ID: 553163
Sample Name: Ziraat Bankasi Swift Mesaji.exe
Cookbook: default.jbs
Time: 12:12:27
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

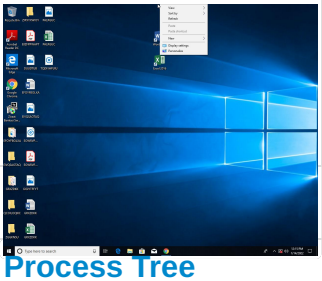
Windows Analysis Report Ziraat Bankasi Swift Mesaji.exe

Overview

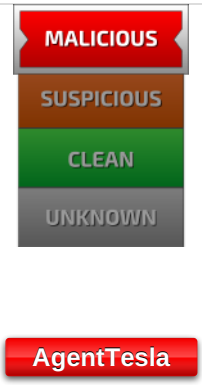
General Information

Sample Name:	Ziraat Bankasi Swift Mesaji.exe
Analysis ID:	553163
MD5:	16152365132008..
SHA1:	df8fae3ff1125841..
SHA256:	f4d91c834da24d6.
Tags:	AgentTesla exe geo TUR ZiraatBank
Infos:	

Most interesting Screenshot:



Detection



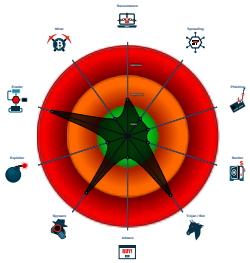
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Detected unpacking (creates a PE fi…
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal ftp login c…
- Machine Learning detection for samp…
- Found evasive API chain (trying to d…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- Ziraat Bankasi Swift Mesaji.exe (PID: 6988 cmdline: "C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe" MD5: 161523651320083122D05DD374C87EC4)
  - Ziraat Bankasi Swift Mesaji.exe (PID: 7108 cmdline: "C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe" MD5: 161523651320083122D05DD374C87EC4)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "fizikokimya@antimikrop.com.tr",
  "Password": "fiziko2016Kimya",
  "Host": "mail.antimikrop.com.tr"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.554087278.00000000037F1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.554087278.00000000037F1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000002.551571985.0000000000508000.00000004.00000020.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.551571985.0000000000508000.00000004.00000020.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000000.292334595.0000000000414000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.Ziraat Bankasi Swift Mesaji.exe.37f3258.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.Ziraat Bankasi Swift Mesaji.exe.37f3258.3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.1.Ziraat Bankasi Swift Mesaji.exe.415058.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.1.Ziraat Bankasi Swift Mesaji.exe.415058.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.2.Ziraat Bankasi Swift Mesaji.exe.415058.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 55 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Detected unpacking (creates a PE file in dynamic memory)

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

Detected unpacking (creates a PE file in dynamic memory)

Malware Analysis System Evasion:

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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 ftp login credentials

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

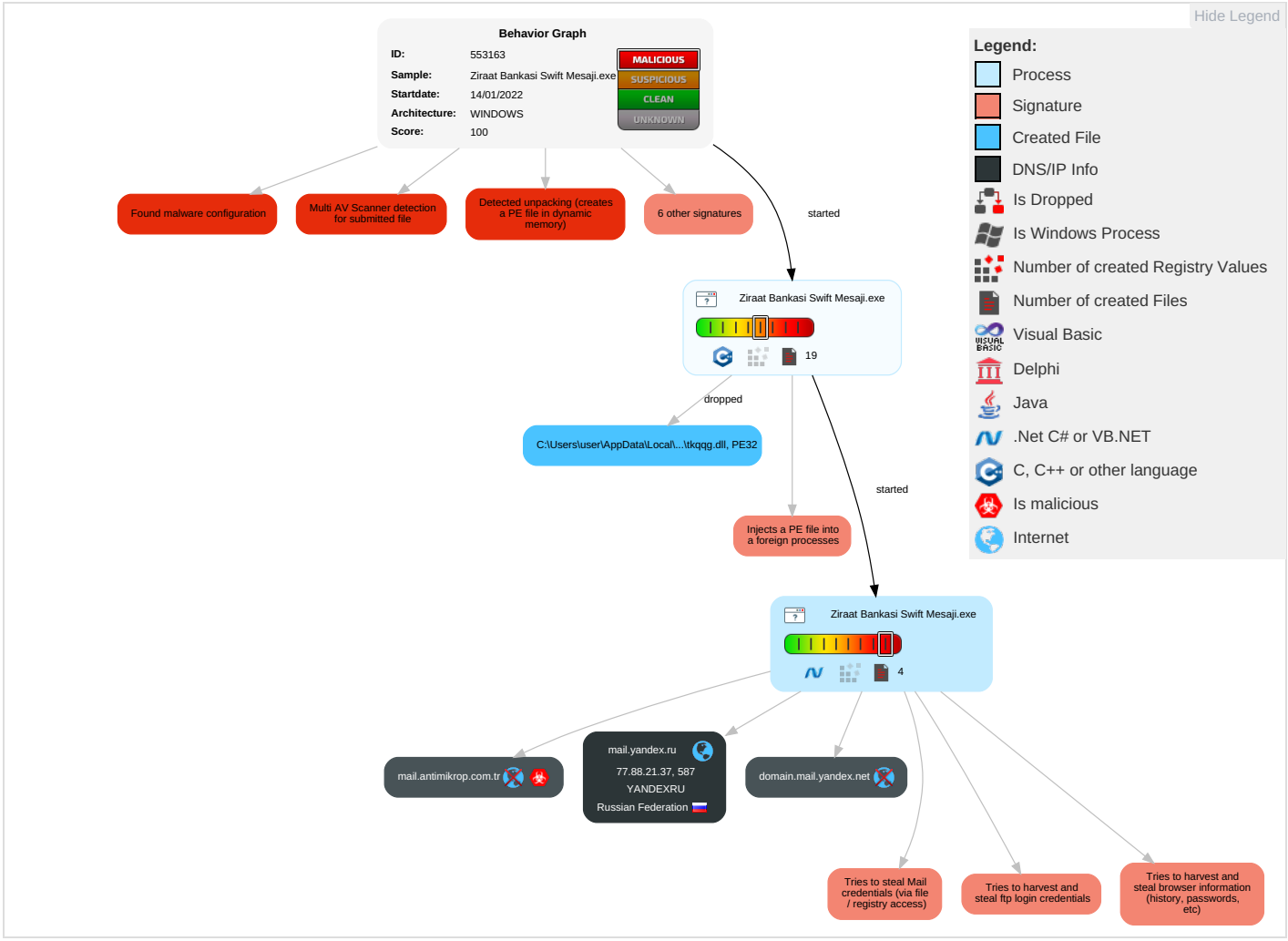
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Access Token Manipulation 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	System Information Discovery 1 2 6	Distributed Component Object Model	Input Capture 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 3 1	LSA Secrets	Query Registry 1	SSH	Clipboard Data 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Security Software Discovery 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Virtualization/Sandbox Evasion 1 3 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

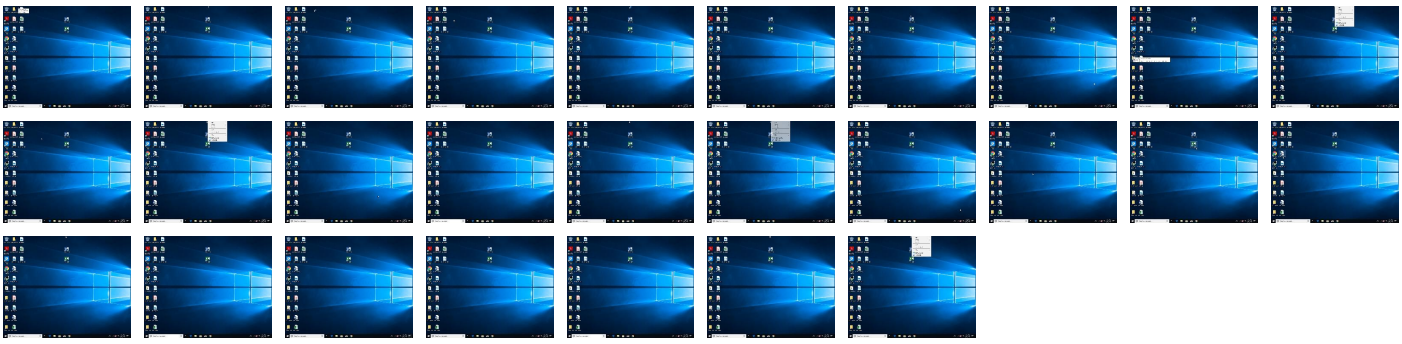
Behavior Graph



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
Ziraat Bankasi Swift Mesaji.exe	23%	ReversingLabs	Win32.Trojan.AgentTesla	
Ziraat Bankasi Swift Mesaji.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.Ziraat Bankasi Swift Mesaji.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.1.Ziraat Bankasi Swift Mesaji.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.Ziraat Bankasi Swift Mesaji.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Ziraat Bankasi Swift Mesaji.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Ziraat Bankasi Swift Mesaji.exe.400000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Ziraat Bankasi Swift Mesaji.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Ziraat Bankasi Swift Mesaji.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Ziraat Bankasi Swift Mesaji.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Ziraat Bankasi Swift Mesaji.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.Ziraat Bankasi Swift Mesaji.exe.4970000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.antimikrop.com.tr	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://api.ipify.org%(	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://lRguGt.com	0%	Avira URL Cloud	safe	
http://https://Wm2Dt2zcSt3c655v3va.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%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	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.yandex.ru	77.88.21.37	true	false		high
mail.antimikrop.com.tr	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.37	mail.yandex.ru	Russian Federation		13238	YANDEXRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553163
Start date:	14.01.2022
Start time:	12:12:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ziraat Bankasi Swift Mesaji.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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/4@9/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 38.3% (good quality ratio 35.7%) • Quality average: 78.6% • Quality standard deviation: 30.1%
HCA Information:	• Successful, ratio: 87% • 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

Simulations

Behavior and APIs

Time	Type	Description
12:13:56	API Interceptor	430x Sleep call for process: Ziraat Bankasi Swift Mesaji.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\078s89jqsxc08eyh	
Process:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
File Type:	data
Category:	dropped
Size (bytes):	291839
Entropy (8bit):	7.963840034244116
Encrypted:	false
SSDEEP:	6144:jpk7RyrNkcMOsZA7e0QzUwAwDHQ9tdTp3+4rALig5qDCiIt4hrBp4wyPcdG:jW7RyrS5BBzQxp+335qDXHrBp4BPcA
MD5:	EA24D857020EB4FB65D427260C084C97
SHA1:	CB446E36E6BDF214A3DFFB410F2F31E2EDE119E6

C:\Users\user\AppData\Local\Temp\078s89jqsxc08eyh	
SHA-256:	66F56E1C142E94CAB30C05F6E510304593544E760A9C0B1CA09D86F5D6390419
SHA-512:	422C02D523C16E343865BC163E1C44F0AC4AB158BE647CE71FEA303B84C270A718AF4330D4AC51B88F061DD8CDBF25D9FEFFD13220E796A4992B173C3E4C8E1
Malicious:	false
Reputation:	low
Preview:	(..{h..*[N...B.5X.....j.....S. s..$E....W.Q..._.qV....~..z.{F...:=C...I.....K.pO.....(.`..H.g.}..{....\|P..L.b.j$'B.xao..A.+m..~p&D..2..E.....0.....wy!..LC.. .....gd.H.6.l8.....CjG.....e:)..._ ..u).,C.wr.....vb.....LY.J..X.y.!...@4.W.iC.+L.X{...*.K....O51+=V....i.....J.cu s(.$EM...W.Q.t._..V....~C,.....^.....]T.4.gq..B1.8.I...q..w..@%.R.mYP.B.x.o..5.h"#.....X.?.`...C.1.....M...e<($.M.2Z1.....{..1.a|3....~S>....Y\w.....\f.%T.....N.|.....ph....R..w..<.R4.W.iC.+...M...*.....e.5.H.....i....S. ..l.U...B.Q..._..V..{.~C.z.....0..D.....]v+.]T_..gq..Bh .8n.&..q..w..@%...lP.2E.u...4.h"#..m.$XlB..`....:1....H.....e<(.rG.2....nZ....1.a\|3....~S>.^..Z\w.....<.f.%T.....N.\|...$..ph....R..w..<.R4.W.iC.+L.X{...*.N...o.5.....i.....S. s..$E.... W.Q..._.qV....~C,z.....0..D.....r....]T.t.gqC..B1.8nI...q..w..@%..mlP.B.xao..5.h"#...m]$Xl?.`....:1.....M...e<($.M.2Z1.....1.a\|3...~S>....Y\w.....<.f.%T.....N.\|...$..

C:\Users\user\AppData\Local\Temp\fdazqvak	
Process:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
File Type:	data
Category:	dropped
Size (bytes):	5177
Entropy (8bit):	6.122705645881862
Encrypted:	false
SSDEEP:	96:i+LPt1QjqbEf4hXCNtd6C04Dg3yDck9uBTdQXTCXt+IGNMTUdUMfyOw:tLbQjqbcw+qQ0WuQW9aSct5w
MD5:	80D6D3B339EF43FCB75B2B520A128560
SHA1:	1C5FC2DE82F3E04606EC99E9657CD4FE268D4879
SHA-256:	E40995D5D9195DDC3FE5D3AA67ED4212D41C21B8C7420D7F91EB8CD3386FA792
SHA-512:	A7F3FBA52BED2BDB39034C970CDCC4AB90C64148597D1E51EB6AF697EF3D4EC863E8C5FB8D0DA1471ECAEE5101B8F262EF659ED7536918EF48D0E6058F6ABB8
Malicious:	false
Reputation:	low
Preview:	B1 ....=.=.....Y....9.Y....A....`.....A.....1..-.....AA.....)..%.....A$.....a..]..... .AO.....Y..U.....!..Y....r..9..5...A..b..A..=..A.....Z.+.....A.....[.....5...A.....\.....1...).. .a...Y...9...A.....?.....1...!.....A....`.....\.....6.[....=...Y.....!.....!.....Z.....!....!.....6.[.....W.A....A....[.....8.A....A....[!....!.A....A....[!...=.=..Y....A`.....1..... .....W.....<5A.....Y...!r.!..b....1...-..Ar.!.Z:....1...-...!..Y....1....8.A*....A_.....<..A...!A.....<..`.....6.[....=.=..Y....A`.....Y.....W.....<5A.....Y.....!r.!..b....Y.. .U...r.!.Z:....Y...U...r.!.*:...Y...U....b.!..+....Y...U..Ar.!.Z:....Y...U...!..Y....Y....W.A7....A4.....!..A....<.....!A.....<..`.....6.[....=.=.`.....5.....W.....<5A... ..Y...!r.!..b....5...A...r.!.Z:....5...A...!..Y....5....!.A.....A.....<...

C:\Users\user\AppData\Local\Temp\nsyAE25.tmp	
Process:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
File Type:	data
Category:	dropped
Size (bytes):	321764
Entropy (8bit):	7.815561849982555
Encrypted:	false
SSDEEP:	6144:NHpk7RyrNkcMOsZA7e0QzUwAwDHQ9tdTp3+4rALig5qDCiIt4hrBp4wyPcd1:BW7RyrS5BBzQxp+335qDXHrBp4BPc
MD5:	B533A0B04B17F00B9F73B661D48D04D2
SHA1:	BF3D337FEB9029E4FB11D96229330CE4F2CEC87F
SHA-256:	89D35CC1F3C79201E3E5A8E617D2DDB8597AF3CB56018164014746E4CFED320D
SHA-512:	2190182461931FA9A4739BDF96010C1A12C3F5C9E3F01993D20B30690D8608301271242A667C454AA20E5D68D3C626D3612B040D666459137BCBC5AF8068500C
Malicious:	false
Reputation:	low
Preview:	.P.....,.....<.....O.....P..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsyAE26.tmp\tkqqg.dll	
Process:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	4096
Entropy (8bit):	3.7725519810575148
Encrypted:	false
SSDEEP:	24:e1GSb0JDlNmEcQqV3ax/+sK4RHJiDTyaNt01a5DTyxk8q6I1nPnRuV4MPgicisCm:SgZzhWipKxt9r6IPRuqSjsvyO
MD5:	6D4D09737E9AB179CAB4481188F7C904
SHA1:	F49AD85CA74D5D83F7E26E09C2B251F9FF5750EF
SHA-256:	F8F3827A1D513BE5607BADD8AB724D264360B65321DF7338425E44BB8185A274
SHA-512:	CBD50F889DF5AEB03A539F3965D965AA009F3EBA41CCDA15831AC0516820BFDF7F313A8DE1758DC42BC5F6396644D8A40AAC023F922C374E1A3D462B831004
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\nsyAE26.tmp\tkqqg.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U.CU.CU.C...CT.C0..BZ.CU.Cw.C..BT.C..BT.C.QCT.C. .BT.CRichU.C.....PE..L..."2.a.....!..... .....P.....@..... ..L.... .....0.....@..L..... .....text...v..... ..`.rdata..j.... .....@..@.rsrc.....0.....@..@.reloc..L...@.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.936184384803921
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Ziraat Bankasi Swift Mesaji.exe
File size:	270191
MD5:	161523651320083122d05dd374c87ec4
SHA1:	df8fae3ff1125841de5aa2306de3501e8204919a
SHA256:	f4d91c834da24d653fef9049355102bcb68be411280268af61ac8f59bce581db
SHA512:	0280e226de497d257b1a11f15e9dfd765ab0491b051997:1dc71728c6a4fe9faff0a987a71ab97d37aa1af9cd4144e9611912add9d3abb507ec7efcee019ec76
SSDEEP:	6144:owt4pSsfMNAKw5CFFe3NJMn9aiMcRmrEktnwVroIDx:Ze+wkCG9aptPBwVcS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403225
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94693169534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 12:14:21.615456104 CET	192.168.2.7	8.8.8.8	0x490e	Standard query (0)	mail.antimikrop.com.tr	A (IP address)	IN (0x0001)
Jan 14, 2022 12:14:30.377652884 CET	192.168.2.7	8.8.8.8	0x1e5	Standard query (0)	mail.antimikrop.com.tr	A (IP address)	IN (0x0001)
Jan 14, 2022 12:14:43.011908054 CET	192.168.2.7	8.8.8.8	0xb33b	Standard query (0)	mail.antimikrop.com.tr	A (IP address)	IN (0x0001)
Jan 14, 2022 12:14:51.723941088 CET	192.168.2.7	8.8.8.8	0xa1d3	Standard query (0)	mail.antimikrop.com.tr	A (IP address)	IN (0x0001)
Jan 14, 2022 12:15:04.228090048 CET	192.168.2.7	8.8.8.8	0x115c	Standard query (0)	mail.antimikrop.com.tr	A (IP address)	IN (0x0001)
Jan 14, 2022 12:15:12.769236088 CET	192.168.2.7	8.8.8.8	0xac0c	Standard query (0)	mail.antimikrop.com.tr	A (IP address)	IN (0x0001)
Jan 14, 2022 12:15:25.449325085 CET	192.168.2.7	8.8.8.8	0x9d67	Standard query (0)	mail.antimikrop.com.tr	A (IP address)	IN (0x0001)
Jan 14, 2022 12:15:34.207704067 CET	192.168.2.7	8.8.8.8	0xf45a	Standard query (0)	mail.antimikrop.com.tr	A (IP address)	IN (0x0001)
Jan 14, 2022 12:15:46.811651945 CET	192.168.2.7	8.8.8.8	0x8a6b	Standard query (0)	mail.antimikrop.com.tr	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 12:14:21.774374962 CET	8.8.8.8	192.168.2.7	0x490e	No error (0)	mail.antimikrop.com.tr	domain.mail.yandex.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:14:21.774374962 CET	8.8.8.8	192.168.2.7	0x490e	No error (0)	domain.mail.yandex.net	mail.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:14:21.774374962 CET	8.8.8.8	192.168.2.7	0x490e	No error (0)	mail.yandex.ru		77.88.21.37	A (IP address)	IN (0x0001)
Jan 14, 2022 12:14:30.638633013 CET	8.8.8.8	192.168.2.7	0x1e5	No error (0)	mail.antimikrop.com.tr	domain.mail.yandex.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:14:30.638633013 CET	8.8.8.8	192.168.2.7	0x1e5	No error (0)	domain.mail.yandex.net	mail.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:14:30.638633013 CET	8.8.8.8	192.168.2.7	0x1e5	No error (0)	mail.yandex.ru		77.88.21.37	A (IP address)	IN (0x0001)
Jan 14, 2022 12:14:43.133341074 CET	8.8.8.8	192.168.2.7	0xb33b	No error (0)	mail.antimikrop.com.tr	domain.mail.yandex.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:14:43.133341074 CET	8.8.8.8	192.168.2.7	0xb33b	No error (0)	domain.mail.yandex.net	mail.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:14:43.133341074 CET	8.8.8.8	192.168.2.7	0xb33b	No error (0)	mail.yandex.ru		77.88.21.37	A (IP address)	IN (0x0001)
Jan 14, 2022 12:14:51.741537094 CET	8.8.8.8	192.168.2.7	0xa1d3	No error (0)	mail.antimikrop.com.tr	domain.mail.yandex.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:14:51.741537094 CET	8.8.8.8	192.168.2.7	0xa1d3	No error (0)	domain.mail.yandex.net	mail.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:14:51.741537094 CET	8.8.8.8	192.168.2.7	0xa1d3	No error (0)	mail.yandex.ru		77.88.21.37	A (IP address)	IN (0x0001)
Jan 14, 2022 12:15:04.381839037 CET	8.8.8.8	192.168.2.7	0x115c	No error (0)	mail.antimikrop.com.tr	domain.mail.yandex.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:15:04.381839037 CET	8.8.8.8	192.168.2.7	0x115c	No error (0)	domain.mail.yandex.net	mail.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:15:04.381839037 CET	8.8.8.8	192.168.2.7	0x115c	No error (0)	mail.yandex.ru		77.88.21.37	A (IP address)	IN (0x0001)
Jan 14, 2022 12:15:12.997183084 CET	8.8.8.8	192.168.2.7	0xac0c	No error (0)	mail.antimikrop.com.tr	domain.mail.yandex.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:15:12.997183084 CET	8.8.8.8	192.168.2.7	0xac0c	No error (0)	domain.mail.yandex.net	mail.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:15:12.997183084 CET	8.8.8.8	192.168.2.7	0xac0c	No error (0)	mail.yandex.ru		77.88.21.37	A (IP address)	IN (0x0001)
Jan 14, 2022 12:15:25.739602089 CET	8.8.8.8	192.168.2.7	0x9d67	No error (0)	mail.antimikrop.com.tr	domain.mail.yandex.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:15:25.739602089 CET	8.8.8.8	192.168.2.7	0x9d67	No error (0)	domain.mail.yandex.net	mail.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:15:25.739602089 CET	8.8.8.8	192.168.2.7	0x9d67	No error (0)	mail.yandex.ru		77.88.21.37	A (IP address)	IN (0x0001)
Jan 14, 2022 12:15:34.226948977 CET	8.8.8.8	192.168.2.7	0xf45a	No error (0)	mail.antimikrop.com.tr	domain.mail.yandex.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:15:34.226948977 CET	8.8.8.8	192.168.2.7	0xf45a	No error (0)	domain.mail.yandex.net	mail.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:15:34.226948977 CET	8.8.8.8	192.168.2.7	0xf45a	No error (0)	mail.yandex.ru		77.88.21.37	A (IP address)	IN (0x0001)
Jan 14, 2022 12:15:46.829662085 CET	8.8.8.8	192.168.2.7	0x8a6b	No error (0)	mail.antimikrop.com.tr	domain.mail.yandex.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:15:46.829662085 CET	8.8.8.8	192.168.2.7	0x8a6b	No error (0)	domain.mail.yandex.net	mail.yandex.ru		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 12:15:46.829662085 CET	8.8.8.8	192.168.2.7	0x8a6b	No error (0)	mail.yandex.ru		77.88.21.37	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Ziraat Bankasi Swift Mesaji.exe PID: 6988 Parent PID: 2900

General

Start time:	12:13:43
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe"
Imagebase:	0x400000
File size:	270191 bytes
MD5 hash:	161523651320083122D05DD374C87EC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.294724890.0000000003090000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.294724890.0000000003090000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Ziraat Bankasi Swift Mesaji.exe PID: 7108 Parent PID: 6988

General

Start time:	12:13:45

Start date:	14/01/2022
Path:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe"
Imagebase:	0x400000
File size:	270191 bytes
MD5 hash:	161523651320083122D05DD374C87EC4
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: 00000003.00000002.554087278.00000000037F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.554087278.00000000037F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.551571985.0000000000508000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.551571985.0000000000508000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.292334595.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.292334595.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.554248422.0000000004930000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.554248422.0000000004930000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000001.292756258.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000001.292756258.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.291447047.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.291447047.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.554299855.0000000004972000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.554299855.0000000004972000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.548601003.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.548601003.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.552826458.00000000027F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.552826458.00000000027F1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis