ID: 755920
Sample Name: Ziraat Bankasi Swift Mesaji20221129-34221.exe
Cookbook: default.jbs
Time: 10:15:36
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

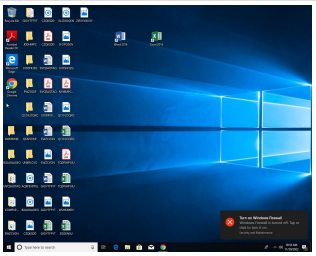
Windows Analysis Report

Ziraat Bankasi Swift Mesaji20221129-34221.exe

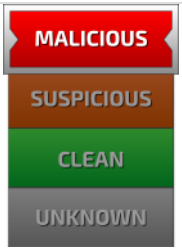
Overview

General Information

Sample Name:	Ziraat Bankasi Swift Mesaji20221129-34221.exe
Analysis ID:	755920
MD5:	6a0ff43510923c2..
SHA1:	880c264f12ea21..
SHA256:	52426e75e25f69..
Infos:	



Detection



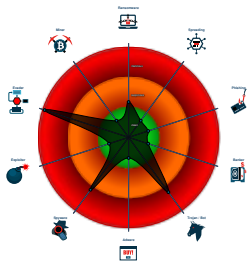
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- Ziraat Bankasi Swift Mesaji20221129-34221.exe (PID: 3176 cmdline: C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji20221129-34221.exe MD5: 6A0FF43510923C27B144BF86B5E0A867)
  - Ziraat Bankasi Swift Mesaji20221129-34221.exe (PID: 5152 cmdline: C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji20221129-34221.exe MD5: 6A0FF43510923C27B144BF86B5E0A867)
  - Ziraat Bankasi Swift Mesaji20221129-34221.exe (PID: 1308 cmdline: C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji20221129-34221.exe MD5: 6A0FF43510923C27B144BF86B5E0A867)
    - explorer.exe (PID: 3528 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - systray.exe (PID: 1312 cmdline: C:\Windows\SysWOW64\systray.exe MD5: 1373D481BE4C8A6E5F5030D2FB0A0C68)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.erwgcb.top/qmpa/"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.560048415.0000000000820000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.560048415.0000000000820000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6611:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1f040:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa8af:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x17de7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
0000000A.00000002.560048415.0000000000820000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x17be5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17691:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x17ce7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x17e5f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa47a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x168dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1ddb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1edaa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000002.560048415.0000000000820000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1a0b9:$sqlite3step: 68 34 1C 7B E1 • 0x1ac31:$sqlite3step: 68 34 1C 7B E1 • 0x1a0fb:$sqlite3text: 68 38 2A 90 C5 • 0x1ac76:$sqlite3text: 68 38 2A 90 C5 • 0x1a112:$sqlite3blob: 68 53 D8 7F 8C • 0x1ac8c:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000002.559572185.00000000003C0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.Ziraat Bankasi Swift Mesaji20221129-34221.exe.31854c4.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
2.2.Ziraat Bankasi Swift Mesaji20221129-34221.exe.31854c4.1.raw.unpack	INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste	Detects executables potentially checking for WinJail sandbox window	ditekSHen	• 0xa79e:$v1: SbieDll.dll • 0xa7b8:$v2: USER • 0xa7c4:$v3: SANDBOX • 0xa7d6:$v4: VIRUS • 0xa826:$v4: VIRUS • 0xa7e4:$v5: MALWARE • 0xa7f6:$v6: SCHMIDTI • 0xa80a:$v7: CURRENTUSER
2.2.Ziraat Bankasi Swift Mesaji20221129-34221.exe.3169a9c.0.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
2.2.Ziraat Bankasi Swift Mesaji20221129-34221.exe.3169a9c.0.raw.unpack	INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste	Detects executables potentially checking for WinJail sandbox window	ditekSHen	• 0x261c6:$v1: SbieDll.dll • 0x261e0:$v2: USER • 0x261ec:$v3: SANDBOX • 0x261fe:$v4: VIRUS • 0x2624e:$v4: VIRUS • 0x2620c:$v5: MALWARE • 0x2621e:$v6: SCHMIDTI • 0x26232:$v7: CURRENTUSER

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

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

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

Tries to steal Mail credentials (via file / registry access)

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

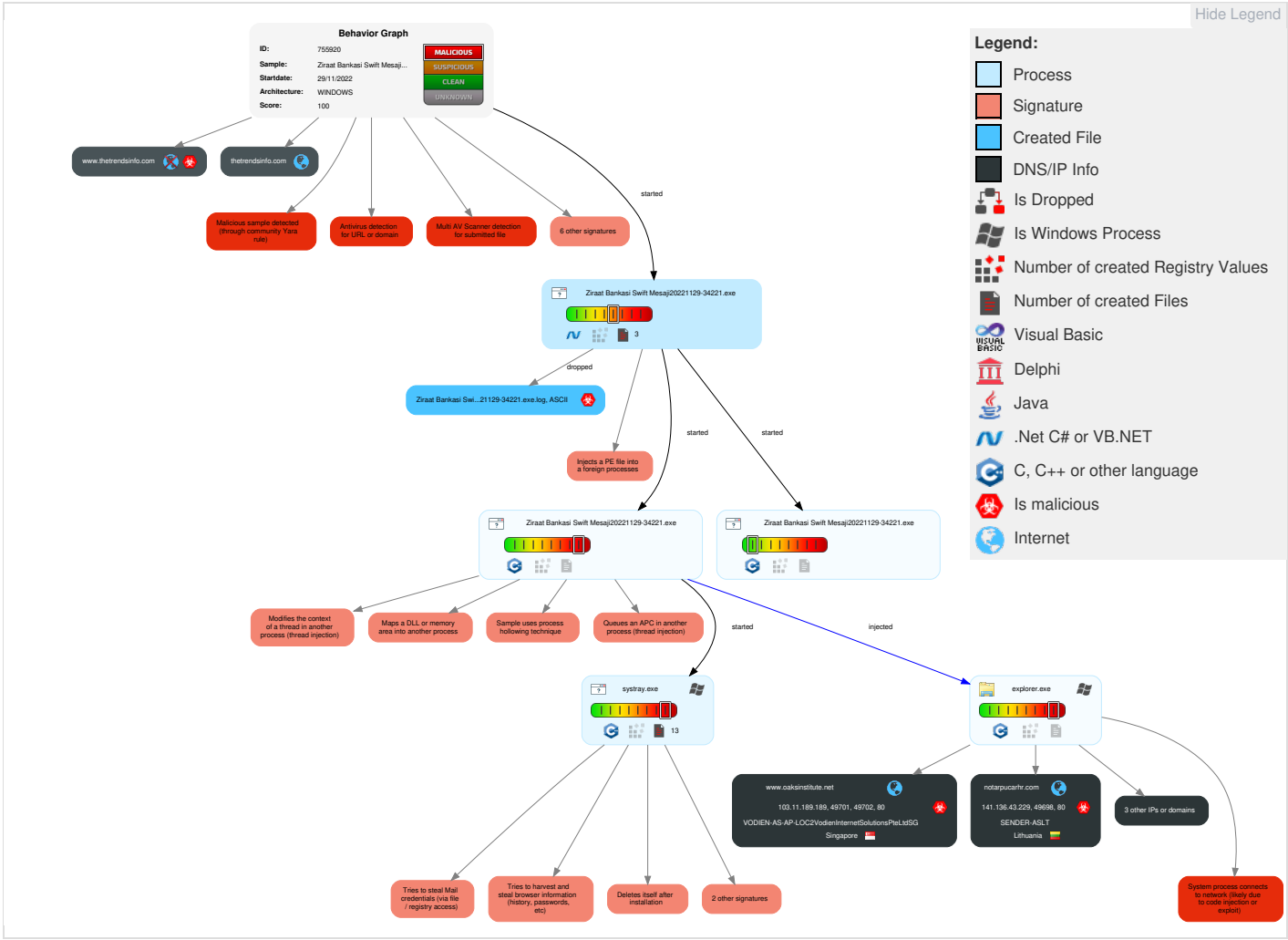
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	6 1 2 Process Injection	1 Masquerading	1 OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	6 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 2 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Timestomp	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

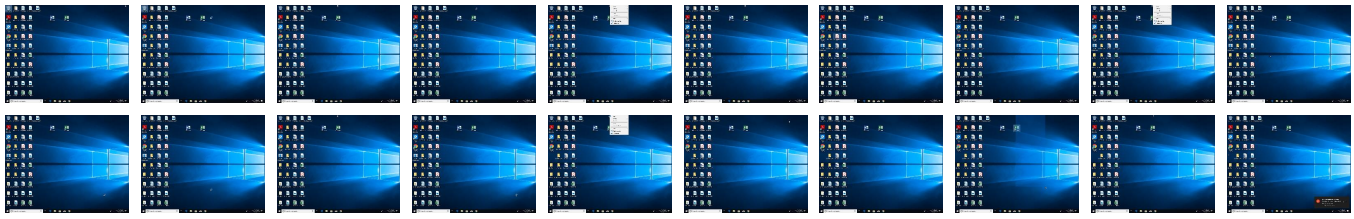
Behavior Graph



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 Mesaji20221129-34221.exe	44%	Virustotal		Browse
Ziraat Bankasi Swift Mesaji20221129-34221.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.Worefl int	
Ziraat Bankasi Swift Mesaji20221129-34221.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.Ziraat Bankasi Swift Mesaji20221129-34221.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.oaksinstitute.net	0%	Virustotal		Browse
thetrendsinfo.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/$	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/S	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/l	0%	URL Reputation	safe	
http://www.carterandcone.comFH	0%	Avira URL Cloud	safe	
http://www.carterandcone.com69	0%	Avira URL Cloud	safe	
http://www.fontbureau.commsedY	0%	Avira URL Cloud	safe	
http://www.carterandcone.comre	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.oaksinstitute.net/qmpa/?mRh4lr=5Yvs1mt+8koK04wDmvle7hFJkaWhy6okw1CCpgEhtGW9Nwizn2cFt5qaMIq71RWOXG0+Z4ku5zJzPR6AZImqbF2d7jl61SlZkw==&VrWd=-Z5PLbzhUhYhR8K	100%	Avira URL Cloud	malware	
http://www.jiyu-kobo.co.jp/jp/l	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.carterandcone.comfac	0%	URL Reputation	safe	
http://www.fontbureau.comL.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml-B(	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.carterandcone.comhy/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cntsP=	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.z	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ry	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnV	0%	Avira URL Cloud	safe	
http://www.carterandcone.compe	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0P	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comegr	0%	Avira URL Cloud	safe	
http://www.fontbureau.comicu	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalicg	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comU	0%	Avira URL Cloud	safe	
http://www.multimediapages.com/qmpa/?mRh4lr=rejTwVtqfB30O9nwV+ATTccd4/r3ZShDvm2ExT48d5W41t5gt2xe96xDcyDktEvrNydQ6GKmhPSZbQq/61ftArfg9GGH4Fupqg==&VrWd=-Z5PLbzhUhYhR8K	100%	Avira URL Cloud	malware	
http://www.fontbureau.coma$	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.comers0J	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cntsP=tx	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comegrjJH	0%	Avira URL Cloud	safe	
http://www.carterandcone.com8I	0%	Avira URL Cloud	safe	
http://www.carterandcone.comsigW	0%	Avira URL Cloud	safe	
http://www.carterandcone.comily	0%	Avira URL Cloud	safe	
http://www.notarpucarhr.com/qmpa/?mRh4lr=EgIWtG18ZIzAqtaO1OmvkFLdPjhKt8Mp7J5Y1fxWkEB6Q9kPLkR881s923Q+G4W9S+aNob6MQv0YuDJ73ehw8miGBWwdljwfXw==&VrWd=-Z5PLbzhUhYhR8K	0%	Avira URL Cloud	safe	
http://www.carterandcone.comits	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmtr-tr	0%	Avira URL Cloud	safe	
http://www.oaksinstitute.net/qmpa/	100%	Avira URL Cloud	malware	
http://www.carterandcone.comsign	0%	Avira URL Cloud	safe	
http://www.carterandcone.comGr	0%	Avira URL Cloud	safe	
http://www.fontbureau.comueedl	0%	Avira URL Cloud	safe	
http://www.fonts.comcom	0%	Avira URL Cloud	safe	
www.erwgcb.top/qmpa/	0%	Avira URL Cloud	safe	
http://www.multimediapages.com/qmpa/	100%	Avira URL Cloud	malware	
http://www.carterandcone.comitse	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdP	0%	Avira URL Cloud	safe	
http://www.sakkal.comP1	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.oaksinstitute.net	103.11.189.189	true	true	• 0%, Virustotal, Browse	unknown
notarpucarhr.com	141.136.43.229	true	true		unknown
www.multimediapages.com	38.239.92.131	true	true		unknown
thetrendsinfo.com	68.66.216.12	true	false	• 3%, Virustotal, Browse	unknown
www.thetrendsinfo.com	unknown	unknown	true		unknown
www.notarpucarhr.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.oaksinstitute.net/qmpa/?mRh4lr=5Yvs1mt+8koK04wDmvle7hFJkaWhy6okw1CCpgEhtGW9Nwizn2cFt5qaMlq71RWOXG0+Z4ku5zJzPR6AZImqbF2d7jl61SlZkw==&VrWd=-Z5PLbzhUhYhR8K	true	• Avira URL Cloud: malware	unknown
http://www.multimediapages.com/qmpa/?mRh4lr=rejTwVtqfB30O9nwV+ATTccd4/r3ZShDvm2ExT48d5W41t5gt2xe96xDcyDktEvrNydQ6GKmhPSZbQq/61ftArfg9GGH4Fupqg==&VrWd=-Z5PLbzhUhYhR8K	true	• Avira URL Cloud: malware	unknown
http://www.notarpucarhr.com/qmpa/?mRh4lr=EgIWtG18ZIzAqtaO1OmvkFLdPjhKt8Mp7J5Y1fxWkEB6Q9kPLkR881s923Q+G4W9S+aNob6MQv0YuDJ73ehw8miGBWwdljwfXw==&VrWd=-Z5PLbzhUhYhR8K	true	• Avira URL Cloud: safe	unknown
www.erwgcb.top/qmpa/	true	• Avira URL Cloud: safe	low
http://www.oaksinstitute.net/qmpa/	true	• Avira URL Cloud: malware	unknown
http://www.multimediapages.com/qmpa/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.vodien.com/	systray.exe, 0000000A.00000002.564786967.0000000004FFA000.00000004.10000000.00040000.00000000.sdmp, systray.exe, 0000000A.00000002.565197079.0000000006EB0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	systray.exe, 0000000A.00000003.530735455.0000000000915000.00000004.00000020.00020000.00000000.sdmp, q3W1-4699.10.dr	false		high
http://https://duckduckgo.com/ac/?q=	q3W1-4699.10.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.vodien.com/singapore-email-hosting.php	systray.exe, 0000000A.00000002.564786967.0000000004FFA000.00000004.10000000.00040000.00000000.sdmp, systray.exe, 0000000A.00000002.565197079.0000000006EB0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.com69	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300403427.000000000603400.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300174244.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301530080.0000000006038000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300428223.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300331288.0000000006037000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301709757.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300233806.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300190057.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300258498.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300558881.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300141919.000000000603500.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301117508.0000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300849965.0000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301599425.0000000006032000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300357512.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301307567.0000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300634815.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301060629.0000000006033000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300342875.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300950320.0000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301645997.000000000603100.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.304677827.000000000603400.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.commsedY	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.306938961.000000000600B00.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comFH	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299938247.000000000601A00.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comhy/	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300403427.000000000603400 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300428223.000000000603400 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300558881.000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300634815.0000000006034000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coml1	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.320113972.000000000600600 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297293605.000000000601B000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297563125.000000000601B000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297534420.0000000601B000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297455873.000000000601B000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297323577.000000000601B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/0	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301567715.000000000600D00 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301491988.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301216806.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301779924.000000000600D00 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301567715.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301491988.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301677692.0000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/$	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302865321.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302414369.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302326537.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.303167686.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302564228.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.303077151.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301779924.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302653539.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302751937.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301567715.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302146273.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301888455.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301491988.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302492163.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301677692.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302077028.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.303316822.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301987162.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.303418082.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.303007184.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301216806.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299882505.000000000603000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Y	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302865321.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302414369.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302326537.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302564228.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301779924.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302653539.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302751937.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301567715.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302146273.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301888455.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301491988.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302492163.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301677692.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302077028.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301987162.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301216806.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302803561.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302242022.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302950130.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/ry	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301083951.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301779924.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301567715.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302146273.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301888455.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301491988.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301677692.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302077028.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301987162.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301216806.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301157376.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comicu	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.320113972.000000000600600.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.308810403.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.308658468.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.compe	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300403427.000000000603400 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300174244.000000000603400 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301530080.000000006038000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300428223.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300331288.0000000006037000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301709757.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300233806.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300190057.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300258498.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300558881.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300141919.000000000603500 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301117508.000000000603100 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300849965.000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301599425.0000000006032000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300357512.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301307567.0000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300634815.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301060629.0000000006033000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300119023.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300099384.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300342875.000000000603500 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/S	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301083951.000000000600D00 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300913114.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comegr	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297293605.000000000601B00 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297323577.000000000601B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/P	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301779924.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301567715.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301491988.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301677692.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301216806.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301157376.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0P	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301779924.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301677692.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	q3W1-4699.10.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	systray.exe, 0000000A.00000003.530735455.0000000000915000.00000004.00000020.00020000.00000000.sdmp, q3W1-4699.10.dr	false		high
http://www.carterandcone.coml	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml-B(	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299985983.000000000603500.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cntsP=	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299462548.000000000603300.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/x	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301083951.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301779924.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301567715.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301491988.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301677692.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301216806.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301157376.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cnV	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299882505.000000000603300.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cno.z	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299882505.000000000603300.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/l	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300913114.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalicg	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.305767115.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.306938961.000000000600B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cntsP=tx	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299447483.000000000603300 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma$	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.320113972.000000000600600 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersH	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.304189881.000000000603400 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.comegrjJH	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297615331.000000000601B00 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297563125.000000000601B000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297590159.000000000601B000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297534420.000000000601B000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297455873.000000000601B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comre	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300357512.000000000603500 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300342875.000000000603500.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	systray.exe, 0000000A.00000003.530735455.0000000000915000.00000004.00000020.00020000.00000000.sdmp, q3W1-4699.10.dr	false		high
http://www.fontbureau.com/designersW	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.312655895.000000000603400 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300487990.000000000601600 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300403427.000000000603400 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299949266.000000006033000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300174244.000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301530080.000000006038000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300428223.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300331288.0000000006037000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301709757.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300233806.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300190057.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300258498.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300558881.000000000603400 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300033238.000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300141919.000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301117508.000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300849965.0000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301599425.0000000006032000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300357512.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301307567.0000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300634815.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301060629.0000000006033000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300119023.000000000603500 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comsigW	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300403427.000000000603400 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300174244.000000000603400 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299985983.000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300428223.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300331288.0000000006037000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300233806.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300190057.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300258498.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300033238.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300141919.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300357512.000000000603500 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300119023.000000000603500 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300099384.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300342875.0000000006035000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C2000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.308674164.000000000612000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.308958537.0000000006012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comers0J	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297563125.000000000601B000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297590159.000000000601B000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297534420.0000000000601B000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297455873.0000000000601B000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297323577.000000000601B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comily	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300331288.000000000603700 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300357512.000000000603500 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300342875.0000000006035000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com8I	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299938247.000000000601A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comU	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297563125.000000000601B000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297534420.000000006001B000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297455873.000000000601B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comits	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300403427.000000000603400.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300174244.000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300428223.000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301948951.0000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300331288.0000000006037000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301709757.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300233806.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300190057.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300258498.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300558881.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300141919.000000000603500.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301117508.000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300849965.000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301599425.0000006032000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302181801.0000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300357512.0000000006035000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301307567.0000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300634815.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301855291.0000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302114099.0000000006031000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301060629.000000000603300.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

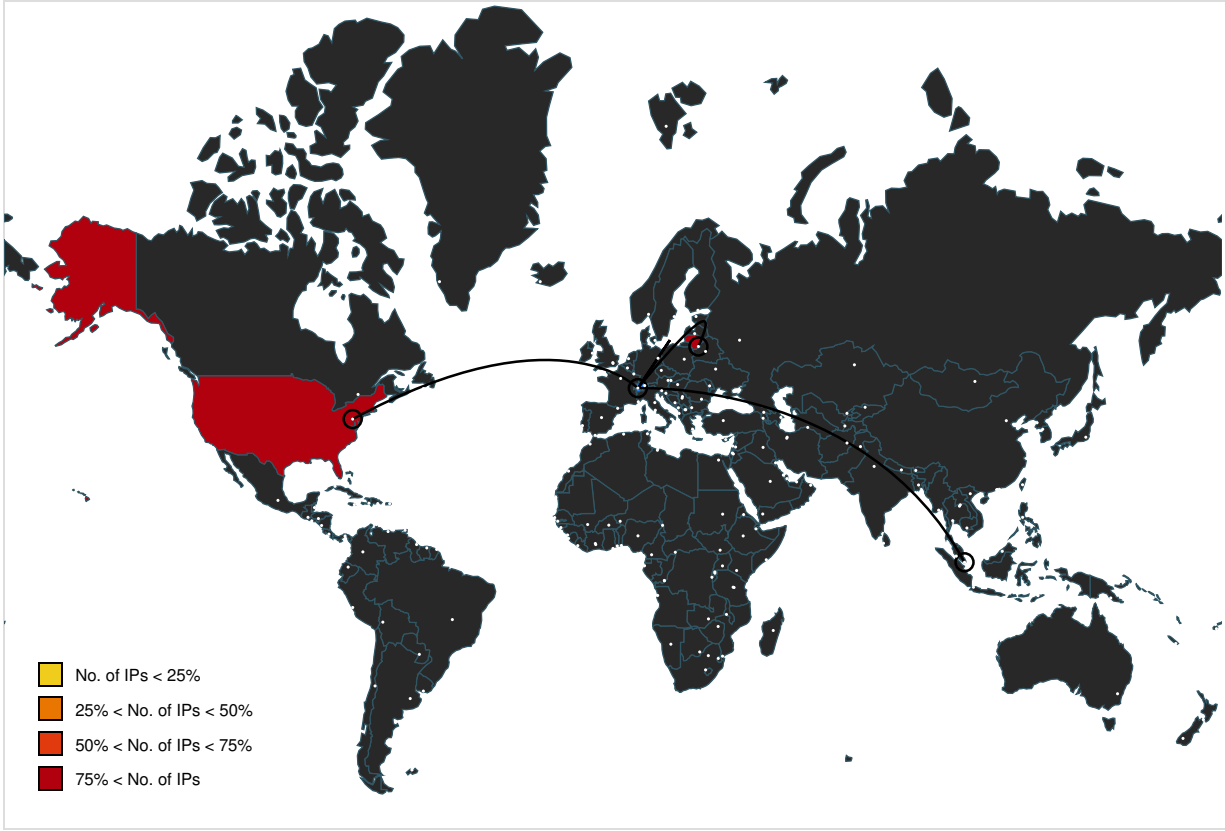
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htmtr-tr	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.309958548.000000000603400 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.309176604.000000000603400 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.309323595.000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.309409920.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.309038359.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.309119313.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.308591362.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.309275276.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.309634439.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.308723291.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.309847410.000000000603400 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.309538175.000000000603400 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.308827341.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.309771643.0000000006034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.308893439.0000000006034000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comGr	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299949266.000000000603300 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299985983.000000000603500 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/l	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301083951.000000000600D00 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301779924.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301567715.0000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301491988.000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301677692.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301216806.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301157376.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297868606.000000000601B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comsign	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300331288.000000000603700 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300233806.000000000603500 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300190057.000000000 6035000.00000004.00000800.00020000.00000 0000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300258498.000 0000006035000.00000004.00000800.00020000 .00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300357512 .0000000006035000.00000004.00000800.0002 0000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.30034 2875.0000000006035000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comcom	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.297839542.000000000601B00 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comueedl	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.306938961.000000000600B00 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersiv	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.312655895.000000000603400 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.312618448.000000000603500 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299768442.000000000601A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C200 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.306938961.000000000600B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comF	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.306938961.000000000600B00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	systray.exe, 0000000A.00000003.530735455 .0000000000915000.00000004.00000020.00020000.00000000.sdmp, q3W1-4699.10.dr	false		high
http://www.carterandcone.comitse	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300233806.000000000603500 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comfac	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300141919.000000000603500 0.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300119023.000000000603500 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	systray.exe, 0000000A.00000003.530735455 .0000000000915000.00000004.00000020.00020000.00000000.sdmp, q3W1-4699.10.dr	false		high
http://www.fontbureau.comL.TTF	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.306938961.000000000600B00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301779924.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301567715.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302146273.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301888455.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301491988.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301677692.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302077028.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301987162.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301216806.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301157376.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	q3W1-4699.10.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	systray.exe, 0000000A.00000003.530735455.0000000000915000.00000004.00000020.00020000.00000000.sdmp, q3W1-4699.10.dr	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C2000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299606103.000000000633000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299501081.000000000600B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comdP	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.305767115.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.306938961.000000000600B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.305767115.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.monotype.	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300403427.000000000603400.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers%	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.306012210.000000000603400.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comm	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.306938961.000000000600B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.300913114.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301779924.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302653539.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302751937.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301567715.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302146273.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301888455.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301491988.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302492163.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301677692.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302077028.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301987162.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301216806.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301157376.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.302242022.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/:	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.308810403.000000000600D000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.308658468.000000000600D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.comP1	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301976081.000000000604400.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.301878220.000000000604300.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cno.	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.299882505.000000000603300.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.305003600.000000000603400.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000002.336589275.00000000072C2000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.305032513.000000000600034000.00000004.00000800.00020000.00000000.sdmp, Ziraat Bankasi Swift Mesaji20221129-34221.exe, 00000002.00000003.305068305.000000006035000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.11.189.189	www.oaksinstitute.net	Singapore		58621	VODIEN-AS-AP-LOC2VodienInternetSolutionsPteLtdSG	true
141.136.43.229	notarpucarhr.com	Lithuania		207291	SENDER-ASLT	true
38.239.92.131	www.multimediapages.com	United States		174	COGENT-174US	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755920
Start date and time:	2022-11-29 10:15:36 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ziraat Bankasi Swift Mesaji20221129-34221.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/2@4/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 43.7% (good quality ratio 38.2%) • Quality average: 71.9% • Quality standard deviation: 33.2%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing d isassembly code information.
- Report size getting too big, t oo many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:16:34	API Interceptor	2x Sleep call for process: Ziraat Bankasi Swift Mesaji20221129-34221.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Ziraat Bankasi Swift Mesaji20221129-34221.exe.log

Process:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji20221129-34221.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859

Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\q3W1-4699

Process:	C:\Windows\SysWOW64\systray.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.808753534771263
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:	Ziraat Bankasi Swift Mesaji20221129-34221.exe
File size:	736256
MD5:	6a0ff43510923c27b144bf86b5e0a867
SHA1:	880c264f12ea2175a81f7030dec9c7043093253f
SHA256:	52426e75e25f69d9d7a8121464fe16a213ab48519ae10b2e2fc028ce86794a8b
SHA512:	18f0247de11b5d3a7139f8c577560a2987fa706ed0b1eb8f08b01384d320508edbce31ceab050a82a09a97b8892680b3cab3e878bac4a1e7bfaa797ac8595c60
SSDEEP:	12288:vX1wDXZCg8FEJLIJWyBgFuPDhd55slqVvsH4B4oks60PoSpK:vFwJpVIJxBnTzsOBl0Poo
TLSH:	1CF4F1BEB1D39F52C38415B2C5D2A92003E685871576FB463B8142DAEE237E45C4BBCB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....]..... .....0..2.....Q... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b51ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xE3C25DA2 [Thu Feb 1 10:59:46 2091 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb5180	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb6000	0x5b8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb513d	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb31d4	0xb3200	False	0.8954308051290998	data	7.8163399193374055	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x5b8	0x600	False	0.427734375	data	4.111112445993303	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb8000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xb60a0	0x32c	data		
RT_MANIFEST	0xb63cc	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

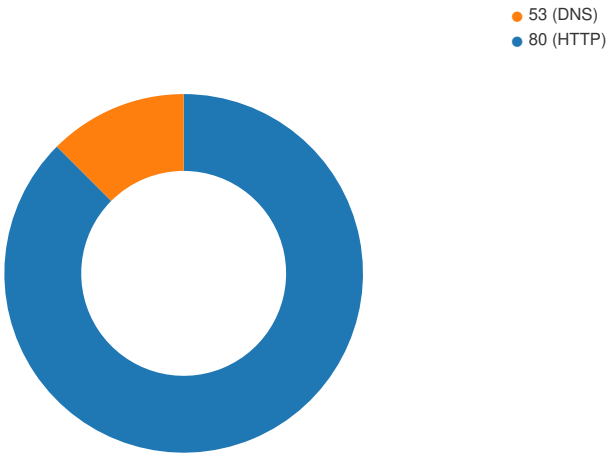
Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution

Total Packets: 32



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 10:18:12.099618912 CET	49698	80	192.168.2.4	141.136.43.229
Nov 29, 2022 10:18:12.132400036 CET	80	49698	141.136.43.229	192.168.2.4
Nov 29, 2022 10:18:12.132574081 CET	49698	80	192.168.2.4	141.136.43.229
Nov 29, 2022 10:18:12.132653952 CET	49698	80	192.168.2.4	141.136.43.229
Nov 29, 2022 10:18:12.166188002 CET	80	49698	141.136.43.229	192.168.2.4
Nov 29, 2022 10:18:12.166218996 CET	80	49698	141.136.43.229	192.168.2.4
Nov 29, 2022 10:18:12.166239977 CET	80	49698	141.136.43.229	192.168.2.4
Nov 29, 2022 10:18:12.166260958 CET	80	49698	141.136.43.229	192.168.2.4
Nov 29, 2022 10:18:12.166452885 CET	49698	80	192.168.2.4	141.136.43.229
Nov 29, 2022 10:18:12.166454077 CET	49698	80	192.168.2.4	141.136.43.229
Nov 29, 2022 10:18:12.166740894 CET	49698	80	192.168.2.4	141.136.43.229
Nov 29, 2022 10:18:12.199331999 CET	80	49698	141.136.43.229	192.168.2.4
Nov 29, 2022 10:18:17.455929995 CET	49699	80	192.168.2.4	38.239.92.131
Nov 29, 2022 10:18:17.713973045 CET	80	49699	38.239.92.131	192.168.2.4
Nov 29, 2022 10:18:17.714298010 CET	49699	80	192.168.2.4	38.239.92.131
Nov 29, 2022 10:18:17.714528084 CET	49699	80	192.168.2.4	38.239.92.131
Nov 29, 2022 10:18:17.972193003 CET	80	49699	38.239.92.131	192.168.2.4
Nov 29, 2022 10:18:17.976200104 CET	80	49699	38.239.92.131	192.168.2.4
Nov 29, 2022 10:18:17.976226091 CET	80	49699	38.239.92.131	192.168.2.4
Nov 29, 2022 10:18:17.976337910 CET	49699	80	192.168.2.4	38.239.92.131
Nov 29, 2022 10:18:18.715300083 CET	49699	80	192.168.2.4	38.239.92.131
Nov 29, 2022 10:18:19.732419014 CET	49700	80	192.168.2.4	38.239.92.131
Nov 29, 2022 10:18:19.991139889 CET	80	49700	38.239.92.131	192.168.2.4
Nov 29, 2022 10:18:19.991379976 CET	49700	80	192.168.2.4	38.239.92.131
Nov 29, 2022 10:18:19.991839886 CET	49700	80	192.168.2.4	38.239.92.131
Nov 29, 2022 10:18:20.250371933 CET	80	49700	38.239.92.131	192.168.2.4
Nov 29, 2022 10:18:20.253719091 CET	80	49700	38.239.92.131	192.168.2.4
Nov 29, 2022 10:18:20.253741980 CET	80	49700	38.239.92.131	192.168.2.4
Nov 29, 2022 10:18:20.253756046 CET	80	49700	38.239.92.131	192.168.2.4
Nov 29, 2022 10:18:20.253885984 CET	49700	80	192.168.2.4	38.239.92.131
Nov 29, 2022 10:18:20.253931046 CET	49700	80	192.168.2.4	38.239.92.131
Nov 29, 2022 10:18:20.254262924 CET	49700	80	192.168.2.4	38.239.92.131
Nov 29, 2022 10:18:20.514318943 CET	80	49700	38.239.92.131	192.168.2.4
Nov 29, 2022 10:18:25.456048012 CET	49701	80	192.168.2.4	103.11.189.189
Nov 29, 2022 10:18:25.636853933 CET	80	49701	103.11.189.189	192.168.2.4
Nov 29, 2022 10:18:25.637147903 CET	49701	80	192.168.2.4	103.11.189.189
Nov 29, 2022 10:18:25.637303114 CET	49701	80	192.168.2.4	103.11.189.189
Nov 29, 2022 10:18:25.817992926 CET	80	49701	103.11.189.189	192.168.2.4
Nov 29, 2022 10:18:25.818844080 CET	80	49701	103.11.189.189	192.168.2.4
Nov 29, 2022 10:18:25.818865061 CET	80	49701	103.11.189.189	192.168.2.4
Nov 29, 2022 10:18:25.818928003 CET	80	49701	103.11.189.189	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 10:18:25.818967104 CET	49701	80	192.168.2.4	103.11.189.189
Nov 29, 2022 10:18:25.819005966 CET	49701	80	192.168.2.4	103.11.189.189
Nov 29, 2022 10:18:26.653980970 CET	49701	80	192.168.2.4	103.11.189.189
Nov 29, 2022 10:18:27.664506912 CET	49702	80	192.168.2.4	103.11.189.189
Nov 29, 2022 10:18:27.854477882 CET	80	49702	103.11.189.189	192.168.2.4
Nov 29, 2022 10:18:27.854909897 CET	49702	80	192.168.2.4	103.11.189.189
Nov 29, 2022 10:18:27.855137110 CET	49702	80	192.168.2.4	103.11.189.189
Nov 29, 2022 10:18:28.044476032 CET	80	49702	103.11.189.189	192.168.2.4
Nov 29, 2022 10:18:28.045181036 CET	80	49702	103.11.189.189	192.168.2.4
Nov 29, 2022 10:18:28.045207024 CET	80	49702	103.11.189.189	192.168.2.4
Nov 29, 2022 10:18:28.045227051 CET	80	49702	103.11.189.189	192.168.2.4
Nov 29, 2022 10:18:28.064215899 CET	49702	80	192.168.2.4	103.11.189.189
Nov 29, 2022 10:18:28.064922094 CET	49702	80	192.168.2.4	103.11.189.189
Nov 29, 2022 10:18:28.254328012 CET	80	49702	103.11.189.189	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 10:18:12.005403042 CET	50911	53	192.168.2.4	8.8.8.8
Nov 29, 2022 10:18:12.036030054 CET	53	50911	8.8.8.8	192.168.2.4
Nov 29, 2022 10:18:17.173329115 CET	59683	53	192.168.2.4	8.8.8.8
Nov 29, 2022 10:18:17.454163074 CET	53	59683	8.8.8.8	192.168.2.4
Nov 29, 2022 10:18:25.268935919 CET	64167	53	192.168.2.4	8.8.8.8
Nov 29, 2022 10:18:25.443312883 CET	53	64167	8.8.8.8	192.168.2.4
Nov 29, 2022 10:18:33.067755938 CET	58565	53	192.168.2.4	8.8.8.8
Nov 29, 2022 10:18:33.199367046 CET	53	58565	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 10:18:12.005403042 CET	192.168.2.4	8.8.8.8	0xb2cb	Standard query (0)	www.notarpucarhr.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:18:17.173329115 CET	192.168.2.4	8.8.8.8	0xa946	Standard query (0)	www.multimediapages.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:18:25.268935919 CET	192.168.2.4	8.8.8.8	0xc60f	Standard query (0)	www.oaksinstitute.net	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:18:33.067755938 CET	192.168.2.4	8.8.8.8	0x2fe9	Standard query (0)	www.thetrendsinfo.com	A (IP address)	IN (0x0001)	false

DNS Answers

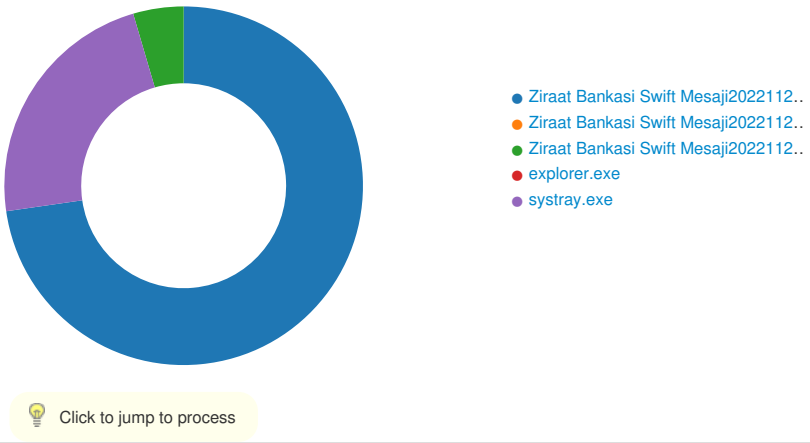
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 10:18:12.036030054 CET	8.8.8.8	192.168.2.4	0xb2cb	No error (0)	www.notarpucarhr.com	notarpucarhr.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 10:18:12.036030054 CET	8.8.8.8	192.168.2.4	0xb2cb	No error (0)	notarpucarhr.com		141.136.43.229	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:18:17.454163074 CET	8.8.8.8	192.168.2.4	0xa946	No error (0)	www.multimediapages.com		38.239.92.131	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:18:25.443312883 CET	8.8.8.8	192.168.2.4	0xc60f	No error (0)	www.oaksinstitute.net		103.11.189.189	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:18:33.199367046 CET	8.8.8.8	192.168.2.4	0x2fe9	No error (0)	www.thetrendsinfo.com	thetrendsinfo.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 10:18:33.199367046 CET	8.8.8.8	192.168.2.4	0x2fe9	No error (0)	thetrendsinfo.com		68.66.216.12	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.notarpucarhr.com
- www.multimediapages.com
- www.oaksinstitute.net

Statistics

Behavior



System Behavior

Analysis Process: Ziraat Bankasi Swift Mesaji20221129-34221.exe PID: 3176, Parent PID: 3528

General

Target ID:	2
Start time:	10:16:23
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji20221129-34221.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji20221129-34221.exe
Imagebase:	0xbd0000
File size:	736256 bytes
MD5 hash:	6A0FF43510923C27B144BF86B5E0A867
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000002.00000002.331328236.0000000003337000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000002.00000002.329721340.0000000003121000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: Ziraat Bankasi Swift Mesaji20221129-34221.exe PID: 5152, Parent PID: 3176

General	
Target ID:	5
Start time:	10:16:35
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji20221129-34221.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji20221129-34221.exe
Imagebase:	0x30000
File size:	736256 bytes
MD5 hash:	6A0FF43510923C27B144BF86B5E0A867
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Ziraat Bankasi Swift Mesaji20221129-34221.exe PID: **1308**, Parent PID: **3176**

General	
Target ID:	6
Start time:	10:16:36
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji20221129-34221.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji20221129-34221.exe
Imagebase:	0x7e0000
File size:	736256 bytes
MD5 hash:	6A0FF43510923C27B144BF86B5E0A867
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.450620046.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.450620046.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.450620046.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.450620046.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.451409709.0000000001150000.00000040.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41DF6E	NtReadFile

Analysis Process: explorer.exe PID: **3528**, Parent PID: **1308**

General	
Target ID:	7
Start time:	10:16:42
Start date:	29/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff618f60000
File size:	3933184 bytes

MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.413620011.000000000DEDE000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000007.00000000.413620011.000000000DEDE000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.413620011.000000000DEDE000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.413620011.000000000DEDE000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.388632949.000000000DEDE000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000007.00000000.388632949.000000000DEDE000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.388632949.000000000DEDE000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.388632949.000000000DEDE000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: systray.exe PID: 1312, Parent PID: 1308

General

Target ID:	10
Start time:	10:17:35
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\systray.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\systray.exe
Imagebase:	0x1010000
File size:	9728 bytes
MD5 hash:	1373D481BE4C8A6E5F5030D2FB0A0C68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.560048415.0000000000820000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000002.560048415.0000000000820000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.560048415.0000000000820000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.560048415.0000000000820000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.559572185.00000000003C0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000002.559572185.00000000003C0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.559572185.00000000003C0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.559572185.00000000003C0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.562531717.0000000000ED0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000002.562531717.0000000000ED0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.562531717.0000000000ED0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.562531717.0000000000ED0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji20221129-34221.exe	success or wait	1	3DC867	NtDeleteFile
C:\Users\user\AppData\Local\Temp\q3W1-4699	object name not found	1	3DC867	NtDeleteFile
C:\Users\user\AppData\Local\Temp\q3W1-4699	sharing violation	1	3DC867	NtDeleteFile
C:\Users\user\AppData\Local\Temp\q3W1-4699	sharing violation	1	3DC867	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	3DC837	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Disassembly

No disassembly