ID: 553162
Sample Name: Ziraat Bankasi Swift Mesaji.exe
Cookbook: default.jbs
Time: 12:12:26
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

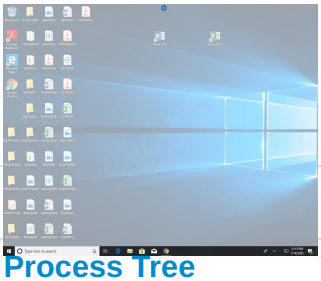
Windows Analysis Report Ziraat Bankasi Swift Mesaji.exe

Overview

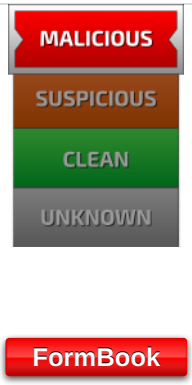
General Information

Sample Name:	Ziraat Bankasi Swift Mesaji.exe
Analysis ID:	553162
MD5:	bb5ab5b4895da7..
SHA1:	8fcfc099505b7d8..
SHA256:	c274f37d52a6ef7..
Tags:	exe Formbook geo TUR ZiraatBank
Infos:	

Most interesting Screenshot:



Detection

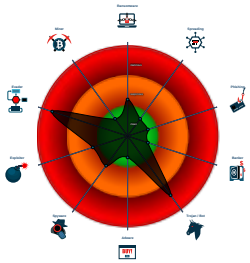


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for samp…
- Performs DNS queries to domains w…
- Self deletion via cmd delete
- Injects a PE file into a foreign proce…
- Queues an APC in another process …
- Tries to detect virtualization through…

Classification



Process Tree

- **System is w10x64**
- Ziraat Bankasi Swift Mesaji.exe (PID: 2940 cmdline: "C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe" MD5: BB5AB5B4895DA7F1EDDBAF67D7FE6067)
  - Ziraat Bankasi Swift Mesaji.exe (PID: 4652 cmdline: "C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe" MD5: BB5AB5B4895DA7F1EDDBAF67D7FE6067)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - colorcpl.exe (PID: 4552 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
        - cmd.exe (PID: 6256 cmdline: /c del "C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6916 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - explorer.exe (PID: 6468 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 728 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.freedomwoofpackcom.com/a0p6/"
  ],
  "decoy": [
    "taxlaws.info",
    "porn-star-depot.com",
    "cpf-comptes.com",
    "metropark.xyz",
    "transformselfhypnosis.com",
    "wu8g8aerxgjr.xyz",
    "jingzhouhan.net",
    "granicors.com",
    "monografiaonline.com",
    "4972hillcrestdrive.com",
    "gridironagriculturist.com",
    "xtrasomething.com",
    "scbndirects.com",
    "agglutinatesmicromanagers.xyz",
    "butsuyokulog.xyz",
    "parttimejobsinuk.site",
    "kriylzf.xyz",
    "sinashakib.com",
    "hpessoa.website",
    "interscopealbums.com",
    "bathandlicious.com",
    "jrowlandmarketing.com",
    "okforbk.com",
    "xjbyctc.com",
    "vitospark.com",
    "threewisewords.com",
    "antonioloiodice.com",
    "fastvpnreward.com",
    "baamusa.com",
    "yanatransportationsrvs.net",
    "ol0vdw.xyz",
    "climbingtreehollow.com",
    "barterlinealarmselect.com",
    "integrant.xyz",
    "nepalgci.com",
    "wu8j3tx49l5a.xyz",
    "surpmel.xyz",
    "autocarbying101.com",
    "otakusofneverland.com",
    "pawsitiveclosings.com",
    "h9220.com",
    "newshaiya.com",
    "progressiveprizes.com",
    "groovybingo.com",
    "iconuncle.com",
    "icon-club-dxb.com",
    "ruokanetti.com",
    "cooperjss.com",
    "governorperdue.com",
    "brfujdersomngreqt.com",
    "bcubnk.com",
    "digitalmedicinetechnologies.com",
    "logiqtrading.com",
    "anti-tfboys.com",
    "ateliercarbon.com",
    "wesovereign.com",
    "wein-quadrat.com",
    "www37118.com",
    "morethanalittlemarley.com",
    "coslogenex.com",
    "bondic-listjournal.com",
    "choicesidownloadnv.com",
    "ys688.xyz",
    "nftrack.xyz"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000001.376553796.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000001.376553796.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000001.376553796.0000000000400000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.436846842.0000000000490000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.436846842.0000000000490000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.1.Ziraat Bankasi Swift Mesaji.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.1.Ziraat Bankasi Swift Mesaji.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.1.Ziraat Bankasi Swift Mesaji.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
3.0.Ziraat Bankasi Swift Mesaji.exe.400000.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.Ziraat Bankasi Swift Mesaji.exe.400000.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

Performs DNS queries to domains with low reputation

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 delete

Malware Analysis System Evasion:

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:

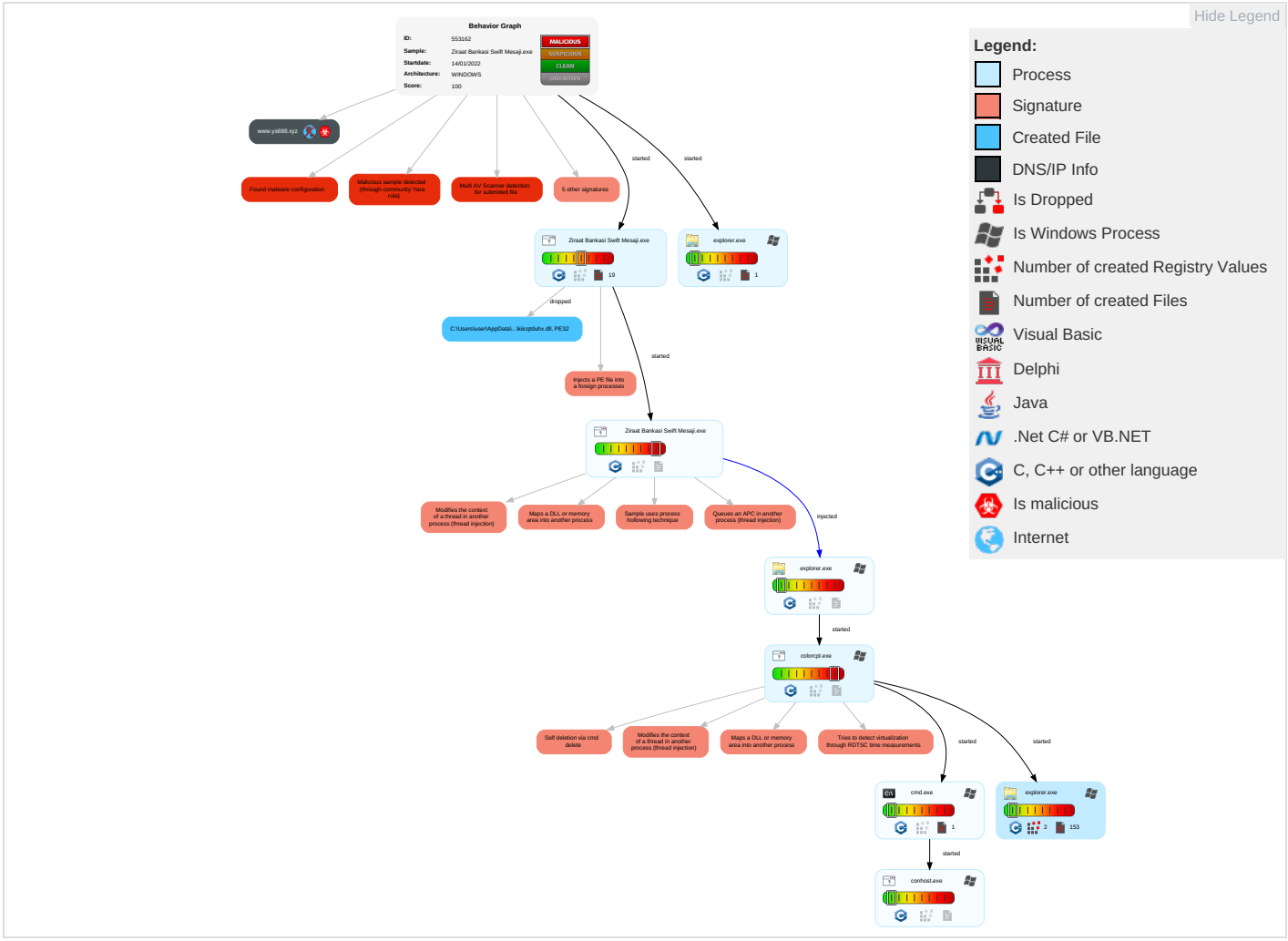
Yara detected FormBook

Remote Access Functionality:

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1 3 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

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	33%	ReversingLabs	Win32.Trojan.Risis	
Ziraat Bankasi Swift Mesaji.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.Ziraat Bankasi Swift Mesaji.exe.3050000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.1.Ziraat Bankasi Swift Mesaji.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.2.colorcpl.exe.4def840.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
19.0.explorer.exe.bacf840.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.0.Ziraat Bankasi Swift Mesaji.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.Ziraat Bankasi Swift Mesaji.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.Ziraat Bankasi Swift Mesaji.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.Ziraat Bankasi Swift Mesaji.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.2.colorcpl.exe.b02338.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
33.2.explorer.exe.c07f840.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.gridironagriculturist.com	0%	Avira URL Cloud	safe	
http://www.ruokanetti.com/a0p6/www.barterlinealarmselect.com	0%	Avira URL Cloud	safe	
http://www.barterlinealarmselect.com/a0p6/www.autocarbying101.com	0%	Avira URL Cloud	safe	
http://www.freedomwoofpackcom.com	0%	Avira URL Cloud	safe	
http://components.groove.net/Groove/Components/SystemComponents/SystemComponents.osd?Package=net.gro	0%	Avira URL Cloud	safe	
http://www.barterlinealarmselect.com/a0p6/	0%	Avira URL Cloud	safe	
http://www.surpmel.xyz/a0p6/www.pawsitiveclosings.com	0%	Avira URL Cloud	safe	
http://www.ys688.xyz/a0p6/www.transformselfhypnosis.com	0%	Avira URL Cloud	safe	
http://www.surpmel.xyz	0%	Avira URL Cloud	safe	
http://www.www37118.com/a0p6/	0%	Avira URL Cloud	safe	
http://www.gridironagriculturist.com/a0p6/www.hpessoa.website	0%	Avira URL Cloud	safe	
http://www.taxlaws.info/a0p6/	0%	Avira URL Cloud	safe	
http://www.gridironagriculturist.comReferer:	0%	Avira URL Cloud	safe	
http://www.transformselfhypnosis.com/a0p6/www.www37118.com	0%	Avira URL Cloud	safe	
http://www.wu8g8aerxgjr.xyz	0%	Avira URL Cloud	safe	
http://www.wu8g8aerxgjr.xyz/a0p6/www.surpmel.xyz	0%	Avira URL Cloud	safe	
http://www.progressiveprizes.com/a0p6/www.fastvpnreward.com	0%	Avira URL Cloud	safe	
http://www.autocarbying101.comReferer:	0%	Avira URL Cloud	safe	
http://www.transformselfhypnosis.com	0%	Avira URL Cloud	safe	
http://www.ys688.xyz	0%	Avira URL Cloud	safe	
http://www.ruokanetti.comReferer:	0%	Avira URL Cloud	safe	
http://www.www37118.com/a0p6/www.gridironagriculturist.com	0%	Avira URL Cloud	safe	
http://www.fastvpnreward.com/a0p6/www.digitalmedicinetechnologies.com	0%	Avira URL Cloud	safe	
http://www.pawsitiveclosings.comReferer:	0%	Avira URL Cloud	safe	
http://www.taxlaws.info	0%	Avira URL Cloud	safe	
http://www.digitalmedicinetechnologies.com	0%	Avira URL Cloud	safe	
http://www.autocarbying101.com/a0p6/www.progressiveprizes.com	0%	Avira URL Cloud	safe	
http://www.hpessoa.websiteReferer:	0%	Avira URL Cloud	safe	
http://www.progressiveprizes.comReferer:	0%	Avira URL Cloud	safe	
http://www.gridironagriculturist.com/a0p6/	0%	Avira URL Cloud	safe	
http://www.pawsitiveclosings.com/a0p6/	0%	Avira URL Cloud	safe	
http://www.barterlinealarmselect.comReferer:	0%	Avira URL Cloud	safe	
http://www.barterlinealarmselect.com	0%	Avira URL Cloud	safe	
http://www.www37118.comReferer:	0%	Avira URL Cloud	safe	
http://www.fastvpnreward.com/a0p6/	0%	Avira URL Cloud	safe	
http://www.freedomwoofpackcom.com/a0p6/	0%	Avira URL Cloud	safe	
http://www.taxlaws.infoReferer:	0%	Avira URL Cloud	safe	
http://www.freedomwoofpackcom.comReferer:	0%	Avira URL Cloud	safe	
http://www.hpessoa.website/a0p6/www.freedomwoofpackcom.com	0%	Avira URL Cloud	safe	
http://components.groove.net/Groove/Components/Root.osd?Package=net.groove.Groove.Tools.System.Groov	0%	Avira URL Cloud	safe	
http://www.fastvpnreward.com	0%	Avira URL Cloud	safe	
http://www.freedomwoofpackcom.com/a0p6/www.taxlaws.info	0%	Avira URL Cloud	safe	
www.freedomwoofpackcom.com/a0p6/	0%	Avira URL Cloud	safe	
http://www.transformselfhypnosis.com/a0p6/	0%	Avira URL Cloud	safe	
http://www.hpessoa.website/a0p6/	0%	Avira URL Cloud	safe	
http://www.www37118.com	0%	Avira URL Cloud	safe	
http://www.autocarbying101.com/a0p6/	0%	Avira URL Cloud	safe	
http://www.ys688.xyz/a0p6/	0%	Avira URL Cloud	safe	
http://www.ruokanetti.com	0%	Avira URL Cloud	safe	
http://www.transformselfhypnosis.comReferer:	0%	Avira URL Cloud	safe	
http://www.surpmel.xyz/a0p6/	0%	Avira URL Cloud	safe	
http://www.wu8g8aerxgjr.xyz/a0p6/	0%	Avira URL Cloud	safe	
http://www.autocarbying101.com	0%	Avira URL Cloud	safe	
http://www.digitalmedicinetechnologies.comReferer:	0%	Avira URL Cloud	safe	
http://www.hpessoa.website	0%	Avira URL Cloud	safe	
http://www.surpmel.xyzReferer:	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.fastvpnreward.comReferer:	0%	Avira URL Cloud	safe	
http://www.pawsitiveclosings.com/a0p6/www.ruokanetti.com	0%	Avira URL Cloud	safe	
http://www.ys688.xyzReferer:	0%	Avira URL Cloud	safe	
http://www.digitalmedicinetechnologies.com/a0p6/	0%	Avira URL Cloud	safe	
http://www.ruokanetti.com/a0p6/	0%	Avira URL Cloud	safe	
http://www.taxlaws.info/a0p6/www.wu8g8aerxgjr.xyz	0%	Avira URL Cloud	safe	
http://www.wu8g8aerxgjr.xyzReferer:	0%	Avira URL Cloud	safe	
http://www.progressiveprizes.com/a0p6/	0%	Avira URL Cloud	safe	
http://www.pawsitiveclosings.com	0%	Avira URL Cloud	safe	
http://www.progressiveprizes.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.ys688.xyz	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.freedomwoofpackcom.com/a0p6/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553162
Start date:	14.01.2022
Start time:	12:12:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 20s
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:	33
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@9/4@1/0
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 36.8% (good quality ratio 33%) • Quality average: 74.9% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 87% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:14:44	API Interceptor	315x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\aaafqvv	
Process:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
File Type:	data
Category:	dropped
Size (bytes):	5080
Entropy (8bit):	6.142571300023832
Encrypted:	false
SSDEEP:	96:H4Qn50iM/USgcGWFDFBGXhxx8InKcZX0FsZxoHCCnzYoRD:35zIvRLQmUKcZXqi4YoZ
MD5:	23922E85EE8459083CE2625E78A155A6
SHA1:	2FB6640CAEF2522888D90FABEED29AC3C03A8B70
SHA-256:	F0BD0A6B004414957490ACE6DFC219B3A9A84DDBEF4C173333E4FF9349D448F2
SHA-512:	9A530371CC1212AECDA4CD9BD9D9D81E9C7B15AE466D5B428C5448B696C0ADB165A4749FBB6B43B78B438308729F7D8D97EEDBD50ACA04B89536F23BAAAE5BE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\aaafqvv	
Preview:	-(w....$.$.....0...`...@..`.....7.....!..!.....(..4.!..!.....P..<.!..!....K.....8..D.!..!....J.....`..L.....x..`.....@..,.....kM....$.....UkF....%.....V.....,0.k.....l.3...!(..!P..!8..!`..!@..!...2.....!0.!(...x....0.....7.l.{.....l.3.....0....1.V....$...`....x.....x....|U.....U.....x....x.....1.V.....b.....V|...?.....Vx.....Vx...$.$..`...7.....(.....b.....,|....`....x..x..M...(...4....x.U5...(...4...x..`...(...?..E....:.....!x.....0..w7.0.....0.1.V....$.$...`...7.....`.....b.....,.....`.....x..x..M...`...L....x.U5...`...L....x.E5..`...L..|kM.x..F...`..L....x.U5...`...L...x..`...`....b..B....;.....h..x....h...g.!h.!|.!..!..!x.....0..w7.0.....0.1.V|...$.$t7.....,.....b.....,.....`....x..x..M...,.....x.U5...,.....x..`...,.....l.....z.!

C:\Users\user\AppData\Local\Temp\fwb2jz7v09bp1l5p5b	
Process:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
File Type:	data
Category:	dropped
Size (bytes):	219922
Entropy (8bit):	**7.99314474006626**
Encrypted:	**true**
SSDEEP:	6144:heFFpHd3XORiMtWb71jHFoHazbPH5IKQqd+UPOwuO69:EjBTMsNhEavpwUA
MD5:	933EC2281DD8AA578A2514079575BD9F
SHA1:	4BF4E25B2DE0F35E57CCCA6C6C401EB15DD01B29
SHA-256:	6548B64155A7E33D1097C82F3A0B21D7A05DE87265E3575EF792A83CE7032F64
SHA-512:	303671B94C0A7C0FEB784F920902E3E6C56851C4AD6F1801DBE8F2E49D7489CC05197C95EA83A55B913915528880171AD7773CA73F0568FD882E4E1C73C3720C
Malicious:	false
Reputation:	low
Preview:	5.K.}Y..*..y...m..{%.X...S`)A`..},`.*.!.%].....<..i..?.K.u.Y.>...g2.....O...z....a.....V..CJ@L...&.....k..@...&.^..:..I...D.3,.7.L~^..e...G0 .n.q|..9.D..-FN..'3k..*.cr....H..[j...j.w..a^W k..$..W.|..p..UF.$5~.$...;K.c9a..N.....C..1....!....|Y.....{.!....%>....{.2..h.},..*.!.%].....<..i..?.K..Y..u..g.lr^..#.$../..n...0...r.....).:.....{.36..&.^..:.....W`....!.....3.... TDQu..[9?... ..GOXh...*.cr...aBy1Wj.....w].....[...$..W.|r...#.vUZij1~.$...;@..9a..N.K.....C..1..l.!K.t.\|Y..*...{.!..<.%>]...{.2]..},`.*.!.%].....<..i..?.K..Y..u..g.lr^..#.$../..n...0...r.....).:.....{.36 ..&.^..:.....W`....!.....3.... TDQu..[9?.....GOXh...*.cr....H..[j.....w].....K..$..W.\|r...#.vUFij5~.$...;@..9a..N.K.....C..1..l.!K.t.|Y..*...{.!..<.%>]...{.2]..},`.*.!.%].....<..i..?.K..Y..u..g.lr ^..#.$../..n...0...r.....).:.....{.36..&.^..:.....W`....!.....3.... TDQu..[9?.....GOXh...*.cr....H..[j.....w].....K..$..W.|r...#.vUFij5~.$...;

C:\Users\user\AppData\Local\Temp\nsrE0A0.tmp	
Process:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
File Type:	data
Category:	dropped
Size (bytes):	256999
Entropy (8bit):	7.698968485447416
Encrypted:	false
SSDEEP:	6144:BUs4eFFpHd3XORiMtWb71jHFoHazbPH5IKQqd+UPOwuO6n:XRjBTMsNhEavpwUc
MD5:	158AEB31B92164491FC3B713E71BFAE5
SHA1:	BC4384095260A6AD3FFF1C9C13A621448E1170C9
SHA-256:	63879322D4A8655F3D164368EAD45E3179EACDAC101ACB0592EE3132983ED638
SHA-512:	536A9540A9EA5C574F685D0354F5480FC0CA5911A91E44D9D2280663B2CCA15A67986C88E0329EBE251E534710242E5ABEFC430707FA0123A36ABBF285F2F76C
Malicious:	false
Reputation:	low
Preview:	.I.....,.....Q.....I.....I.....=..... .....J.....w...j.....\..... ....

C:\Users\user\AppData\Local\Temp\nsrE0A1.tmp\kiicqtduhx.dll	
Process:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	3.8015980505764273
Encrypted:	false
SSDEEP:	24:e1GSb0JDlhEcQMV3ax/+A6zDctxVrJ00JDTyj1a5DTyxk8q6l1nPnRuV4MPgicfk:SgZ8h4Wzrqi79r6IPRuqSyOyO
MD5:	A85B7C70D00F1A15BE15108BB6F5601E
SHA1:	E3BD606BE8D0C6DBF87BC4F92CAC260F5353C507
SHA-256:	DE9BF1EAFF348707D8ED3F4DDF31B696EDAAF6A2E1B2287851982 58EC8CD6706
SHA-512:	48F40F0095F31C9666D555A73D10A34A058ABCE9FD17A5A99ACCA7DCC2A8E90AEB18877126BD34456747B264425AE9A9DD937B79E3330690BCAB4A816C76A72 5
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U.CU.CU.C...CT.C0..BZ.CU.Cw.C..BT.C..BT.C.QCT.C. .BT.CRichU.C.....PE..L....+.a.....!..... .....P.....@..... ..L... .....0.....@..L..... .. ..text...|..... ..`.rdata..j.... .....@..@.rsrc.....0.....@..@.reloc..L....@.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.927294615366343
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Ziraat Bankasi Swift Mesaji.exe
File size:	248844
MD5:	bb5ab5b4895da7f1eddbaf67d7fe6067
SHA1:	8fcfc099505b7d825f8176af5d2a0dedfd7f39f2
SHA256:	c274f37d52a6ef7300164ed5c964426b853c7cd3938310a10211439a4b5413ba
SHA512:	fe558a8fe2f91888ba090b091a1e8e1b04b21ebfc05fcdf4e633790597f597ae437801df7b489ef3f1faff4a9c51db6a7c77de765be2f3df8426ee1d65e507ca
SSDEEP:	3072:oNyah0mJo5+uoVPvlKLhdo9auOECcQV6a5il3cHPWexwwqt2DbXfwlFLahXs4VSi:ow1Ivod29iECcQ0IsvWexwdUwZs4kgNr
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

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

Entrypoint Preview

Rich Headers

Data Directories

Sections

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

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 12:15:59.854818106 CET	192.168.2.6	8.8.8.8	0xd9f4	Standard query (0)	www.ys688.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 12:15:59.887609959 CET	8.8.8.8	192.168.2.6	0xd9f4	Name error (3)	www.ys688.xyz	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Ziraat Bankasi Swift Mesaji.exe PID: 2940 Parent PID: 2200

General

Start time:	12:13:38
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe"
Imagebase:	0x400000
File size:	248844 bytes
MD5 hash:	BB5AB5B4895DA7F1EDDBAF67D7FE6067
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: 00000001.00000002.377484332.0000000003050000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.377484332.0000000003050000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.377484332.0000000003050000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Ziraat Bankasi Swift Mesaji.exe PID: 4652 Parent PID: 2940

General

Start time:	12:13:40
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe"
Imagebase:	0x400000
File size:	248844 bytes
MD5 hash:	BB5AB5B4895DA7F1EDDBAF67D7FE6067
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: 00000003.00000001.376553796.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000001.376553796.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000001.376553796.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.436846842.0000000000490000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.436846842.0000000000490000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.436846842.0000000000490000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.374508026.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.374508026.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.374508026.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.375573868.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.375573868.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.375573868.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.436931041.00000000004C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.436931041.00000000004C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.436931041.00000000004C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.436115346.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.436115346.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.436115346.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 4652

General

Start time:	12:13:45
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
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: 00000005.00000000.412084086.000000000F0C5000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.412084086.000000000F0C5000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.412084086.000000000F0C5000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: colorcpl.exe PID: 4552 Parent PID: 3440

General

Start time:	12:14:07
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\colorcpl.exe
Imagebase:	0x1150000
File size:	86528 bytes
MD5 hash:	746F3B5E7652EA0766BA10414D317981
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.00000002.647118949.0000000000880000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.647118949.0000000000880000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.647118949.0000000000880000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.649679782.00000000010F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.649679782.00000000010F0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.649679782.00000000010F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.649486951.00000000010C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.649486951.00000000010C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.649486951.00000000010C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6256 Parent PID: 4552

General

Start time:	12:14:13
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\Ziraat Bankasi Swift Mesaji.exe"
Imagebase:	0x2a0000
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 Show Windows behavior

Analysis Process: conhost.exe PID: 6916 Parent PID: 6256

General

Start time:	12:14:15
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6468 Parent PID: 3716

General

Start time:	12:14:43
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff6f22f0000
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 Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: explorer.exe PID: 728 Parent PID: 3668

General

Start time:	12:15:42
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe

Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff6f22f0000
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 Show Windows behavior

Registry Activities Show Windows behavior

Disassembly

Code Analysis