ID: 635167
Sample Name: SWIFT,pdf.exe
Cookbook: default.jbs
Time: 16:16:09
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

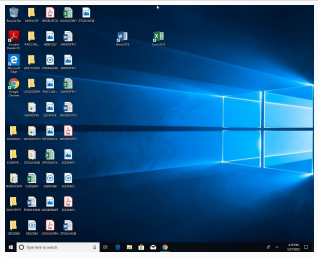
Windows Analysis Report

SWIFT,pdf.exe

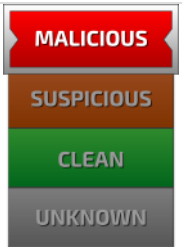
Overview

General Information

Sample Name:	SWIFT,pdf.exe
Analysis ID:	635167
MD5:	01844ea0e93a3c..
SHA1:	80e590ab91b859.
SHA256:	0605d3622a953e.
Tags:	agenttesla exe
Infos:	



Detection



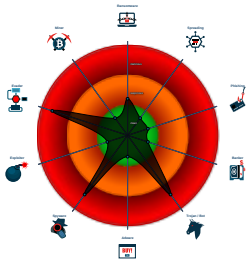
AgentTesla

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
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…

Classification



Process Tree

- **System is w10x64**
- SWIFT,pdf.exe (PID: 480 cmdline: "C:\Users\user\Desktop\SWIFT,pdf.exe" MD5: 01844EA0E93A3C408E3D37C577723B85)
  - BackgroundTransferHost.exe (PID: 1428 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: 02BA81746B929ECC9DB6665589B68335)
  - SWIFT,pdf.exe (PID: 1428 cmdline: C:\Users\user\Desktop\SWIFT,pdf.exe MD5: 01844EA0E93A3C408E3D37C577723B85)
  - SWIFT,pdf.exe (PID: 4956 cmdline: C:\Users\user\Desktop\SWIFT,pdf.exe MD5: 01844EA0E93A3C408E3D37C577723B85)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "sandra.vasic@pickerr.com",
  "Password": "L@ur@24Filip04",
  "Host": "mail.your-server.de"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.292324885.000000000286F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000000.288508913.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.288508913.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.501638862.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.501638862.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.SWIFT,pdf.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.SWIFT,pdf.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.0.SWIFT,pdf.exe.400000.6.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32b92:$s10: logins • 0x325f9:$s11: credential • 0x2ebc4:$g1: get_Clipboard • 0x2ebd2:$g2: get_Keyboard • 0x2ebdf:$g3: get_Password • 0x2fede:$g4: get_CtrlKeyDown • 0x2feee:$g5: get_ShiftKeyDown • 0x2feff:$g6: get_AltKeyDown
5.2.SWIFT,pdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.SWIFT,pdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 32 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.4 - Destination IP: 78.46.5.205

Timestamp:	192.168.2.478.46.5.205497635872030171 05/27/22-16:17:51.099555
SID:	2030171
Source Port:	49763
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.4 - Destination IP: 78.46.5.205

Timestamp:	192.168.2.478.46.5.205497635872840032 05/27/22-16:17:51.099661
SID:	2840032
Source Port:	49763
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection

Moves itself to temp directory

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

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 Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

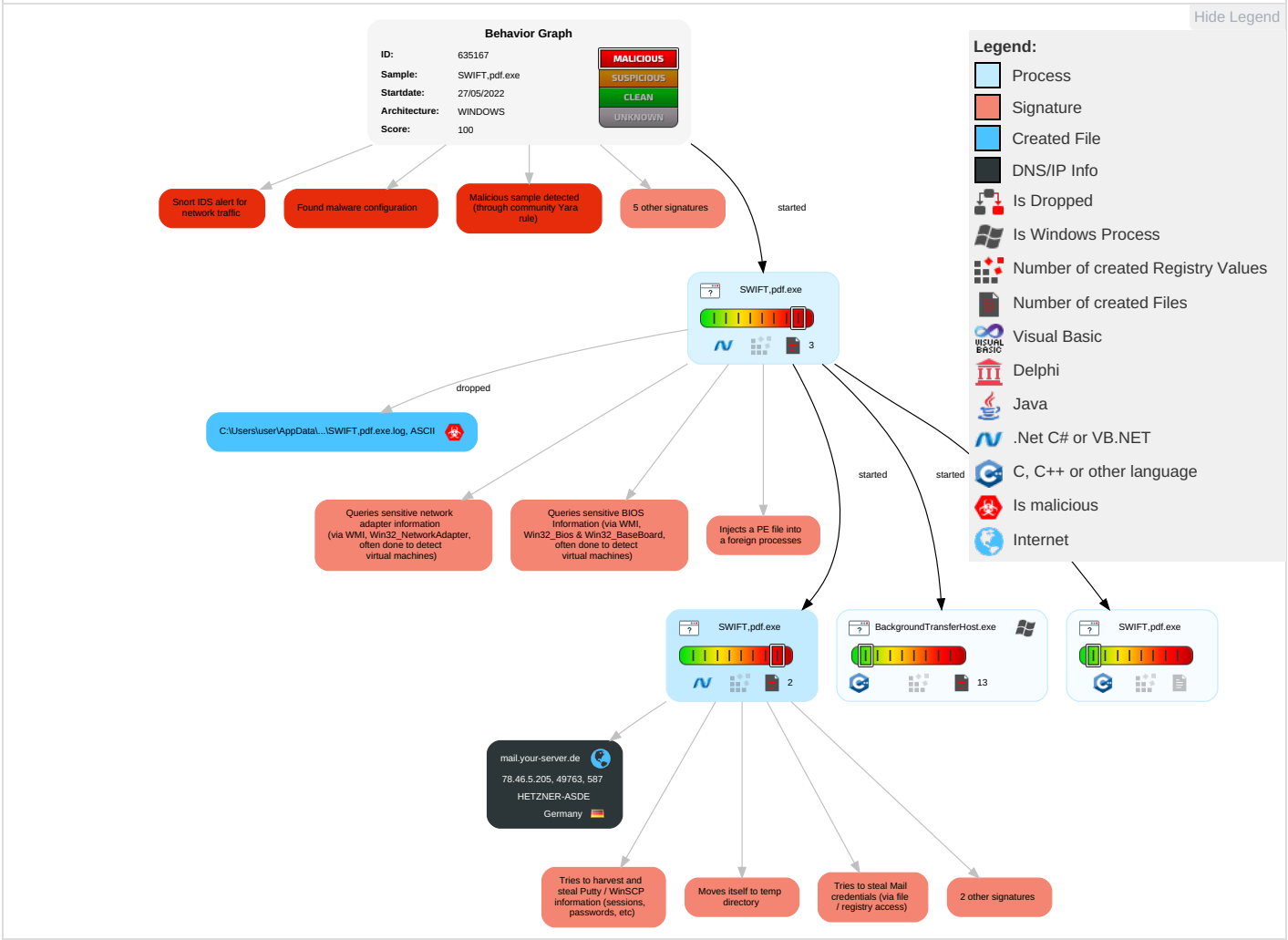
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 1 Masquerading	2 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	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	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,pdf.exe	46%	Virustotal		Browse
SWIFT,pdf.exe	24%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.SWIFT,pdf.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.SWIFT,pdf.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.SWIFT,pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.SWIFT,pdf.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.SWIFT,pdf.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.SWIFT,pdf.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.sakkal.comnlE	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnv-s	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdiaF	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/7	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.commx	0%	Avira URL Cloud	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	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.jiyu-kobo.co.jp/jp/N	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.fontbureau.com7	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comE	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnkM&	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.founder.com.cn/cnh-cp	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.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://RuEJKW.com	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comitu	0%	URL Reputation	safe	
http://www.fontbureau.comtuedN	0%	Avira URL Cloud	safe	
http://ar78QkSNCRu5mqvP5Vd.org	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/a	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.your-server.de	78.46.5.205	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SWIFT,pdf.exe, 00000005.00000002.5042750 24.0000000002F71000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://github.com/dcoetzee/plants-vs-zombies-user-file-editor	SWIFT,pdf.exe	false		high
http://www.sakkal.comnlE	SWIFT,pdf.exe, 00000000.00000003.2502764 00.00000000057ED000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.250710433.00000000057ED00 0.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.250529607.000 00000057ED000.00000004.00000800.00020000 .00000000.sdmp, SWIFT,pdf.exe, 00000000. 00000003.250364352.00000000057ED000.0000 0004.00000800.00020000.00000000.sdmp, SW IFT,pdf.exe, 00000000.00000003.250669943 .00000000057ED000.00000004.00000800.0002 0000.00000000.sdmp, SWIFT,pdf.exe, 00000 000.00000003.250372591.00000000057EF000. 00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.25044 1324.00000000057ED000.00000004.00000800. 00020000.00000000.sdmp, SWIFT,pdf.exe, 0 0000000.00000003.250756551.00000000057ED 000.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.250477413.0 0000000057ED000.00000004.00000800.000200 00.00000000.sdmp, SWIFT,pdf.exe, 0000000 0.00000003.250631867.00000000057ED000.00 000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://github.com	SWIFT,pdf.exe	false		high
http://www.founder.com.cn/cnv-s	SWIFT,pdf.exe, 00000000.00000003.2468125 24.00000000057B4000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.246960820.00000000057B600 0.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.247128946.000 00000057B7000.00000004.00000800.00020000 .00000000.sdmp, SWIFT,pdf.exe, 00000000. 00000003.247052636.00000000057B7000.0000 0004.00000800.00020000.00000000.sdmp, SW IFT,pdf.exe, 00000000.00000003.247089450 .00000000057B7000.00000004.00000800.0002 0000.00000000.sdmp, SWIFT,pdf.exe, 00000 000.00000003.246878944.00000000057B4000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdiaF	SWIFT,pdf.exe, 00000000.00000003.2592821 90.00000000057BC000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.259163600.00000000057B600 0.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.259541752.000 00000057BD000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SWIFT,pdf.exe, 00000000.00000003.2523806 63.00000000057ED000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.259330287.00000000057EB00 0.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.259109067.000 00000057EB000.00000004.00000800.00020000 .00000000.sdmp, SWIFT,pdf.exe, 00000000. 00000003.251876573.00000000057ED000.0000 0004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%%startupfolder%	SWIFT,pdf.exe, 00000005.00000002.5042750 24.0000000002F71000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.goodfont.co.kr	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnn	SWIFT,pdf.exe, 00000000.00000003.2468125 24.00000000057B4000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.246960820.00000000057B600 0.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.247128946.000 00000057B7000.00000004.00000800.00020000 .00000000.sdmp, SWIFT,pdf.exe, 00000000. 00000003.247052636.00000000057B7000.0000 0004.00000800.00020000.00000000.sdmp, SW IFT,pdf.exe, 00000000.00000003.247089450 .00000000057B7000.00000004.00000800.0002 0000.00000000.sdmp, SWIFT,pdf.exe, 00000 000.00000003.246878944.00000000057B4000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/7	SWIFT,pdf.exe, 00000000.00000003.2501235 68.00000000057BB000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.250050537.00000000057BB00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrita	SWIFT,pdf.exe, 00000000.00000002.2981397 24.00000000057B0000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.259282190.00000000057BC00 0.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.259671144.000 00000057BB000.00000004.00000800.00020000 .00000000.sdmp, SWIFT,pdf.exe, 00000000. 00000003.259163600.00000000057B6000.0000 0004.00000800.00020000.00000000.sdmp, SW IFT,pdf.exe, 00000000.00000003.259541752 .00000000057BD000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersers	SWIFT,pdf.exe, 00000000.00000003.2538783 91.00000000057ED000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.commx	SWIFT,pdf.exe, 00000000.00000002.2981397 24.00000000057B0000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.259282190.00000000057BC00 0.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.259671144.000 00000057BB000.00000004.00000800.00020000 .00000000.sdmp, SWIFT,pdf.exe, 00000000. 00000003.259163600.00000000057B6000.0000 0004.00000800.00020000.00000000.sdmp, SW IFT,pdf.exe, 00000000.00000003.259541752 .00000000057BD000.00000004.00000800.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comB.TTF	SWIFT,pdf.exe, 00000000.00000003.2545394 22.00000000057BC000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//	SWIFT,pdf.exe, 00000000.00000003.2501235 68.00000000057BB000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.250050537.00000000057BB00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designerse	SWIFT,pdf.exe, 00000000.00000002.2982602 32.00000000057EB000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.259518641.00000000057EB00 0.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.259142205.000 00000057EB000.00000004.00000800.00020000 .00000000.sdmp, SWIFT,pdf.exe, 00000000. 00000003.259330287.00000000057EB000.0000 0004.00000800.00020000.00000000.sdmp, SW IFT,pdf.exe, 00000000.00000003.259109067 .00000000057EB000.00000004.00000800.0002 0000.00000000.sdmp, SWIFT,pdf.exe, 00000 000.00000003.259572889.00000000057E3000. 00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.25187 6573.00000000057ED000.00000004.00000800. 00020000.00000000.sdmp, SWIFT,pdf.exe, 0 0000000.00000003.259652752.00000000057EB 000.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.259617196.0 0000000057E9000.00000004.00000800.000200 00.00000000.sdmp	false		high
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	SWIFT,pdf.exe, 00000005.00000002.5042750 24.0000000002F71000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	SWIFT,pdf.exe, 00000000.00000003.2502848 96.00000000057BC000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.250123568.00000000057BB00 0.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.250050537.000 00000057BB000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/N	SWIFT,pdf.exe, 00000000.00000003.2501235 68.00000000057BB000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.250050537.00000000057BB00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com7	SWIFT,pdf.exe, 00000000.00000003.2545394 22.00000000057BC000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org%	SWIFT,pdf.exe, 00000005.00000002.5042750 24.0000000002F71000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.apache.org/licenses/LICENSE-2.0	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.fontbureau.com	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.254539422.00000000057BC00 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	SWIFT,pdf.exe, 00000000.00000003.2567903 18.00000000057BB000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comE	SWIFT,pdf.exe, 00000000.00000003.2545394 22.00000000057BC000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnkM&	SWIFT,pdf.exe, 00000000.00000003.2468125 24.00000000057B4000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.246960820.00000000057B600 0.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.247128946.000 00000057B7000.00000004.00000800.00020000 .00000000.sdmp, SWIFT,pdf.exe, 00000000. 00000003.247052636.00000000057B7000.0000 0004.00000800.00020000.00000000.sdmp, SW IFT,pdf.exe, 00000000.00000003.247089450 .00000000057B7000.00000004.00000800.0002 0000.00000000.sdmp, SWIFT,pdf.exe, 00000 000.00000003.246878944.00000000057B4000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.your-server.de	SWIFT,pdf.exe, 00000005.00000002.5073365 43.00000000032CF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	SWIFT,pdf.exe, 00000005.00000002.5042750 24.0000000002F71000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnh-cp	SWIFT,pdf.exe, 00000000.00000003.2468125 24.00000000057B4000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.246960820.00000000057B600 0.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.247128946.000 00000057B7000.00000004.00000800.00020000 .00000000.sdmp, SWIFT,pdf.exe, 00000000. 00000003.247052636.00000000057B7000.0000 0004.00000800.00020000.00000000.sdmp, SW IFT,pdf.exe, 00000000.00000003.247089450 .00000000057B7000.00000004.00000800.0002 0000.00000000.sdmp, SWIFT,pdf.exe, 00000 000.00000003.246878944.00000000057B4000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	SWIFT,pdf.exe, 00000000.00000003.2502848 96.00000000057BC000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.250123568.00000000057BB00 0.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.250050537.000 00000057BB000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	SWIFT,pdf.exe, 00000000.00000003.2592821 90.00000000057BC000.00000004.00000800.00 020000.00000000.sdmp, SWIFT,pdf.exe, 000 00000.00000003.259671144.00000000057BB00 0.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.259163600.000 00000057B6000.00000004.00000800.00020000 .00000000.sdmp, SWIFT,pdf.exe, 00000000. 00000003.259541752.00000000057BD000.0000 0004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SWIFT,pdf.exe, 00000000.00000002.2990322 19.0000000006A42000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	SWIFT,pdf.exe, 00000000.00000003.246812524.00000000057B4000.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.246960820.00000000057B6000.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.247128946.00000000057B7000.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.247052636.00000000057B7000.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000002.299032219.0000000006A42000.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.247089450.00000000057B7000.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.246878944.00000000057B4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	SWIFT,pdf.exe, 00000000.00000003.252967761.00000000057ED000.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000002.299032219.0000000006A42000.00000004.00000800.00020000.00000000.sdmp	false		high
http://RuEJKW.com	SWIFT,pdf.exe, 00000005.00000002.504275024.0000000002F71000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	SWIFT,pdf.exe, 00000000.00000002.291715681.0000000000F77000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	SWIFT,pdf.exe, 00000000.00000003.250050537.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SWIFT,pdf.exe, 00000000.00000002.299032219.0000000006A42000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comitu	SWIFT,pdf.exe, 00000000.00000003.254539422.00000000057BC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comtuedN	SWIFT,pdf.exe, 00000000.00000003.254539422.00000000057BC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ar78QkSNCRu5mqvP5Vd.org	SWIFT,pdf.exe, 00000005.00000002.507141679.00000000032C5000.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000005.00000002.504275024.0000000002F7100.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000005.00000002.507466470.00000000032DC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/a	SWIFT,pdf.exe, 00000000.00000003.250284896.00000000057BC000.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.250123568.00000000057BB000.00000004.00000800.00020000.00000000.sdmp, SWIFT,pdf.exe, 00000000.00000003.250050537.00000000057BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
78.46.5.205	mail.your-server.de	Germany		24940	HETZNER-ASDE	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635167
Start date and time: 27/05/202216:16:09	2022-05-27 16:16:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SWIFT,pdf.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:	26
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@6/1@1/1
EGA Information:	• Successful, ratio: 33.3%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0

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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target SWIFT,pdf.exe, PID 1428 because there are no exe cuted function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:17:27	API Interceptor	635x Sleep call for process: SWIFT,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,pdf.exe.log

Process:	C:\Users\user\Desktop\SWIFT,pdf.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):	7.820224390379348
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,pdf.exe
File size:	749056
MD5:	01844ea0e93a3c408e3d37c577723b85
SHA1:	80e590ab91b85948fc890a1726ca529de30c9a3c
SHA256:	0605d3622a953ea5b976b34f80e5fd3704c6937644cb6fb11a88351aaf0d110c
SHA512:	5c690b8492f5dd8211b5f9c2883782d7aee9db8fa1e4eab715a1c0582b3a4df73d69a0b90193e5ea7613759635109fe7fb064dfd9967ee0dbb22730830e03c3b
SSDEEP:	12288:uxdZ9bHoAU/vqVGy3hfiZsRxINqlraIWSA8xTR8YWKfUJlRqyn7dXjg/t:ux5bHo5y3hwixlraIWojcwynJ+t
TLSH:	C5F4F180707A4863C2AC15F941A1F5801BBC9D276D1DE1C76CC279CFB8E6F898ACE957
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....Z.....1... ...@....@.. .....@.....

File Icon

Icon Hash:	4462f276dcec30e6

Static PE Info

General

Entrypoint:	0x4b31d2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x629018AA [Fri May 27 00:17:46 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb3178	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb4000	0x5788	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xba000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb11d8	0xb1200	False	0.886924124471	data	7.82024778382	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb4000	0x5788	0x5800	False	0.964533025568	data	7.90382013915	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xba000	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	0xb4130	0x51a3	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xb92d4	0x14	data		
RT_VERSION	0xb92e8	0x2ec	data		
RT_MANIFEST	0xb95d4	0x1b4	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

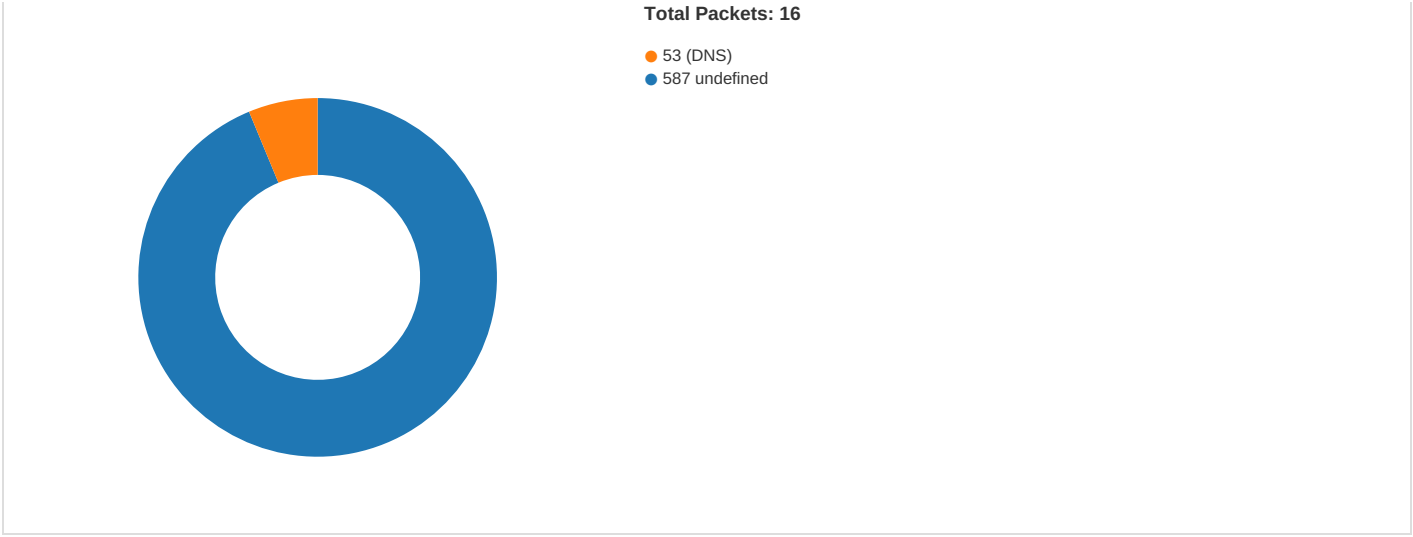
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	1.0.0.0
InternalName	ImageFileMach.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	ImageFileMach.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.478.46.5.205497635872030171 05/27/22-16:17:51.099555	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49763	587	192.168.2.4	78.46.5.205
192.168.2.478.46.5.205497635872840032 05/27/22-16:17:51.099661	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49763	587	192.168.2.4	78.46.5.205

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 16:17:49.427047014 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:49.448726892 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:49.448837996 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:49.472358942 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:49.535193920 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:50.351075888 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:50.373107910 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:50.431512117 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:50.453226089 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:50.535346985 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:50.912290096 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:50.976419926 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:50.984155893 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:50.995080948 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:51.019408941 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:51.054641008 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:51.076780081 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:51.077076912 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:51.098633051 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:51.098654985 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:51.099555016 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:51.099661112 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:51.100368977 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:51.100446939 CEST	49763	587	192.168.2.4	78.46.5.205
May 27, 2022 16:17:51.120975018 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:51.121015072 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:51.121656895 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:51.121726036 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:51.123563051 CEST	587	49763	78.46.5.205	192.168.2.4
May 27, 2022 16:17:51.222820997 CEST	49763	587	192.168.2.4	78.46.5.205

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 16:17:49.336064100 CEST	64277	53	192.168.2.4	8.8.8.8
May 27, 2022 16:17:49.354921103 CEST	53	64277	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 16:17:49.336064100 CEST	192.168.2.4	8.8.8.8	0x953f	Standard query (0)	mail.your-server.de	A (IP address)	IN (0x0001)

DNS Answers

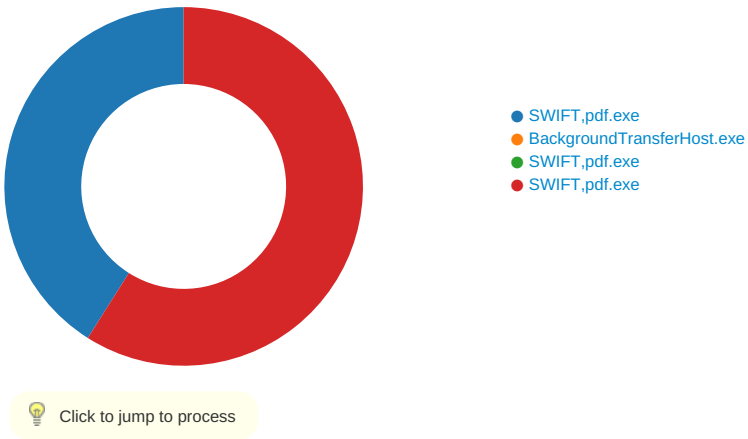
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 16:17:49.354921103 CEST	8.8.8.8	192.168.2.4	0x953f	No error (0)	mail.your-server.de		78.46.5.205	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 27, 2022 16:17:49.472358942 CEST	587	49763	78.46.5.205	192.168.2.4	220 sslproxy02.your-server.de Exim ESMTP Service ready
May 27, 2022 16:17:50.351075888 CEST	49763	587	192.168.2.4	78.46.5.205	EHLO 376483
May 27, 2022 16:17:50.373107910 CEST	587	49763	78.46.5.205	192.168.2.4	250-sslproxy02.your-server.de Hello 376483 [102.129.143.42] 250-SIZE 104857600 250-8BITMIME 250-ETRN 250-PIPELINING 250-AUTH LOGIN PLAIN 250-CHUNKING 250-STARTTLS 250 HELP
May 27, 2022 16:17:50.431512117 CEST	49763	587	192.168.2.4	78.46.5.205	AUTH login c2FuZHJhLnZhc2ljQHBpY2tlcnIuY29t
May 27, 2022 16:17:50.453226089 CEST	587	49763	78.46.5.205	192.168.2.4	334 UGFzc3dvcmQ6
May 27, 2022 16:17:50.984155893 CEST	587	49763	78.46.5.205	192.168.2.4	235 Authentication succeeded
May 27, 2022 16:17:50.995080948 CEST	49763	587	192.168.2.4	78.46.5.205	MAIL FROM:<sandra.vasic@pickerr.com>
May 27, 2022 16:17:51.019408941 CEST	587	49763	78.46.5.205	192.168.2.4	250 OK
May 27, 2022 16:17:51.054641008 CEST	49763	587	192.168.2.4	78.46.5.205	RCPT TO:<ceo-speedbs@dr.com>
May 27, 2022 16:17:51.076780081 CEST	587	49763	78.46.5.205	192.168.2.4	250 Accepted
May 27, 2022 16:17:51.077076912 CEST	49763	587	192.168.2.4	78.46.5.205	DATA
May 27, 2022 16:17:51.098654985 CEST	587	49763	78.46.5.205	192.168.2.4	354 Enter message, ending with "." on a line by itself
May 27, 2022 16:17:51.100446939 CEST	49763	587	192.168.2.4	78.46.5.205	.
May 27, 2022 16:17:51.123563051 CEST	587	49763	78.46.5.205	192.168.2.4	250 OK id=1nuaml-000Vt8-2q

Statistics

Behavior



System Behavior

Analysis Process: SWIFT,pdf.exe PID: **480**, Parent PID: **4136**

General

Target ID:	0
Start time:	16:17:12

Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SWIFT,pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SWIFT,pdf.exe"
Imagebase:	0x350000
File size:	749056 bytes
MD5 hash:	01844EA0E93A3C408E3D37C577723B85
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.292324885.000000000286F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.292711818.0000000002984000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.295567908.0000000003A7A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.295567908.0000000003A7A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.300286578.0000000007070000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
Reputation:	low

File Activities

Analysis Process: BackgroundTransferHost.exe PID: **1428**, Parent PID: **804**

General

Target ID:	2
Start time:	16:17:18
Start date:	27/05/2022
Path:	C:\Windows\System32\BackgroundTransferHost.exe
Wow64 process (32bit):	false
Commandline:	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1
Imagebase:	0x7ff74bbf0000
File size:	36864 bytes
MD5 hash:	02BA81746B929ECC9DB6665589B68335
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: SWIFT,pdf.exe PID: **1428**, Parent PID: **480**

General

Target ID:	4
Start time:	16:17:34
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SWIFT,pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SWIFT,pdf.exe
Imagebase:	0x390000
File size:	749056 bytes
MD5 hash:	01844EA0E93A3C408E3D37C577723B85
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SWIFT,pdf.exe PID: 4956, Parent PID: 480

General

Target ID:	5
Start time:	16:17:35
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SWIFT,pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SWIFT,pdf.exe
Imagebase:	0xc40000
File size:	749056 bytes
MD5 hash:	01844EA0E93A3C408E3D37C577723B85
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: 00000005.00000000.288508913.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.288508913.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.501638862.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.501638862.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.287160504.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.287160504.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.287602943.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.287602943.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.289277501.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.289277501.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.504275024.0000000002F71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.504275024.0000000002F71000.00000004.00000800.00020000.00000000.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	6DCCCF06	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	6DCCCF06	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SWIFT,pdf.exe	C:\Users\user\AppData\Local\Temp\tmpG636.tmp	success or wait	1	6166BE2	MoveFileExW

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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\d1aef8e4-b864-479c-bf86-f42c63d352b2	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CB11B4F	ReadFile

Disassembly

No disassembly