ID: 358328
Sample Name: Swift doc. ZD.1.19022021_PDF.exe
Cookbook: default.jbs
Time: 12:19:54
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

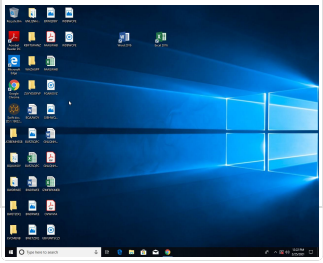
Analysis Report Swift doc. ZD.1.19022021_PDF.exe

Overview

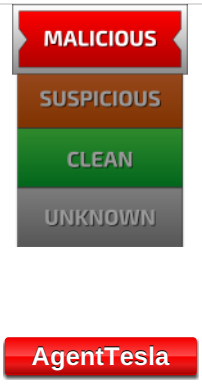
General Information

Sample Name:	Swift doc. ZD.1.19022021_PDF.exe
Analysis ID:	358328
MD5:	5679c66fd0ebcd6..
SHA1:	dbba96ad2d1c38..
SHA256:	949138db57c941..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



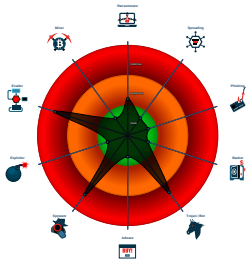
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- Swift doc. ZD.1.19022021_PDF.exe (PID: 7020 cmdline: 'C:\Users\user\Desktop\Swift doc. ZD.1.19022021_PDF.exe' MD5: 5679C66FD0EBCD6B8702C5C9E8F1ECB6)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "SYgLhOXLAKJaD",
  "URL: ": "https://T4gAxtuj18rwIFW1VRIf.com",
  "To: ": "fikriye@turuncoglu.com",
  "ByHost: ": "smtp.yandex.com:587",
  "Password: ": "EbOiB",
  "From: ": "fikriye@turuncoglu.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.922521029.000000000448B000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.923663679.00000000063E0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.917324348.000000000324 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.917324348.000000000324 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: Swift doc. ZD.1.19022021_PDF.exe PID: 7020	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 2 entries

Unpacked PEs

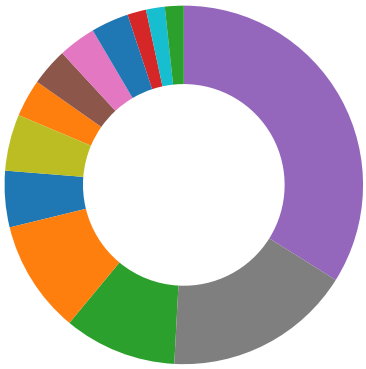
Source	Rule	Description	Author	Strings
1.2.Swift doc. ZD.1.19022021_PDF.exe.63e0000.9.raw .unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Swift doc. ZD.1.19022021_PDF.exe.44f98c0.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Swift doc. ZD.1.19022021_PDF.exe.44f98c0.5.raw .unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Swift doc. ZD.1.19022021_PDF.exe.63e0000.9.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Swift doc. ZD.1.19022021_PDF.exe.3270530.2.raw .unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Click to see the 1 entries

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

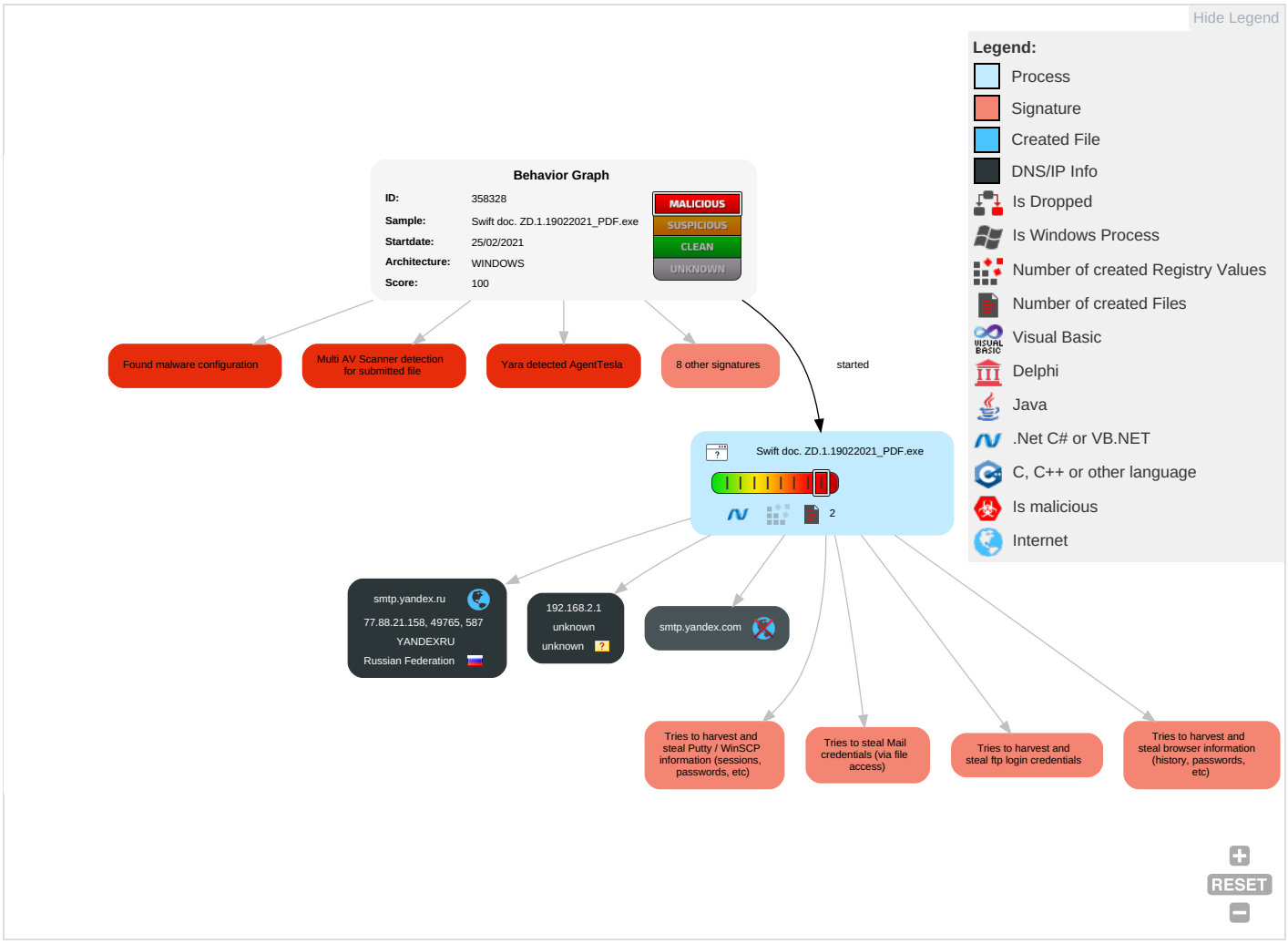
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 3	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E I N C
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	E R C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2 1	NTDS	Process Discovery 2	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Application Layer Protocol 1 1 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A

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 doc. ZD.1.19022021_PDF.exe	11%	ReversingLabs	Win32.Trojan.Wacatac	
Swift doc. ZD.1.19022021_PDF.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	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://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://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://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://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://https://T4gAxtuj18rwIFW1VRIf.com	0%	Avira URL Cloud	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://NfuOAc.com	0%	Avira URL Cloud	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.yandex.ru	77.88.21.158	true	false		high
smtp.yandex.com	unknown	unknown	false		high

Contacted URLs

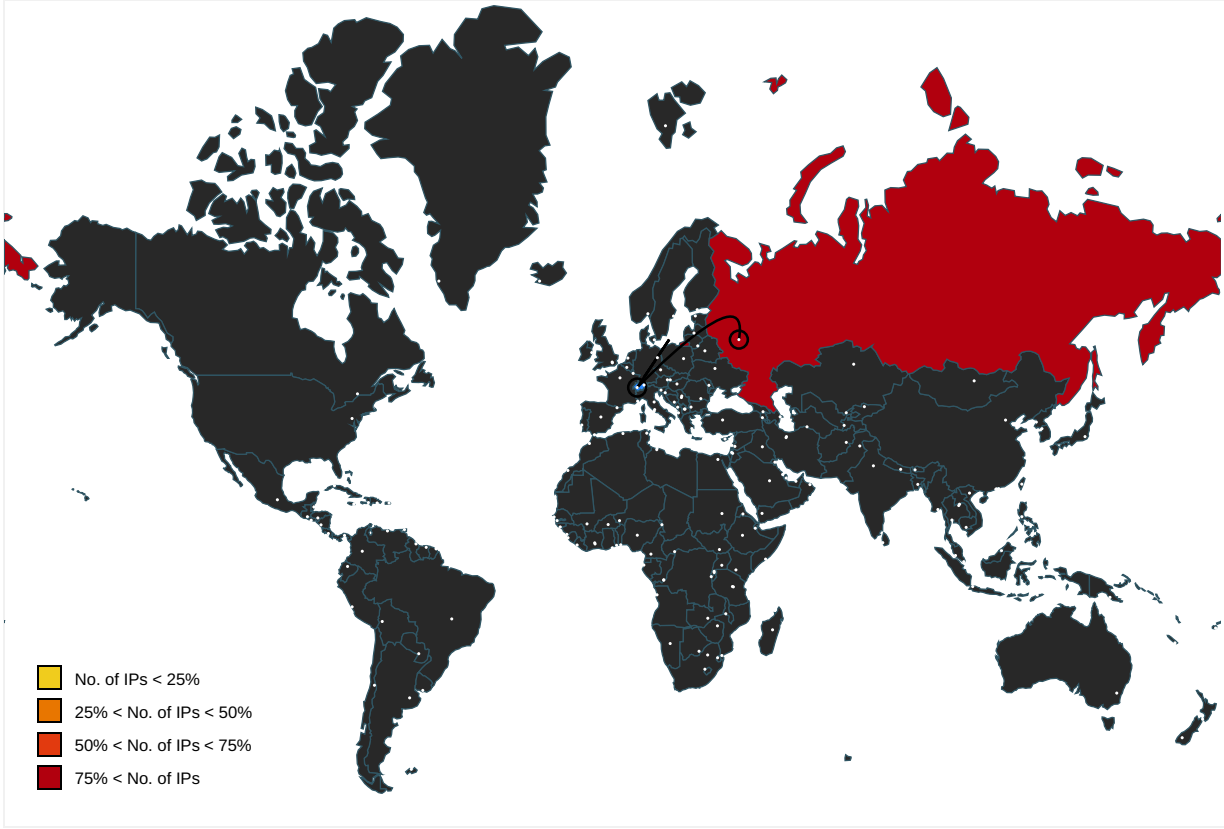
Name	Malicious	Antivirus Detection	Reputation
http://https://T4gAxtuj18rwIFW1VRIf.com	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://subca.ocsp-certum.com0.	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.924041258.0000000006DAF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ca.cer09	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.924041258.0000000006DAF000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.917324348.0000000003241000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.917324348.0000000003241000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ctnca.cer09	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.924041258.0000000006DAF000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://crls.yandex.net/certum/ycasha2.crl0-	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.92404125 8.0000000006DAF000.00000004.00 000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/ 9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.91732434 8.0000000003241000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.certum.pl/ctnca.crl0k	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.92404125 8.0000000006DAF000.00000004.00 000001.sdmp	false		high
http://subca.ocsp-certum.com01	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.92404125 8.0000000006DAF000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://yandex.crl.certum.pl/ycasha2.crl0q	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.92404125 8.0000000006DAF000.00000004.00 000001.sdmp	false		high
http://crl.certum.pl/ca.crl0h	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.92404125 8.0000000006DAF000.00000004.00 000001.sdmp	false		high
http://https://www.certum.pl/CPS0	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.92404125 8.0000000006DAF000.00000004.00 000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.91732434 8.0000000003241000.00000004.00 000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/ 9.5.3/tor-win32-0.4.3.6.zip	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.92252102 9.000000000448B000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certum.pl/CPS0	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.92404125 8.0000000006DAF000.00000004.00 000001.sdmp	false		high
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstr ap.min.css	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.91732434 8.0000000003241000.00000004.00 000001.sdmp	false		high
http://smtp.yandex.com	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.91960628 9.0000000003566000.00000004.00 000001.sdmp	false		high
http://NfuOAc.com	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.91732434 8.0000000003241000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://yandex.ocsp-responder.com03	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.92404125 8.0000000006DAF000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ycasha2.cer0	Swift doc. ZD.1.19022021_PDF.exe, 00000001.00000002.92404125 8.0000000006DAF000.00000004.00 000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.158	unknown	Russian Federation		13238	YANDEXRU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358328
Start date:	25.02.2021
Start time:	12:19:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Swift doc. ZD.1.19022021_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:	17
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@1/0@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 84% • Quality standard deviation: 5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 13.88.21.125, 23.211.6.115, 168.61.161.212, 104.42.151.234, 52.147.198.201, 51.104.139.180, 52.155.217.156, 20.54.26.129, 2.20.142.209, 2.20.142.210, 51.132.208.181, 92.122.213.194, 92.122.213.247, 51.11.168.160 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:20:43	API Interceptor	845x Sleep call for process: Swift doc. ZD.1.19022021_PDF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
77.88.21.158	inmyB8Hxr9.exe	Get hash	malicious	Browse	
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	
	KBU0o30E6s.exe	Get hash	malicious	Browse	
	FspMzSMtYA.exe	Get hash	malicious	Browse	
	w0dAcJpIm1.exe	Get hash	malicious	Browse	
	VfUlDo471c.exe	Get hash	malicious	Browse	
	FEB PROCESSED.xlsx	Get hash	malicious	Browse	
	q13a8EbUPB.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe	Get hash	malicious	Browse	
	PO Contract -SCPL0882021 & sales contract ZD.1.190 22021_PDF.exe	Get hash	malicious	Browse	
	pass.exe	Get hash	malicious	Browse	
	nXKdiUgIYy.exe	Get hash	malicious	Browse	
	x4cXV3784J.exe	Get hash	malicious	Browse	
	Request For Quotation #D22022021_pdf.exe	Get hash	malicious	Browse	
	RFQ_PDRVK2200248_00667_PDF.exe	Get hash	malicious	Browse	
	emI0MqOvFw.exe	Get hash	malicious	Browse	
	ZnsXrCAriL.exe	Get hash	malicious	Browse	
	zyp9gbDQHw.exe	Get hash	malicious	Browse	
	DHL Shipment Notification.PDF.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.yandex.ru	inmyB8Hxr9.exe	Get hash	malicious	Browse	• 77.88.21.158
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	• 77.88.21.158
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	• 77.88.21.158
	KBU0o30E6s.exe	Get hash	malicious	Browse	• 77.88.21.158
	FspMzSMtYA.exe	Get hash	malicious	Browse	• 77.88.21.158
	w0dAcJpIm1.exe	Get hash	malicious	Browse	• 77.88.21.158
	VfUlDo471c.exe	Get hash	malicious	Browse	• 77.88.21.158
	FEB PROCESSED.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	q13a8EbUPB.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO Contract -SCPL0882021 & sales contract ZD.1.190 22021_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	pass.exe	Get hash	malicious	Browse	• 77.88.21.158
	nXKdiUgIYy.exe	Get hash	malicious	Browse	• 77.88.21.158
	x4cXV3784J.exe	Get hash	malicious	Browse	• 77.88.21.158
	Request For Quotation #D22022021_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ_PDRVK2200248_00667_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	emI0MqOvFw.exe	Get hash	malicious	Browse	• 77.88.21.158
	ZnsXrCAriL.exe	Get hash	malicious	Browse	• 77.88.21.158
	zyp9gbDQHw.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL Shipment Notification.PDF.exe	Get hash	malicious	Browse	• 77.88.21.158

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YANDEXRU	inmyB8Hxr9.exe	Get hash	malicious	Browse	• 77.88.21.158
	rtofwqxq.exe	Get hash	malicious	Browse	• 87.250.250.22
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	• 77.88.21.158
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	• 77.88.21.158
	KBU0o30E6s.exe	Get hash	malicious	Browse	• 77.88.21.158
	FspMzSMtYA.exe	Get hash	malicious	Browse	• 77.88.21.158
	Wd8LBdddKD.exe	Get hash	malicious	Browse	• 37.9.96.19
	Wd8LBdddKD.exe	Get hash	malicious	Browse	• 37.9.96.14
	w0dAcJpIm1.exe	Get hash	malicious	Browse	• 77.88.21.158
	VfUlDo471c.exe	Get hash	malicious	Browse	• 77.88.21.158
	FEB PROCESSED.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	q13a8EbUPB.exe	Get hash	malicious	Browse	• 77.88.21.158

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO Contract -SCPL0882021 & sales contract ZD.1.190 22021_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	pass.exe	Get hash	malicious	Browse	• 77.88.21.158
	nXKdiUgIYy.exe	Get hash	malicious	Browse	• 77.88.21.158
	x4cXV3784J.exe	Get hash	malicious	Browse	• 77.88.21.158
	Request For Quotation #D22022021_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ_PDRVK2200248_00667_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	emI0MqOvFw.exe	Get hash	malicious	Browse	• 77.88.21.158

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.023314877630659
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 doc. ZD.1.19022021_PDF.exe
File size:	770048
MD5:	5679c66fd0ebcd6b8702c5c9e8f1ecb6
SHA1:	dbba96ad2d1c3811812eadd985401822f9ef54b9
SHA256:	949138db57c941e64a0a14bc7e87f68576dadf09f8ac56faa6776476161fb0b8
SHA512:	90c5e00b545dc5f8d54c9580643a9ebe3ba0a40131eb6a98d3501058dd9879ae2041c42bbdc89ba7ddf2936a35902c8d4c83d84d0fda0d3124e1a358e573faa7
SSDEEP:	12288:T9v6xdnFRrwvjnjBCTo+DH2JgapeB1wMrEssALmx1:Tt6x1r4nVYTDHYMB1wOsALE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...wj7`.....P..h...V..... .....@.. ....@.....

File Icon

Icon Hash:	e0dad4adc4d2d870

Static PE Info

General

Entrypoint:	0x4b86da
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60376A77 [Thu Feb 25 09:14:31 2021 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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb8688	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xba000	0x5208	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xb66e0	0xb6800	False	0.598153895548	data	7.03776347249	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xba000	0x5208	0x5400	False	0.185360863095	data	4.1978823981	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	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	0xba100	0x4228	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0xbe338	0x14	data		
RT_VERSION	0xbe35c	0x380	data		
RT_MANIFEST	0xbe6ec	0xb15	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

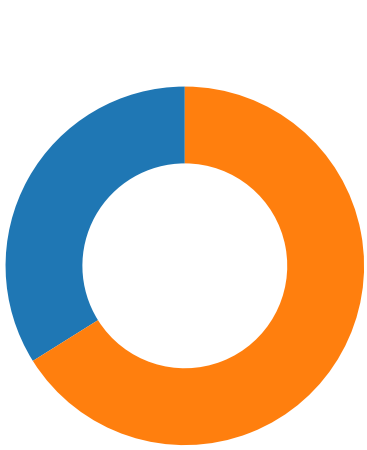
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014
Assembly Version	3.0.0.0
InternalName	RSAPKCS1SignatureDescription.exe
FileVersion	3.0.0.0
CompanyName	KTV
LegalTrademarks	
Comments	
ProductName	KTVManagement
ProductVersion	3.0.0.0
FileDescription	KTVManagement
OriginalFilename	RSAPKCS1SignatureDescription.exe

Network Behavior

Network Port Distribution

Total Packets: 59

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:22:16.032483101 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:16.111545086 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:16.111645937 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:16.330151081 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:16.330543995 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:16.411638021 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:16.411660910 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:16.412049055 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:16.491178989 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:16.536336899 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:16.618381977 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:16.618442059 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:16.618484020 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:16.618515968 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:16.618598938 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:16.618653059 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:16.664922953 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:16.746551037 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:16.796453953 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:16.810801983 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:16.889812946 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:16.891663074 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:16.972093105 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:16.973011971 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:17.063858032 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:17.065093040 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:17.151715994 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:17.152304888 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:17.239497900 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:17.239990950 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:17.321471930 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:17.323180914 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:17.323326111 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:17.323971033 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:17.324101925 CET	49765	587	192.168.2.4	77.88.21.158
Feb 25, 2021 12:22:17.403855085 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:17.404289007 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:18.069082975 CET	587	49765	77.88.21.158	192.168.2.4
Feb 25, 2021 12:22:18.109025955 CET	49765	587	192.168.2.4	77.88.21.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:20:35.466200113 CET	54531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:35.519671917 CET	53	54531	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:20:36.660303116 CET	49714	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:36.709070921 CET	53	49714	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:36.863770962 CET	58028	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:36.924093962 CET	53	58028	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:38.031158924 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:38.080015898 CET	53	53097	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:39.030683041 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:39.079600096 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:40.288960934 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:40.349018097 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:41.962757111 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:42.015674114 CET	53	49910	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:43.185733080 CET	55854	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:43.238775969 CET	53	55854	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:45.527916908 CET	64549	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:45.578366041 CET	53	64549	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:47.279995918 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:47.331563950 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:48.540069103 CET	52991	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:48.589719057 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:49.871844053 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:49.934281111 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:51.045453072 CET	51726	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:51.094162941 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:51.841162920 CET	56794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:51.890017033 CET	53	56794	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:53.079277039 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:53.129333019 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:54.201761961 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:54.260245085 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:55.025892019 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:55.086498976 CET	53	56621	8.8.8.8	192.168.2.4
Feb 25, 2021 12:20:56.517249107 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:20:56.568813086 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:00.983846903 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:01.036426067 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:08.085619926 CET	64801	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:08.138427973 CET	53	64801	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:24.894157887 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:24.956551075 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:25.540385962 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:25.600578070 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:26.285353899 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:26.296955109 CET	52337	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:26.347690105 CET	53	52337	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:26.349694967 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:26.801425934 CET	55046	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:26.858725071 CET	53	55046	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:27.302660942 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:27.377688885 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:28.015033960 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:28.072329044 CET	53	49285	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:28.658046007 CET	50601	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:28.717907906 CET	53	50601	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:29.442985058 CET	60875	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:29.500087023 CET	53	60875	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:30.367633104 CET	56448	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:30.416379929 CET	53	56448	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:30.707478046 CET	59172	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:30.775352001 CET	53	59172	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:30.905088902 CET	62420	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:30.965547085 CET	53	62420	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:43.019121885 CET	60579	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:43.038861990 CET	50183	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:21:43.068176985 CET	53	60579	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:43.110400915 CET	53	50183	8.8.8.8	192.168.2.4
Feb 25, 2021 12:21:50.055668116 CET	61531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:21:50.117507935 CET	53	61531	8.8.8.8	192.168.2.4
Feb 25, 2021 12:22:15.870568991 CET	49228	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:22:15.928117037 CET	53	49228	8.8.8.8	192.168.2.4
Feb 25, 2021 12:22:15.954482079 CET	59794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:22:16.011673927 CET	53	59794	8.8.8.8	192.168.2.4
Feb 25, 2021 12:22:16.998469114 CET	55916	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:22:17.047694921 CET	53	55916	8.8.8.8	192.168.2.4
Feb 25, 2021 12:22:19.553073883 CET	52752	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:22:19.628139019 CET	53	52752	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 12:22:15.870568991 CET	192.168.2.4	8.8.8.8	0x1e09	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Feb 25, 2021 12:22:15.954482079 CET	192.168.2.4	8.8.8.8	0xc40	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 12:22:15.928117037 CET	8.8.8.8	192.168.2.4	0x1e09	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 12:22:15.928117037 CET	8.8.8.8	192.168.2.4	0x1e09	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Feb 25, 2021 12:22:16.011673927 CET	8.8.8.8	192.168.2.4	0xc40	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 12:22:16.011673927 CET	8.8.8.8	192.168.2.4	0xc40	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 12:22:16.330151081 CET	587	49765	77.88.21.158	192.168.2.4	220 vla3-23c3b031fed5.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Feb 25, 2021 12:22:16.330543995 CET	49765	587	192.168.2.4	77.88.21.158	EHLO 305090
Feb 25, 2021 12:22:16.411660910 CET	587	49765	77.88.21.158	192.168.2.4	250-vla3-23c3b031fed5.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Feb 25, 2021 12:22:16.412049055 CET	49765	587	192.168.2.4	77.88.21.158	STARTTLS
Feb 25, 2021 12:22:16.491178989 CET	587	49765	77.88.21.158	192.168.2.4	220 Go ahead

Code Manipulations

Statistics

System Behavior

Analysis Process: Swift doc. ZD.1.19022021_PDF.exe PID: 7020 Parent PID: 5968

General

Start time:	12:20:42
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Swift doc. ZD.1.19022021_PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Swift doc. ZD.1.19022021_PDF.exe'
Imagebase:	0xe00000
File size:	770048 bytes
MD5 hash:	5679C66FD0EBCD6B8702C5C9E8F1ECB6
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: 00000001.00000002.922521029.000000000448B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.923663679.00000000063E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.917324348.0000000003241000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.917324348.0000000003241000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	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	6D3DCF06	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	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C221B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\2f200813-6b95-4fa2-9471-1d5bf82d4fe6	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C221B4F	ReadFile

Disassembly

Code Analysis