ID: 635278
Sample Name: Ziraat Bankasi Swift Mesaji.exe
Cookbook: default.jbs
Time: 18:19:17
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

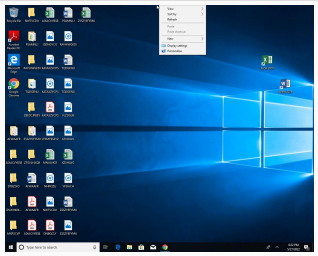
Windows Analysis Report

Ziraat Bankasi Swift Mesaji.exe

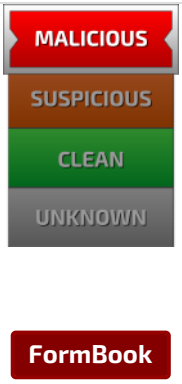
Overview

General Information

Sample Name:	Ziraat Bankasi Swift Mesaji.exe
Analysis ID:	635278
MD5:	07131c250d5f2b..
SHA1:	6d0f76adbbcd00..
SHA256:	15e17fe1832e83..
Tags:	exe Formbook geo TUR ZiraatBank
Infos:	



Detection



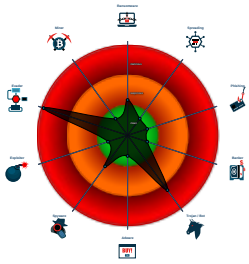
FormBook

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…
- Modifies the prolog of user mode fun…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- Ziraat Bankasi Swift Mesaji.exe (PID: 6156 cmdline: "C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe" MD5: 07131C250D5F2B4B46DA02828C5DA58C)
  - Ziraat Bankasi Swift Mesaji.exe (PID: 3548 cmdline: C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe MD5: 07131C250D5F2B4B46DA02828C5DA58C)
  - Ziraat Bankasi Swift Mesaji.exe (PID: 4528 cmdline: C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe MD5: 07131C250D5F2B4B46DA02828C5DA58C)
    - explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msiexec.exe (PID: 6892 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
        - cmd.exe (PID: 6112 cmdline: /c del "C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **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
00000002.00000002.624472503.00000000018F0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.624472503.00000000018F0000.00000040.10000000.00040000.00000000.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.624472503.00000000018F0000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$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:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.620578277.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.620578277.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$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
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.Ziraat Bankasi Swift Mesaji.exe.400000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.0.Ziraat Bankasi Swift Mesaji.exe.400000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.0.Ziraat Bankasi Swift Mesaji.exe.400000.4.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a39:$sqlite3step: 68 34 1C 7B E1 • 0x17b4c:$sqlite3step: 68 34 1C 7B E1 • 0x17a68:$sqlite3text: 68 38 2A 90 C5 • 0x17b8d:$sqlite3text: 68 38 2A 90 C5 • 0x17a7b:$sqlite3blob: 68 53 D8 7F 8C • 0x17ba3:$sqlite3blob: 68 53 D8 7F 8C

Source	Rule	Description	Author	Strings
0.2.Ziraat Bankasi Swift Mesaji.exe.70d0000.9.unpack	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x4fd7b:$s1: file:/// • 0x4fc8b:$s2: {11111-22222-10009-11112} • 0x4fd0b:$s3: {11111-22222-50001-00000} • 0x4d17d:$s4: get_Module • 0x4d5c3:$s5: Reverse • 0x4f5ba:$s6: BlockCopy • 0x4f3fe:$s7: ReadByte • 0x4fd8d:$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 5 6 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...
0.2.Ziraat Bankasi Swift Mesaji.exe.3989ee0.7.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 26 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)

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd or bat file

Modifies the prolog of user mode functions (user mode inline hooks)

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

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

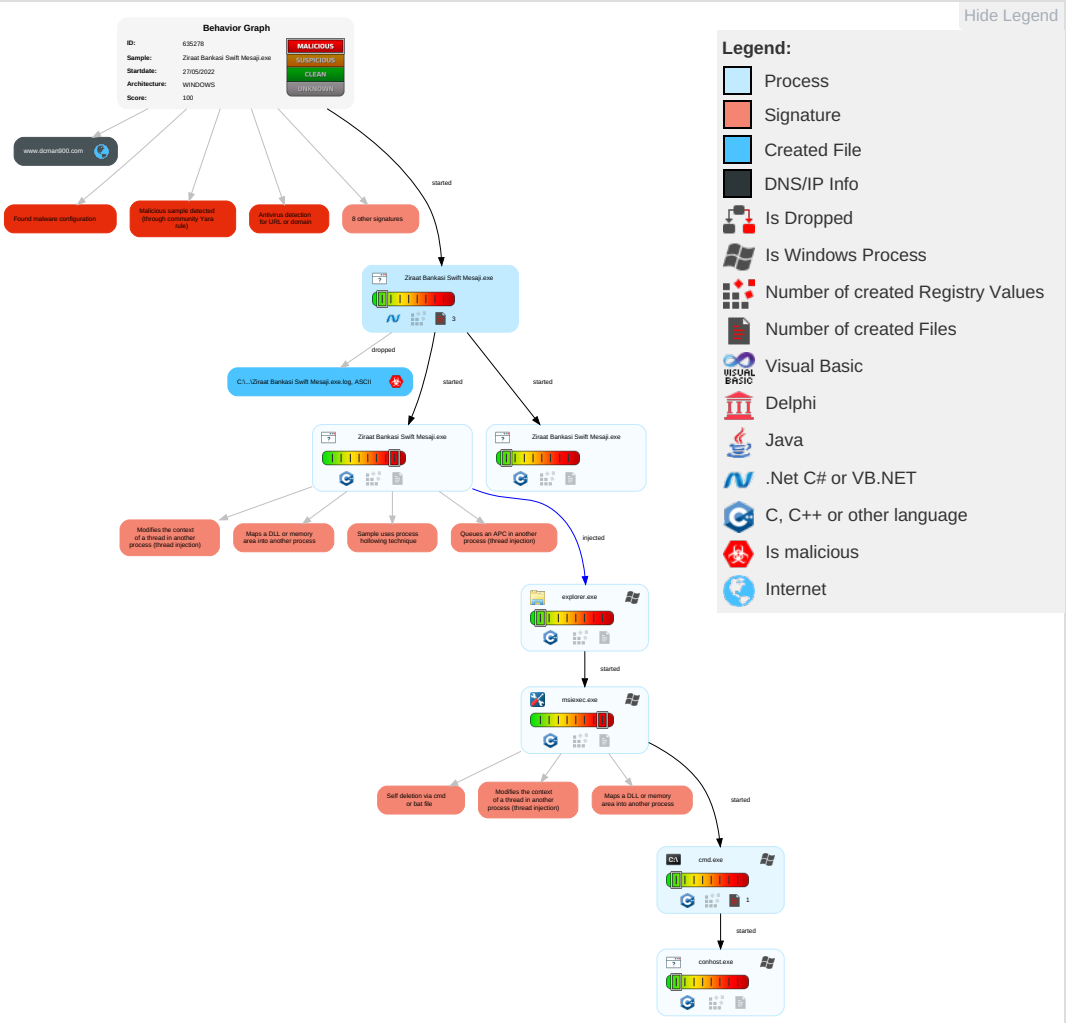
Yara detected FormBook

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	1 DLL Side-Loading	4 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	2 2 1 Security Software Discovery	Remote Services	1 Credential API Hooking	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	1 DLL Side-Loading	1 Masquerading	1 Input Capture	2 Process Discovery	Remote Desktop Protocol	1 Input Capture	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)	1 Disable or Modify Tools	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	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)	3 1 Virtualization/Sandbox Evasion	NTDS	1 1 2 System Information 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	4 1 2 Process Injection	LSA Secrets	Remote System 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	1 Deobfuscate/Decode 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 Obfuscated Files or Information	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 3 Software Packing	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/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
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Ziraat Bankasi Swift Mesaji.exe	22%	Virustotal		Browse
Ziraat Bankasi Swift Mesaji.exe	62%	ReversingLabs	ByteCode-MSIL.Trojan.RedLineStealer	

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

Source	Detection	Scanner	Label	Link	Download
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

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
www.wwohead.com/ah6m/	1%	Virustotal		Browse
www.wwohead.com/ah6m/	100%	Avira URL Cloud	malware	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.dcman900.com	54.225.97.249	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.wwohead.com/ah6m/	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Ziraat Bankasi Swift Mesaji.exe, 00000000.00000002.504687745.0000000006772000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal

Analysis ID:	635278
Start date and time: 27/05/202218:19:17	2022-05-27 18:19:17 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ziraat Bankasi Swift Mesaji.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/1@1/0
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 25.3% (good quality ratio 22.5%) • Quality average: 69% • Quality standard deviation: 32.8%
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): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.152.110.14, 40.125.122.176
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- Execution Graph export aborted for target Ziraat Bankasi Swift Mesaji.exe, PID 3548 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:20:48	API Interceptor	2x Sleep call for process: Ziraat Bankasi Swift Mesaji.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):	2148
Entropy (8bit):	5.349175784572625
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjAHKx1qHitHoxHhAHKzvFHxvAHj:iqXeqm00YqhQnouRqjAqxwCtlxHeqzNI
MD5:	945DECF362D4312BCF2BC59AAB588224
SHA1:	B8A9CD1EC92D5778D394F7F564CA4EB5D83BAE6A
SHA-256:	D85162B3E02C7B540C88441C74C2B7AD0270D70CA94A960BE08C31B2BA53DFE6
SHA-512:	300B7409CC405BDE24C2FAA3419E4C5CD0F35CAE57EBB66EE76E1CC731F1C48E395FB6CA5937E29F354D99EDCA27FE16CD4D2C59AE65598391695ECCD23B4 7B8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf 3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"Present ationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f #\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.85318717422122
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:	704512
MD5:	07131c250d5f2b4b46da02828c5da58c
SHA1:	6d0f76adbbcd0088660ded26e97866d3b3bba02a
SHA256:	15e17fe1832e832ad58893aa8d5f2e8e33e2fa756d509d2e855daa6a1f4d4027
SHA512:	f83a990a4864bd9dbd2459bd20753af867fb4e31a21afa2933ef67fee90c9077b1751278db9f37effd271374d97aa0bbbda6903f26d49e3f16d76bfcfe755de9
SSDEEP:	12288:uM1+hfTuIJZbHomdHEUEN00BVn456X38EmoH91bMrVCY8Wn65+Qho:uM1UKcZbHoEEN5B7sKH9xUVN88cJO
TLSH:	8EE4126835DC4525F7FB1BB92078410017F9B68BA713D70E6E8670E96CD3F814B22A67
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...z6.b.....0..z...D.....*.... .....@.. ....@.....

File Icon

Icon Hash:	ccaacecccca8aecc

Static PE Info

General

Entrypoint:	0x4a992a
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:	0x628F367A [Thu May 26 08:12:42 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
or al, byte ptr [eax]
add byte ptr [eax], al
adc al, 00h
add byte ptr [eax], al
push ds
add byte ptr [eax], al
add byte ptr [eax], ch
add byte ptr [eax], al
add byte ptr [eax+eax], bh
add byte ptr [eax], al
push eax
add byte ptr [eax], al
add al, ch
add eax, dword ptr [eax]
add al, ch
add eax, dword ptr [eax]
add byte ptr [eax+00h], dl
add byte ptr [eax], al
cmp al, 00h
add byte ptr [eax], al
sub byte ptr [eax], al
add byte ptr [eax], al
push ds
add byte ptr [eax], al
add byte ptr [eax+eax], dl
add byte ptr [eax], al
or al, byte ptr [eax]
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add eax, dword ptr [eax]
add byte ptr [eax], al
add eax, 07000000h
add byte ptr [eax], al
add byte ptr [eax], cl
add byte ptr [eax], al
add byte ptr [edx], cl
add byte ptr [eax], al
add byte ptr [eax+eax], cl
add byte ptr [eax], al
push cs
add byte ptr [eax], al
add byte ptr [ecx], dl
add byte ptr [eax], al
add byte ptr [ebx], dl
add byte ptr [eax], al
add byte ptr [17000000h], dl
add byte ptr [eax], al
add byte ptr [eax], bl
add byte ptr [eax], al
add byte ptr [edx], bl
add byte ptr [eax], al
add byte ptr [eax+eax], bl
add byte ptr [eax], al
push ds
add byte ptr [eax], al
add byte ptr [ecx], ah
add byte ptr [eax], al
add byte ptr [ebx], ah
add byte ptr [eax], al
add byte ptr [27000000h], ah
add byte ptr [eax], al
add byte ptr [eax], ch
add byte ptr [eax], al
add byte ptr [edx], ch
add byte ptr [eax], al
add byte ptr [eax+eax], ch
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], dh
add byte ptr [eax], al
add byte ptr [ebx], dh
add byte ptr [eax], al
add byte ptr [37000000h], dh
add byte ptr [eax], al
add byte ptr [eax], bh
add byte ptr [eax], al
add byte ptr [edx], bh
add byte ptr [eax], al
add byte ptr [eax+eax], bh
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	0xa98d8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xaa000	0x4118	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0xa79f0	0xa7a00	False	0.893987987043	data	7.85829151308	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x4118	0x4200	False	0.947798295455	data	7.79073059697	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb0000	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	0xaa0c8	0x3cb9	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xadd94	0x14	data		
RT_VERSION	0xaddb8	0x35c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Karel Pospil 2011
Assembly Version	1.1.0.0
InternalName	DateMapp.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	Gothic
Comments	
ProductName	Gothic Checkers
ProductVersion	1.0.0.0
FileDescription	Gothic Checkers
OriginalFilename	DateMapp.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:22:49.413631916 CEST	52333	53	192.168.2.5	8.8.8.8
May 27, 2022 18:22:49.443959951 CEST	53	52333	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 18:22:49.413631916 CEST	192.168.2.5	8.8.8.8	0xf7fb	Standard query (0)	www.dcman900.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 18:22:49.443959951 CEST	8.8.8.8	192.168.2.5	0xf7fb	No error (0)	www.dcman900.com		54.225.97.249	A (IP address)	IN (0x0001)

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

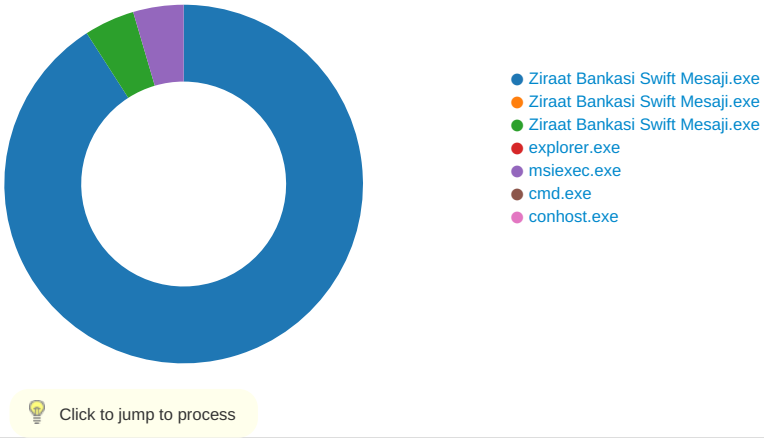
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xE0
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xE0
GetMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xE0
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xE0

Statistics

Behavior



System Behavior

Analysis Process: Ziraat Bankasi Swift Mesaji.exe PID: **6156**, Parent PID: **4672**

General

Target ID:	0
Start time:	18:20:33
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:	0x2b0000
File size:	704512 bytes
MD5 hash:	07131C250D5F2B4B46DA02828C5DA58C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.501864070.00000000037E4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.501864070.00000000037E4000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.501864070.00000000037E4000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.505751759.00000000070D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.502390712.000000000390E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.502390712.000000000390E000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.502390712.000000000390E000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.499472204.0000000002727000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: Ziraat Bankasi Swift Mesaji.exe PID: **3548**, Parent PID: **6156**

General

Target ID:	1
Start time:	18:20:56
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
Imagebase:	0xf0000
File size:	704512 bytes
MD5 hash:	07131C250D5F2B4B46DA02828C5DA58C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Ziraat Bankasi Swift Mesaji.exe PID: **4528**, Parent PID: **6156**

General

Target ID:	2
Start time:	18:20:57
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:	0xb90000
File size:	704512 bytes
MD5 hash:	07131C250D5F2B4B46DA02828C5DA58C
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: 00000002.00000002.624472503.00000000018F0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.624472503.00000000018F0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.624472503.00000000018F0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.620578277.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.620578277.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.620578277.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.494680608.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.494680608.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.494680608.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.624676953.0000000001930000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.624676953.0000000001930000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.624676953.0000000001930000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.494153519.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.494153519.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.494153519.0000000000400000.00000040.00000400.00020000.00000000.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: **684**, Parent PID: **4528**

General

Target ID:	5
Start time:	18:21:02
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff74fc70000
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: 00000005.00000000.592289149.000000000DAA7000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.592289149.000000000DAA7000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.592289149.000000000DAA7000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.544575814.000000000DAA7000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.544575814.000000000DAA7000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.544575814.000000000DAA7000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: msiexec.exe PID: **6892**, Parent PID: **684**

General

Target ID:	14
Start time:	18:21:55
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0x990000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
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: 0000000E.00000002.708353190.0000000002EC0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.708353190.0000000002EC0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.708353190.0000000002EC0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.708681430.00000000047B0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.708681430.00000000047B0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.708681430.00000000047B0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.707520982.0000000000880000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.707520982.0000000000880000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.707520982.0000000000880000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	89A447	NtReadFile

Analysis Process: cmd.exe PID: **6112**, Parent PID: **6892**

General

Target ID:	16
Start time:	18:22:00
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:	0x1100000
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: **6680**, Parent PID: **6112**

General

Target ID:	18
Start time:	18:22:02
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly