872030171 08/08/22-17:36:37.122505
SID:	2030171
Source Port:	49744
Destination Port:	587
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 185.162.171.75	
Timestamp:	192.168.2.3185.162.171.75497445872840032 08/08/22-17:36:37.122597
SID:	2840032
Source Port:	49744
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

System Summary

Malicious sample detected (through community Yara rule)

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)

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

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

HIPS / PFW / Operating System Protection Evasion

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

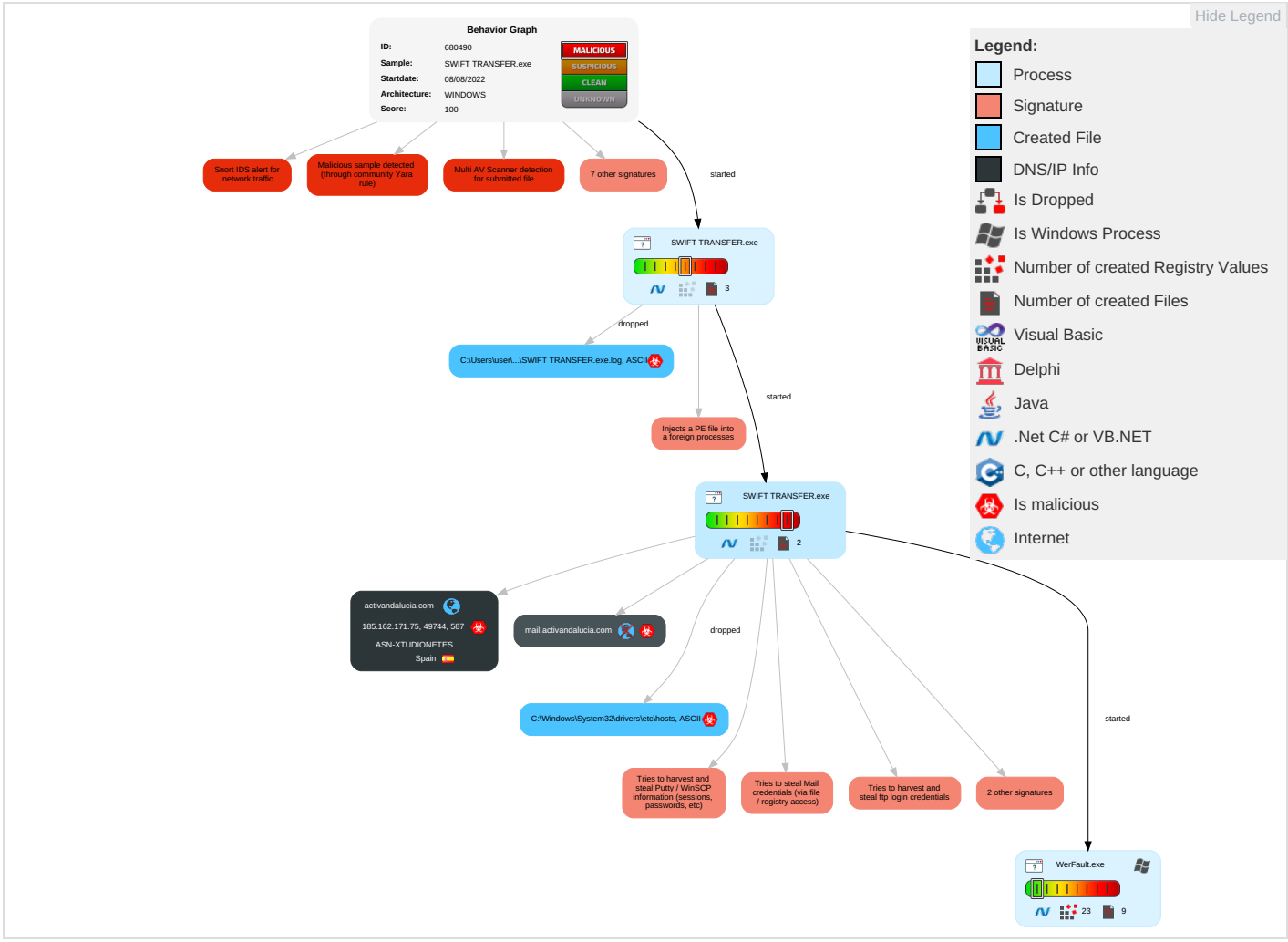
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File and Directory Permissions Modification	1 Input Capture	1 Process Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	1 Credentials in Registry	1 4 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 1 Archive Collected Data	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 4 1 Virtualization/Sandbox Evasion	NTDS	1 Application Window Discovery	Distributed Component Object Model	2 Data from Local System	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 1 Process Injection	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 2 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

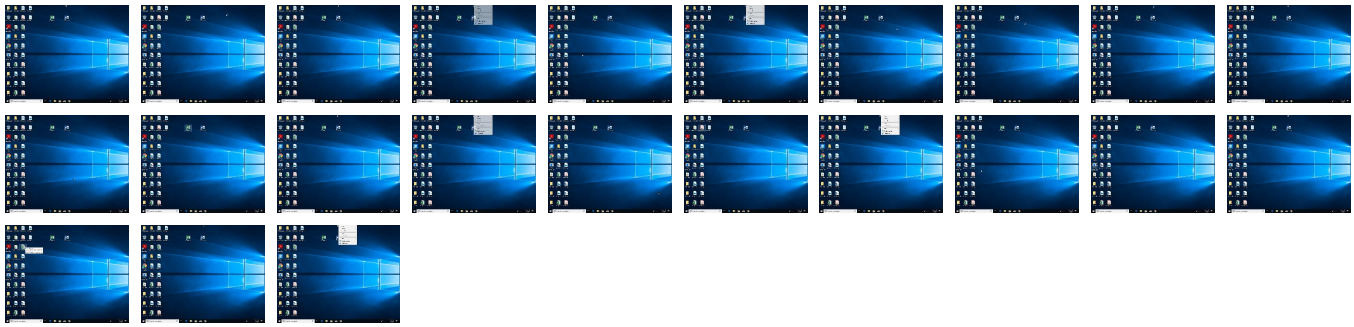
Behavior Graph



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 TRANSFER.exe	38%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
SWIFT TRANSFER.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.SWIFT TRANSFER.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203035		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comalsa	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cncro	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/G	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.com.cF	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comFN	0%	Avira URL Cloud	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/6	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.com6	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/$	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.galapagosdesign.com/U	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.fontbureau.como$	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/N	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://mail.activandalucia.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//$	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnz	0%	URL Reputation	safe	
http://TWzBs3cliDHX5nVtjxF.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/u	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.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/=	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://activandalucia.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/u	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidPsi/Psi	0%	Avira URL Cloud	safe	
http://ohMkNy.com	0%	Avira URL Cloud	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/j	0%	URL Reputation	safe	
http://www.fontbureau.comFc	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/c	0%	URL Reputation	safe	
http://www.sajatypeworks.com#	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%facebooktwittergmailinstagrammovieskypepornhackwhatsappdiscordemailpassword%st	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cns-e	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
activandalucia.com	185.162.171.75	true	true		unknown
mail.activandalucia.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comalsa	SWIFT TRANSFER.exe, 00000000.00000003.253917347.00000000057B7000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.254122853.00000000057B8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	SWIFT TRANSFER.exe, 00000004.00000000.305229027.0000000002E71000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cncro	SWIFT TRANSFER.exe, 00000000.00000003.248500769.00000000057B7000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/G	SWIFT TRANSFER.exe, 00000000.00000003.250668134.00000000057BB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.250582444.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cF	SWIFT TRANSFER.exe, 00000000.00000003.248660470.00000000057B7000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comFN	SWIFT TRANSFER.exe, 00000000.00000003.253917347.00000000057B7000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.254122853.00000000057B8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coml1	SWIFT TRANSFER.exe, 00000000.00000003.257295199.00000000057BA000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.268803149.00000000057B0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	SWIFT TRANSFER.exe, 00000000.00000003.247148499.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247768317.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249183528.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247719338.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247113059.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.248747408.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247087736.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.250081839.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.248557469.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249647219.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249350396.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249593958.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.248948890.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247811179.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247225943.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249378726.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.248205329.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247253094.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247669947.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249845353.00000000057CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/6	SWIFT TRANSFER.exe, 00000000.00000003.250668134.00000000057BB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.250582444.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com6	SWIFT TRANSFER.exe, 00000000.00000003.253917347.00000000057B7000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.254122853.00000000057B8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	SWIFT TRANSFER.exe, 00000000.00000002.28 3513984.00000000069C2000.00000004.000008 00.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SWIFT TRANSFER.exe, 00000000.00000002.28 3513984.00000000069C2000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SWIFT TRANSFER.exe, 00000000.00000002.28 3513984.00000000069C2000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/$	SWIFT TRANSFER.exe, 00000000.00000003.25 0668134.00000000057BB000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SWIFT TRANSFER.exe, 00000000.00000002.28 3513984.00000000069C2000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.come	SWIFT TRANSFER.exe, 00000000.00000003.24 7148499.00000000057CB000.00000004.000008 00.00020000.00000000.sdmp, SWIFT TRANSFE R.exe, 00000000.00000003.247768317.00000 000057CB000.00000004.00000800.00020000.0 0000000.sdmp, SWIFT TRANSFER.exe, 000000 00.00000003.249183528.00000000057CB000.0 0000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.2 47719338.00000000057CB000.00000004.00000 800.00020000.00000000.sdmp, SWIFT TRANSF ER.exe, 00000000.00000003.247035784.0000 0000057CB000.00000004.00000800.00020000. 00000000.sdmp, SWIFT TRANSFER.exe, 00000 000.00000003.247113059.00000000057CB000. 00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003. 248747408.00000000057CB000.00000004.0000 0800.00020000.00000000.sdmp, SWIFT TRANS FER.exe, 00000000.00000003.247087736.000 00000057CB000.00000004.00000800.00020000 .00000000.sdmp, SWIFT TRANSFER.exe, 0000 0000.00000003.250081839.00000000057CB000 .00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003 .248557469.00000000057CB000.00000004.000 00800.00020000.00000000.sdmp, SWIFT TRAN SFER.exe, 00000000.00000003.249647219.00 000000057CB000.00000004.00000800.0002000 0.00000000.sdmp, SWIFT TRANSFER.exe, 000 00000.00000003.249350396.00000000057CB00 0.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.0000000 3.249593958.00000000057CB000.00000004.00 000800.00020000.00000000.sdmp, SWIFT TRA NSFER.exe, 00000000.00000003.248948890.0 0000000057CB000.00000004.00000800.000200 00.00000000.sdmp, SWIFT TRANSFER.exe, 00 000000.00000003.247811179.00000000057CB0 00.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.000000 03.247225943.00000000057CB000.00000004.0 0000800.00020000.00000000.sdmp, SWIFT TR ANSFER.exe, 00000000.00000003.249378726. 00000000057CB000.00000004.00000800.00020 000.00000000.sdmp, SWIFT TRANSFER.exe, 0 0000000.00000003.248205329.00000000057CB 000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247060 632.00000000057CB000.00000004.00000800.0 0020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247253094.000000000 57CB000.00000004.00000800.00020000.00000 000.sdmp, SWIFT TRANSFER.exe, 00000000.0 0000003.247669947.00000000057CB000.00000 004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	SWIFT TRANSFER.exe, 00000000.00000002.28 3513984.00000000069C2000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	SWIFT TRANSFER.exe, 00000004.00000000.30 5229027.0000000002E71000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.fontbureau.comalsd	SWIFT TRANSFER.exe, 00000000.00000003.25 3917347.00000000057B7000.00000004.000008 00.00020000.00000000.sdmp, SWIFT TRANSFE R.exe, 00000000.00000003.254122853.00000 000057B8000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown

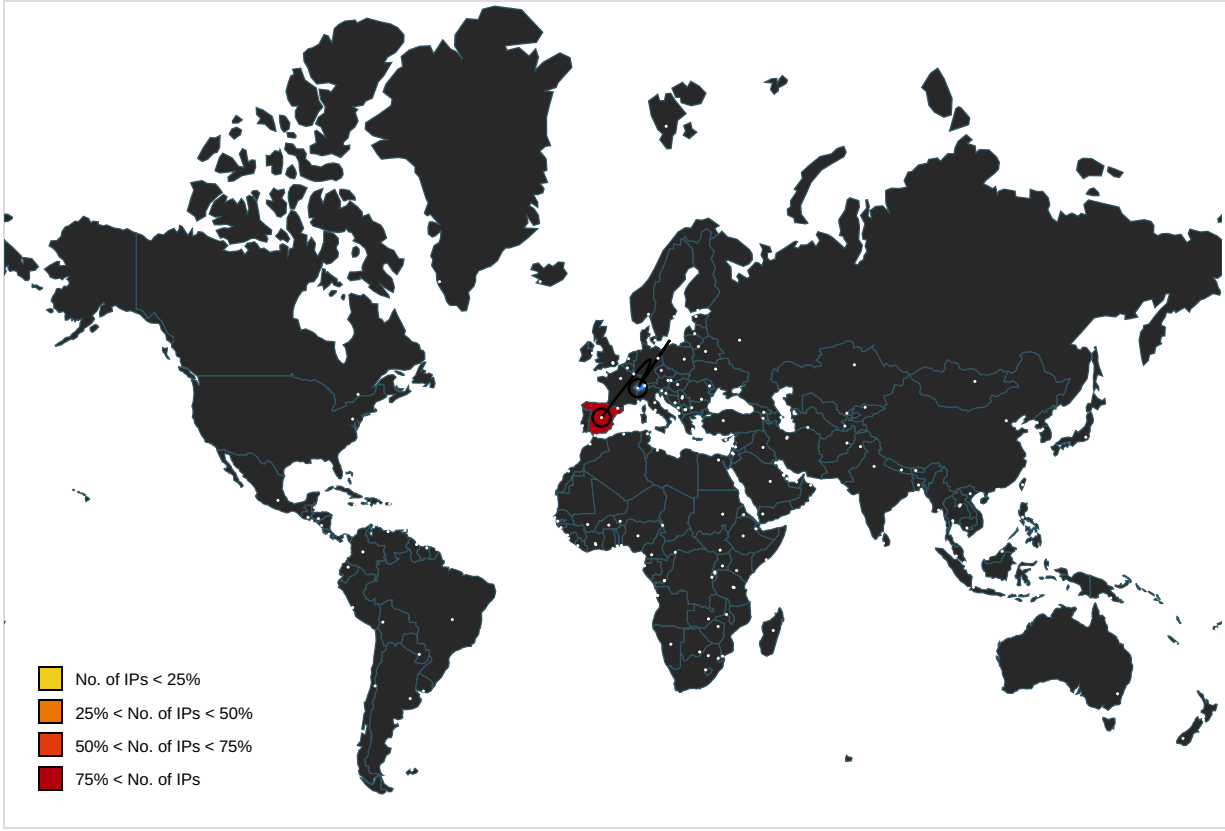
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SWIFT TRANSFER.exe, 00000000.00000003.253917347.00000000057B7000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.254122853.00000000057B8000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.comt	SWIFT TRANSFER.exe, 00000000.00000003.247148499.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247768317.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249183528.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247719338.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247035784.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247113059.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.248747408.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247087736.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.250081839.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.248557469.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249647219.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249350396.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249593958.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.248948890.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247811179.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247225943.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249378726.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.248205329.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247060632.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247253094.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247669947.00000000057CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/U	SWIFT TRANSFER.exe, 00000000.00000003.255063791.00000000057E8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/P	SWIFT TRANSFER.exe, 00000000.00000003.250668134.00000000057BB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.250582444.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como$	SWIFT TRANSFER.exe, 00000000.00000003.257295199.00000000057BA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/N	SWIFT TRANSFER.exe, 00000000.00000003.250668134.00000000057BB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.250582444.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	SWIFT TRANSFER.exe, 00000004.00000000.305229027.0000000002E71000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.activandalucia.com	SWIFT TRANSFER.exe, 00000004.00000000.307405307.00000000031CA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp//$	SWIFT TRANSFER.exe, 00000000.00000003.250582444.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnz	SWIFT TRANSFER.exe, 00000000.00000003.248500769.00000000057B7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://TWzBs3cliDHX5nVtjxF.com	SWIFT TRANSFER.exe, 00000004.00000000.307405307.00000000031CA000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000004.00000000.307429408.00000000031D7000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/u	SWIFT TRANSFER.exe, 00000000.00000003.250668134.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	SWIFT TRANSFER.exe, 00000000.00000003.250582444.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	SWIFT TRANSFER.exe, 00000000.00000003.253917347.00000000057B7000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.254122853.00000000057B8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	SWIFT TRANSFER.exe, 00000000.00000003.253917347.00000000057B7000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.254122853.00000000057B8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.come.com	SWIFT TRANSFER.exe, 00000000.00000003.257295199.00000000057BA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	SWIFT TRANSFER.exe, 00000000.00000003.247217501.00000000057B6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/=	SWIFT TRANSFER.exe, 00000000.00000003.250668134.00000000057BB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.250582444.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://activandalucia.com	SWIFT TRANSFER.exe, 00000004.00000000.307405307.00000000031CA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	SWIFT TRANSFER.exe, 00000000.00000003.248660470.00000000057B7000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.248581922.00000000057B8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/u	SWIFT TRANSFER.exe, 00000000.00000003.250582444.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidPsi/Psi	SWIFT TRANSFER.exe, 00000004.00000000.305229027.0000000002E71000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ohMkNy.com	SWIFT TRANSFER.exe, 00000004.00000000.305229027.0000000002E71000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.250668134.00000000057BB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.250582444.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como	SWIFT TRANSFER.exe, 00000000.00000003.257295199.00000000057BA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SWIFT TRANSFER.exe, 00000000.00000002.283513984.00000000069C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/j	SWIFT TRANSFER.exe, 00000000.00000003.250668134.00000000057BB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.250582444.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comFc	SWIFT TRANSFER.exe, 00000000.00000003.253917347.00000000057B7000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.254122853.00000000057B8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/c	SWIFT TRANSFER.exe, 00000000.00000003.250668134.00000000057BB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.250582444.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com#	SWIFT TRANSFER.exe, 00000000.00000003.247148499.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247768317.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249183528.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247719338.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247113059.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.248747408.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247087736.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.250081839.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.248557469.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249647219.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249350396.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249593958.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.248948890.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247811179.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247225943.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249378726.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.248205329.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247253094.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247669947.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.249845353.00000000057CB000.00000004.00000800.00020000.00000000.sdmp, SWIFT TRANSFER.exe, 00000000.00000003.247410435.00000000057CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%facebooktwittergmailinstagrammovieskypepornhackwhatsappdiscordemailpassword%st	SWIFT TRANSFER.exe, 00000004.00000000.305229027.0000000002E71000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cns-e	SWIFT TRANSFER.exe, 00000000.00000003.248660470.00000000057B7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.162.171.75	activandalucia.com	Spain		60458	ASN-XTUDIONETES	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680490
Start date and time: 08/08/202217:35:08	2022-08-08 17:35:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SWIFT TRANSFER.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:	29
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.adwa.spyw.evad.winEXE@4/6@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 20.189.173.21
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, onedsblobprdwus16.westus.cloudapp.azure.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- 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 NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- VT rate limit hit for: SWIFT TRANSFER.exe

Simulations

Behavior and APIs

Time	Type	Description
17:36:18	API Interceptor	126x Sleep call for process: SWIFT TRANSFER.exe modified
17:36:49	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SWIFT TRANSFER.e_e02ad048c9bab2cfb5fa7c41a51938c2ea97c964_73dd571f_0481d645\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536

Entropy (8bit):	1.1717842007123833
Encrypted:	false
SSDEEP:	192:WD12vRB2dHBUZMX6aPXUAaEIr/u7smS274ItdAh:xvRBMBUZMX6apnIr/u7smX4ItdA
MD5:	9BBCEF06BC366DB22F394811ECC2E6D7
SHA1:	B3AFE3A62915A9E74FC9296F1A61E52749304B2F
SHA-256:	444FB5FC85085539A24AB252CB41EFF89D9E7C83044F10EF9E9AF3E23E771A5D
SHA-512:	3C530FF658B9A2F39F0596E6C0905E64F7C75E3F08A00EFEDEB2A39B815CB3EF13BF50D6155F4B95A6CB05B8B096EA9140AAE4F6ED93C37C4A567A75304B588
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.4.4.7.9.0.0.2.9.5.9.6.6.7.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.0.4.4.7.9.0.0.7.8.6.5.9.0.4.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.d.3.4.6.c.3.e.-.9.0.5.0.-.4.7.c.c.-.9.e.e.f.-.c.9.2.1.5.5.b.6.0.7.d.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.a.6.6.d.c.1.6.-.5.9.1.c.-.4.a.7.6.-.8.a.8.1.-.9.f.7.5.8.6.2.b.8.5.7.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.W.I.F.T. .T.R.A.N.S.F.E.R...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.S.o.a.p.P.a.r.a.m.e.t.e.r.A.t.t.r.i.b...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.7.8.-.0.0.0.1.-.0.0.1.d.-.b.d.e.e.-.0.4.0.b.8.8.a.b.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.d.5.5.d.4.c.3.1.c.d.a.d.5.c.b.8.7.1.1.7.0.7.4.1.7.8.f.a.b.6.3.0.0.0.0.0.0.0.0.!.0.0.0.0.a.4.4.3.8.d.8.6.4.9.d.a.6.0.b.9.e.d.1.9.a.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Aug 9 00:36:46 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	331284
Entropy (8bit):	3.465530901495165
Encrypted:	false
SSDEEP:	3072:tTYDLKiKrjd+pmpXCguOy9gIOgF5+R0UUCgU0YGjYemWSM31oCRuX1d0/F:qKopKq9RpD+9Tj0pSGncFd0d
MD5:	F3D587948F8CAD181F73774BF2FA79A3
SHA1:	381A1CBD15ABB78F2CFBE480631B2D1CD86207CE
SHA-256:	E4F59323D84504378AD9A7F73E7B5496332C677436DF9C3E8ADED197902839BB
SHA-512:	476ED7D44792AA64251B4B29185E98BBDE9F71CADF559A5A7EB41C383160EA1E4E882804505C93275037C73E69111BD01791498894D2CE28084BC8F3A6FE4D69
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....b.....4..... ...H.....$...h'.....*...d.....`.....8.....T..... @.....'.....x).....U.....B.....*... ...GenuineIntelW.....T.....x.....b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	6398
Entropy (8bit):	3.7184008918597233
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiYy6UkzeqYZWSGXqCprs89b3usflj9m:RrlsNi16VYESGXL3tfj
MD5:	AF74ADB6BDF2F6E9969733D15DB19EE9
SHA1:	429BF764B6F5F4B2156758A737C3A87839D78479
SHA-256:	AB36802BCF813D147F98CCC027383FA39834F7879B6E3496447185263688B704
SHA-512:	5D621527F858D6E30319FCDB8AF8E70364C1D948AF35FA48E9245DA2F80921B5CF6EFF5E6F79F389A7A7A411E3897FBDD7A70331D63B2B5518CF5A8CE38C36C5
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.7.5.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF71.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4762

Entropy (8bit):	4.490459471843885
Encrypted:	false
SSDEEP:	48:cvIwSD8zsXJgtWI9YUhWgc8sqYjk8fm8M4JwLjJ2Fns+q8vALjJVR+ZOOotXd:uITf5HPgrsqYtJGKDoOoxd
MD5:	E6331D171E1B25BCEF4B236C7E4E37E2
SHA1:	8F416276567B3692F3D0873208F6C3952BE17EA4
SHA-256:	10F01086E08F58084EE6181CAB60B33DE1EF630CF5F3DB857066AAA6FC99CF28
SHA-512:	5A5EFB43B71B6F503554099831E3D77F6DD03CD11E66810FDA94566101E98673655608DB70F19C0AAE152EC38766FBE9647047C537250EB791F82E5962BD3C86
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1639307" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

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

Process:	C:\Users\user\Desktop\SWIFT TRANSFER.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
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

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Users\user\Desktop\SWIFT TRANSFER.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FAF
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.786674550423878
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SWIFT TRANSFER.exe
File size:	834048
MD5:	735ee862055fcbcc574b73b1695af599
SHA1:	a4438d8649da60b9ed19aa5d98962dc1de1efa3a
SHA256:	b496205d5045c9c9f9407bfca6a4c9088218560c2884fd737c8efe76352ae3ca
SHA512:	30792e3468246e6145c37f9bc7502ad20e88912dcc82c3e608eb7ff3522f11ba14890abe2a33425b14d249352ec33a46f63e8d7602a88f3d1def215d89dcac36
SSDEEP:	24576:H96FxgV10gJ+em8LKYXFWYNe9IbUDHDl:2gVWgflnWYN7U
TLSH:	7B05BF5BAF147708C5A7AAB5EE0BBD72A7F61C1D3175D0783A64BC0A4AFF301D51202A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...&..b.....0..... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4cd0fa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F0B226 [Mon Aug 8 06:50:14 2022 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xcd0a8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xce000	0x3c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd0000	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	0xcb100	0xcb200	False	0.8196189903846154	data	7.792812997909333	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0x3c0	0x400	False	0.3837890625	data	3.001696674534704	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xce058	0x364	data		

Imports

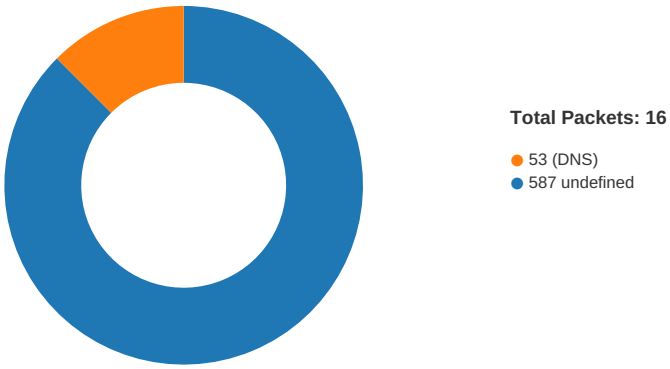
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3185.162.171.75497445872851779 08/08/22-17:36:37.122597	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49744	587	192.168.2.3	185.162.171.75
192.168.2.3185.162.171.75497445872030171 08/08/22-17:36:37.122505	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49744	587	192.168.2.3	185.162.171.75
192.168.2.3185.162.171.75497445872840032 08/08/22-17:36:37.122597	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49744	587	192.168.2.3	185.162.171.75

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:36:36.486733913 CEST	49744	587	192.168.2.3	185.162.171.75
Aug 8, 2022 17:36:36.532057047 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:36.532193899 CEST	49744	587	192.168.2.3	185.162.171.75
Aug 8, 2022 17:36:36.733409882 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:36.733877897 CEST	49744	587	192.168.2.3	185.162.171.75
Aug 8, 2022 17:36:36.779390097 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:36.781019926 CEST	49744	587	192.168.2.3	185.162.171.75
Aug 8, 2022 17:36:36.826838017 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:36.827361107 CEST	49744	587	192.168.2.3	185.162.171.75
Aug 8, 2022 17:36:36.911923885 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:36.917680025 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:36.973114014 CEST	49744	587	192.168.2.3	185.162.171.75
Aug 8, 2022 17:36:37.018518925 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:37.018560886 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:37.023947954 CEST	49744	587	192.168.2.3	185.162.171.75

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:36:37.075958967 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:37.076226950 CEST	49744	587	192.168.2.3	185.162.171.75
Aug 8, 2022 17:36:37.121546030 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:37.121611118 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:37.122504950 CEST	49744	587	192.168.2.3	185.162.171.75
Aug 8, 2022 17:36:37.122596979 CEST	49744	587	192.168.2.3	185.162.171.75
Aug 8, 2022 17:36:37.123333931 CEST	49744	587	192.168.2.3	185.162.171.75
Aug 8, 2022 17:36:37.123416901 CEST	49744	587	192.168.2.3	185.162.171.75
Aug 8, 2022 17:36:37.167886972 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:37.168486118 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:37.206161976 CEST	587	49744	185.162.171.75	192.168.2.3
Aug 8, 2022 17:36:37.343115091 CEST	49744	587	192.168.2.3	185.162.171.75
Aug 8, 2022 17:36:50.403903961 CEST	49744	587	192.168.2.3	185.162.171.75

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:36:36.304270029 CEST	56417	53	192.168.2.3	8.8.8.8
Aug 8, 2022 17:36:36.350898027 CEST	53	56417	8.8.8.8	192.168.2.3
Aug 8, 2022 17:36:36.407972097 CEST	55923	53	192.168.2.3	8.8.8.8
Aug 8, 2022 17:36:36.456037045 CEST	53	55923	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 17:36:36.304270029 CEST	192.168.2.3	8.8.8.8	0xcb34	Standard query (0)	mail.activandalucia.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:36:36.407972097 CEST	192.168.2.3	8.8.8.8	0xecf6	Standard query (0)	mail.activandalucia.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 17:36:36.350898027 CEST	8.8.8.8	192.168.2.3	0xcb34	No error (0)	mail.activandalucia.com	activandalucia.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:36:36.350898027 CEST	8.8.8.8	192.168.2.3	0xcb34	No error (0)	activandalucia.com		185.162.171.75	A (IP address)	IN (0x0001)
Aug 8, 2022 17:36:36.456037045 CEST	8.8.8.8	192.168.2.3	0xecf6	No error (0)	mail.activandalucia.com	activandalucia.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:36:36.456037045 CEST	8.8.8.8	192.168.2.3	0xecf6	No error (0)	activandalucia.com		185.162.171.75	A (IP address)	IN (0x0001)

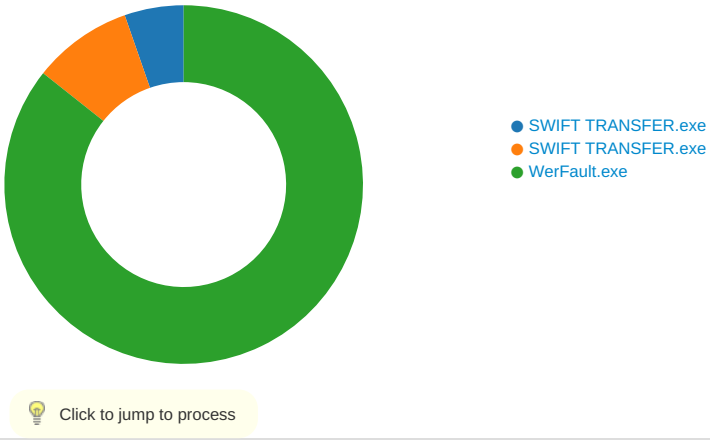
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 17:36:36.733409882 CEST	587	49744	185.162.171.75	192.168.2.3	220-cloudvip3.45st.com ESMTP Exim 4.95 #2 Mon, 08 Aug 2022 17:36:36 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 8, 2022 17:36:36.733877897 CEST	49744	587	192.168.2.3	185.162.171.75	EHLO 376483
Aug 8, 2022 17:36:36.779390097 CEST	587	49744	185.162.171.75	192.168.2.3	250-cloudvip3.45st.com Hello 376483 [102.129.143.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 8, 2022 17:36:36.781019926 CEST	49744	587	192.168.2.3	185.162.171.75	AUTH login bWFya2V0aW5nOUBhY3RpdmFuZGFsdWNpYS5jb20=
Aug 8, 2022 17:36:36.826838017 CEST	587	49744	185.162.171.75	192.168.2.3	334 UGFzc3dvcmQ6
Aug 8, 2022 17:36:36.917680025 CEST	587	49744	185.162.171.75	192.168.2.3	235 Authentication succeeded
Aug 8, 2022 17:36:36.973114014 CEST	49744	587	192.168.2.3	185.162.171.75	MAIL FROM:<marketing9@activandalucia.com>
Aug 8, 2022 17:36:37.018560886 CEST	587	49744	185.162.171.75	192.168.2.3	250 OK
Aug 8, 2022 17:36:37.023947954 CEST	49744	587	192.168.2.3	185.162.171.75	RCPT TO:<sales9@activandalucia.com>

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 17:36:37.075958967 CEST	587	49744	185.162.171.75	192.168.2.3	250 Accepted
Aug 8, 2022 17:36:37.076226950 CEST	49744	587	192.168.2.3	185.162.171.75	DATA
Aug 8, 2022 17:36:37.121611118 CEST	587	49744	185.162.171.75	192.168.2.3	354 Enter message, ending with "." on a line by itself
Aug 8, 2022 17:36:37.123416901 CEST	49744	587	192.168.2.3	185.162.171.75	.
Aug 8, 2022 17:36:37.206161976 CEST	587	49744	185.162.171.75	192.168.2.3	250 OK id=1oL4o2-0006XH-2q

Statistics

Behavior



System Behavior

Analysis Process: SWIFT TRANSFER.exe PID: 5952, Parent PID: 5280

General

Target ID:	0
Start time:	17:36:09
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\SWIFT TRANSFER.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SWIFT TRANSFER.exe"
Imagebase:	0x4e0000
File size:	834048 bytes
MD5 hash:	735EE862055FCBCC574B73B1695AF599
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.271754334.0000000002B22000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.270173185.00000000028D3000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.274677900.0000000003999000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.274677900.0000000003999000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.274677900.0000000003999000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6CDECF06	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	6CDECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SWIFT TRANSFER.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D0FC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SWIFT TRANSFER.exe.log	0	1308	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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D0FC907	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	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC31B4F	ReadFile

Analysis Process: SWIFT TRANSFER.exe PID: **5752**, Parent PID: **5952**

General

Target ID:	4
Start time:	17:36:19
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\SWIFT TRANSFER.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SWIFT TRANSFER.exe
Imagebase:	0xae0000
File size:	834048 bytes
MD5 hash:	735EE862055FCBCC574B73B1695AF599
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.266929046.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.266929046.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000004.00000000.266929046.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.305229027.0000000002E71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.305229027.0000000002E71000.00000004.00000800.00020000.00000000.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	6CDECF06	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	6CDECF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6BC31B4F	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	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC31B4F	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	6BC31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BC31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BC31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BC31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC31B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6BC31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC31B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6CDAD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6CDAD72F	unknown
C:\Users\user\Desktop\SWIFT TRANSFER.exe	unknown	4096	success or wait	1	6CDAD72F	unknown
C:\Users\user\Desktop\SWIFT TRANSFER.exe	unknown	512	success or wait	1	6CDAD72F	unknown

Analysis Process: WerFault.exe PID: **1228**, Parent PID: **5752**

General

Target ID:	15
Start time:	17:36:41
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5752 -s 1700
Imagebase:	0x800000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	69AA1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF71.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	69A9497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF71.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SWIFT TRANSFER.e_e02ad048c9bab2c fb5fa7c41a51938c2ea97c964_73dd571f_0481d645	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SWIFT TRANSFER.e_e02ad048c9bab2c fb5fa7c41a51938c2ea97c964_73dd 571f_0481d645\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	69A9497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF71.tmp	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF71.tmp.xml	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FFE.tmp.csv	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER502E.tmp.txt	success or wait	1	69A9497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 1e fd fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	10768	6	00 00 00 00 00 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 10 2a 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 78 16 00 00 03 fd fd 62 01 00 00 00 03 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 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 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UB*GenuineIntelWTxb0Pacific Standard TimePacific Daylight Time	success or wait	1	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	12908	716	7f 00 01 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 14 fd fd 00 05 00 00 00 00 00 00 00 05 00 00 00 50 fd fd 00 fd fd fd 00 22 fd fd 75 23 00 00 00 16 02 00 00 50 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++P"u#P+	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	1632	168	fd 11 00 00 00 00 00 00 52 43 43 fd 01 00 00 00 00 00 00 00 00 00 00 00 22 fd fd 75 00 00 00 00 05 00 00 00 00 00 00 00 57 00 07 fd fd fd fd 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 fd 6c 00 00 00 00 00 00 00 00 00 00 00 00 50 71 21 01 00 00 00 00 68 fd fd 00 00 00 00 00 01 00 00 00 00 00 00 00 5f 00 01 00 00 00 00 00 04 0f 09 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 30 11 7c 6b 00 00 00 00 fd 1b fd 6b 00 00 00 00 fd 02 00 00 6c 32 00 00	RCC"uWlPq!h_0|kkl2	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	25796	20	fd 02 00 00 fd 42 1f 01 00 00 00 00 04 00 00 00 fd fd 00 00	B	success or wait	684	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	36744	4	fd fd 1d 01		success or wait	683	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	304228	4	14 12 46 77	Fw	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	1800	4	11 00 00 00		success or wait	17	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	13624	716	3f 00 01 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 68 fd fd 00 fd fd 4c 77 23 00 00 00 06 02 00 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++hLw#+	success or wait	17	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	2572	48	04 01 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 fd fd 06 00 00 00 00 3c 0f 00 00 1e 27 03 00 fd 02 00 00 fd 61 00 00	<'a	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	2632	4	45 00 00 00	E	success or wait	69	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	10774	42	24 00 00 00 53 00 57 00 49 00 46 00 54 00 20 00 54 00 52 00 41 00 4e 00 53 00 46 00 45 00 52 00 2e 00 65 00 78 00 65 00 00 00	$SWIFT TRANSFER.exe	success or wait	69	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	9980	120	00 00 fd 69 00 00 00 00 00 fd 0e 00 00 08 0f 00 fd 60 fd 5a 2e 32 00 00 fd 04 fd fd 00 00 01 00 07 00 0e 00 00 00 fd 0b 07 00 0e 00 00 00 fd 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	i`Z.2?)@A	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	12884	24	12 00 00 00 70 00 73 00 61 00 70 00 69 00 2e 00 64 00 6c 00 6c 00 00 00	psapi.dll	success or wait	1	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	10100	668	00 00 3e 74 00 00 00 00 00 60 00 00 fd 0a 01 00 51 32 fd 44 54 32 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 10 fd 02 00 00 00 00 63 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 4a fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7d fd 1a 00 00 00 00 00 fd 1e 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 4d 4c 05 00 00 00 00 00 fd fd 4f 00 00 00 00 03 fd 75 1c 00 00 00 00 fd 05 fd 20 00 00 00 00 fd 19 01 00 00 00 00 fd fd 00 00 fd 1c 01 00 fd 12 07 00 fd 7e 0a 00 fd 1e 05 00 06 7f 15 00 4d 4c 05 00 a0 45 00 fd fd 01 00 fd 16 18 00 00 00 00 00 3d fd 2e 00 45 73 04	>t`Q2DT2ZbcJ}@MLOu ~MLE=.Es	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	304232	27052	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDDB.tmp.dmp	32	120	03 00 00 00 34 03 00 00 08 07 00 00 04 00 00 00 20 1d 00 00 48 0a 00 00 0e 00 00 00 24 00 00 00 68 27 00 00 05 00 00 00 fd 2a 00 00 fd 64 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 20 40 00 00 fd fd 04 00 15 00 00 00 fd 01 00 00 fd 27 00 00 16 00 00 00 fd 00 00 00 78 29 00 00	4 H$h'*d`8T @'x)	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5752</Pid>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1002	82	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 57 00 49 00 46 00 54 00 20 00 54 00 52 00 41 00 4e 00 53 00 46 00 45 00 52 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>SWIFT TRANSFER.exe< /ImageName>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1084	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1088	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1092	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000 00000</Cm dLineSignature>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1182	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1186	2	09 00		success or wait	2	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1190	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 37 00 35 00 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>27542</Uptime>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1234	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1238	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1242	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1324	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1328	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1332	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1384	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1388	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1392	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1436	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1440	2	09 00		success or wait	3	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1446	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 31 00 32 00 39 00 35 00 39 00 32 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>212959232</PeakVirtualSize>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1534	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1538	2	09 00		success or wait	3	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1544	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 31 00 32 00 39 00 35 00 31 00 30 00 34 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>212951040</VirtualSize>	success or wait	1	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1626	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 38 00 34 00 35 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>18458</PageFaultCount>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1712	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 38 00 38 00 30 00 35 00 35 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>38805504</PeakWorkingSetSize>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1810	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1814	2	09 00		success or wait	3	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1820	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 38 00 38 00 30 00 35 00 35 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>38805504</WorkingSetSize>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	1912	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 32 00 32 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>322744</QuotaPeakPagedPoolUsage>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2036	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 32 00 32 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>322744</QuotaPagedPoolUsage>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2144	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 36 00 34 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>116400</QuotaPeakNonPagedPoolUsage>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2270	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2274	2	09 00		success or wait	3	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2280	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 36 00 30 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>116016</QuotaNonPagedPoolUsage>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2390	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2394	2	09 00		success or wait	3	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2400	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 31 00 39 00 33 00 32 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>20193280</PagefileUsage>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2478	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2482	2	09 00		success or wait	3	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2488	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 32 00 32 00 36 00 30 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>20226048</PeakPagefileUsage>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2582	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2586	2	09 00		success or wait	3	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2592	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 31 00 39 00 33 00 32 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>20193280</PrivateUsage>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2666	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2670	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2674	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2720	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2724	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2726	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2768	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2772	