Homeland Security

Modeling Exercise: FOX IT TorrentLocker Report

August 2015

Office of Cybersecurity & Communications

Exercise

- Your participation is essential!
- Translate the prose report into structured STIX:
  - Identify the top level constructs in the report
  - And relationships between them
- Don’t worry about exhaustive detail into each top-level construct

Report

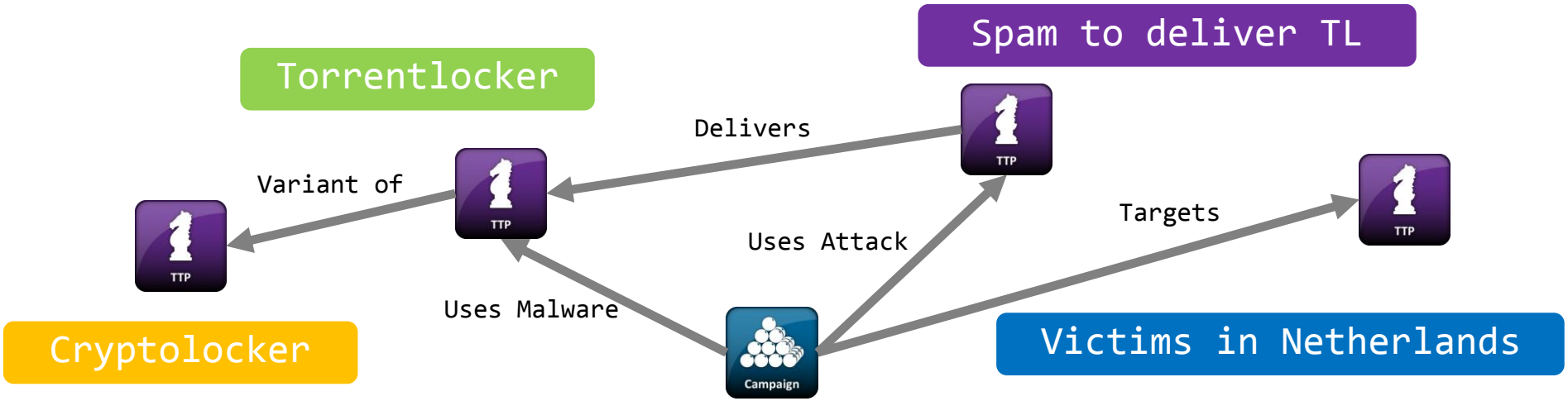
"Cryptolocker variant Torrentlocker making new victims in NL"

http://blog.fox-it.com/2014/11/06

- Describes a variant of Cryptolocker
- Discusses origins and targeting
- Provides potential remediations
- Includes host and network indicators of compromise

Introduction

Since past weekend, the Netherlands were hit with another spam run spreading the Cryptolocker variant known as Torrentlocker. Torrentlocker presents itself to victims as Cryptolocker in all cases, however this is a completely different malware. Fox-IT received multiple reports of new victims in the Netherlands and we are currently analyzing the new spam run and malware that was subsequently used.



IOCs in Email

To detect the latest Torrentlocker spam run, you may search your messaging logs for e-mails with the subjects:

```
Den Haag - Incassoburea Nederland.
Den Haag - Intrum Justitia
Den Haag - Intrum Incasso
Den Haag Incasso Nederland.
INCASSO NEDERLAND.
*INCASSO* NEDERLAND.
```

And you may search for e-mails from the following sender:

```
bdiu@inkasso.nl
```

E-mail Object

Subject Field

E-mail Object

Sender Field

IOCs on Disk

The dropper is downloaded to the user's temporary folder:

```
c:\Users\<username>\AppData\Local\Temp\[A-Z]{10}.exe
```

Depending on whether it has admin privileges, the dropper drops malware at the following locations:

```
c:\Windows\[a-z]{8}.exe
c:\ProgramData\[a-z]{8}.exe
```

- Pattern matching

IOCs in network traffic

Dropper download location:

defanging

```
hxxp://109.105.193.99/a.png
```

URI Object

Value Field

Command and control server IP's

```
46.161.30.16
46.161.30.17
46.161.30.18
46.161.30.19
46.161.30.20
46.161.30.21
```

Address Object

Value Field

Command and control server hostname:

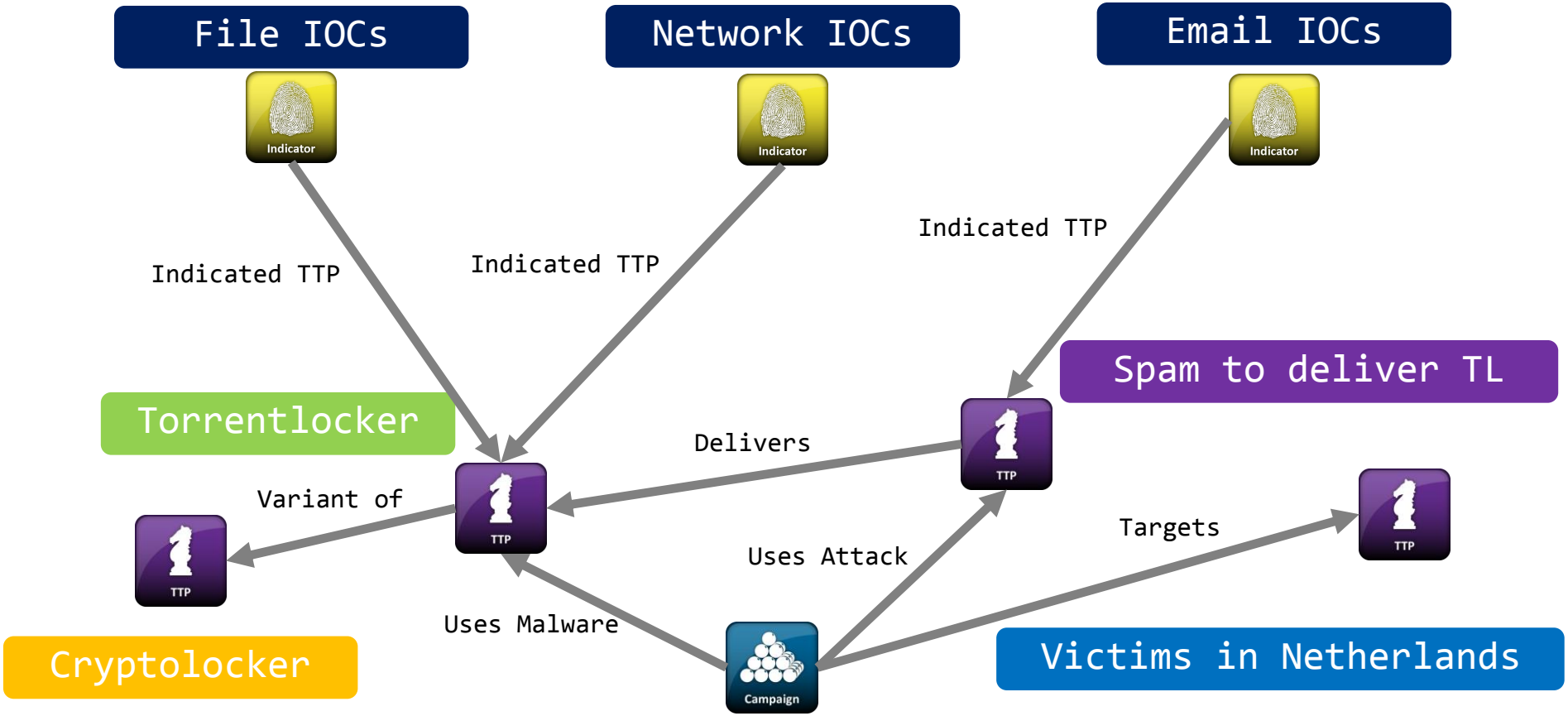
```
allwayshappy.ru
```

Domain Name Object

Value Field

Connecting the IOCs

- How do we give them context?



Response and Prevention

1. **Block access to certain resources on the internet** in order to minimize the risk of further infections. For information on which resources to block, see section "Indicators of compromise in network traffic".
2. **Activate system policies** that prevent further activity by torrentlocker:
   a. **Restrict "delete" permissions.** Activate a policy that prevents users from deleting files from shares. We have indications that such a policy may prevent torrentlocker from working effectively. We are currently investigating this claim.
   b. **Restrict "write" permissions.** To be extra careful, you may change user's rights on all files to "read-only". This will prevent any changes to files.

3. **Identify the systems that are infected with torrentlocker**. The following steps will help with identification:
   a. **Identify who received emails as part of the spam run**. In your email messaging logs, search for email messages with characteristics as described in the section "Indicators of compromise in email". Any hits should provide you with information about who within your organization received emails as part of the spam run and will allow you to remove these emails.
   b. **Identify who visited suspicious torrentlocker websites**. In your gateway logs (proxy logs, firewall logs, IDS logs etc), search for visits to websites known to be associated with this spam run. Any hits should provide you with evidence which systems within your infrastructure visited those websites and are potentially infected with torrentlocker. More information about what to look for can be found in section "Indicators of compromise in network traffic".
   c. **Identify which systems are infected**. After the previous two steps, you may have narrowed down the number of systems that are potentially infected and have caused the files to be encrypted. On suspected systems, you may use the information in the section "Indicators of compromise on hosts".

4. **Isolate the infected systems from your infrastructure**. Once identified, these systems should be **carefully** isolated from the infrastructure, to prevent further encryption of additional files but at the same time preserve digital traces.
   1. **Immediately cease all user activity on infected systems** as they may contain important clues for decryption of the encrypted files or additional information about the infection.
   2. **Physically disconnect the infected systems from the network.**
   3. **Do not power off, wipe or reimage infected systems.**

5. **Restore backups of the infected files.** Backups that are stored offline are not affected. Torrentlocker is known to disable the built-in "Previous Versions" feature in Windows. This fails in some cases allowing you to recover your files via the "Previous Versions" tab in the file properties window. Also, the "Previous versions" feature of cloud storage services like Dropbox might still contain the unencrypted version of your data.
6. **Seek professional assistance.** In case backups are not available or only partly available, and you have preserved sufficient digital evidence, you may seek professional assistance in an effort to recover infected files.

Preventative COA:
Low Cost
High Effectiveness
Medium Confidence

Recovery COA:
Medium Cost
Medium Effectiveness
Medium Confidence

About paying the ransom

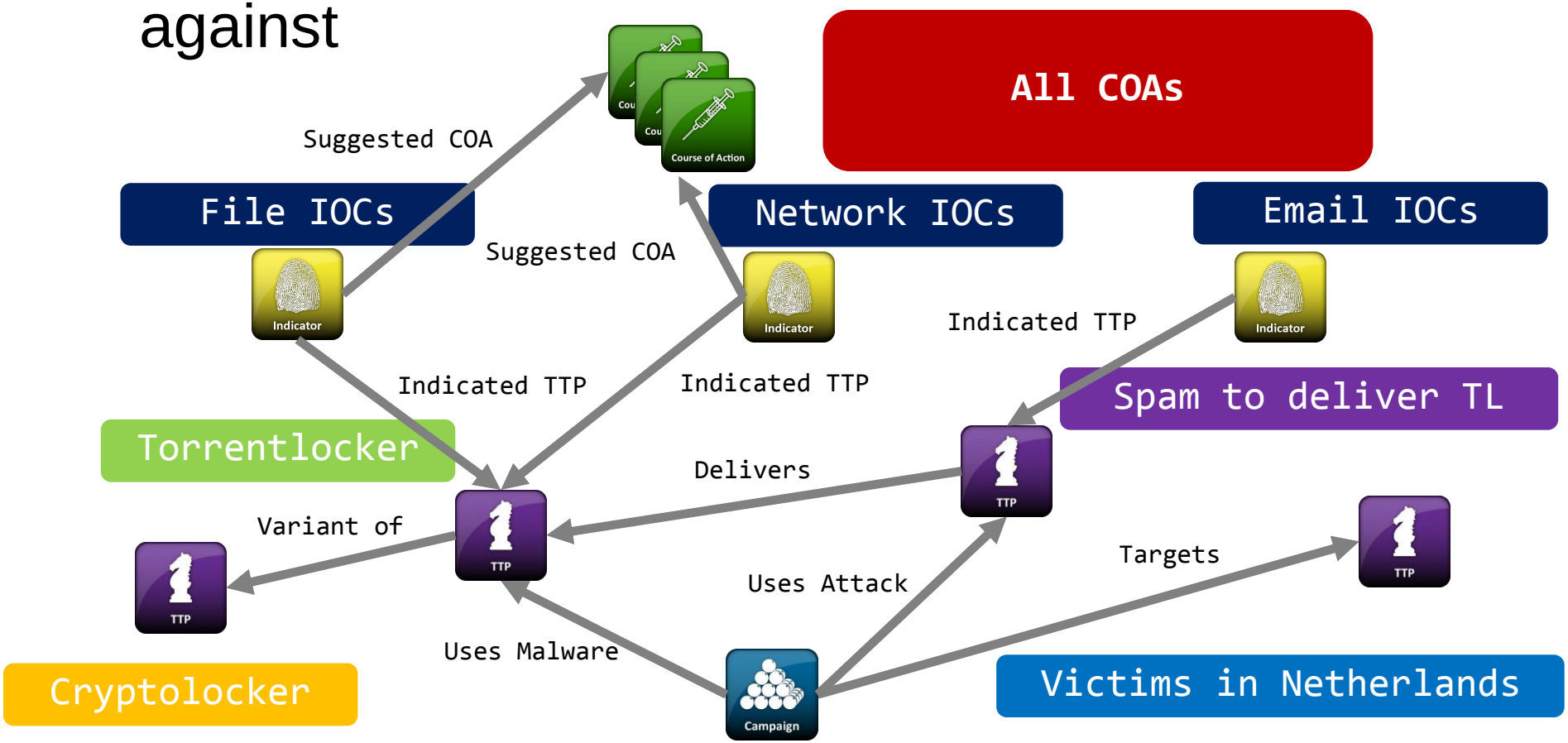
Several reports have reached us of people who have paid the ransom in order to get their files back. In some cases they were successful or partly successful, in other cases they were not. The currently known problems with paying the ransom to get your files decrypted are:

- There is no guarantee whatsoever that you will receive a decryption tool after paying;
- In case your files are encrypted by multiple different infections of Torrentlocker, you will have to pay multiple times;
- The decryption tool as distributed by the criminals contains flaws. After decryption, the resulting files will be partly corrupted, which may render them unusable;
- Last but not least: you are aiding criminals.

Recovery COA:
High Cost
High Effectiveness
Low Confidence

Connecting the COAs

- Connect the COAs to what they're effective against



The big picture