ID: 635281
Sample Name: Ziraat Bankasi Swift Mesaji.exe
Cookbook: default.jbs
Time: 18:22:08
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

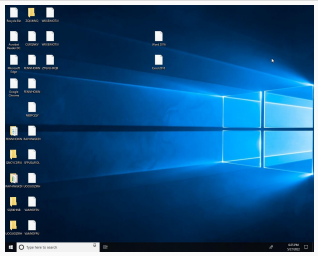
Windows Analysis Report

Ziraat Bankasi Swift Mesaji.exe

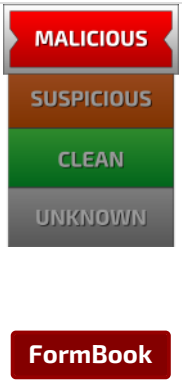
Overview

General Information

Sample Name:	Ziraat Bankasi Swift Mesaji.exe
Analysis ID:	635281
MD5:	d891e26c070797..
SHA1:	039457a2c4d73c..
SHA256:	2979a77144d0df..
Tags:	exe Formbook geo TUR ZiraatBank
Infos:	



Detection



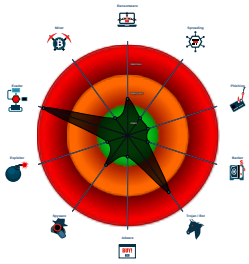
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Self deletion via cmd or bat file
- Tries to detect sandboxes and other…
- Injects a PE file into a foreign proce…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- Ziraat Bankasi Swift Mesaji.exe (PID: 6344 cmdline: "C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe" MD5: D891E26C0707977398E963D6076EEAE1)
  - Ziraat Bankasi Swift Mesaji.exe (PID: 6572 cmdline: C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe MD5: D891E26C0707977398E963D6076EEAE1)
    - explorer.exe (PID: 3808 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 4708 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
        - cmd.exe (PID: 3736 cmdline: /c del "C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - explorer.exe (PID: 1388 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.wwohead.com/ah6m/"
  ],
  "decoy": [
    "saudeybeleza.com",
    "ethereumtiger.business",
    "thesoupproject.net",
    "cedarwoodtownhomesnp.com",
    "gyascool.com",
    "gosourcecap.com",
    "womeninnetworking.net",
    "nahade-gostar.com",
    "dcman900.com",
    "mirrorparcel.com",
    "lamowlettu.xyz",
    "glencoreprocurement.com",
    "codsini.com",
    "thripear.space",
    "movierepository.com",
    "51cdfang.com",
    "hananiabeauty.store",
    "mortgagemanuas.com",
    "remotingpeople.com",
    "myimpressivefashion.com",
    "northhamptonapartments.com",
    "lostinsmokemint.xyz",
    "sebhbr.xyz",
    "hummingbirdfeederhat.com",
    "maplebakers.com",
    "unwrapmelingerie.com",
    "felipekamakura.com",
    "stringm.com",
    "ukgdimensions.red",
    "shopofplaythings.com",
    "jinlebao.com",
    "alenapolozkova.com",
    "aerialdatainc.com",
    "metaverseiop.com",
    "yuh-gal-p.xyz",
    "thebluejaybuilder.com",
    "my-mallorca.estate",
    "experteee.com",
    "difan-mobile.com",
    "postalhistoryworld.com",
    "codifyrear.xyz",
    "cankiribelediyespor.net",
    "alizandracloset.com",
    "everythingmandab.com",
    "africabet365.bet",
    "ww223343.com",
    "xpresslinkshippement.com",
    "xiaochunge.top",
    "parkerbeautyfragrance.com",
    "makerthejackets.com",
    "souldig.xyz",
    "irstaxbenfits.com",
    "audiopilot.xyz",
    "theguaranteedadmissions.com",
    "nontradebulkcement.online",
    "alltinyildiz.com",
    "celestialtherapy.net",
    "11milliondreams.com",
    "matadorbet182.com",
    "gabimejia.com",
    "planet-ideam.com",
    "os00hpaeo4hu726fp.life",
    "etudier-medecine-roumanie.com",
    "zilong88.top"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.403126818.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000000.403126818.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000000.403126818.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
0000000B.00000002.632202833.0000000000B90000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000002.632202833.0000000000B90000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 33 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Ziraat Bankasi Swift Mesaji.exe.44eb6c0.5.unpack	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x4f7eb:$s1: file:/// • 0x4f6fb:$s2: {11111-22222-10009-11112} • 0x4f77b:$s3: {11111-22222-50001-00000} • 0x4cc15:$s4: get_Module • 0x4d05b:$s5: Reverse • 0x4f02a:$s6: BlockCopy • 0x4ee6e:$s7: ReadByte • 0x4f7fd:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 56 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...
0.2.Ziraat Bankasi Swift Mesaji.exe.44bbf10.6.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.Ziraat Bankasi Swift Mesaji.exe.44bbf10.6.raw.unpack	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x80d9b:$s1: file:/// • 0x80cab:$s2: {11111-22222-10009-11112} • 0x80d2b:$s3: {11111-22222-50001-00000} • 0x7e1c5:$s4: get_Module • 0x7e60b:$s5: Reverse • 0x805da:$s6: BlockCopy • 0x8041e:$s7: ReadByte • 0x80dad:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 56 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...

Source	Rule	Description	Author	Strings
0.2.Ziraat Bankasi Swift Mesaji.exe.44bbf10.6.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xc2ed8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xc3142:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xcec75:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xce761:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xced77:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xceeef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xc3b5a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xcd9dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xc4853:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xd4ee7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xd5eea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.Ziraat Bankasi Swift Mesaji.exe.44bbf10.6.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0xd1e09:$sqlite3step: 68 34 1C 7B E1 • 0xd1f1c:$sqlite3step: 68 34 1C 7B E1 • 0xd1e38:$sqlite3text: 68 38 2A 90 C5 • 0xd1f5d:$sqlite3text: 68 38 2A 90 C5 • 0xd1e4b:$sqlite3blob: 68 53 D8 7F 8C • 0xd1f73:$sqlite3blob: 68 53 D8 7F 8C
Click to see the 31 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd or bat file

Malware Analysis System Evasion

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

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

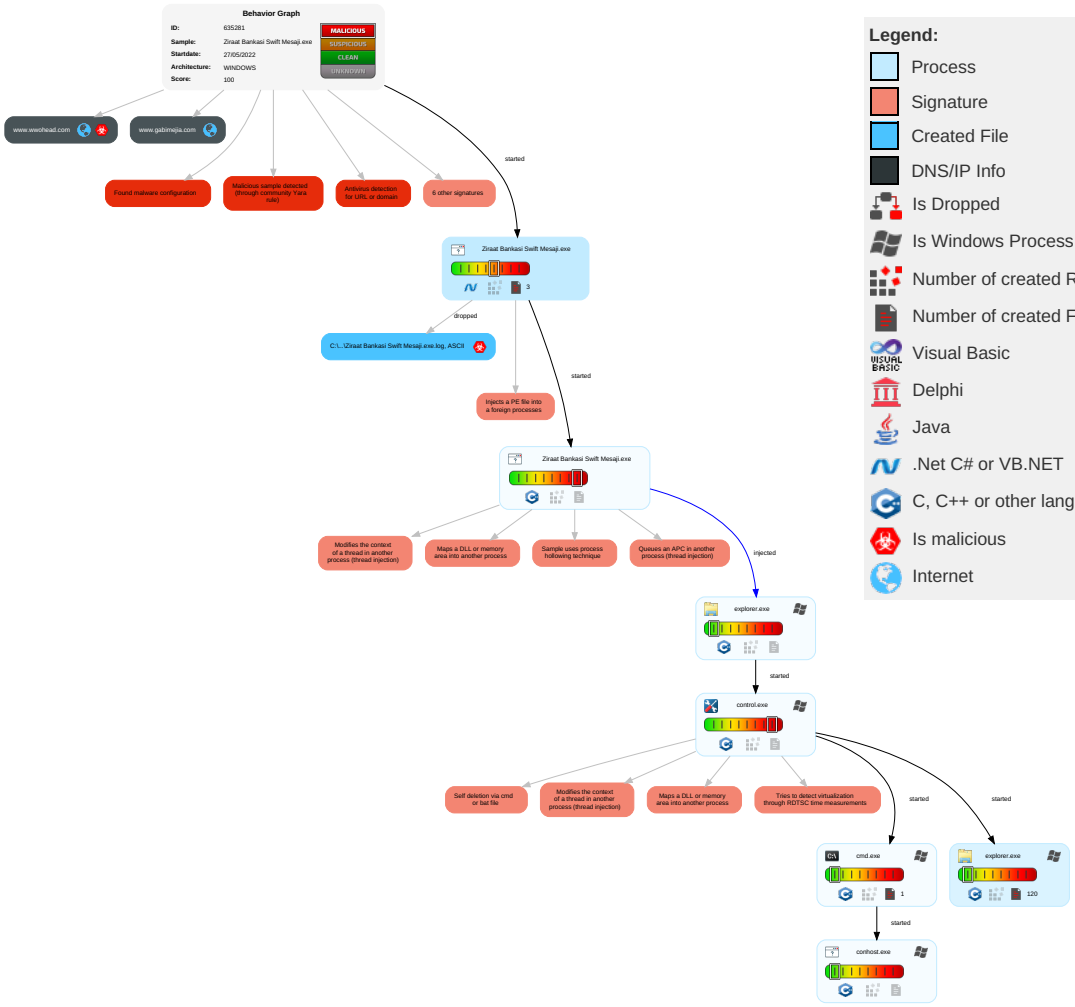
Remote Access Functionality

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	5 1 2 Process Injection	1 Masquerading	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	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	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	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	Data from Network Shared Drive	Automated Exfiltration	1 1 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)	5 1 2 Process Injection	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 1 2 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	3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	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

