ID: 433036
Sample Name: HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe
Cookbook: default.jbs
Time: 08:03:26
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

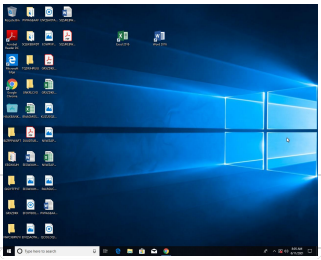
Analysis Report HALKBANK_EKSTRE_20210611_08020…

Overview

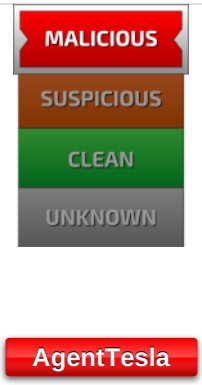
General Information

Sample Name:	HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe
Analysis ID:	433036
MD5:	14f4f4356a708f1…
SHA1:	a04edf6cb2d9753.
SHA256:	0a27c51c891f44c..
Tags:	exe geo Halkbank TUR
Infos:	

Most interesting Screenshot:



Detection

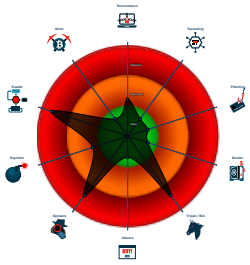


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains method …
- .NET source code contains very larg…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…

Classification



Process Tree

- **System is w10x64**
- HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe (PID: 2600 cmdline: 'C:\Users\user\Desktop\HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe' MD5: 14F4F4356A708F1E9E18C6C71EF3153E)
  - HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe (PID: 6044 cmdline: C:\Users\user\Desktop\HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe MD5: 14F4F4356A708F1E9E18C6C71EF3153E)
  - HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe (PID: 3508 cmdline: C:\Users\user\Desktop\HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe MD5: 14F4F4356A708F1E9E18C6C71EF3153E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "service@bmrtecpack.comABdiamond6_mail.bmrtecpack.commozsahim67@gmail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.219661677.000000000253 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000002.482152633.000000000307 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.482152633.000000000307 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000003.00000000.217706120.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.217706120.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe.35f2748.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe.35f2748.1.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.0.HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.2.HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

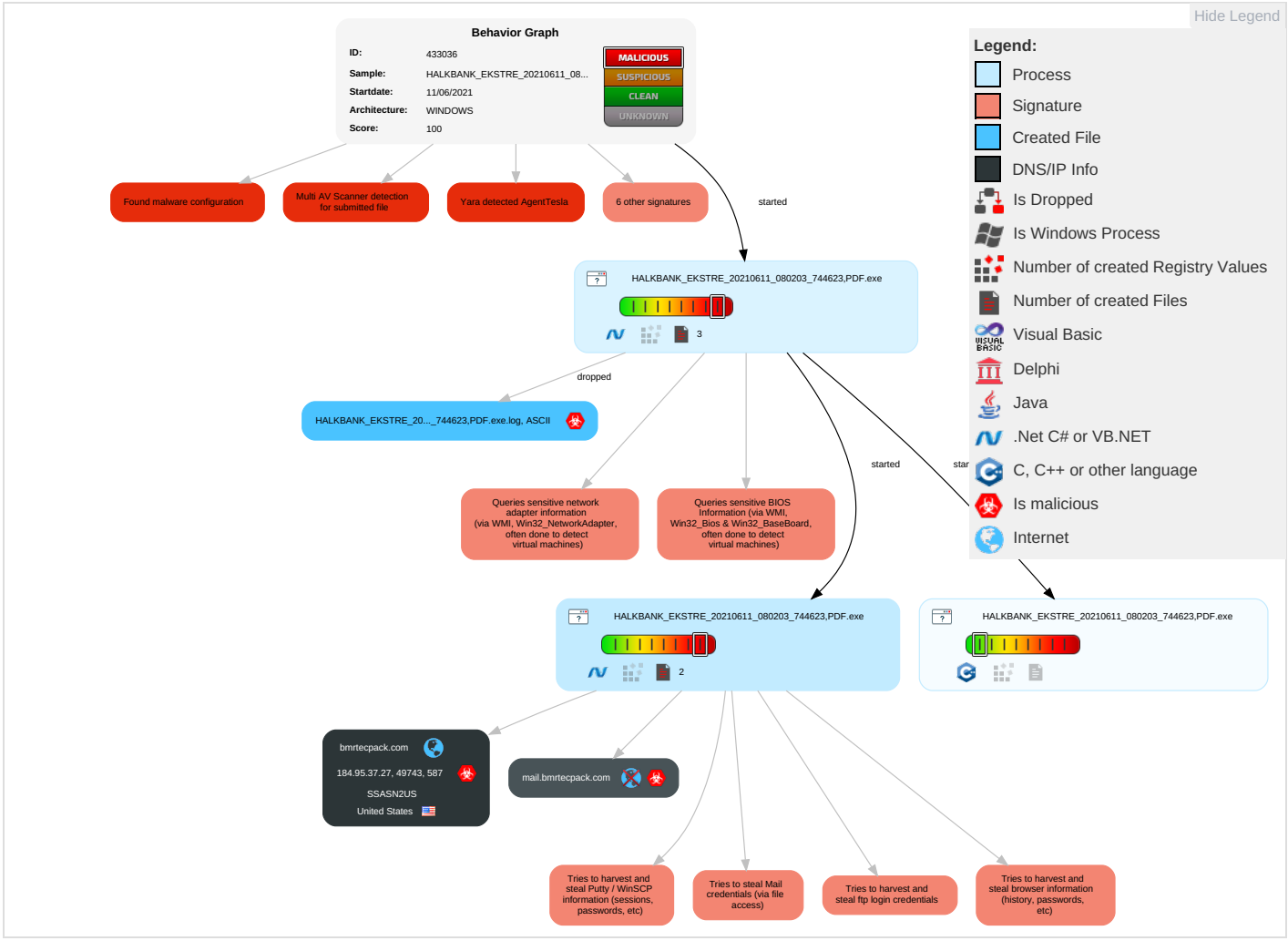
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E Ir N C
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Standard Port 1	E R C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Credentials in Registry 1	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Non-Application Layer Protocol 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Layer Protocol 1 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A

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
HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe	24%	ReversingLabs	Win32.Trojan.AgentTesla	
HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
bmrtecpack.com	1%	Virustotal		Browse
mail.bmrtecpack.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://https://9YHNdCcoTaUn.org	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0B	0%	Avira URL Cloud	safe	
http://mail.bmrtecpack.com	0%	Avira URL Cloud	safe	
http://ePfJSq.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://bmrtecpack.com	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bmrtecpack.com	184.95.37.27	true	true	• 1%, Virustotal, Browse	unknown
mail.bmrtecpack.com	unknown	unknown	true	• 3%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.95.37.27	bmrtecpack.com	United States		20454	SSASN2US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433036
Start date:	11.06.2021
Start time:	08:03:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HALKBANK_EKSTRE_20210611_080203_744623,PDF.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:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/1@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2% (good quality ratio 1%) • Quality average: 39.2% • Quality standard deviation: 41.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:04:19	API Interceptor	832x Sleep call for process: HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
184.95.37.27	PO210530_332641.doc	Get hash	malicious	Browse	
	#U4e2d#U56fd#U6d77#U5173#U65b0#U89c4(chinese version).exe	Get hash	malicious	Browse	
	new.exe	Get hash	malicious	Browse	
	c1.exe	Get hash	malicious	Browse	
	NEW_CV.dox.x.exe	Get hash	malicious	Browse	
	PO210530_332641-pdf.gz.exe	Get hash	malicious	Browse	
	qoute_pdf.exe	Get hash	malicious	Browse	
	Krediler_Odeme_Plani_20210526_171707048.exe	Get hash	malicious	Browse	
	PO879654433.PDF.exe	Get hash	malicious	Browse	
	Payment_Advice_05-24-2021_pdf.exe	Get hash	malicious	Browse	
	3hATtmBa3Q.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SSASN2US	PO210530_332641.doc	Get hash	malicious	Browse	• 184.95.37.27
	HRnyUiNliV.exe	Get hash	malicious	Browse	• 184.95.51.175
	#U4e2d#U56fd#U6d77#U5173#U65b0#U89c4(chinese version).exe	Get hash	malicious	Browse	• 184.95.37.27
	Hd1mBP2yIQ.exe	Get hash	malicious	Browse	• 184.95.51.183
	new.exe	Get hash	malicious	Browse	• 184.95.37.27
	c1.exe	Get hash	malicious	Browse	• 184.95.37.27
	dE1IuYMv2a.exe	Get hash	malicious	Browse	• 184.95.51.183
	NEW_CV.dox.x.exe	Get hash	malicious	Browse	• 184.95.37.27
	N05mKfkULx.exe	Get hash	malicious	Browse	• 184.95.51.183
	FLkiltoJYT.exe	Get hash	malicious	Browse	• 184.95.51.183
	TdiFSP890W.exe	Get hash	malicious	Browse	• 184.95.51.183
	XLbV2SrTfv.exe	Get hash	malicious	Browse	• 184.95.51.183
	9l2fgn5tTv.exe	Get hash	malicious	Browse	• 184.95.51.183
	SecuriteInfo.com.Variant.Bulz.383129.23206.exe	Get hash	malicious	Browse	• 108.170.22.198
	SecuriteInfo.com.Variant.Bulz.383129.29566.exe	Get hash	malicious	Browse	• 108.170.22.198
	Icb8VZwQqM.exe	Get hash	malicious	Browse	• 184.95.51.183
	nkedbLsEM6.exe	Get hash	malicious	Browse	• 184.95.51.183
	Fv5dq78YGC.exe	Get hash	malicious	Browse	• 184.95.51.183
	aUAryqmVWH.exe	Get hash	malicious	Browse	• 184.95.51.183
	dEalVCTox2.exe	Get hash	malicious	Browse	• 184.95.51.183

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe.log	
Process:	C:\Users\user\Desktop\HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe.log	
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.509397955171368
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe
File size:	951296
MD5:	14f4f4356a708f1e9e18c6c71ef3153e
SHA1:	a04edf6cb2d97539a509d17411a5884f75d5e5cf
SHA256:	0a27c51c891f44c26d8db8848822880a8209830faf2d8c00e8729151ae76be4f
SHA512:	f52170e2ca58b9c1c4496ba1c27dda4afff45e5a1631b026fd58f0fdb682b0250ca059ffa69d0883dc896d96204c5bdb87855d0a7be7fcdfcafcfbec17379b5a
SSDEEP:	12288:wM441/0V9+4tKB7rmCmOcF4my0uJC0b/YvNaOpkXT1KoUflLJ0pZM4e/ZUdtb:D2V9+BfmCcy0CKNaZ1KoUfl2NeBUdt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.../.`.....n.... .....@.. .....@.....

File Icon

Icon Hash:	8c8caa8e9692aa00

Static PE Info

General

Entrypoint:	0x4bf76e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C2E92F [Fri Jun 11 04:40:15 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General

OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbd774	0xbd800	False	0.896744619888	data	7.85752472578	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xc0000	0x1e8	0x200	False	0.859375	data	6.61330803525	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc2000	0x2a380	0x2a400	False	0.124323918269	data	4.1712627728	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xee000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 08:06:02.939363003 CEST	192.168.2.3	8.8.8.8	0x6c97	Standard query (0)	mail.bmrtecpack.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:06:03.177987099 CEST	192.168.2.3	8.8.8.8	0xbe8d	Standard query (0)	mail.bmrtecpack.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 08:06:03.160412073 CEST	8.8.8.8	192.168.2.3	0x6c97	No error (0)	mail.bmrtecpack.com	bmrtecpack.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 08:06:03.160412073 CEST	8.8.8.8	192.168.2.3	0x6c97	No error (0)	bmrtecpack.com		184.95.37.27	A (IP address)	IN (0x0001)
Jun 11, 2021 08:06:03.399930954 CEST	8.8.8.8	192.168.2.3	0xbe8d	No error (0)	mail.bmrtecpack.com	bmrtecpack.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 08:06:03.399930954 CEST	8.8.8.8	192.168.2.3	0xbe8d	No error (0)	bmrtecpack.com		184.95.37.27	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 08:06:03.908809900 CEST	587	49743	184.95.37.27	192.168.2.3	220-gains.impressbss.com ESMTP Exim 4.93 #2 Fri, 11 Jun 2021 11:36:02 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 11, 2021 08:06:03.909461021 CEST	49743	587	192.168.2.3	184.95.37.27	EHLO 436432
Jun 11, 2021 08:06:04.102353096 CEST	587	49743	184.95.37.27	192.168.2.3	250-gains.impressbss.com Hello 436432 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-DSN 250-PIPELINING 250-STARTTLS 250 HELP
Jun 11, 2021 08:06:04.102859974 CEST	49743	587	192.168.2.3	184.95.37.27	STARTTLS
Jun 11, 2021 08:06:04.299942970 CEST	587	49743	184.95.37.27	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe PID: 2600 Parent PID: 5804

General

Start time:	08:04:18
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe'
Imagebase:	0x150000
File size:	951296 bytes
MD5 hash:	14F4F4356A708F1E9E18C6C71EF3153E
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: 00000000.00000002.219661677.0000000002531000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.220437474.0000000003539000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.220437474.0000000003539000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe PID: 6044 Parent PID: 2600

General

Start time:	08:04:21
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe
Imagebase:	0x240000
File size:	951296 bytes
MD5 hash:	14F4F4356A708F1E9E18C6C71EF3153E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe PID: 3508 Parent PID: 2600

General

Start time:	08:04:22
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\HALKBANK_EKSTRE_20210611_080203_744623,PDF.exe
Imagebase:	0x9d0000
File size:	951296 bytes
MD5 hash:	14F4F4356A708F1E9E18C6C71EF3153E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.482152633.0000000003071000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.482152633.0000000003071000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.217706120.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.217706120.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.476523997.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.476523997.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities — Show Windows behavior

File Created

File Read

Disassembly

Code Analysis