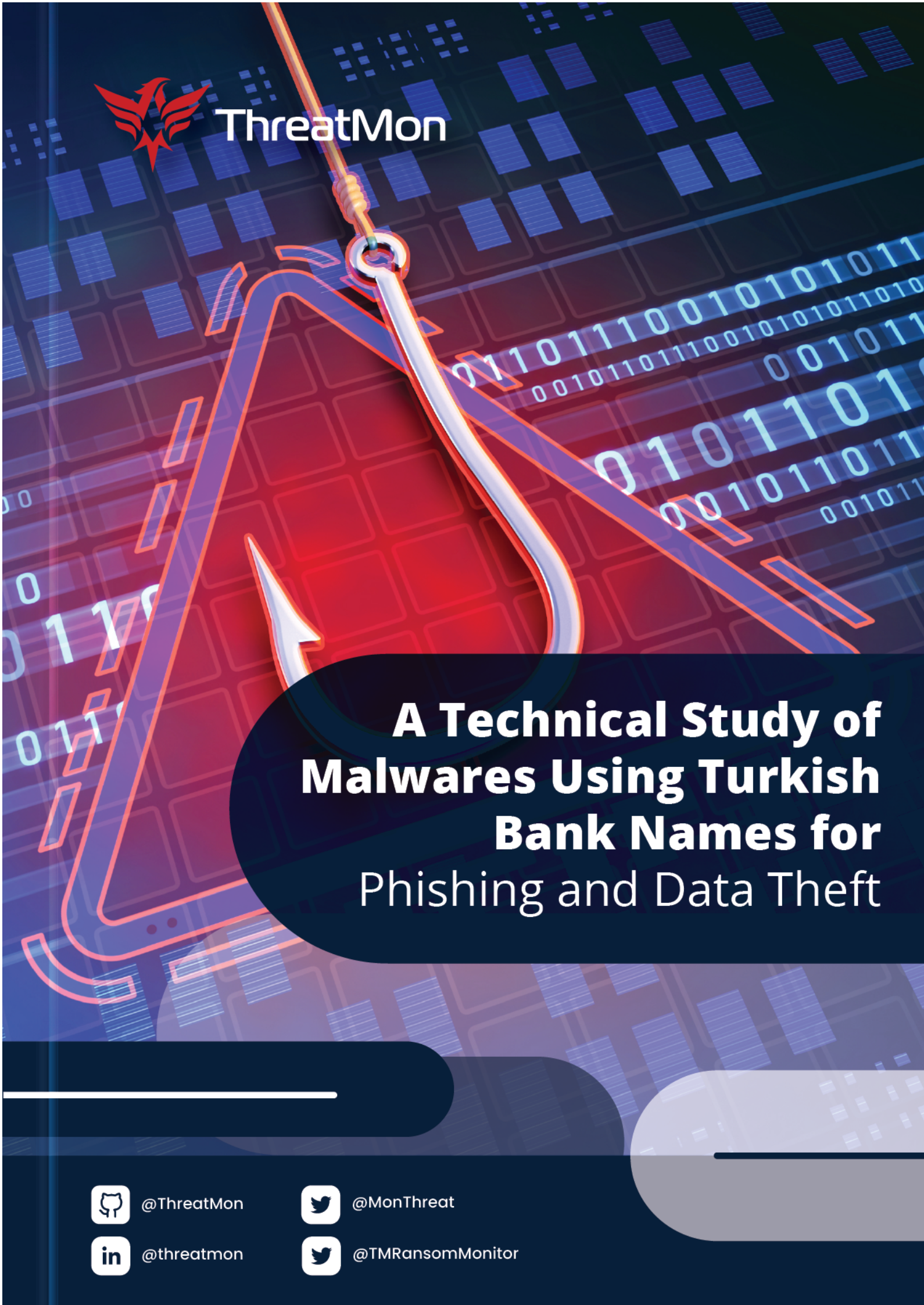

ThreatMon
A Technical Study of Malwares Using Turkish Bank Names for Phishing and Data Theft
@ThreatMon
@MonThreat
@threatmon
@TMRansomMonitor

Contents

Contents **2**
Introduction **3**
Stealers and Data Theft **3**
Malware Delivery **4**
Initial Execution **5**
Technical Analysis **6**
Agent Tesla 6
Snake Keylogger 8
Formbook 9
MITRE ATT&CK **10**
Indicators Of Compromise (IOCs) **10**

Introduction

The rise of cybercrime has led to an increase in the use of malicious software, commonly known as malware, that targets individuals and organizations with the aim of stealing sensitive information. In Turkey, there has been a significant increase in the use of malware that utilizes Turkish bank names for phishing and data theft. This report presents a technical study of three types of malware families - Formbook, Agent Tesla, and Snake Keylogger - that are commonly used in data theft in Turkey.

The report provides an in-depth analysis of these malware families, including their capabilities, tactics, and techniques used to deceive victims and steal sensitive information.The study is based on extensive research of various sources, including technical reports, academic papers, and industry publications. The report is intended to provide valuable insights into the nature of these malware families and the threats they pose, as well as to help organizations and individuals protect themselves against these threats.

Stealers and Data Theft

A stealer malware, also known as a credential stealer, is a type of malicious software designed to steal sensitive information from a victim's computer system. This can include usernames, passwords, credit card numbers, and other personal and financial information.

Data theft, on the other hand, refers to the act of stealing sensitive data from a computer system, network, or storage device. This can include personally identifiable information (PII), financial information, intellectual property, and other types of sensitive information. The stolen data can then be used for malicious purposes, such as identity theft, fraud, or espionage.

A stealer malware typically works by infecting a victim's computer system and then searching for sensitive information stored on the system, such as login credentials and saved passwords. The malware can then send this information to a remote server controlled by the attacker, who can then use it for malicious purposes.

In addition to stealing login credentials, some stealer malwares can also capture other types of data, such as browsing history, email content, and documents stored on the victim's computer. The specific types of data that can be stolen depend on the capabilities of the malware and the information that is stored on the victim's computer.

Malware Delivery

In these kinds of attacks, almost all malwares delivered victims using spear-phishing attachments. Victims are deceived with messages such as 'Money has been deposited into your account', 'The Swift message sent is attached', 'Your payment is delayed, please view the attached pdf', and are prompted to run malicious files that have been sent.

Here is an example by [Difesa&Sicurezza]:

GA **Garanti Bankası AŞ.-** In entrat...icurezza.com 13:47
Para Transferi Bilgilendirmesi-
A: Difesa e Sicurezza (difesaesicurezza.com)

Garanti Sayın,

Hatırlatma

EFT

Para transferi işleminiz gerçekleşmiştir.

5 Kolay bankacılık yolu

Bu e-posta'nın size ait olmadığını düşünüyorsanız 444 0 333 Müşteri İletişim Merkezi' ni arayarak yanlış mail gönderimini bildirebilirsiniz.

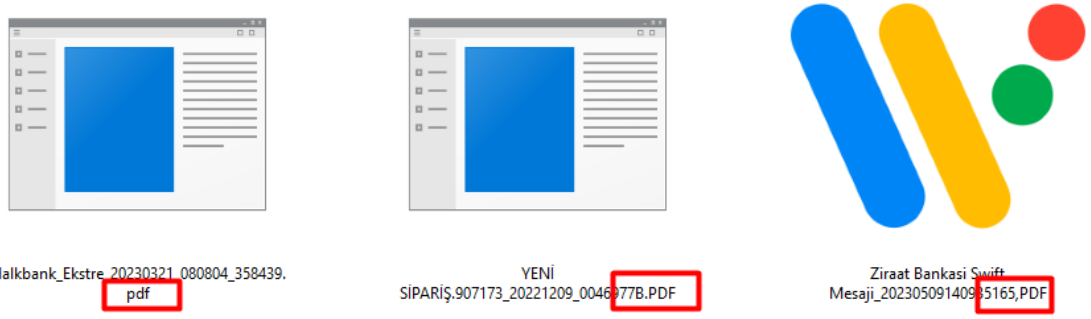
T. Garanti Bankası A.Ş.
Genel Müdürlük: Nispetiye Mah. Aytar Cad. No: 2 Beşiktaş 34340 Levent İstanbul
Mersis Numarası: 0879 0017 5660 0379
www.garantibbva.com.tr

Para Transferi Bilgilen...329.7z
249 KB

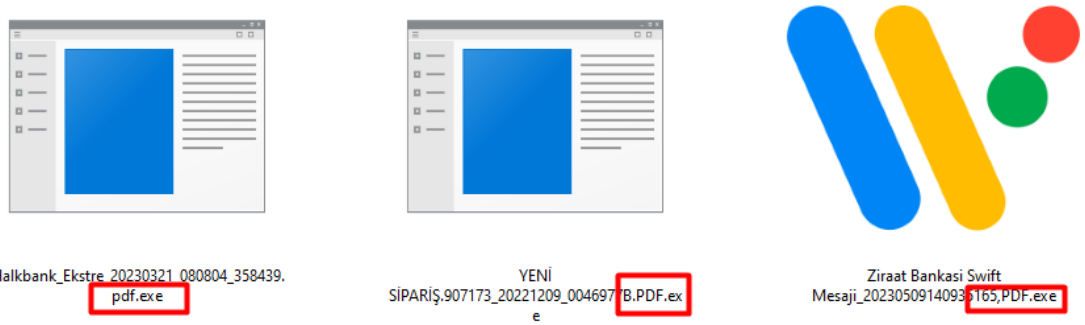
Initial Execution

The Initial Execution part includes a phishing tactic similar to the delivery part. Almost all of them, whether it's Formbook, Agent Tesla, or Snake Keylogger, use the same tactic because people constantly fall into this trap.

As seen in the screenshots below, when you don't enable file name extensions, the files appear as PDF files. (Although clumsy hackers failed to hide them properly.) But if you enable file name extensions, you can see that the files are actually executable files (".exe" files).



Without File name extensions



File name extensions enabled

Technical Analysis

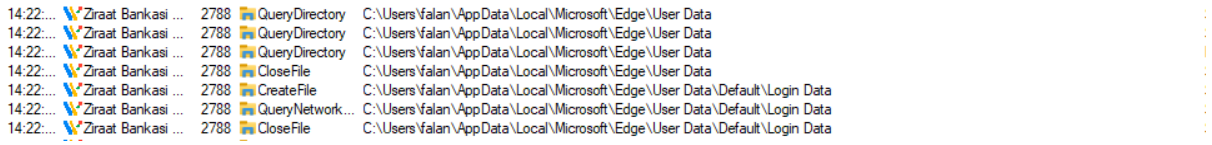
In this part, a technical analysis will be performed on Agent Tesla, Snake Keylogger, and Formbook, which are three of the most commonly used malware examples in these types of phishing attacks. However, a detailed analysis will not be carried out. Additionally, MITRE ATT&CK Technique IDs and latest IOCs will be shared.

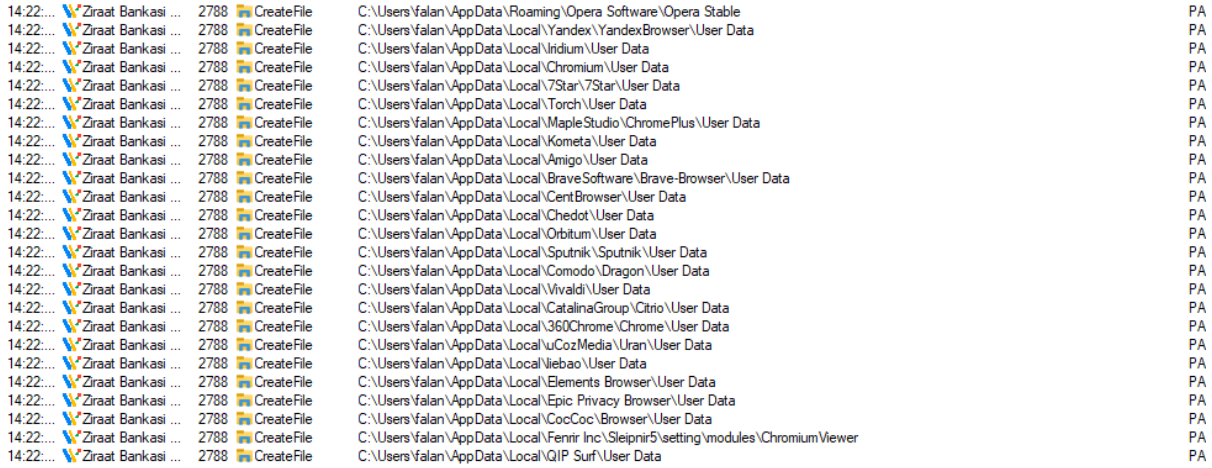
Agent Tesla

Agent Tesla is a type of malware that is designed to steal sensitive information from a victim's computer. It is a sophisticated keylogger that is capable of capturing keystrokes, taking screenshots, and stealing passwords, credit card information, and other personal data. Agent Tesla can also record audio and video from the victim's computer, as well as control the computer remotely.

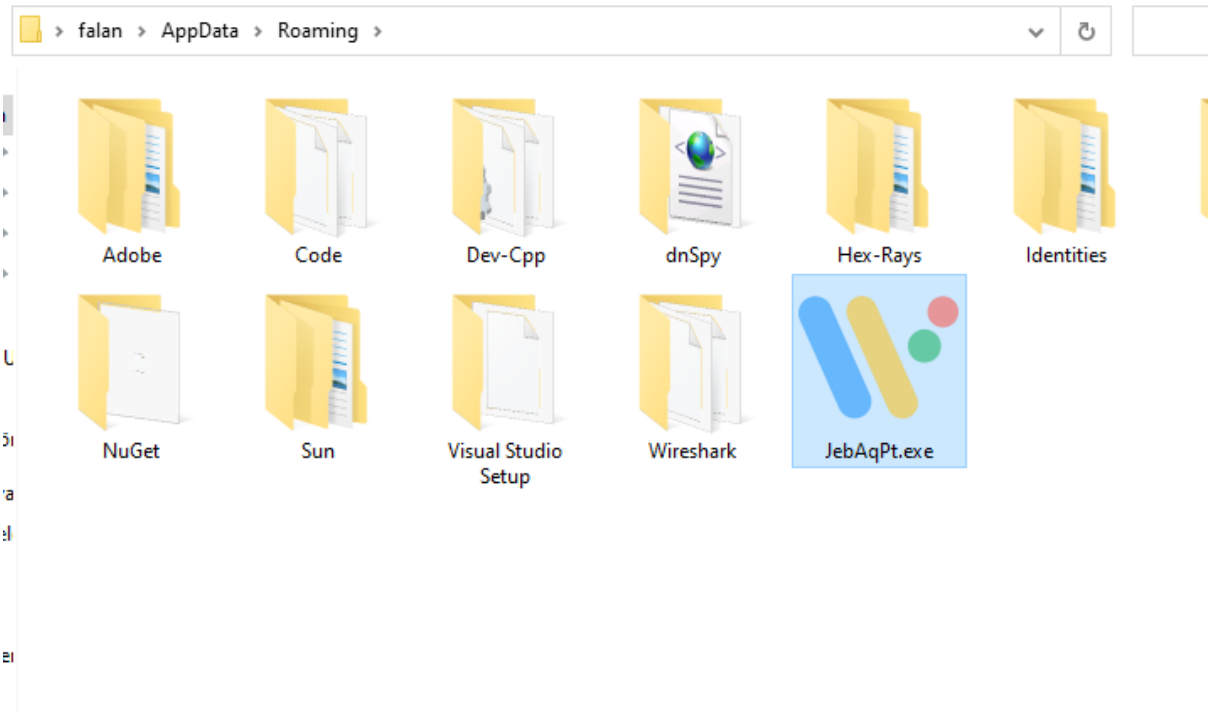
After executing the portable executable, it:

- Checks computer location settings
- Reads FTP credentials
- Reads user data of email clients
- Reads credentials of web browsers (cookies, passwords etc)





It creates scheduled tasks for persistence. So it will be executed at logon.



Then it exfiltrates all the information it collects to its C2 Server which abuses Telegram.

192.168.2.13	8.8.8.8	DNS	76	Standard query 0xf010 A api.telegram.org
8.8.8.8	192.168.2.13	DNS	92	Standard query response 0xf010 A api.telegram.org A 149.154.167.220

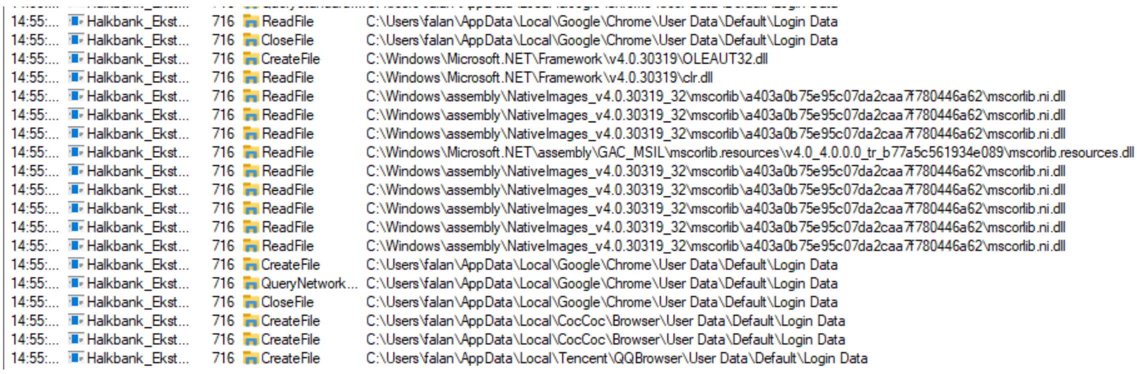
192.168.2.13	149.154.167.220	TCP	60	49702 → 443 [ACK] Seq=266 Ack=5800 Win=65280 Len=0
192.168.2.13	149.154.167.220	TLSv1.2	343	Application Data
149.154.167.220	192.168.2.13	TLSv1.2	108	Application Data
192.168.2.13	149.154.167.220	TLSv1.2	1005	Application Data
149.154.167.220	192.168.2.13	TCP	54	443 → 49702 [ACK] Seq=5854 Ack=1506 Win=69632 Len=0
149.154.167.220	192.168.2.13	TLSv1.2	1126	Application Data
192.168.2.13	149.154.167.220	TCP	60	49702 → 443 [ACK] Seq=1506 Ack=6926 Win=65536 Len=0
192.168.2.13	149.154.167.220	TLSv1.2	321	Application Data
149.154.167.220	192.168.2.13	TCP	54	443 → 49702 [ACK] Seq=6926 Ack=1773 Win=71680 Len=0
149.154.167.220	192.168.2.13	TLSv1.2	108	Application Data

Snake Keylogger

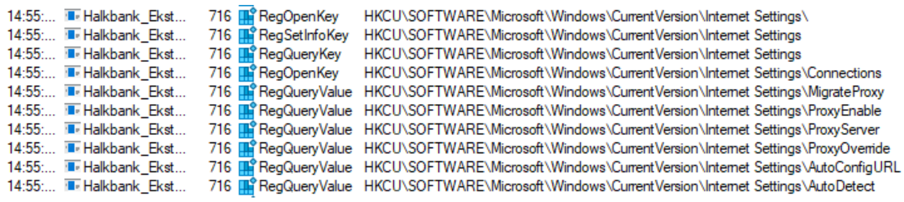
Snake Keylogger is a type of malicious software (malware) that is designed to capture keystrokes typed on a victim's computer. It is a type of keylogger that can capture passwords, credit card information, and other sensitive data entered by the victim.

After executing the file, it:

- Reads FTP credentials
- Reads user data of local email clients
- Reads credentials of web browsers (cookies, passwords etc)
- Checks external IP address
- Logs keystrokes



14:55:...	Halkbank_Ekst...	716	ReadFile	C:\Users\falan\AppData\Local\Google\Chrome\User Data\Default\Login Data
14:55:...	Halkbank_Ekst...	716	CloseFile	C:\Users\falan\AppData\Local\Google\Chrome\User Data\Default\Login Data
14:55:...	Halkbank_Ekst...	716	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\OLEAUT32.dll
14:55:...	Halkbank_Ekst...	716	ReadFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
14:55:...	Halkbank_Ekst...	716	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll
14:55:...	Halkbank_Ekst...	716	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll
14:55:...	Halkbank_Ekst...	716	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll
14:55:...	Halkbank_Ekst...	716	ReadFile	C:\Windows\Microsoft.NET\assembly\GAC_MSIL\mscorlib.resources\v4.0_4.0.0.0_tr_b77a5c561934e089\mscorlib.resources.dll
14:55:...	Halkbank_Ekst...	716	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll
14:55:...	Halkbank_Ekst...	716	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll
14:55:...	Halkbank_Ekst...	716	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll
14:55:...	Halkbank_Ekst...	716	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll
14:55:...	Halkbank_Ekst...	716	ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll
14:55:...	Halkbank_Ekst...	716	CreateFile	C:\Users\falan\AppData\Local\Google\Chrome\User Data\Default\Login Data
14:55:...	Halkbank_Ekst...	716	QueryNetwork...	C:\Users\falan\AppData\Local\Google\Chrome\User Data\Default\Login Data
14:55:...	Halkbank_Ekst...	716	CloseFile	C:\Users\falan\AppData\Local\Google\Chrome\User Data\Default\Login Data
14:55:...	Halkbank_Ekst...	716	CreateFile	C:\Users\falan\AppData\Local\CocCoc\Browser\User Data\Default\Login Data
14:55:...	Halkbank_Ekst...	716	CreateFile	C:\Users\falan\AppData\Local\CocCoc\Browser\User Data\Default\Login Data
14:55:...	Halkbank_Ekst...	716	CreateFile	C:\Users\falan\AppData\Local\Tencent\QQBrowser\User Data\Default\Login Data



14:55:...	Halkbank_Ekst...	716	RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\
14:55:...	Halkbank_Ekst...	716	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
14:55:...	Halkbank_Ekst...	716	RegQueryKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
14:55:...	Halkbank_Ekst...	716	RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
14:55:...	Halkbank_Ekst...	716	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\MigrateProxy
14:55:...	Halkbank_Ekst...	716	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
14:55:...	Halkbank_Ekst...	716	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
14:55:...	Halkbank_Ekst...	716	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride
14:55:...	Halkbank_Ekst...	716	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL
14:55:...	Halkbank_Ekst...	716	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect

Then it exfiltrates all the information it collects to its C2 Server which abuses Telegram again, same as Agent Tesla.

Formbook

Formbook is a type of malware that is designed to steal sensitive information from a victim's computer. It is a type of spyware that is capable of capturing keystrokes, taking screenshots, and stealing passwords, credit card information, and other personal data. Formbook can also record audio and video from the victim's computer, as well as control the computer remotely.

After executing the Formbook, it:

- Checks computer location settings
- Reads FTP credentials
- Reads user data of email clients
- Reads credentials of web browsers (cookies, passwords etc)

Almost exactly the same as Agent Tesla, they even create the same scheduled task under the same folder .

```
Folder: \Updates
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
JebAqPt                                  N/A                    Ready
zerQTfyuOwBoc                            N/A                    Ready
```

But there are some differences:

- Functionality: While both malware can capture keystrokes, take screenshots, and steal passwords and other personal information, Agent Tesla is also capable of recording audio and video from the victim's computer, as well as controlling the computer remotely. Formbook, on the other hand, is primarily focused on stealing data from web forms.
- Distribution: Both malware can be distributed through phishing emails, fake software updates, or malicious websites, but Agent Tesla is more commonly spread through targeted attacks, while Formbook is more commonly spread through mass spam campaigns.
- Detection: While both malware can operate silently in the background, evading detection by security software, Agent Tesla is generally considered to be more difficult to detect than Formbook.

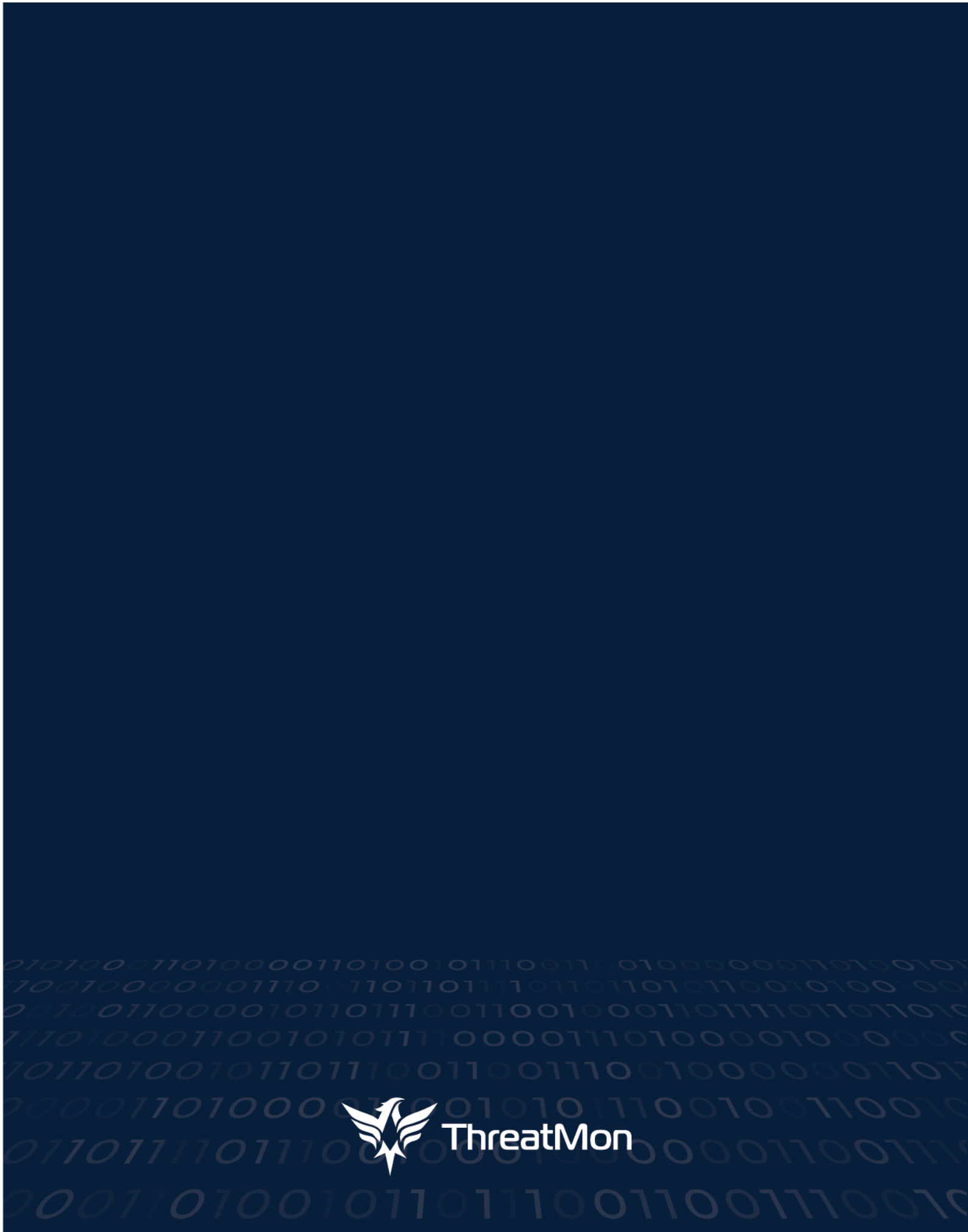
MITRE ATT&CK

TECHNIC NAME	ID
Steal Web Session Cookie	T1539
Credentials From Password Stores	T1555
Unsecured Credentials	T1552
Query Registry	T1012
Software Discovery	T1518
System Information Discovery	T1082
Ingress Tool Transfer	T1105
Application Layer Protocol	T1071
Input Capture	T1056

Indicators Of Compromise (IOCs)

TYPE	IOC
SHA256	392ee3c9d47409b170b5e4d6f7eedf427bf1121be42b024a663340bed3025bd4
URL	hxxps://api.telegram[.]org/bot6277254729:AAH9hHYZNSDZac0nNvgmchkZF8WVRKU5dJ0/sendDocument
SHA256	54c042777168fbf754e0bb6de6547d13398f958344d2e0aa76060ef4daa02419
URL	hxxps://api.telegram[.]org/bot5990689485:AAF2-uAQqkGmyMf-HkQ_5G1q8B9Ce_oT6o0/sendDocument
SHA256	d7fb90a1b438f34eb157d31442167e611c5517027bd52bb2fe9688fa44879757
URL	hxxp://www.subuwu[.]com

Only a part of the IOCs have been shared here. Don't forget to check out our Github Page for more.



45305 Catalina cs St 150, Sterling VA 20166