ID: 756157
Sample Name: SWIFT copy.29112022.Pdf.exe
Cookbook: default.jbs
Time: 18:24:07
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

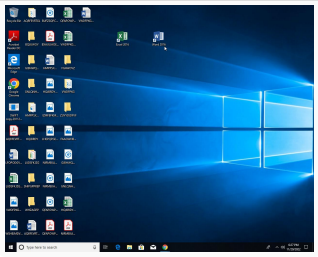
Windows Analysis Report

SWIFT copy.29112022.Pdf.exe

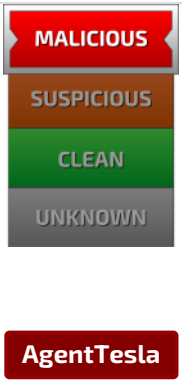
Overview

General Information

Sample Name:	SWIFT copy.29112022.Pdf.exe
Analysis ID:	756157
MD5:	5f400bae896422..
SHA1:	e90b7c431d34b3..
SHA256:	d5de496be1535d.
Tags:	agenttesla exe
Infos:	



Detection



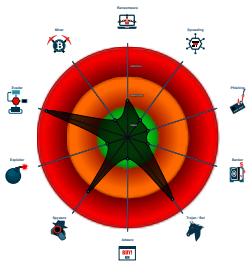
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- .NET source code references suspic…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader
- .NET source code contains method …

Classification



Process Tree

- **System is w10x64**
- SWIFT copy.29112022.Pdf.exe (PID: 5752 cmdline: C:\Users\user\Desktop\SWIFT copy.29112022.Pdf.exe MD5: 5F400BAE896422A69DB460A4507FD657)
  - SWIFT copy.29112022.Pdf.exe (PID: 6072 cmdline: C:\Users\user\Desktop\SWIFT copy.29112022.Pdf.exe MD5: 5F400BAE896422A69DB460A4507FD657)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "humhum@nutiribio.com",
  "Password": "zGNVO(l5",
  "Host": "smtp.nutiribio.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.269625557.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000000.269625557.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000000.269625557.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x306fa:$a3: MailAccountConfiguration • 0x30713:$a5: SmtpAccountConfiguration • 0x306da:$a8: set_BindingAccountConfiguration • 0x2f670:$a11: get_securityProfile • 0x2f511:$a12: get_useSeparateFolderTree • 0x30e6c:$a13: get_DnsResolver • 0x2f920:$a14: get_archivingScope • 0x2f748:$a15: get_providerName • 0x31e33:$a17: get_priority • 0x3140a:$a18: get_advancedParameters • 0x30814:$a19: get_disabledByRestriction • 0x2f2ea:$a20: get_LastAccessed • 0x2f9ba:$a21: get_avatarType • 0x31521:$a22: get_signaturePresets • 0x2ffb9:$a23: get_enableLog • 0x2f7c5:$a26: set_accountName • 0x3196c:$a27: set_InternalServerPort • 0x2ec84:$a28: set_bindingConfigurationUID • 0x314e7:$a29: set_IdnAddress • 0x31ce7:$a30: set_GuidMasterKey • 0x2f820:$a31: set_username
00000000.00000002.276283014.0000000004061000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.276283014.0000000004061000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SWIFT copy.29112022.Pdf.exe.4724888.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SWIFT copy.29112022.Pdf.exe.4724888.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.SWIFT copy.29112022.Pdf.exe.4724888.12.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x2e5b5:$s1: get_kbok • 0x2eef8:$s2: get_CHoo • 0x2fb52:$s3: set_passwordIsSet • 0x2e3b9:$s4: get_enableLog • 0x32a28:$s8: torbrowser • 0x31404:$s10: logins • 0x30d7c:$s11: credential • 0x2d7d5:$g1: get_Clipboard • 0x2d7e3:$g2: get_Keyboard • 0x2d7f0:$g3: get_Password • 0x2ed97:$g4: get_CtrlKeyDown • 0x2eda7:$g5: get_ShiftKeyDown • 0x2edb8:$g6: get_AltKeyDown
0.2.SWIFT copy.29112022.Pdf.exe.4724888.12.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2eafa:$a3: MailAccountConfiguration • 0x2eb13:$a5: SmtpAccountConfiguration • 0x2eada:$a8: set_BindingAccountConfiguration • 0x2da70:$a11: get_securityProfile • 0x2d911:$a12: get_useSeparateFolderTree • 0x2f26c:$a13: get_DnsResolver • 0x2dd20:$a14: get_archivingScope • 0x2db48:$a15: get_providerName • 0x30233:$a17: get_priority • 0x2f80a:$a18: get_advancedParameters • 0x2ec14:$a19: get_disabledByRestriction • 0x2d6ea:$a20: get_LastAccessed • 0x2ddba:$a21: get_avatarType • 0x2f921:$a22: get_signaturePresets • 0x2e3b9:$a23: get_enableLog • 0x2dbc5:$a26: set_accountName • 0x2fd6c:$a27: set_InternalServerPort • 0x2d084:$a28: set_bindingConfigurationUID • 0x2f8e7:$a29: set_IdnAddress • 0x300e7:$a30: set_GuidMasterKey • 0x2dc20:$a31: set_username
0.2.SWIFT copy.29112022.Pdf.exe.4724888.12.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 23 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains method to dynamically call methods (often used by packers)

Malware Analysis System Evasion

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

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)

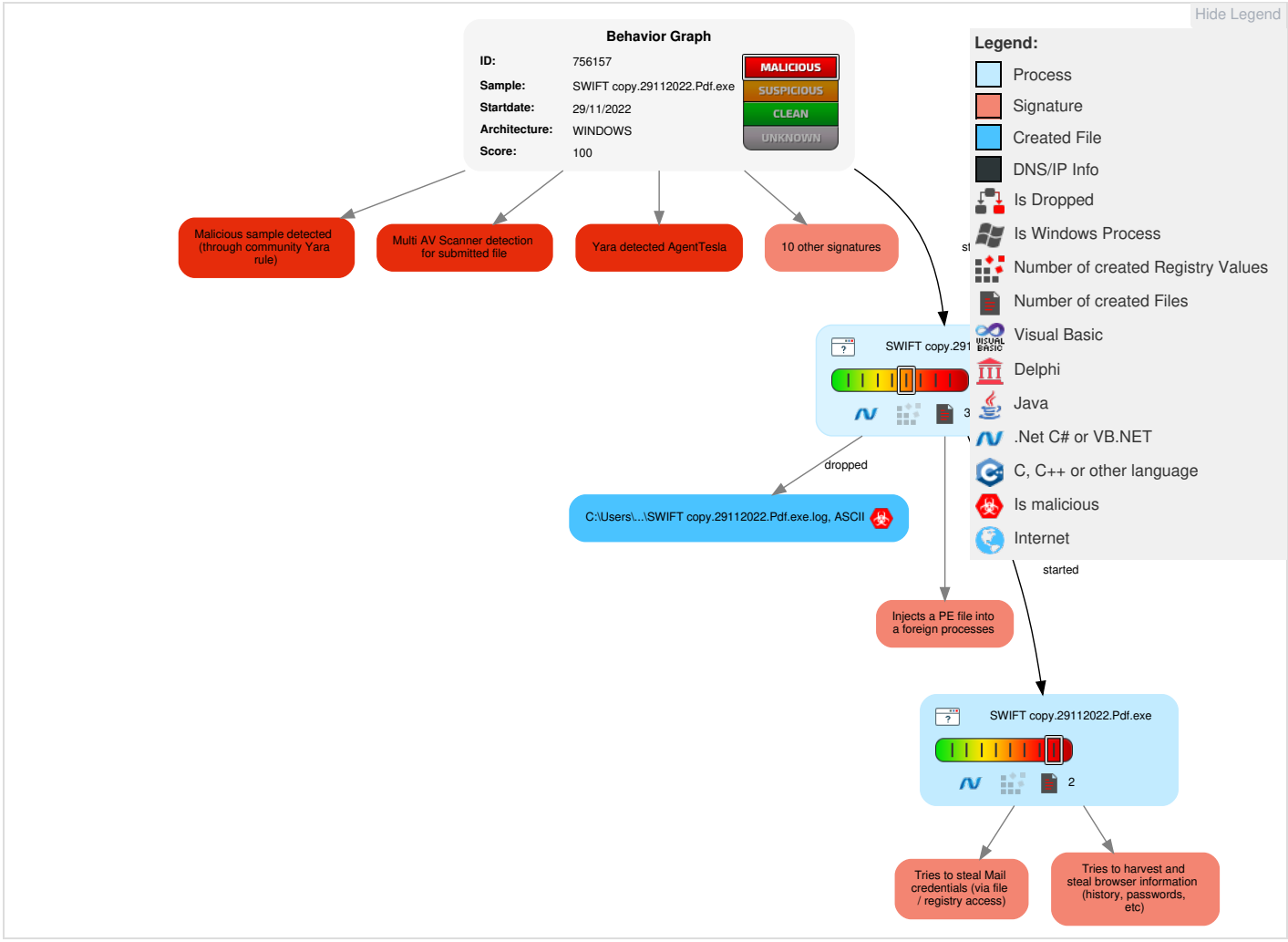
Remote Access Functionality

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 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	1 Native API	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 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 Account 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	1 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	1 3 Software Packing	DCSync	1 1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Timestomp	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

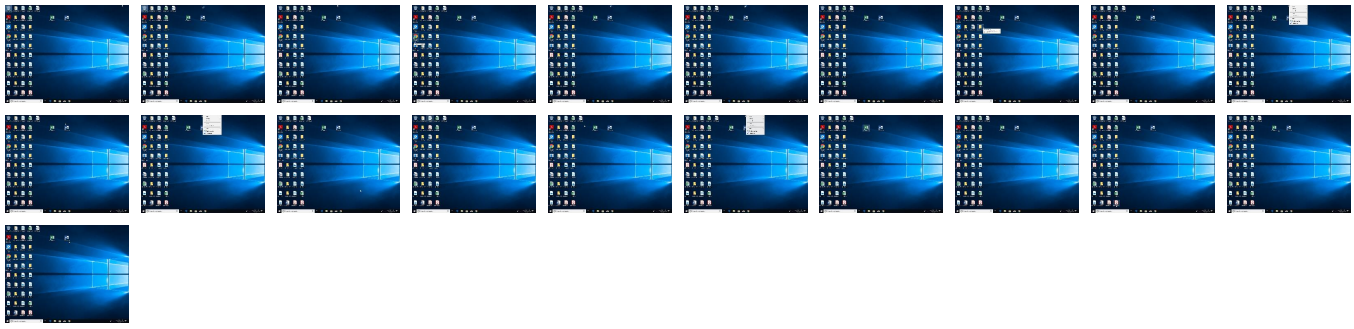
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SWIFT copy.29112022.Pdf.exe	73%	ReversingLabs	Win32.Trojan.Leoncem	
SWIFT copy.29112022.Pdf.exe	30%	Virustotal		Browse
SWIFT copy.29112022.Pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.SWIFT copy.29112022.Pdf.exe.400000.0.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.sakkal.comrm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Verd	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.fontbureau.comas	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	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.carterandcone.comtig	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.carterandcone.comf	0%	URL Reputation	safe	
http://www.fontbureau.comcoma	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.fonts.comjat	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.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.fontbureau.comionF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comams	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/?9g	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://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnf	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comsiva	0%	URL Reputation	safe	
http://www.carterandcone.comexc	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comL.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Xx	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/i9	0%	Avira URL Cloud	safe	
http://www.sakkal.comf	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/i9	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/M95	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0nf9	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/W8	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/t9	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comegr	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/M95	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.agfamonotype.A	0%	Avira URL Cloud	safe	
http://www.carterandcone.comont	0%	Avira URL Cloud	safe	
http://MBStZn.com	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comria	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn=	0%	Avira URL Cloud	safe	
http://www.carterandcone.comsig	0%	Avira URL Cloud	safe	
http://www.carterandcone.comcin	0%	Avira URL Cloud	safe	
http://www.monotype.UC	0%	Avira URL Cloud	safe	
http://www.carterandcone.comits	0%	Avira URL Cloud	safe	
http://www.fontbureau.comW8	0%	Avira URL Cloud	safe	
http://www.carterandcone.comw.m	0%	Avira URL Cloud	safe	
http://www.founder.ce	0%	Avira URL Cloud	safe	
http://www.fontbureau.comttoF	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmQ	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comu	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comalv	0%	Avira URL Cloud	safe	
http://www.tiro.comicf	0%	Avira URL Cloud	safe	
http://www.fontbureau.comf9	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comof	0%	Avira URL Cloud	safe	
http://www.fontbureau.comM95	0%	Avira URL Cloud	safe	
http://www.fonts.comw.m	0%	Avira URL Cloud	safe	
http://www.carterandcone.comce	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/ei	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 copy.29112022.Pdf.exe, 00000001.00000002.520553295.0000000003151000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sakkal.comrm	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255282999.0000000006114000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255224533.0000000006113000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comjat	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.251323429.00000000060EB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.258138745.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.259693042.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.265884768.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.257911788.0000000006104000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Xx	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254634935.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254794551.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254595717.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254860385.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254538096.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Verd	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254634935.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254794551.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254595717.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254429222.00000000060DA000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254860385.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254538096.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250782932.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250927671.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250846587.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250578869.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250629587.00000000060EB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comas	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.271326038.00000000060D6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/i9	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254794551.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254860385.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersers	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.258022793.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.258138745.0000000006104000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/?9g	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254634935.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254794551.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255290205.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254595717.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255391228.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254429222.00000000060DA000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255232174.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254860385.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254538096.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255439619.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255536119.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255031466.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255607455.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255481061.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255099459.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.comf	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255401180.00000000060E6000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255308698.00000000060E6000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255250069.00000000060E6000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/i9	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254634935.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254634935.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254595717.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255262809.0000000006101000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255202145.0000000006101000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253689927.0000000006103000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com.TTF	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.260416887.00000000060DB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.259471570.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	SWIFT copy.29112022.Pdf.exe, 00000001.00000002.521371650.00000000031F2000.00000004.00000800.00020000.00000000.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 copy.29112022.Pdf.exe, 00000000.00000002.287383086.00000000046ED000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000001.00000000.269625557.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comtig	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255750448.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255693586.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253933848.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255516044.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.256346314.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255262809.0000000006101000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.256544652.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255635634.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254256532.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255461197.0000000006101000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254664468.0000000006101000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253917497.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253857719.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254357438.0000000006101000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254029297.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255970374.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255202145.0000000006101000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255320276.0000000006101000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254571950.0000000006108000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254070990.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.256649188.0000000006104000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/M95	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.261645746.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.261742667.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Y0nf9	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254634935.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254794551.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254860385.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.261645746.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.261742667.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/t9	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254634935.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254794551.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254595717.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254429222.00000000060DA000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254860385.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254538096.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255031466.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255099459.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comf	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253857719.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253819477.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253804133.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253836809.0000000006105000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcoma	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.260416887.00000000060DB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comd	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253857719.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253819477.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253836809.0000000006105000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comegr	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250782932.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250578869.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250629587.00000000060EB000.00000004.00000800.00020000.00000000.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 copy.29112022.Pdf.exe, 00000001.00000002.520553295.0000000003151000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/W8	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254794551.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254860385.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255031466.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255099459.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/M95	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254794551.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255290205.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255391228.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255232174.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254860385.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255439619.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255031466.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255099459.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254029297.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254070990.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254099387.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253979663.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253997155.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254013548.0000000006105000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253482553.0000000006103000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comont	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254070990.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254099387.0000000006104000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.agfamonotype.A	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.257939001.0000000006113000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://MBStZn.com	SWIFT copy.29112022.Pdf.exe, 00000001.00000002.520553295.0000000003151000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comria	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250629587.00000000060EB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comionF	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.271326038.00000000060D6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comsig	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253933848.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253917497.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253857719.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254029297.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254070990.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254099387.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253979663.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253819477.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253997155.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253997155.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254013548.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253897098.0000000006104000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn=	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253689927.0000000006103000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html/	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.259471570.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comcin	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254029297.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253997155.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254013548.0000000006105000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comams	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253933848.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255262809.0000000006101000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254256532.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254664468.0000000006101000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253917497.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253857719.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254357438.0000000006101000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254029297.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255202145.0000000006101000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254571950.0000000006108000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254070990.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255068805.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254099387.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253979663.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254516942.0000000006103000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254933421.0000000006108000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254150676.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254821011.0000000006108000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254466136.0000000006101000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254991909.0000000006101000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253997155.0000000006105000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com//w	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.251283967.00000000060EB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.monotype.UC	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.261855251.00000000060E2000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.261539461.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.262337254.00000000060E2000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.261656122.00000000060E2000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.262264309.00000000060E2000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comW8	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.260416887.00000000060DB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersZ	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.257433913.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.257374815.0000000006104000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253897098.0000000006104000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersh	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.258710516.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.258780346.0000000006104000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htm	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.261855251.00000000060E2000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.262337254.00000000060E2000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.261656122.00000000060E2000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.262264309.00000000060E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comw.m	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254256532.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254029297.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254070990.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254099387.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254150676.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254013548.0000000006105000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comits	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253933848.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253917497.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254029297.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253979663.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253997155.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254013548.0000000006105000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerse	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.265995122.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.266070435.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.265884768.0000000006104000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.ce	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253405708.0000000006103000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	SWIFT copy.29112022.Pdf.exe, 00000001.00000002.520553295.0000000003151000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.fontbureau.com/designersv	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.259946306.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.259985359.0000000006105000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comttoF	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.260416887.00000000060DB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnf	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253366138.0000000006103000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253347704.0000000006103000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmQ	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.261586821.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.261709013.0000000006104000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.261757335.0000000006104000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comsiva	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.260416887.00000000060DB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253632184.00000000060EA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comexc	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253857719.0000000006105000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNS	SWIFT copy.29112022.Pdf.exe, 00000001.00000002.520553295.0000000003151000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comF	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.260416887.00000000060DB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comu	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250782932.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250927671.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250846587.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250963346.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250995609.00000000060EB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comf9	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.260416887.00000000060DB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.comicf	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254124405.00000000060E6000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comL.TTF	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.260416887.00000000060DB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.259471570.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.259380642.00000000060DB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255099459.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.259471570.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.259380642.00000000060DB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.260416887.00000000060DB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.259471570.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.259380642.00000000060DB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comalv	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250578869.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250629587.00000000060EB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comof	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250782932.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250927671.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.251160398.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250846587.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250963346.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250995609.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.251206432.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.251041022.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.250629587.00000000060EB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253357265.00000000060EA000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.259471570.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254538096.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255439619.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255536119.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255031466.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255607455.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255481061.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255829393.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255099459.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.255925563.00000000060DD000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.256145848.00000000060DD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comw.m	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.251323429.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.251406146.00000000060EB000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.251283967.00000000060EB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.como	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.271326038.00000000060D6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SWIFT copy.29112022.Pdf.exe, 00000000.00000002.290363546.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comM95	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.271326038.00000000060D6000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comce	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253933848.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253917497.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254029297.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253979663.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253997155.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.254013548.0000000006105000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253897098.0000000006104000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/ei	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.253482553.0000000006103000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/	SWIFT copy.29112022.Pdf.exe, 00000000.00000003.257560437.0000000006112000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.257499785.0000000006113000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.257336197.0000000006113000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.257812332.0000000006113000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.257867723.0000000006113000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.257765651.0000000006113000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.257891265.0000000006112000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.257388371.0000000006112000.00000004.00000800.00020000.00000000.sdmp, SWIFT copy.29112022.Pdf.exe, 00000000.00000003.257305464.0000000006104000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756157
Start date and time:	2022-11-29 18:24:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SWIFT copy.29112022.Pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
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: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information

- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:25:10	API Interceptor	708x Sleep call for process: SWIFT copy.29112022.Pdf.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 copy.29112022.Pdf.exe.log

Process:	C:\Users\user\Desktop\SWIFT copy.29112022.Pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
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):	7.8190439753914545
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 copy.29112022.Pdf.exe
File size:	763392
MD5:	5f400bae896422a69db460a4507fd657
SHA1:	e90b7c431d34b39bef8492de7fb987f51c3fb804
SHA256:	d5de496be1535d0b8d9c8f57087e9ae2a26aaf7c33c2ddca65b3231dc3b2460b
SHA512:	7e54192c570d2a7fe7700d69bd782173dfe41dc102afceffbda47207d4bfcb80783f7c70bf9666e287ccbcf413bf482aeb321fe559ba7b75ae43416b0feee643
SSDEEP:	12288:ZYn2P8Ai1FDasqS6/0kz0z63eR7J/ZmhOQQVvedp:qn20t1Ffl+0kzAttq62
TLSH:	83F4F1BEF2EA8F12C69415F2C0D2DE3403F69683A976E75B294102D94E437E18CD67C6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...d.....0.....>.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4bbb3e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xCCE2C364 [Sun Dec 4 21:00:20 2078 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0xbbaf0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x5b8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbe000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xbbaa7	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	0xb9b44	0xb9c00	False	0.899130162769179	data	7.826301761256588	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x5b8	0x600	False	0.4283854166666667	data	4.110542837134713	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xbe000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xbc0a0	0x32c	data		
RT_MANIFEST	0xbc3cc	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

No network behavior found

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SWIFT copy.29112022.Pdf.exe PID: 5752, Parent PID: 3452

General

Target ID:	0
Start time:	18:25:00
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SWIFT copy.29112022.Pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SWIFT copy.29112022.Pdf.exe
Imagebase:	0xc50000
File size:	763392 bytes

MD5 hash:	5F400BAE896422A69DB460A4507FD657
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: 00000000.00000002.276283014.0000000004061000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.276283014.0000000004061000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.276283014.0000000004061000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.274800625.00000000032D6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.287383086.00000000046ED000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.287383086.00000000046ED000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.287383086.00000000046ED000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D19CF06	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	6D19CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SWIFT copy.29112022.Pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4AC78D	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 copy.29112022.Pdf.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",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	6D4AC907	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	6D175705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D175705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D17CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFE1B4F	ReadFile

Analysis Process: SWIFT copy.29112022.Pdf.exe PID: **6072**, Parent PID: **5752**

General

Target ID:	1
Start time:	18:25:11
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SWIFT copy.29112022.Pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SWIFT copy.29112022.Pdf.exe
Imagebase:	0xd00000
File size:	763392 bytes
MD5 hash:	5F400BAE896422A69DB460A4507FD657
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: 00000001.00000000.269625557.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.269625557.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000000.269625557.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.521412516.00000000031FA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.520553295.0000000003151000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.520553295.0000000003151000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000001.00000002.520553295.0000000003151000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
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	6D19CF06	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	6D19CF06	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	6D175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D175705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D17CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFE1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6BFE1B4F	ReadFile

Disassembly

No disassembly