

ID: 339368
Sample Name:
Halkbank_Ekstre_20210113_162325_384771.exe
Cookbook: default.jbs
Time: 21:45:38
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Halkbank_Ekstre_20210113_162325_384771.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 14
Rich Headers 15
Data Directories 15

Sections 15
Resources 15
Imports 15
Possible Origin 16
Network Behavior 16
Snort IDS Alerts 16
Network Port Distribution 16
TCP Packets 16
UDP Packets 17
DNS Queries 18
DNS Answers 18
SMTP Packets 18
Code Manipulations 19
Statistics 19
Behavior 19
System Behavior 20
Analysis Process: Halkbank_Ekstre_20210113_162325_384771.exe PID: 4684 Parent PID: 5632 20
General 20
File Activities 20
Analysis Process: Halkbank_Ekstre_20210113_162325_384771.exe PID: 6128 Parent PID: 4684 20
General 20
File Activities 21
File Created 21
File Deleted 21
File Written 21
File Read 22
Disassembly 22
Code Analysis 22

Copyright null 2021

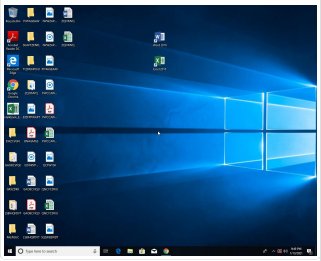
Analysis Report Halkbank_Ekstre_20210113_162325_38…

Overview

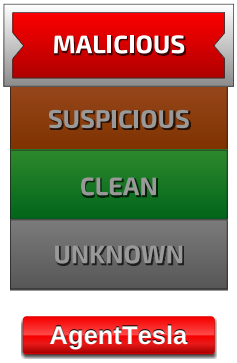
General Information

Sample Name:	Halkbank_Ekstre_20210113_162325_384771.exe
Analysis ID:	339368
MD5:	8bdf3d3cb7c7680..
SHA1:	442eaa27d23dc7..
SHA256:	a3c564db9537f84.
Tags:	AgentTesla exe geo Halkbank TUR

Most interesting Screenshot:



Detection

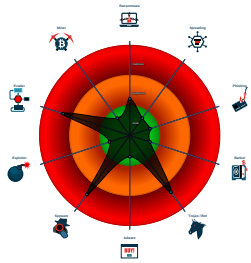


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- Halkbank_Ekstre_20210113_162325_384771.exe (PID: 4684 cmdline: 'C:\Users\user\Desktop\Halkbank_Ekstre_20210113_162325_384771.exe' MD5: 8BDF3D3CB7C7680DF5B8D6385DC5DB82)
  - Halkbank_Ekstre_20210113_162325_384771.exe (PID: 6128 cmdline: 'C:\Users\user\Desktop\Halkbank_Ekstre_20210113_162325_384771.exe' MD5: 8BDF3D3CB7C7680DF5B8D6385DC5DB82)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "VVkDExoCFG4o1k",
  "URL: ": "http://2cRhONggGD4U87PUSY.com",
  "To: ": "muhasebe@ceotech.com.tr",
  "ByHost: ": "mail.ceotech.com.tr:587",
  "Password: ": "JRuuV68u86gFWkr",
  "From: ": "muhasebe@ceotech.com.tr"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.628915716.00000000054D2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.625929224.0000000003020000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.628470056.0000000004091000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.253943134.0000000000F70000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.622605392.000000000040000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

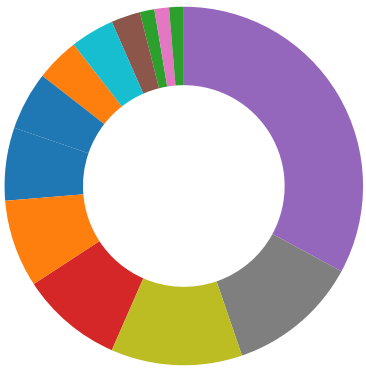
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Halkbank_Ekstre_20210113_162325_384771.exe.3020000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Halkbank_Ekstre_20210113_162325_384771.exe.54d0000.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Halkbank_Ekstre_20210113_162325_384771.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Halkbank_Ekstre_20210113_162325_384771.exe.f70000.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Halkbank_Ekstre_20210113_162325_384771.exe.f70000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:



Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

System Summary:



Copyright null 2021

.NET source code contains very large array initializations

Malware Analysis System Evasion:



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)

HIPS / PFW / Operating System Protection Evasion:



Maps a DLL or memory area into another process

Stealing of Sensitive Information:



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:



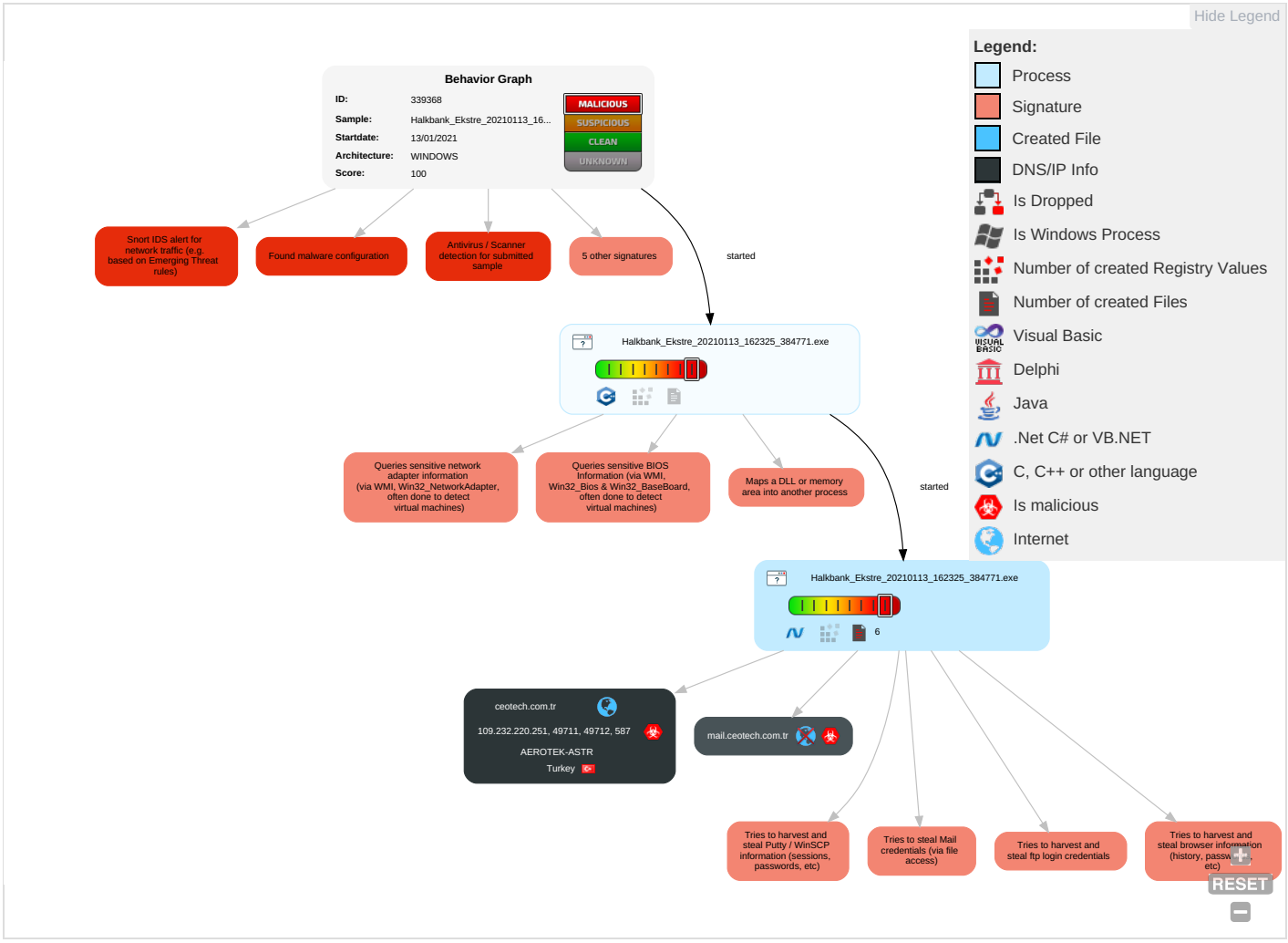
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command ar Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1 1	Credentials in Registry 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standarc Port 1
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 2 5	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Applicati Layer Protocc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Security Software Discovery 1 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application La Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Us Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application La Protocol

Copyright null 2021

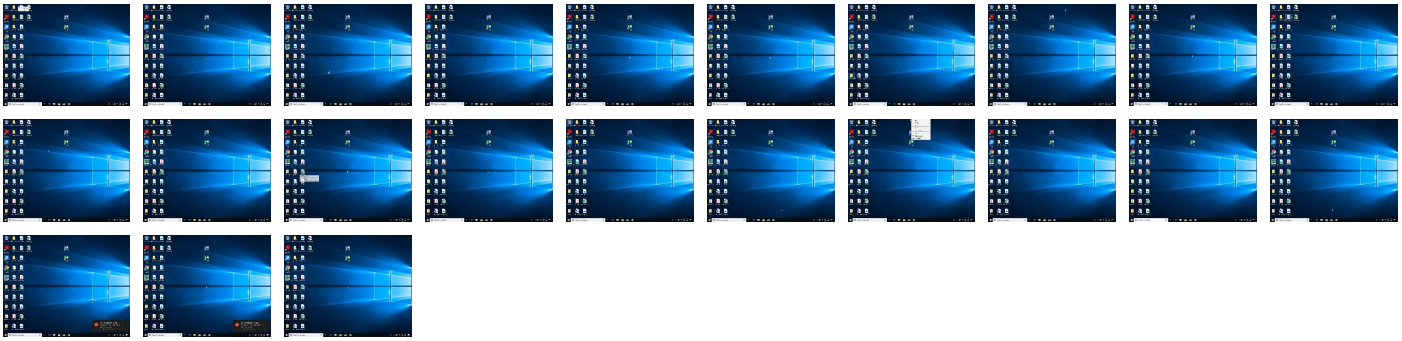
Behavior Graph



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_20210113_162325_384771.exe	36%	Virustotal		Browse
Halkbank_Ekstre_20210113_162325_384771.exe	45%	ReversingLabs	Win32.Trojan.AgentTesla	
Halkbank_Ekstre_20210113_162325_384771.exe	100%	Avira	TR/ATRAPS.Gen	
Halkbank_Ekstre_20210113_162325_384771.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Halkbank_Ekstre_20210113_162325_384771.exe.ec0000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
1.2.Halkbank_Ekstre_20210113_162325_384771.exe.54d0000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.Halkbank_Ekstre_20210113_162325_384771.exe.ec0000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
1.2.Halkbank_Ekstre_20210113_162325_384771.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.Halkbank_Ekstre_20210113_162325_384771.exe.ec0000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
1.2.Halkbank_Ekstre_20210113_162325_384771.exe.ec0000.1.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Domains

Copyright null 2021

Source	Detection	Scanner	Label	Link
ceotech.com.tr	0%	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://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://FStglU.com	0%	Avira URL Cloud	safe	
http://ceotech.com.tr	0%	Avira URL Cloud	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://mail.ceotech.com.tr	0%	Avira URL Cloud	safe	
http://2cRhONggGD4U87PUSY.com	0%	Avira URL Cloud	safe	
http://2cRhONggGD4U87PUSY.comt	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ceotech.com.tr	109.232.220.251	true	true	• 0%, Virustotal, Browse	unknown
mail.ceotech.com.tr	unknown	unknown	true		unknown

Contacted URLs

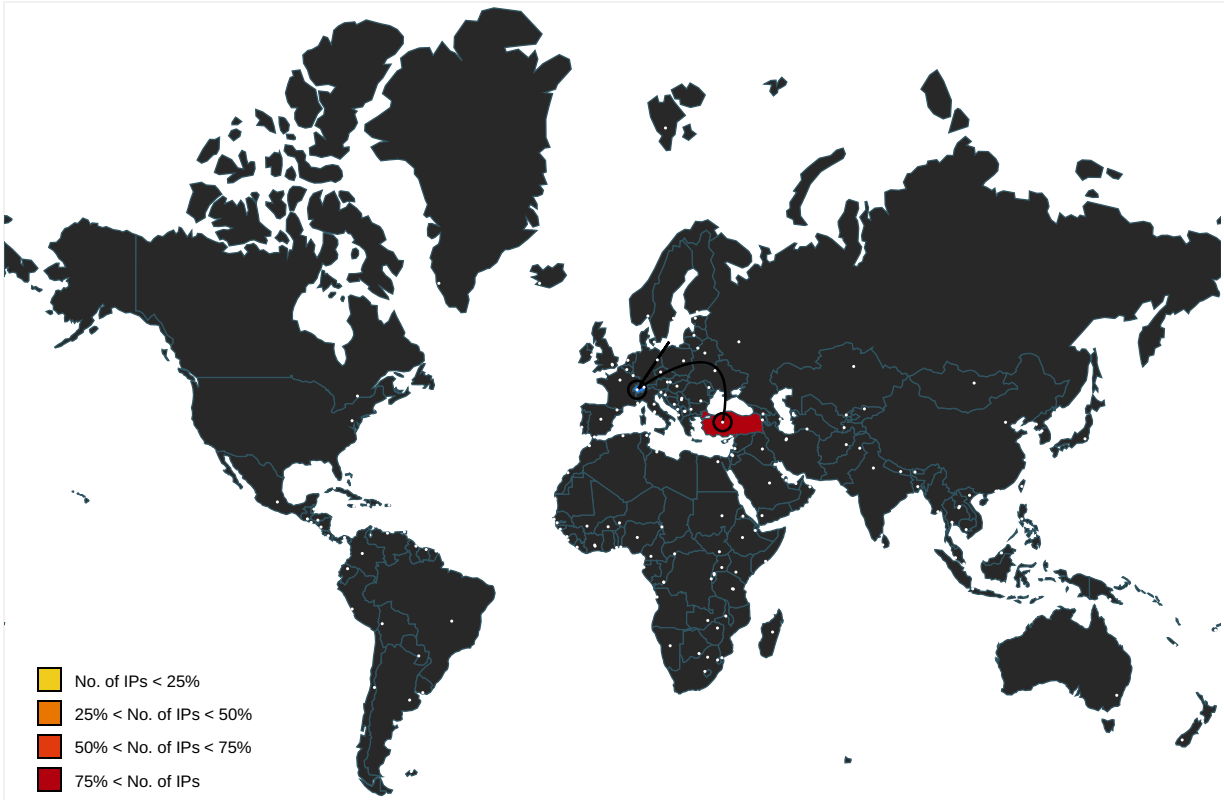
Name	Malicious	Antivirus Detection	Reputation
http://2cRhONggGD4U87PUSY.com	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Halkbank_Ekstre_20210113_162325_384771.exe, 00000001.00000002.626326029.0000000003091000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	Halkbank_Ekstre_20210113_162325_384771.exe, 00000001.00000002.626326029.0000000003091000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Halkbank_Ekstre_20210113_162325_384771.exe, 00000001.00000002.626326029.0000000003091000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://FStglU.com	Halkbank_Ekstre_20210113_162325_384771.exe, 00000001.00000002.626326029.0000000003091000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ceotech.com.tr	Halkbank_Ekstre_20210113_162325_384771.exe, 00000001.00000002.628097347.00000000033E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Halkbank_Ekstre_20210113_162325_384771.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://mail.ceotech.com.tr	Halkbank_Ekstre_20210113_162325_384771.exe, 00000001.00000002.628097347.00000000033E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://2cRhONggGD4U87PUSY.comt	Halkbank_Ekstre_20210113_162325_384771.exe, 00000001.00000002.626326029.0000000003091000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.232.220.251	unknown	Turkey		42807	AEROTEK-ASTR	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339368
Start date:	13.01.2021
Start time:	21:45:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Halkbank_Ekstre_20210113_162325_384771.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:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Copyright null 2021

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@3/1@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 28.2% (good quality ratio 26.4%) • Quality average: 78.6% • Quality standard deviation: 30%
HCA Information:	• Successful, ratio: 94% • 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 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.88.21.125, 104.42.151.234, 23.210.248.85, 104.43.139.144, 2.20.142.209, 2.20.142.210, 8.248.149.254, 8.253.95.249, 8.253.204.121, 67.26.75.254, 67.26.137.254 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, fs.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcoleus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:46:47	API Interceptor	1076x Sleep call for process: Halkbank_Ekstre_20210113_162325_384771.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
109.232.220.251	63Label_00000192672.doc.js	Get hash	malicious	Browse	• ozgurwebtasarim.com/counter/?id=555D5C5E0D0A020B240A05120D1710054A070B095E225E071014034A11175E17525E5550515C54515355555515E55&rnd=2812563
	63Label_00000192672.doc.js	Get hash	malicious	Browse	• ozgurwebtasarim.com/counter/?id=555D5C5E0D0A020B240A05120D1710054A070B095E225E071014034A11175E17525E5550515C54515355555515E55&rnd=2812563

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AEROTEK-ASTR	ZwFwevQtlv.exe	Get hash	malicious	Browse	• 37.230.106.15
	ssDV3d9O9o.exe	Get hash	malicious	Browse	• 37.230.106.15
	wjSwL3KItA.exe	Get hash	malicious	Browse	• 37.230.106.15
	XP-9743 Medical report COVID-19.doc	Get hash	malicious	Browse	• 109.232.216.177
	Re.invoice.exe	Get hash	malicious	Browse	• 37.230.107.14
	36bjGck9ps.exe	Get hash	malicious	Browse	• 37.230.107.15
	n1hou07jRi.exe	Get hash	malicious	Browse	• 37.230.107.14
	SZOSVrCvEl.exe	Get hash	malicious	Browse	• 37.230.107.17
	2LR7qlZpc9.exe	Get hash	malicious	Browse	• 37.230.107.14
	QXfxLv6GGp.exe	Get hash	malicious	Browse	• 37.230.107.17
	0908000090000.exe	Get hash	malicious	Browse	• 37.230.106.17
	Tax Invoices IN102738 IN102739 IN102740 (2).exe	Get hash	malicious	Browse	• 37.230.107.13
	Quotation 7339.exe	Get hash	malicious	Browse	• 37.230.107.16
	kart bilgisizzz.exe	Get hash	malicious	Browse	• 37.230.106.16
	CardFinans09000.exe	Get hash	malicious	Browse	• 37.230.106.17
	0lQnavQlRv.exe	Get hash	malicious	Browse	• 37.230.107.13
	payment invoice090909000.exe	Get hash	malicious	Browse	• 37.230.106.16
	POUIYYY.exe	Get hash	malicious	Browse	• 37.230.106.16
	invoice 2.exe	Get hash	malicious	Browse	• 37.230.107.15
	invoice 2.exe	Get hash	malicious	Browse	• 37.230.107.15

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\bdbdmgwj.xzv\Chrome\Default\Cookies

C:\Users\user\AppData\Roaming\bdbdmgwj.xzv\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\Halkbank_Ekstre_20210113_162325_384771.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6969296358976265
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBo2+tYeF+X:T5LLOpEO5J/Kn7U1uBo2UYeQ
MD5:	A9DBC7B8E523ABE3B02D77DBF2FCD645
SHA1:	DF5EE16ECF4B3B02E312F935AE81D4C5D2E91CA8
SHA-256:	39B4E45A062DEA6F541C18FA1A15C5C0DB43A59673A26E2EB5B8A4345EE767AE
SHA-512:	3CF87455263E395313E779D4F440D8405D86244E04B5F577BB9FA2F4A2069DE019D340F6B2F6EF420DEE3D3DEEFD4B58DA3FCA3BB802DE348E1A810D6379CC3B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.435198963754783
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	Halkbank_Ekstre_20210113_162325_384771.exe
File size:	517632
MD5:	8bdf3d3cb7c7680df5b8d6385dc5db82
SHA1:	442eaa27d23dc72fd96c9d2d984068669afbeb5d
SHA256:	a3c564db9537f84073828e42af85c0558e763cb211e80bc4653e429ecb62ce8b
SHA512:	7356a0586c565076d71ae75e77287d8d10a6636d4e789a078f4ba5b493288dcda0ccfbe721b5a05ea0dbaf37e0b428c0eeb19b77390e3239a3f7baccbfb5896b
SSDEEP:	6144:Lr1l5DbAQcHAORYANc73CoNUkJYUTIHRghDfelenXA87i+uLJl98xCoxCB:/1l5fAPHQNUdHID9Yb7PO9YCB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....tj.m'j.m'j.m'.Q.'k.m'.4.'l.m'.4.'r.m'.4.'..m'j.l'..m'...'..m'M7.'k.m'M7.'k.m'M7.'k.m'Richj.m'.....PE..L....._...

File Icon

Icon Hash:	0f470d0d0d09470c

Static PE Info

General

Entrypoint:	0x4088a7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FFEB4E8 [Wed Jan 13 08:52:56 2021 UTC]
TLS Callbacks:	

General

CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	e7da020c2fad0c59a3d5e97971484548

Entrypoint Preview

Instruction
call 00007F934CBF00A1h
jmp 00007F934CBE8D05h
push 00000014h
push 0041D838h
call 00007F934CBE95A8h
call 00007F934CBEC456h
movzx esi, ax
push 00000002h
call 00007F934CBF0034h
pop ecx
mov eax, 00005A4Dh
cmp word ptr [00400000h], ax
je 00007F934CBE8D06h
xor ebx, ebx
jmp 00007F934CBE8D35h
mov eax, dword ptr [0040003Ch]
cmp dword ptr [eax+00400000h], 00004550h
jne 00007F934CBE8CEDh
mov ecx, 0000010Bh
cmp word ptr [eax+00400018h], cx
jne 00007F934CBE8CDFh
xor ebx, ebx
cmp dword ptr [eax+00400074h], 0Eh
jbe 00007F934CBE8D0Bh
cmp dword ptr [eax+004000E8h], ebx
setne bl
mov dword ptr [ebp-1Ch], ebx
call 00007F934CBED443h
test eax, eax
jne 00007F934CBE8D0Ah
push 0000001Ch
call 00007F934CBE8DD5h
pop ecx
call 00007F934CBEDAACh
test eax, eax
jne 00007F934CBE8D0Ah
push 00000010h
call 00007F934CBE8DC4h
pop ecx
call 00007F934CBEC1E8h
and dword ptr [ebp-04h], 00000000h
call 00007F934CBEA983h
call dword ptr [004180C8h]
mov dword ptr [00424080h], eax
call 00007F934CBF0092h
mov dword ptr [00422284h], eax
call 00007F934CBEFC93h
test eax, eax
jns 00007F934CBE8D0Ah
push 00000008h
call 00007F934CBE78BAh

Instruction
pop ecx
call 00007F934CBEFEAFh

Rich Headers

Programming Language:	• [LNK] VS2012 build 50727 • [RES] VS2012 build 50727 • [C] VS2012 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1db94	0xdc	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x25000	0x14908	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3a000	0x1150	.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	0x1d6e0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x18000	0x1c8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x16d9a	0x16e00	False	0.571016905738	data	6.67353254408	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x18000	0x64f8	0x6600	False	0.572227328431	data	6.01779519415	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1f000	0x5098	0x3400	False	0.285531850962	data	4.70097691284	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x25000	0x14908	0x14a00	False	0.180705492424	data	4.28205034385	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3a000	0x1856	0x1a00	False	0.560546875	data	5.24804526054	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x251c0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x25628	0x988	data	English	United States
RT_ICON	0x25fb0	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294967295, next used block 4294967295	English	United States
RT_ICON	0x27058	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294967295, next used block 4294967295	English	United States
RT_ICON	0x29600	0xe8ac	data	English	United States
RT_RCDATA	0x37f00	0x1a05	data	English	United States
RT_GROUP_ICON	0x37eb0	0x4c	data	English	United States

Imports

DLL	Import

Copyright null 2021

DLL	Import
KERNEL32.dll	RaiseException, ReadConsoleW, ReadFile, CreateFileW, WriteConsoleW, GetStringTypeW, LCMapStringEx, SetConsoleCursorPosition, LoadLibraryW, GetModuleHandleW, HeapReAlloc, HeapSize, OutputDebugStringW, SetFilePointerEx, GetConsoleMode, GetConsoleCP, FlushFileBuffers, SetStdHandle, WideCharToMultiByte, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetProcessHeap, HeapAlloc, GetStdHandle, GetTickCount64, GetSystemTimeAsFileTime, QueryPerformanceCounter, GetModuleFileNameA, GetCurrentThreadId, SetLastError, GetCPInfo, GetOEMCP, GetACP, EncodePointer, DecodePointer, GetLastError, InterlockedDecrement, ExitProcess, GetModuleHandleExW, GetProcAddress, AreFileApisANSI, MultiByteToWideChar, GetLocalTime, GetCommandLineA, IsDebuggerPresent, IsProcessorFeaturePresent, EnterCriticalSection, LeaveCriticalSection, CloseHandle, HeapFree, InitializeCriticalSectionAndSpinCount, RtlUnwind, GetFileType, DeleteCriticalSection, InitOnceExecuteOnce, GetStartupInfoW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, FlsAlloc, FlsGetValue, FlsSetValue, FlsFree, GetCurrentProcess, TerminateProcess, WriteFile, GetModuleFileNameW, Sleep, LoadLibraryExW, InterlockedIncrement, IsValidCodePage, SetEndOfFile
msi.dll	
loadperf.dll	LoadPerfCounterTextStringsA, UnloadPerfCounterTextStringsW, UnloadPerfCounterTextStringsA
MSVFW32.dll	StretchDIB
AVIFIL32.dll	AVIFileExit, AVIStreamReadData
pdh.dll	PdhEnumObjectsW, PdhSetQueryTimeRange, PdhGetDllVersion
WSOCK32.dll	WSASetBlockingHook, WSACancelAsyncRequest, bind, ord1104, ord1108, ord1130
GDI32.dll	StartDocW, GdiGetSpoolFileHandle, PolyBezier
MAPI32.dll	
MSACM32.dll	acmDriverPriority, acmFilterTagDetailsA

Possible Origin

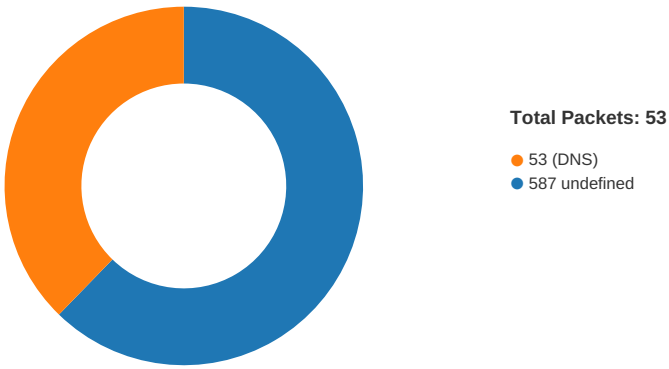
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-21:48:24.132757	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49711	587	192.168.2.7	109.232.220.251
01/13/21-21:48:25.921637	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49712	587	192.168.2.7	109.232.220.251

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:48:23.310643911 CET	49711	587	192.168.2.7	109.232.220.251

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:48:23.391347885 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:23.391645908 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:23.601947069 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:23.602631092 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:23.683430910 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:23.685769081 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:23.767661095 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:23.768654108 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:23.861720085 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:23.862680912 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:23.943025112 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:23.943578005 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:24.043967962 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:24.044297934 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:24.124954939 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:24.125097990 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:24.132756948 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:24.133276939 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:24.133873940 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:24.134016991 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:24.213766098 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:24.214521885 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:24.236974001 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:24.277636051 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.226833105 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.309237957 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:25.309633970 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.309801102 CET	49711	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.310714960 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.383346081 CET	587	49712	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:25.383452892 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.390098095 CET	587	49711	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:25.459893942 CET	587	49712	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:25.460177898 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.532881021 CET	587	49712	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:25.533261061 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.606108904 CET	587	49712	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:25.606667042 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.684650898 CET	587	49712	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:25.687062025 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.761615038 CET	587	49712	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:25.761971951 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.842509031 CET	587	49712	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:25.844945908 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.920116901 CET	587	49712	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:25.920146942 CET	587	49712	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:25.921427011 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.921637058 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.921734095 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.921817064 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.921986103 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.922058105 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.922123909 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.922286987 CET	49712	587	192.168.2.7	109.232.220.251
Jan 13, 2021 21:48:25.994154930 CET	587	49712	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:25.994611979 CET	587	49712	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:25.994637966 CET	587	49712	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:26.023324013 CET	587	49712	109.232.220.251	192.168.2.7
Jan 13, 2021 21:48:26.074748039 CET	49712	587	192.168.2.7	109.232.220.251

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:46:29.657373905 CET	56590	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:46:29.705615044 CET	53	56590	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:30.480578899 CET	60501	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:30.528429031 CET	53	60501	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:31.331312895 CET	53775	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:31.379257917 CET	53	53775	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:32.790518045 CET	51837	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:32.838291883 CET	53	51837	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:34.691339970 CET	55411	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:34.739322901 CET	53	55411	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:35.673193932 CET	63668	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:35.723819971 CET	53	63668	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:36.466608047 CET	54640	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:36.517349005 CET	53	54640	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:38.135898113 CET	58739	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:38.186909914 CET	53	58739	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:39.445326090 CET	60338	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:39.504596949 CET	53	60338	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:41.700320959 CET	58717	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:41.751512051 CET	53	58717	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:44.782391071 CET	59762	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:44.838838100 CET	53	59762	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:46.812696934 CET	54329	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:46.860708952 CET	53	54329	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:47.769114971 CET	58052	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:47.816962004 CET	53	58052	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:54.259582996 CET	54008	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:54.309675932 CET	53	54008	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:55.723229885 CET	59451	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:55.771421909 CET	53	59451	8.8.8.8	192.168.2.7
Jan 13, 2021 21:46:57.217106104 CET	52914	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:46:57.265522957 CET	53	52914	8.8.8.8	192.168.2.7
Jan 13, 2021 21:47:19.243168116 CET	64569	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:47:19.306643009 CET	53	64569	8.8.8.8	192.168.2.7
Jan 13, 2021 21:47:19.401158094 CET	52816	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:47:19.457763910 CET	53	52816	8.8.8.8	192.168.2.7
Jan 13, 2021 21:48:22.759804964 CET	50781	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:48:22.858607054 CET	53	50781	8.8.8.8	192.168.2.7
Jan 13, 2021 21:48:22.876439095 CET	54230	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:48:23.220669985 CET	53	54230	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:48:22.759804964 CET	192.168.2.7	8.8.8.8	0x5085	Standard query (0)	mail.ceotech.com.tr	A (IP address)	IN (0x0001)
Jan 13, 2021 21:48:22.876439095 CET	192.168.2.7	8.8.8.8	0xb9fa	Standard query (0)	mail.ceotech.com.tr	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:48:22.858607054 CET	8.8.8.8	192.168.2.7	0x5085	No error (0)	mail.ceotech.com.tr	ceotech.com.tr		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:48:22.858607054 CET	8.8.8.8	192.168.2.7	0x5085	No error (0)	ceotech.com.tr		109.232.220.251	A (IP address)	IN (0x0001)
Jan 13, 2021 21:48:23.220669985 CET	8.8.8.8	192.168.2.7	0xb9fa	No error (0)	mail.ceotech.com.tr	ceotech.com.tr		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:48:23.220669985 CET	8.8.8.8	192.168.2.7	0xb9fa	No error (0)	ceotech.com.tr		109.232.220.251	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2021 21:48:23.601947069 CET	587	49711	109.232.220.251	192.168.2.7	220-cpanel8.webadam.com ESMTP Exim 4.93 #2 Wed, 13 Jan 2021 23:48:25 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 13, 2021 21:48:23.602631092 CET	49711	587	192.168.2.7	109.232.220.251	EHLO 226533
Jan 13, 2021 21:48:23.683430910 CET	587	49711	109.232.220.251	192.168.2.7	250-cpanel8.webadam.com Hello 226533 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 13, 2021 21:48:23.685769081 CET	49711	587	192.168.2.7	109.232.220.251	AUTH login bXVoYXNlYmVAY2VvdGVjaC5jb20udHI=
Jan 13, 2021 21:48:23.767661095 CET	587	49711	109.232.220.251	192.168.2.7	334 UGFzc3dvcmQ6
Jan 13, 2021 21:48:23.861720085 CET	587	49711	109.232.220.251	192.168.2.7	235 Authentication succeeded
Jan 13, 2021 21:48:23.862680912 CET	49711	587	192.168.2.7	109.232.220.251	MAIL FROM:<muhasebe@ceotech.com.tr>
Jan 13, 2021 21:48:23.943025112 CET	587	49711	109.232.220.251	192.168.2.7	250 OK
Jan 13, 2021 21:48:23.943578005 CET	49711	587	192.168.2.7	109.232.220.251	RCPT TO:<muhasebe@ceotech.com.tr>
Jan 13, 2021 21:48:24.043967962 CET	587	49711	109.232.220.251	192.168.2.7	250 Accepted
Jan 13, 2021 21:48:24.044297934 CET	49711	587	192.168.2.7	109.232.220.251	DATA
Jan 13, 2021 21:48:24.125097990 CET	587	49711	109.232.220.251	192.168.2.7	354 Enter message, ending with "." on a line by itself
Jan 13, 2021 21:48:24.134016991 CET	49711	587	192.168.2.7	109.232.220.251	.
Jan 13, 2021 21:48:24.236974001 CET	587	49711	109.232.220.251	192.168.2.7	250 OK id=1kzn45-003L46-Pb
Jan 13, 2021 21:48:25.226833105 CET	49711	587	192.168.2.7	109.232.220.251	QUIT
Jan 13, 2021 21:48:25.309237957 CET	587	49711	109.232.220.251	192.168.2.7	221 cpanel8.webadam.com closing connection
Jan 13, 2021 21:48:25.459893942 CET	587	49712	109.232.220.251	192.168.2.7	220-cpanel8.webadam.com ESMTP Exim 4.93 #2 Wed, 13 Jan 2021 23:48:27 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 13, 2021 21:48:25.460177898 CET	49712	587	192.168.2.7	109.232.220.251	EHLO 226533
Jan 13, 2021 21:48:25.532881021 CET	587	49712	109.232.220.251	192.168.2.7	250-cpanel8.webadam.com Hello 226533 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 13, 2021 21:48:25.533261061 CET	49712	587	192.168.2.7	109.232.220.251	AUTH login bXVoYXNlYmVAY2VvdGVjaC5jb20udHI=
Jan 13, 2021 21:48:25.606108904 CET	587	49712	109.232.220.251	192.168.2.7	334 UGFzc3dvcmQ6
Jan 13, 2021 21:48:25.684650898 CET	587	49712	109.232.220.251	192.168.2.7	235 Authentication succeeded
Jan 13, 2021 21:48:25.687062025 CET	49712	587	192.168.2.7	109.232.220.251	MAIL FROM:<muhasebe@ceotech.com.tr>
Jan 13, 2021 21:48:25.761615038 CET	587	49712	109.232.220.251	192.168.2.7	250 OK
Jan 13, 2021 21:48:25.761971951 CET	49712	587	192.168.2.7	109.232.220.251	RCPT TO:<muhasebe@ceotech.com.tr>
Jan 13, 2021 21:48:25.842509031 CET	587	49712	109.232.220.251	192.168.2.7	250 Accepted
Jan 13, 2021 21:48:25.844945908 CET	49712	587	192.168.2.7	109.232.220.251	DATA
Jan 13, 2021 21:48:25.920146942 CET	587	49712	109.232.220.251	192.168.2.7	354 Enter message, ending with "." on a line by itself
Jan 13, 2021 21:48:25.922286987 CET	49712	587	192.168.2.7	109.232.220.251	.
Jan 13, 2021 21:48:26.023324013 CET	587	49712	109.232.220.251	192.168.2.7	250 OK id=1kzn47-003L4J-JA

Code Manipulations

Statistics

Behavior

Copyright null 2021



System Behavior

Analysis Process: Halkbank_Ekstre_20210113_162325_384771.exe PID: 4684 Parent PID: 5632

General

Start time:	21:46:34
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Halkbank_Ekstre_20210113_162325_384771.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Halkbank_Ekstre_20210113_162325_384771.exe'
Imagebase:	0xec0000
File size:	517632 bytes
MD5 hash:	8BDF3D3CB7C7680DF5B8D6385DC5DB82
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.253943134.0000000000F70000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Halkbank_Ekstre_20210113_162325_384771.exe PID: 6128 Parent PID: 4684

General

Start time:	21:46:36
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Halkbank_Ekstre_20210113_162325_384771.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Halkbank_Ekstre_20210113_162325_384771.exe'
Imagebase:	0xec0000
File size:	517632 bytes
MD5 hash:	8BDF3D3CB7C7680DF5B8D6385DC5DB82

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: 00000001.00000002.628915716.00000000054D2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.625929224.0000000003020000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.628470056.0000000004091000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.622605392.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.626326029.0000000003091000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.626326029.0000000003091000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.624730399.0000000001209000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D13CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D13CF06	unknown
C:\Users\user\AppData\Roaming\bdbdmgwj.xzv	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BF8BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\bdbdmgwj.xzv\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BF8BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\bdbdmgwj.xzv\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BF8BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\bdbdmgwj.xzv\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6BF8DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bdbdmgwj.xzv\Chrome\Default\Cookies	success or wait	1	6BF86A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bdbdmgwj.xzv\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00

Copyright null 2021