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2774	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2812	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2816	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2820	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>CLR20r3</EventType>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2880	4	0d 00 0a 00		success or wait	9	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2884	2	09 00		success or wait	18	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	2888	86	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 57 00 49 00 46 00 54 00 20 00 54 00 52 00 41 00 4e 00 53 00 46 00 45 00 52 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>SWIFT TRANSFER.exe </Parameter0>	success or wait	9	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	3574	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	3578	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	3580	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	3620	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	3624	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	3626	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	3664	4	0d 00 0a 00		success or wait	6	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	3668	2	09 00		success or wait	12	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	3672	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4226	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4230	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4232	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4272	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4276	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4278	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4316	4	0d 00 0a 00		success or wait	1	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4320	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4324	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4418	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4422	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4426	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 71 00 6e 00 6b 00 61 00 69 00 69 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>qnkaii, Inc.</SystemManufacturer>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4532	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4536	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4540	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 71 00 6e 00 6b 00 61 00 69 00 69 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>qnkaii7,1</SystemProductName>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4636	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4640	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4644	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4764	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4768	2	09 00		success or wait	2	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4772	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 30 00 36 00 34 00 31 00 33 00 32 00 36 00 37 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>16064132 67</OSInstallDate>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4862	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:4 9:21Z</OSInstallTime>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4964	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4968	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	4972	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</ TimeZoneBias>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5040	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5044	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5046	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5086	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5090	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5092	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5126	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5130	2	09 00		success or wait	2	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5134	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5230	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5234	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5236	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5272	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5276	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5278	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5302	4	0d 00 0a 00		success or wait	3	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5306	2	09 00		success or wait	6	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5310	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5568	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5572	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5574	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5600	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5604	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5606	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 38 00 2d 00 30 00 39 00 54 00 30 00 30 00 3a 00 33 00 36 00 3a 00 34 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-08-09T00:36:47Z">	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5706	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5710	2	09 00		success or wait	2	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5714	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 32 00 39 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 37 00 35 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 37 00 30 00 37 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 37 00 30 00 37 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<Process AsId="290" PID="5752" UptimeMS="17078" TimeSinceCreationMS="17078" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5980	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5984	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	5988	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6008	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6012	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6014	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6052	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6056	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6058	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6096	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6100	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6104	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 64 00 33 00 34 00 36 00 63 00 33 00 65 00 2d 00 39 00 30 00 35 00 30 00 2d 00 34 00 37 00 63 00 63 00 2d 00 39 00 65 00 65 00 66 00 2d 00 63 00 39 00 32 00 31 00 35 00 35 00 62 00 36 00 30 00 37 00 64 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>3d346c3e-9050-47cc-9eef-c92155b607d0</Guid>	success or wait	1	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6202	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6206	2	09 00		success or wait	2	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6210	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 38 00 2d 00 30 00 39 00 54 00 30 00 30 00 3a 00 33 00 36 00 3a 00 34 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-08-09T00:36:47Z</CreationTime>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6308	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6312	2	09 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6314	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6354	4	0d 00 0a 00		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE47.tmp.WERInternalMetadata.xml	6358	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF71.tmp.xml	0	4762	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 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SWIFT TRANSFER.e_e02ad048c9bab2cfb5fa7c41a51938c2ea97c964_73dd571f_0481d645\Report.wer	0	2	fd fd		success or wait	1	69A9497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SWIFT TRANSFER.e_e02ad048c9bab2cfb5fa7c41a51938c2ea97c964_73dd571f_0481d645\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	197	69A9497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SWIFT TRANSFER.e_e02ad048c9bab2cfb5fa7c41a51938c2ea97c964_73dd571f_0481d645\Report.wer	15334	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 38 00 34 00 37 00 38 00 35 00 32 00 31 00 34 00	MetadataHash=184785214	success or wait	1	69A9497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	success or wait	1	69AB36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	69AB1FB2	RegCreateKeyExW
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	69A943D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	ProgramId	unicode	0006fd55d4c31cdad5cb87117074178fab6300000000	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	FileId	unicode	0000a4438d8649da60b9ed19aa5d98962dc1de1efa3a	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	LowerCaseLongPath	unicode	c:\users\user\desktop\swift transfer.exe	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	LongPathHash	unicode	swift transfer.e|1dbdce9	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	Name	unicode	swift transfer.exe	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	Publisher	unicode		success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	Version	unicode	1.0.0.0	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	BinFileVersion	unicode	1.0.0.0	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	BinaryType	unicode	pe32_clr_32	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	ProductName	unicode	process explorer	success or wait	1	69AB36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	ProductVersion	unicode	1.0.0.0	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	LinkDate	unicode	08/08/2022 06:50:14	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	BinProductVersion	unicode	1.0.0.0	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	Size	B	00 BA 0C 00 00 00 00 00	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	Language	dword	0	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	IsPeFile	dword	1	success or wait	1	69AB36BF	unknown
\REGISTRY\A\{9e8799aa-f06b-e7c4-b5d6-b890f4bc5bcb}\Root\InventoryApplicationFile\swift transfer.e|1dbdce9	IsOsComponent	dword	0	success or wait	1	69AB36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 F4 75 05 00 00 00 57 00 07 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 C5 6C 00 00 00 00 50 71 21 01 68 EC F5 00 01 00 00 00 5F 00 01 00 04 0F 09 00 00 00 00 80 00 00 00 00 30 11 7C 6B FC 1B 89 6B	success or wait	1	69AB1FE8	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly