ID: 635184
Sample Name: SWIFT_09903094858577_900039388883-TRF.exe
Cookbook: default.jbs
Time: 16:38:10
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report

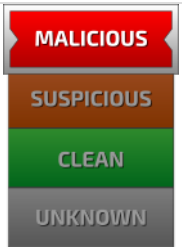
SWIFT_09903094858577_900039388883-TRF.exe

Overview

General Information

Sample Name:	SWIFT_09903094858577_900039388883-TRF.exe
Analysis ID:	635184
MD5:	02d6ac6ec4a12e..
SHA1:	ef8b52fea288cc7..
SHA256:	0cefce0036bdca…
Tags:	agenttesla exe
Infos:	

Detection



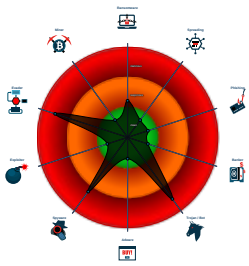
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Tries to detect sandboxes and other…
- Yara detected Generic Downloader
- .NET source code contains very larg…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…
- Queries sensitive BIOS Information…

Classification



Process Tree

- **System is w10x64**
- SWIFT_09903094858577_900039388883-TRF.exe (PID: 3980 cmdline: "C:\Users\user\Desktop\SWIFT_09903094858577_900039388883-TRF.exe" MD5: 02D6AC6EC4A12EBC4C1D9166B9FD0E86)
  - SWIFT_09903094858577_900039388883-TRF.exe (PID: 3452 cmdline: C:\Users\user\Desktop\SWIFT_09903094858577_900039388883-TRF.exe MD5: 02D6AC6EC4A12EBC4C1D9166B9FD0E86)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "info2@obynnehhhan.com",
  "Password": "G$MUuYG3",
  "Host": "smtp.obynnehhhan.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.423506540.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.423506540.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000000.424230467.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000000.424230467.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.658655626.0000000002981000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.SWIFT_09903094858577_900039388883-TRF.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.SWIFT_09903094858577_900039388883-TRF.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.2.SWIFT_09903094858577_900039388883-TRF.exe.400000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
5.2.SWIFT_09903094858577_900039388883-TRF.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x303b8:$s1: get_kbok • 0x30cfb:$s2: get_CHoo • 0x31949:$s3: set_passwordIsSet • 0x301bc:$s4: get_enableLog • 0x3481c:$s8: torbrowser • 0x331f8:$s10: logins • 0x32b70:$s11: credential • 0x2f5e1:$g1: get_Clipboard • 0x2f5ef:$g2: get_Keyboard • 0x2f5fc:$g3: get_Password • 0x30b9a:$g4: get_CtrlKeyDown • 0x30baa:$g5: get_ShiftKeyDown • 0x30bbb:$g6: get_AltKeyDown
5.0.SWIFT_09903094858577_900039388883-TRF.exe.400008.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 42 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

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)

Stealing of Sensitive Information

Yara detected AgentTesla
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal browser information (history, passwords, etc)

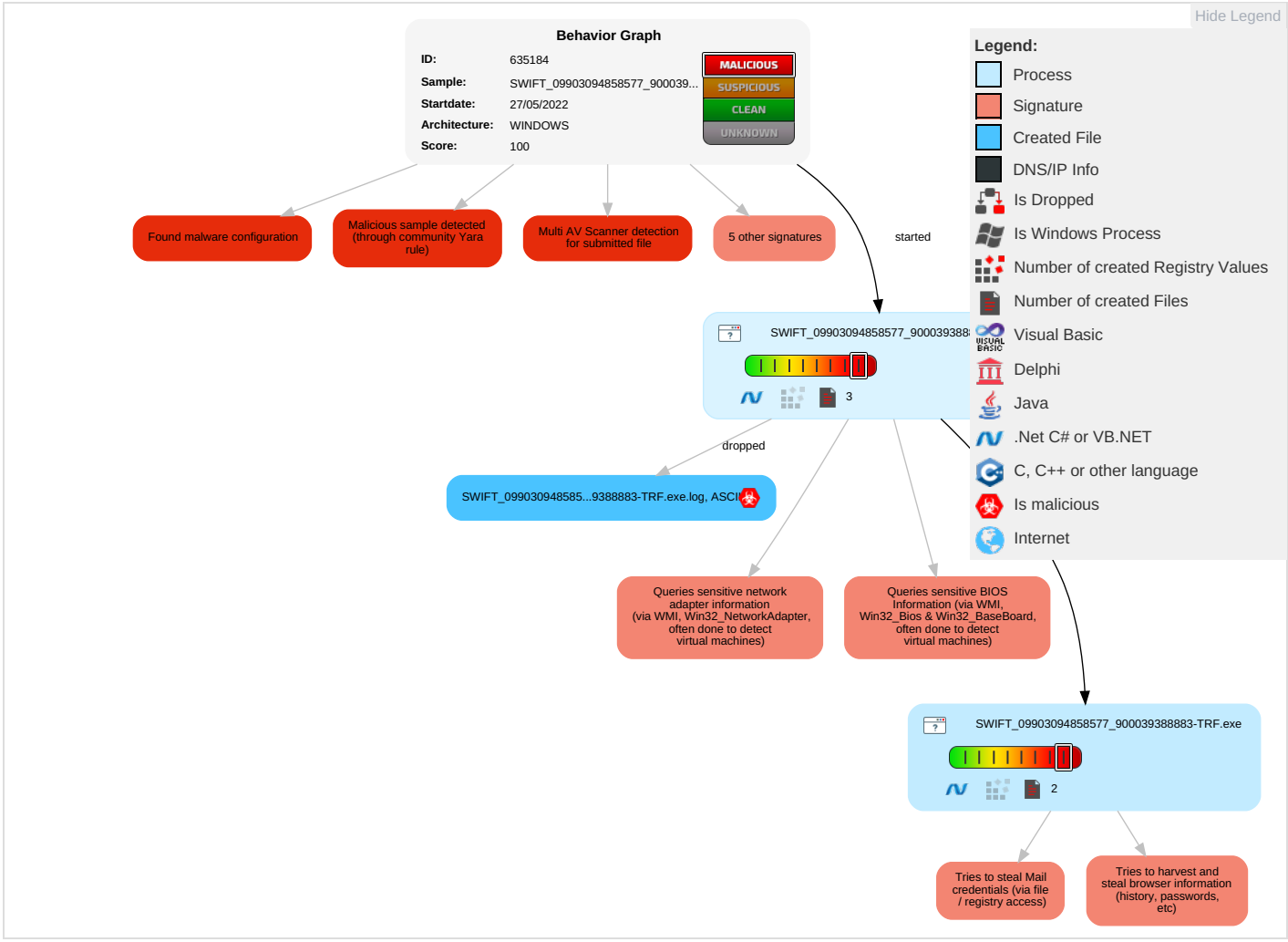
Remote Access Functionality

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 Process Injection	1 Masquerading	1 OS Credential Dumping	2 1 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 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	Junk Data	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 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 1 4 System Information 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	2 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User 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	3 Software Packing	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

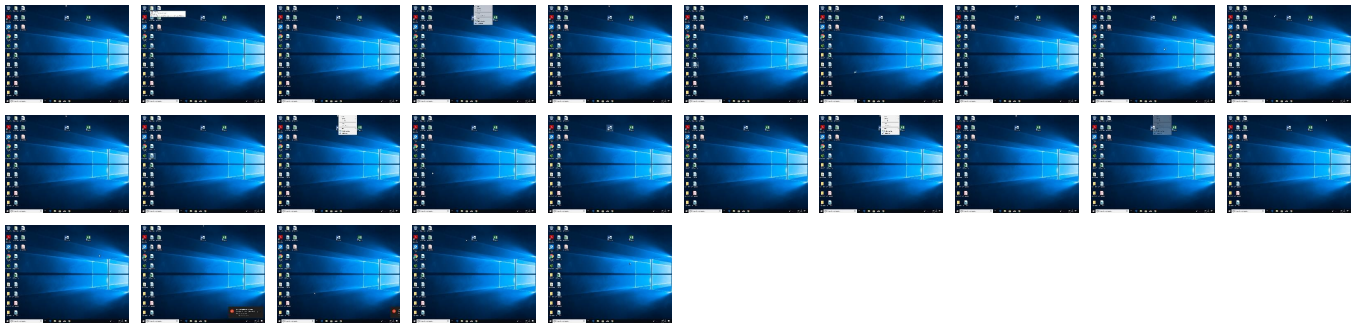
Behavior Graph



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_09903094858577_900039388883-TRF.exe	15%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.SWIFT_09903094858577_900039388883-TRF.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.SWIFT_09903094858577_900039388883-TRF.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.SWIFT_09903094858577_900039388883-TRF.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.SWIFT_09903094858577_900039388883-TRF.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.SWIFT_09903094858577_900039388883-TRF.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.SWIFT_09903094858577_900039388883-TRF.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/siv	0%	URL Reputation	safe	
http://www.tiro.comL	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kra-e	0%	URL Reputation	safe	
http://www.fontbureau.comiva	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.comsief1	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/#	0%	URL Reputation	safe	
http://www.sandoll.co.krF	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/U	0%	URL Reputation	safe	
http://www.carterandcone.como.l	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://www.fontbureau.come.comp	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.urwpp.desiv	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krk	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmt	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/kh	0%	Avira URL Cloud	safe	
http://www.carterandcone.comhe	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/y	0%	URL Reputation	safe	
http://www.fontbureau.comituF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn1	0%	URL Reputation	safe	
http://www.goodfont.co.kr-ey	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/#	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.htmlt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://fontfabrik.com(	0%	Avira URL Cloud	safe	
http://www.tiro.comic	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnmbo#	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnY	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnA	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/:	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnmR	0%	Avira URL Cloud	safe	
http://fontfabrik.comXt	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.como:	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kra-es:	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/k	0%	URL Reputation	safe	
http://www.sandoll.c	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn-u	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/U	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://PcwsIt.com	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sajatypeworks.comn	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comue	0%	URL Reputation	safe	
http://www.sakkal.com-us	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/wa	0%	URL Reputation	safe	
http://www.tiro.comx	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/J	0%	Avira URL Cloud	safe	
http://www.fontbureau.comto	0%	Avira URL Cloud	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.comessed1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.commG	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comp	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.tiro.comg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SWIFT_09903094858577_900039388883-TRF.exe, 00000005.00000002.658655626.000000002981000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://github.com/dcoetzee/plants-vs-zombies-user-file-editor	SWIFT_09903094858577_900039388883-TRF.exe	false		high
http://www.jiyu-kobo.co.jp/siv	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391501258.000000005950000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391418072.000000005953000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comL	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388188419.000000000EEC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kra-e	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386773432.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comiva	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394677111.000000000 594C000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalsF	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397005721.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396726657.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396326776.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397528108.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397361974.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396188515.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comsief1	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397005721.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395905005.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396726657.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396326776.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396066018.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397361974.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396188515.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.381817686.000000000 5932000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000000 6B42000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000000 6B42000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/:	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.393020597.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.393125591.000000005950000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392811435.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392243224.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.393244057.000000005950000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392539140.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.393322673.000000005950000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391501258.000000005950000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394267414.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391610173.000000005948F000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392940393.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394062624.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.393528628.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.393739621.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392310176.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391968800.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.393973304.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394413188.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391661961.000000005948F000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.393838736.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392079319.000000005953000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/8	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391501258.000000005950000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391610173.000000005948F000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391661961.000000005948F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392243224.000000005953000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/#	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392243224.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391890517.000000005952000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391501258.000000005950000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392310176.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391968800.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391418072.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392079319.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392501520.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392126421.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391801811.000000005952000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krF	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386936635.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386773432.000000005948000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389046031.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	SWIFT_09903094858577_900039388883-TRF.exe, 00000005.00000002.658758413.000000002A28000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.432196435.000000003A0B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000005.00000000.423506540.000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399208506.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399402817.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.398838523.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399011827.000000005948000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/U	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391890517.000000005952000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391801811.000000005952000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.como.l	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389820126.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389238092.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389684405.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390043191.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389302234.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcomd	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397005721.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395905005.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395764736.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396726657.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396326776.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397528108.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396066018.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397361974.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396188515.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.come.comp	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.402687040.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.403974726.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.403082621.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.402516805.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	SWIFT_09903094858577_900039388883-TRF.exe, 00000005.00000002.658655626.000000000 2981000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.desiv	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397005721.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396726657.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krk	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386773432.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htmt	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399208506.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399724789.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399485326.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399402817.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.398838523.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399852324.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399635918.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399011827.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/kh	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391501258.000000000 5950000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391418072.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comhe	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389820126.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389238092.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389684405.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389302234.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000000 6B42000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.387659026.000000000 5950000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388003293.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388127665.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.387805345.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/y	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391890517.000000000 5952000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391968800.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392079319.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392126421.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391801811.000000000 5952000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comituF	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395545730.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395608625.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395269106.000000000 594C000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395374356.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395186808.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn1	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388913948.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389046031.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388158710.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390541816.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390098278.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388486451.000000000 5954000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389820126.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.387659026.000000000 5950000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388003293.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390297847.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388127665.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.387805345.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388262758.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389238092.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390448917.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389684405.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388626362.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390043191.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389302234.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr-ey	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386773432.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395186808.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000000 6B42000.00000004.00000800.00020000.00000 000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/#	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391610173.000000000 594F000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391661961.000000000 594F000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/o	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391176269.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391501258.000000000 5950000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391610173.000000000 594F000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391418072.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391661961.000000000 594F000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391256199.000000000 594C000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.htmlt	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392243224.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/k	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392243224.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391890517.000000000 5952000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392310176.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391968800.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391418072.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392079319.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392501520.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392126421.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391801811.000000000 5952000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com(	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.383173518.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.comic	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390098278.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390297847.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390043191.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnmbo#	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389046031.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000000 6B42000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://www.fontbureau.com/designers/?	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000000 6B42000.00000004.00000800.00020000.00000 000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnY	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.387447964.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com	SWIFT_09903094858577_900039388883-TRF.exe	false		high
http://www.galapagosdesign.com/staff/dennis.htmF	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399208506.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399724789.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399485326.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399402817.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.398838523.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399852324.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399635918.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.399011827.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnA	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.387402518.000000005954000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.387364334.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/:	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391890517.000000005952000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391801811.000000005952000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnmR	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389046031.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.comXt	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.383196986.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.383237347.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.383685174.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.383533455.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.382882779.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.382936594.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.383196986.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.383385022.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.383631334.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.383173518.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.383781752.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.383835216.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.383871610.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000000 6B42000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.383237347.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como:	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395545730.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395608625.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395269106.000000000 594C000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395374356.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kra-es:	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386578954.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386773432.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/k	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391501258.000000000 5950000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391610173.000000000 594F000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391661961.000000000 594F000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.c	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386936635.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386989428.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	SWIFT_09903094858577_900039388883-TRF.exe, 00000005.00000002.658655626.000000000 2981000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnn-u	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.387402518.000000005954000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.387364334.000000005 94B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386578954.000000005 94B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/U	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392243224.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391501258.000000005950000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391610173.000000005 94F000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392310176.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391968800.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391661961.000000005 94F000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392079319.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392501520.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392126421.000000005953000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397005721.000000005 94B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394493069.000000005 94B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394267414.000000005 94B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394062624.000000005 94B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396726657.000000005 94B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394413188.000000005 94B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://PcwsIt.com	SWIFT_09903094858577_900039388883-TRF.exe, 00000005.00000002.658655626.000000002981000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392243224.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comn	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.381817686.000000005932000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388913948.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388626362.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000000 6B42000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://www.fontbureau.com	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397005721.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395545730.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395905005.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394677111.000000000 594C000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395269106.000000000 594C000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394982067.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394707605.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395764736.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394772042.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396726657.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396326776.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397528108.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396066018.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394876176.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395374356.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395078050.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397361974.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395186808.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000000 6B42000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395141278.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396188515.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://DynDns.comDynDNS	SWIFT_09903094858577_900039388883-TRF.exe, 00000005.00000002.658655626.000000000 2981000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comue	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395269106.000000000594C000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394982067.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395078050.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394929133.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395186808.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395141278.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com-us	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392243224.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392539140.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392310176.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392501520.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392589542.000000005953000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comF	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.398057554.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397005721.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397833505.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396726657.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396326776.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397528108.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397767310.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397718379.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.398000159.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397361974.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396188515.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/wa	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391176269.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391418072.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391256199.000000000594C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comx	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388127665.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/J	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.387659026.000000005950000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comto	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395545730.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395269106.000000005948C000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394982067.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394707605.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394772042.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394876176.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395374356.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395078050.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394929133.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395186808.000000005948000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395141278.000000005948000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.393020597.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392811435.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392243224.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391890517.000000005952000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392539140.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391610173.000000005948F000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392940393.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392310176.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391968800.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391661961.000000005948F000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392079319.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392501520.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392589542.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.392126421.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391801811.000000005952000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.coma	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395545730.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395269106.000000000594C000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394982067.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395374356.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395078050.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394929133.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395186808.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395141278.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397005721.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395545730.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395608625.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395905005.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395269106.000000000594C000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394982067.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395764736.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396726657.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396326776.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396066018.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395374356.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395078050.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.397361974.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394929133.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395186808.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395141278.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396188515.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comessed1	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395545730.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395269106.000000000594C000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395374356.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388913948.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389046031.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388158710.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390541816.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390098278.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388486451.000000005954000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.387447964.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389820126.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.387659026.000000005950000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388003293.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390297847.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388127665.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.387805345.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388262758.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389238092.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390448917.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389684405.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388626362.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.390043191.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000006B42000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389302234.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.commG	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.402687040.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.403974726.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.403082621.000000005953000.00000004.00000800.00020000.00000000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.402516805.000000005953000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.monotype.	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386437076.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386318697.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396326776.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386578954.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.386773432.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396188515.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comm	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.402687040.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.395905005.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.403974726.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433768992.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396066018.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.403082621.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.426144944.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.402516805.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.396188515.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.391801811.000000000 5952000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comp	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.394707605.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.402687040.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.403974726.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.403082621.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp, SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.402516805.000000000 5953000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.389046031.000000000 594B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000002.433941853.000000000 6B42000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://www.tiro.comg	SWIFT_09903094858577_900039388883-TRF.exe, 00000000.00000003.388188419.000000000 0EEC000.00000004.00000020.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635184
Start date and time: 27/05/202216:38:10	2022-05-27 16:38:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SWIFT_09903094858577_900039388883-TRF.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:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@0/0
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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- 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.
- VT rate limit hit for: SWIFT_09903094858577_900039388883-TRF.exe

Simulations

Behavior and APIs

Time	Type	Description
16:39:42	API Interceptor	564x Sleep call for process: SWIFT_09903094858577_900039388883-TRF.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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SWIFT_09903094858577_900039388883-TRF.exe.log

Process:	C:\Users\user\Desktop\SWIFT_09903094858577_900039388883-TRF.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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.762421941493696
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SWIFT_09903094858577_900039388883-TRF.exe
File size:	754688
MD5:	02d6ac6ec4a12ebc4c1d9166b9fd0e86
SHA1:	ef8b52fea288cc7bc4c7c486d50b84461d73e741

SHA256:	0cefce0036bdcae72d06ede18a35ae7d38ea378aef702c2bd67006670c19bbc1
SHA512:	c83c438212b9d99c0be1f7ce3f97a703fba5ab67d73baa9afb1ccf9723157cc89ef14aa9df00c8690794b2e7afbf857d082756a17584e01afb4bc89aa684f60f
SSDEEP:	12288:sMa172O9bHoAUPvqVwlQ3o7MblZK9+U3ocl+BUrxQ+7JMb/QHdnPwXT5G:iYSbHoNy3awit3ocl+Wr++7c/QHBaT5G
TLSH:	03F4F100B2F82B12E6BA67FA9670609407B67D952530E39E1CD17CDB3A71F524E81F1B
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...I..b..............0..(...Z.......F... ...`....@.. ....@................................

File Icon

	
Icon Hash:	4462f276dcec30e6

Static PE Info

General

Entrypoint:	0x4b461e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x62901549 [Fri May 27 00:03:21 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb45cc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb6000	0x57d4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbc000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb4494	0x1c	.text
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	0xb2624	0xb2800	False	0.866748457195	data	7.76139919747	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x57d4	0x5800	False	0.96484375	data	7.89222649818	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbc000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb6100	0x51a3	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xbb2b4	0x14	data		
RT_VERSION	0xbb2d8	0x2fc	data		
RT_MANIFEST	0xbb5e4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

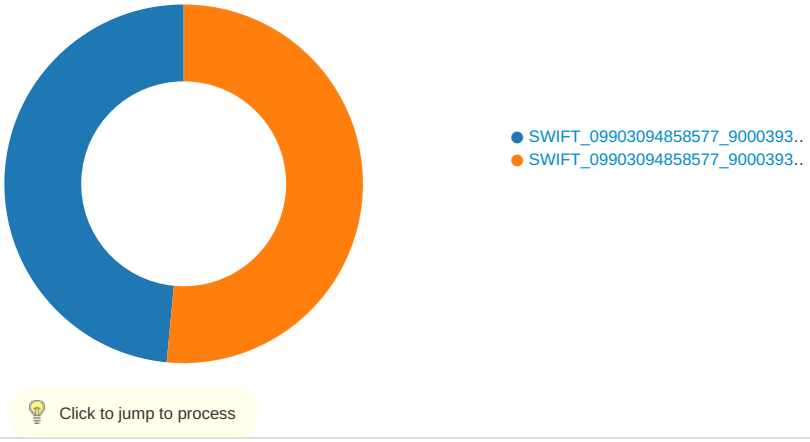
Version Infos	
Description	**Data**
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	1.0.0.0
InternalName	EndNoGCRegionSta.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	EndNoGCRegionSta.exe

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: SWIFT_09903094858577_900039388883-TRF.exe PID: 3980, Parent PID: 3300

General	
Target ID:	0
Start time:	16:39:23
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SWIFT_09903094858577_900039388883-TRF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SWIFT_09903094858577_900039388883-TRF.exe"
Imagebase:	0x470000
File size:	754688 bytes
MD5 hash:	02D6AC6EC4A12EBC4C1D9166B9FD0E86

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.434440348.0000000007170000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.432038283.0000000002CC8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.429866303.0000000002931000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.432196435.0000000003A0B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.432196435.0000000003A0B000.00000004.00000800.00020000.00000000.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	6DC9CF06	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	6DC9CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SWIFT_09903094858577_900039388883-TRF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFAC78D	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_09903094858577_900039388883-TRF.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	6DFAC907	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	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68DA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68DA1B4F	ReadFile

Analysis Process: SWIFT_09903094858577_900039388883-TRF.exe PID: **3452**, Parent PID: **3980**

General

Target ID:	5
Start time:	16:39:44
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SWIFT_09903094858577_900039388883-TRF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SWIFT_09903094858577_900039388883-TRF.exe
Imagebase:	0x590000
File size:	754688 bytes
MD5 hash:	02D6AC6EC4A12EBC4C1D9166B9FD0E86
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: 00000005.00000000.423506540.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.423506540.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.424230467.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.424230467.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.658655626.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.658655626.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000005.00000002.658655626.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.658784371.0000000002A32000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.424900759.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.424900759.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.422855293.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.422855293.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.656994998.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.656994998.0000000000402000.00000040.00000400.00020000.00000000.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	6DC9CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6DC9CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68DA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68DA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68DA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68DA1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	68DA1B4F	ReadFile

Disassembly

No disassembly