Behavior Graph

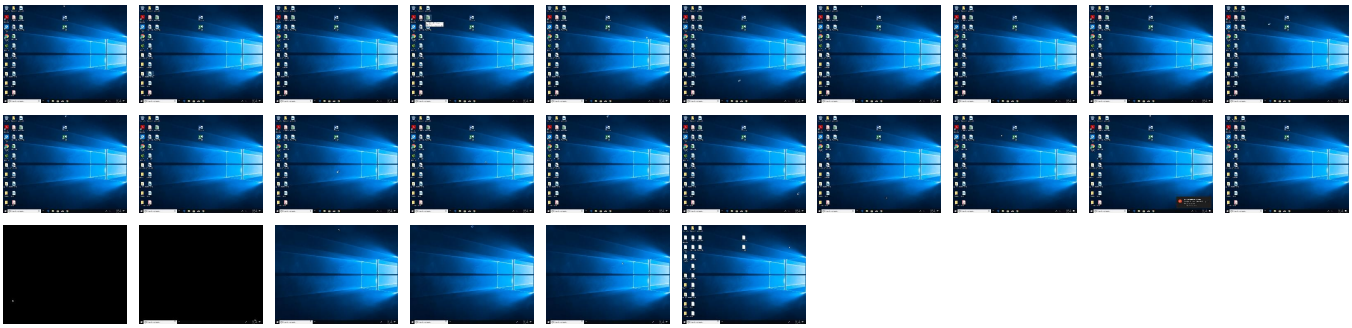


Hide Legend

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Ziraat Bankasi Swift Mesaji.exe	22%	ReversingLabs	ByteCode-MSIL.Spyware.Negasteal	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.Ziraat Bankasi Swift Mesaji.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.Ziraat Bankasi Swift Mesaji.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.Ziraat Bankasi Swift Mesaji.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.Ziraat Bankasi Swift Mesaji.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
dual-a-0001.dc-msedge.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.gabimejia.com	0%	Avira URL Cloud	safe	
http://www.thesoupproject.netReferer:	0%	Avira URL Cloud	safe	
http://www.51cdfang.com/ah6m/www.theguaranteedadmissions.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.yuh-gal-p.xyzReferer:	0%	Avira URL Cloud	safe	
http://www.aerialdatainc.com/ah6m/www.planet-ideam.com	0%	Avira URL Cloud	safe	
www.wwohead.com/ah6m/	100%	Avira URL Cloud	malware	
http://www.glencoreprocurement.comReferer:	0%	Avira URL Cloud	safe	
http://www.xiaochunge.top/ah6m/	0%	Avira URL Cloud	safe	
http://www.alltinyildiz.com/ah6m/www.xiaochunge.top	0%	Avira URL Cloud	safe	
http://www.nontradebulkcement.online/ah6m/	0%	Avira URL Cloud	safe	
http://www.wwohead.comReferer:	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.planet-ideam.com	0%	Avira URL Cloud	safe	
http://www.theguaranteedadmissions.comReferer:	0%	Avira URL Cloud	safe	
http://www.hummingbirdfeederhat.comReferer:	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.alltinyildiz.com	0%	Avira URL Cloud	safe	
http://www.gabimejia.com/ah6m/www.wwohead.com	0%	Avira URL Cloud	safe	
http://www.planet-ideam.comReferer:	0%	Avira URL Cloud	safe	
http://www.aerialdatainc.com/ah6m/	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.thesoupproject.net/ah6m/www.everythingmandab.com	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.nontradebulkcement.onlineReferer:	0%	Avira URL Cloud	safe	
http://www.nontradebulkcement.online/ah6m/www.hummingbirdfeederhat.com	0%	Avira URL Cloud	safe	
http://www.wwohead.com	0%	Avira URL Cloud	safe	
http://www.everythingmandab.com/ah6m/	0%	Avira URL Cloud	safe	
http://www.nontradebulkcement.online	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.xiaochunge.topReferer:	0%	Avira URL Cloud	safe	
http://www.aerialdatainc.comReferer:	0%	Avira URL Cloud	safe	
http://www.planet-ideam.com/ah6m/www.glencoreprocurement.com	0%	Avira URL Cloud	safe	
http://www.wwohead.com/ah6m/	100%	Avira URL Cloud	malware	
http://www.planet-ideam.com/ah6m/	0%	Avira URL Cloud	safe	
http://www.theguaranteedadmissions.com/ah6m/www.aerialdatainc.com	0%	Avira URL Cloud	safe	
http://www.51cdfang.com	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.alltinyildiz.com/ah6m/	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.everythingmandab.comReferer:	0%	Avira URL Cloud	safe	
http://www.difan-mobile.com/ah6m/www.nontradebulkcement.online	0%	Avira URL Cloud	safe	
http://www.aerialdatainc.com	0%	Avira URL Cloud	safe	
http://ns.adobY	0%	URL Reputation	safe	
http://www.thesoupproject.net/ah6m/	0%	Avira URL Cloud	safe	
http://www.hummingbirdfeederhat.com/ah6m/	0%	Avira URL Cloud	safe	
http://www.wwohead.com/ah6m/www.51cdfang.com	100%	Avira URL Cloud	malware	
http://www.yuh-gal-p.xyz/ah6m/	0%	Avira URL Cloud	safe	
http://www.xiaochunge.top/ah6m/www.difan-mobile.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.alltinyildiz.comReferer:	0%	Avira URL Cloud	safe	
http://www.difan-mobile.com/ah6m/	0%	Avira URL Cloud	safe	
http://www.gabimejia.com/ah6m/	0%	Avira URL Cloud	safe	
http://www.51cdfang.comReferer:	0%	Avira URL Cloud	safe	
http://www.glencoreprocurement.com/ah6m/www.thesoupproject.net	0%	Avira URL Cloud	safe	
http://www.yuh-gal-p.xyz	0%	Avira URL Cloud	safe	
http://www.difan-mobile.com	0%	Avira URL Cloud	safe	
http://www.glencoreprocurement.com/ah6m/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.everythingmandab.com/ah6m/www.stringm.com	0%	Avira URL Cloud	safe	
http://www.theguaranteedadmissions.com/ah6m/	0%	Avira URL Cloud	safe	
http://www.51cdfang.com/ah6m/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.stringm.com/ah6m/	100%	Avira URL Cloud	malware	
http://www.hummingbirdfeederhat.com	0%	Avira URL Cloud	safe	
http://www.yuh-gal-p.xyz/ah6m/www.alltinyildiz.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.stringm.comReferer:	0%	Avira URL Cloud	safe	
http://www.difan-mobile.comReferer:	0%	Avira URL Cloud	safe	
http://www.theguaranteedadmissions.com	0%	Avira URL Cloud	safe	
http://www.gabimejia.comReferer:	0%	Avira URL Cloud	safe	
http://www.stringm.com/ah6m/www.yuh-gal-p.xyz	100%	Avira URL Cloud	malware	
http://www.everythingmandab.com	0%	Avira URL Cloud	safe	
http://www.stringm.com	0%	Avira URL Cloud	safe	
http://www.xiaochunge.top	0%	Avira URL Cloud	safe	
http://www.glencoreprocurement.com	0%	Avira URL Cloud	safe	
http://www.thesoupproject.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dual-a-0001.dc-msedge.net	131.253.33.200	true	false	• 0%, Virustotal, Browse	unknown
www.gabimejia.com	104.140.60.254	true	false		unknown
www.wwohead.com	172.252.94.104	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.wwohead.com/ah6m/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.gabimejia.com	explorer.exe, 00000015.00000002.66968480 0.0000000008A8B000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002 .413299631.0000000007422000.00000004.000 00800.00020000.00000000.sdmp	false		high
http://www.thesoupproject.netReferer:	explorer.exe, 00000015.00000002.66968480 0.0000000008A8B000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/dcoetzee/plants-vs-zombies-user-file-editor	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000000.359661923.0000000000EB2000.00000002.00000001.01000000.00000003.sdmp, Ziraat Bankasi Swift Mesaji.exe, 00000002.00000000.401671865.0000000000D72000.00000002.00000001.01000000.00000003.sdmp, control.exe, 00000000B.00000002.666266960.000000000535F000.00000004.10000000.00040000.00000000.sdmp, explorer.exe, 00000015.00000000.615015403.00000000069EF000.00000004.80000000.00040000.00000000.sdmp	false		high
http://www.51cdfang.com/ah6m/www.theguaranteedadmissions.com	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.yuh-gal-p.xyzReferer:	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aerialdatainc.com/ah6m/www.planet-ideam.com	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.glencoreprocurement.comReferer:	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.xiaochunge.top/ah6m/	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com	Ziraat Bankasi Swift Mesaji.exe	false		high
http://www.alltinyildiz.com/ah6m/www.xiaochunge.top	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nontradebulkcement.online/ah6m/	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wwohead.comReferer:	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.planet-ideam.com	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.theguaranteedadmissions.comReferer:	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hummingbirdfeederhat.comReferer:	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.alltinyildiz.com	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gabimejia.com/ah6m/www.wwohead.com	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.planet-ideam.comReferer:	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aerialdatainc.com/ah6m/	explorer.exe, 00000015.00000002.669684800.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.thesoupproject.net/ah6m/www.everythingmandab.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.nontradebulkcement.onlineReferer:	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nontradebulkcement.online/ah6m/www.hummingbirdfeederhat.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wwohead.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.everythingmandab.com/ah6m/	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nontradebulkcement.online	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.xiaochunge.topReferer:	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aerialdatainc.comReferer:	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.planet-ideam.com/ah6m/www.glencoreprocurement.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wwohead.com/ah6m/	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.planet-ideam.com/ah6m/	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.theguaranteedadmissions.com/ah6m/www.aerialdatainc.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.51cdfang.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.alltinyildiz.com/ah6m/	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.everythingmandab.comReferer:	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.difan-mobile.com/ah6m/www.nontradebulkcement.online	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.aerialdatainc.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobY	explorer.exe, 00000004.00000000.463834252.00000000026D0000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.442686652.00000000026D0000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.411056762.00000000026D0000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.498956126.00000000026D0000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.thesoupproject.net/ah6m/	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hummingbirdfeederhat.com/ah6m/	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wwohead.com/ah6m/www.51cdfang.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.yuh-gal-p.xyz/ah6m/	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.xiaochunge.top/ah6m/www.difan-mobile.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.alltinyildiz.comReferer:	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.difan-mobile.com/ah6m/	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gabimejia.com/ah6m/	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.51cdfang.comReferer:	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.glencoreprocurement.com/ah6m/www.thesoupproject.net	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.yuh-gal-p.xyz	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.difan-mobile.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.glencoreprocurement.com/ah6m/	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.everythingmandab.com/ah6m/www.stringm.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.theguaranteedadmissions.com/ah6m/	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.51cdfang.com/ah6m/	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.stringm.com/ah6m/	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.hummingbirdfeederhat.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.yuh-gal-p.xyz/ah6m/www.alltinyildiz.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.stringm.comReferer:	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.difan-mobile.comReferer:	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.theguaranteedadmissions.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.413299631.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.gabimejia.comReferer:	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.stringm.com/ah6m/www.yuh-gal-p.xyz	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.everythingmandab.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.stringm.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.xiaochunge.top	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.glencoreprocurement.com	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thesoupproject.net	explorer.exe, 00000015.00000002.66968480.0000000008A8B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635281
Start date and time: 27/05/202218:22:08	2022-05-27 18:22:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ziraat Bankasi Swift Mesaji.exe

Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
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.evad.winEXE@8/1@2/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 60.9% (good quality ratio 54.3%) • Quality average: 69.5% • Quality standard deviation: 32.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SearchUI.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, ShellExperienceHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.54.89.106, 40.125.122.176, 52.152.110.14, 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.useroor.bigcatalog.commerce.microsoft.com, settings-win.data.microsoft.com, arc.msn.com, a-0001.a-afdentry.net.trafficmanager.net, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:23:37	API Interceptor	2x Sleep call for process: Ziraat Bankasi Swift Mesaji.exe modified
18:25:16	API Interceptor	44x Sleep call for process: explorer.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 Mesaji.exe.log

Process:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.744489165365895
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 Mesaji.exe
File size:	716288
MD5:	d891e26c0707977398e963d6076eeae1
SHA1:	039457a2c4d73c24ef410a7665a04e9d456019e7
SHA256:	2979a77144d0df70f4dff084420d8e034eb6f751027fa44d158de924960f2a6a
SHA512:	f75a0274621ee095f30d01b83a0d07d02974e6876384f4a99d1d818862d09781e600352479fc845a7c3e2cd885ac344d58742dd9b44e322966d710a59188740b
SSDEEP:	12288:O092x9bHoAUOvqVpleUE0q8cf7qb4dHDn8LaRASedck6Q:nUfbHodlC0qj7qcdHDn8La+SCchQ
TLSH:	4EE4F10072F81B22E2BA67FE6578A18403B67D946520E34E5DC278DB3B71F918E45F1B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....y.b.....0.....Z..... .....@.. .....@.....@.....

File Icon

Icon Hash:	4462f276dcec30e6

Static PE Info

General

Entrypoint:	0x4ab1da
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x629079C1 [Fri May 27 07:12:01 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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	0xab188	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xac000	0x57cc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xab050	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	0xa91e0	0xa9200	False	0.860052025591	data	7.74275900541	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xac000	0x57cc	0x5800	False	0.964577414773	data	7.89168206066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xac100	0x51a3	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xb12b4	0x14	data		
RT_VERSION	0xb12d8	0x2f4	data		
RT_MANIFEST	0xb15dc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	1.0.0.0
InternalName	CallingConvent.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	

Description	Data
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	CallingConvent.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:25:36.139713049 CEST	62843	53	192.168.2.7	8.8.8.8
May 27, 2022 18:25:36.309185982 CEST	53	62843	8.8.8.8	192.168.2.7
May 27, 2022 18:25:53.158830881 CEST	49495	53	192.168.2.7	8.8.8.8
May 27, 2022 18:25:53.581492901 CEST	53	49495	8.8.8.8	192.168.2.7

DNS Queries

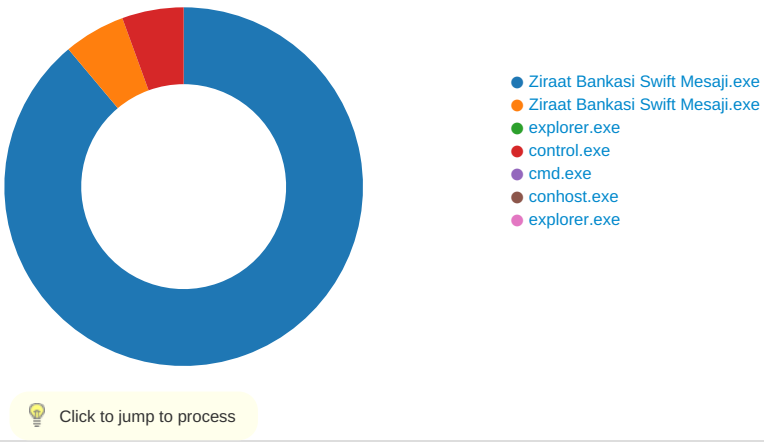
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 18:25:36.139713049 CEST	192.168.2.7	8.8.8.8	0xd167	Standard query (0)	www.gabimejia.com	A (IP address)	IN (0x0001)
May 27, 2022 18:25:53.158830881 CEST	192.168.2.7	8.8.8.8	0x98d2	Standard query (0)	www.wwohead.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 18:25:31.742157936 CEST	8.8.8.8	192.168.2.7	0x7a1c	No error (0)	www-bing-com.dual-a-0001.a-msedge.net	dual-a-0001.dc-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:25:31.742157936 CEST	8.8.8.8	192.168.2.7	0x7a1c	No error (0)	dual-a-0001.dc-msedge.net		131.253.33.200	A (IP address)	IN (0x0001)
May 27, 2022 18:25:31.742157936 CEST	8.8.8.8	192.168.2.7	0x7a1c	No error (0)	dual-a-0001.dc-msedge.net		13.107.22.200	A (IP address)	IN (0x0001)
May 27, 2022 18:25:36.309185982 CEST	8.8.8.8	192.168.2.7	0xd167	No error (0)	www.gabimejia.com		104.140.60.254	A (IP address)	IN (0x0001)
May 27, 2022 18:25:53.581492901 CEST	8.8.8.8	192.168.2.7	0x98d2	No error (0)	www.wwohead.com		172.252.94.104	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: Ziraat Bankasi Swift Mesaji.exe PID: **6344**, Parent PID: **2312**

General

Target ID:	0
Start time:	18:23:24
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe"
Imagebase:	0xeb0000
File size:	716288 bytes
MD5 hash:	D891E26C0707977398E963D6076EEAE1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.409614207.00000000035C7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.414265819.0000000007B70000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.409834205.0000000004322000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.409834205.0000000004322000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.409834205.0000000004322000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.407668611.0000000003251000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: Ziraat Bankasi Swift Mesaji.exe PID: **6572**, Parent PID: **6344**

General

Target ID:	2
Start time:	18:23:43
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
Imagebase:	0xd70000
File size:	716288 bytes
MD5 hash:	D891E26C0707977398E963D6076EEAE1
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: 00000002.00000000.403126818.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.403126818.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.403126818.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.404005637.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.404005637.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.404005637.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.511417797.00000000014C0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.511417797.00000000014C0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.511417797.00000000014C0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.511211883.0000000001380000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.511211883.0000000001380000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.511211883.0000000001380000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.510795876.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.510795876.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.510795876.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
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	41A447	NtReadFile

Analysis Process: explorer.exe PID: **3808**, Parent PID: **6572**

General

Target ID:	4
Start time:	18:23:48
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff631f70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000004.00000000.455844055.000000000DE2E000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.455844055.000000000DE2E000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.455844055.000000000DE2E000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.476604607.000000000DE2E000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.476604607.000000000DE2E000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.476604607.000000000DE2E000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: control.exe PID: **4708**, Parent PID: **3808**

General

Target ID:	11
Start time:	18:24:30
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0xdf0000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
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: 0000000B.00000002.632202833.0000000000B90000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.632202833.0000000000B90000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.632202833.0000000000B90000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.633141128.0000000003390000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.633141128.0000000003390000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.633141128.0000000003390000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.634227955.0000000004AF0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.634227955.0000000004AF0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.634227955.0000000004AF0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	BAA447	NtReadFile

Analysis Process: cmd.exe PID: **3736**, Parent PID: **4708**

General

Target ID:	12
Start time:	18:24:36
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe"
Imagebase:	0xdd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6152**, Parent PID: **3736**

General	
Target ID:	13
Start time:	18:24:38
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: **1388**, Parent PID: **564**

General	
Target ID:	21
Start time:	18:25:15
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer.exe
Imagebase:	0x7ff631f70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly