Automatisierung im Cyberspace

Lars A. Wallenborn

FrOSCon — 21. August 2022

Wie wir die Asymmetrien überwinden können

Welche Asymmetrien?

Quelle: unsplash.com/photos/X3RmtchFJg

Quelle: unsplash.com/photos/rPn6eJUQyuo

- Hacker
  1. Proaktiv
  2. Ein Erfolg reicht
  3. Malware schreiben ist ”einfach”
- Defender
  1. Reaktiv
  2. Muss immer erfolgreich sein
  3. Malware analysieren dauert lang


• Perspektivwechsel: Defender+
• Cyber Threat Intelligence (CTI) Provider
Quelle: unsplash.com/photos/votwQUV9ts4


WHAT THE HELL
Cyber Threat Intelligence (CTI)
IS EVEN THAT

- OSINT / Social Media Intelligence
- HUMINT
- Technical Intelligence
- Forensik
- Internetweiter Traffic / Telemetrie
- Dark Web / Deep Web

Quelle: unsplash.com/photos/FXFz-sW0uwo

Beispielfälle

Beispielfälle

1. Trickbot
2. WannaCry
3. Shamoon

Fall 1: Trickbot

- Trickbot Gruppe
- WIZARD SPIDER
- FIN12

Quelle: unsplash.com/photos/h7dl6uplOOs

Quelle: holdsecurity.com/news/2021/06/trickbot-gang-arrest-story-of-alla-witte/

- Alla Witte a.k.a MAX

Quelle: holdsecurity.com/news/2021/06/trickbot-gang-arrest-story-of-alla-witte/

UNITED STATES DISTRICT COURT

for the

Northern District of Ohio

United States of America
v.
ALLA WITTE, aka MAX

Case No. 1:20 CR 440

1:21-2236-MJ-OTAZO-REYES

Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) ALLA WITTE, aka MAX ,

who is accused of an offense or violation based on the following document filed with the court:

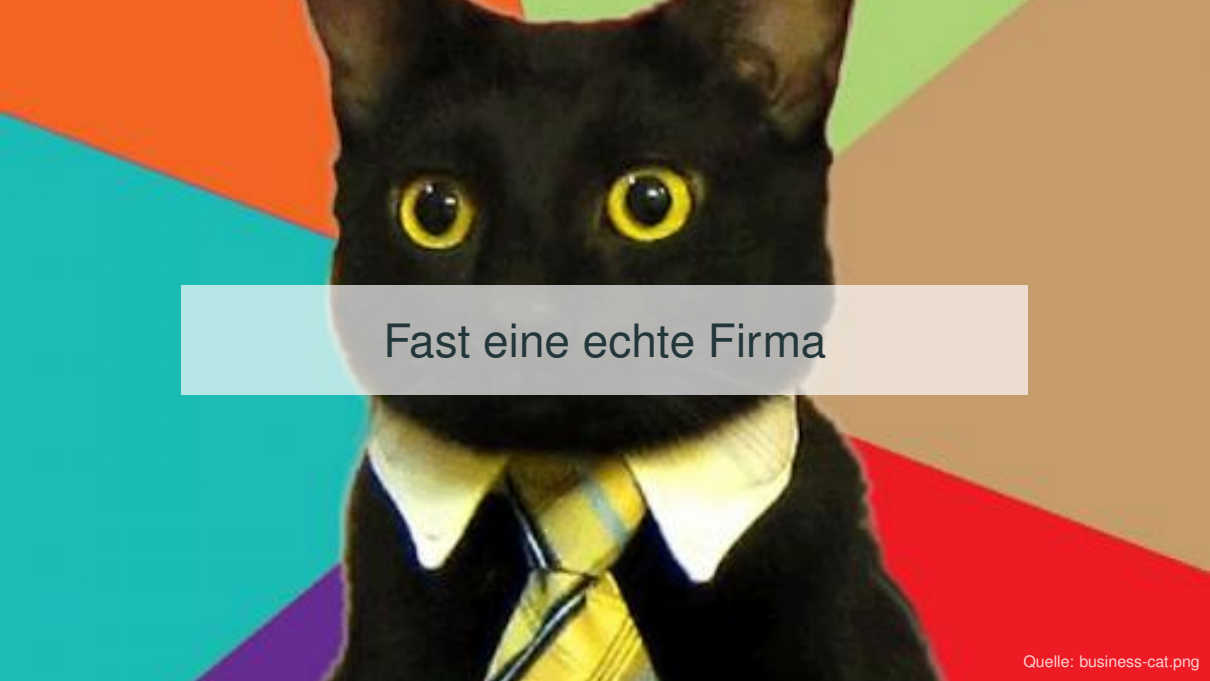
☑ Indictment ☐ Superseding Indictment ☐ Information ☐ Superseding Information ☐ Complaint

☐ Probation Violation Petition ☐ Supervised Release Violation Petition ☐ Violation Notice ☐ Order of the Court

This offense is briefly described as follows:

CC9	The guy did the job.
	Fucking awesome.)
	What are we doing now?
CC9	I'll ask now.
CC9	They'll respond and we'll knock at that guy's door until we get him.
CC9	It seems like he's great.
CC9	He can do both this kind of stuff and that kind.
CC9	What is needed.
CC9	Tell the guy that we tested it and the assignment works.
CC9	Everything's fine with that.

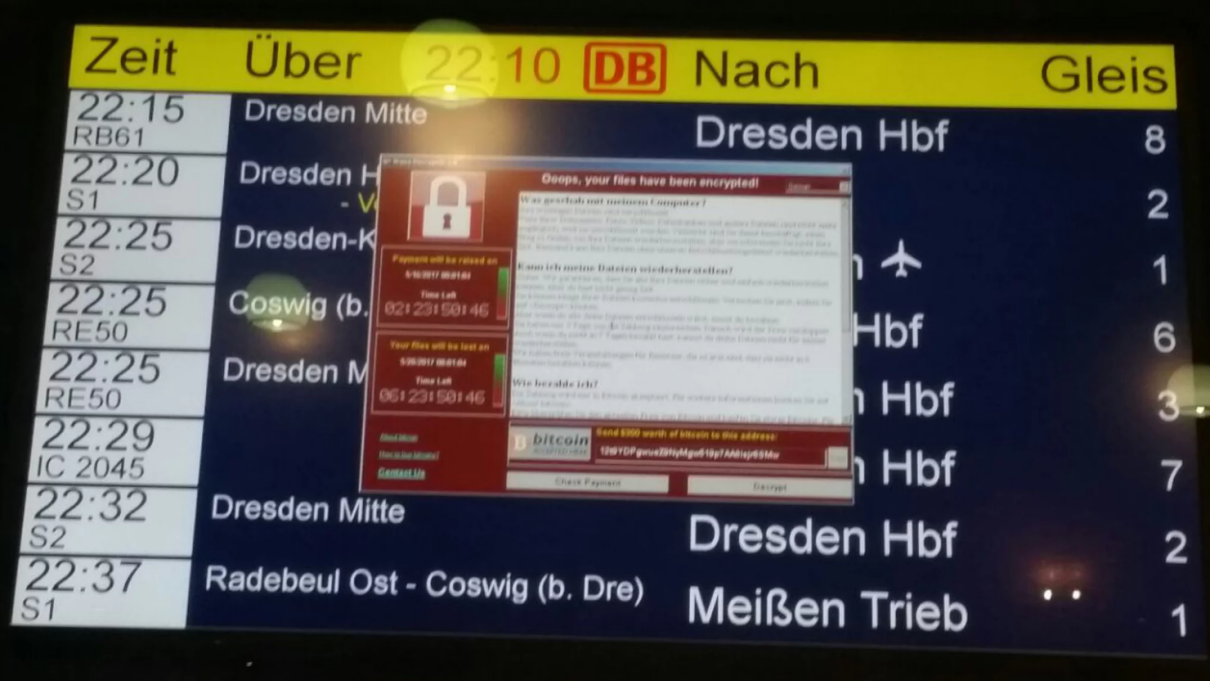
CC9	He's capable of everything.
CC9	Such a person is needed.
	I'm afraid that he can tell the firm to go hell, or ask for more money.
	Well that's something for the leadership to decide.



Quelle: business-cat.png

Fall 2: WannaCry


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
Send $300 worth of bitcoin to this address:
bitcoin ACCEPTED HERE
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


Zeit
Über
22:10
DB
Nach
Gleis
22:15
RB61
Dresden Mitte
Dresden Hbf
8
22:20
S1
Dresden H
2
22:25
S2
Dresden-K
1
22:25
RE50
Coswig (b.
Hbf
6
22:25
RE50
Dresden M
Hbf
3
22:29
IC 2045
Hbf
7
22:32
S2
Dresden Mitte
Dresden Hbf
2
22:37
S1
Radebeul Ost - Coswig (b. Dre)
Meißen Trieb
1
Ooops, your files have been encrypted!
Payments will be raised on
Time Left
02:23:59:46
Your files will be lost on
Time Left
06:23:59:46
Can I recover my files?
How do I pay?
Contact Us
bitcoin
Send $300 worth of bitcoin to this address:
Check Payment
Decrypt

Demo-Time: WannaCry

- Malware ”Stages” in PE Resourcen
- Passwortgeschützte ZIP Datei

Fall 3: Shamoon

Demo-Time: Shamoon

Quelle: unsplash.com/photos/aq9G80Hm8mU

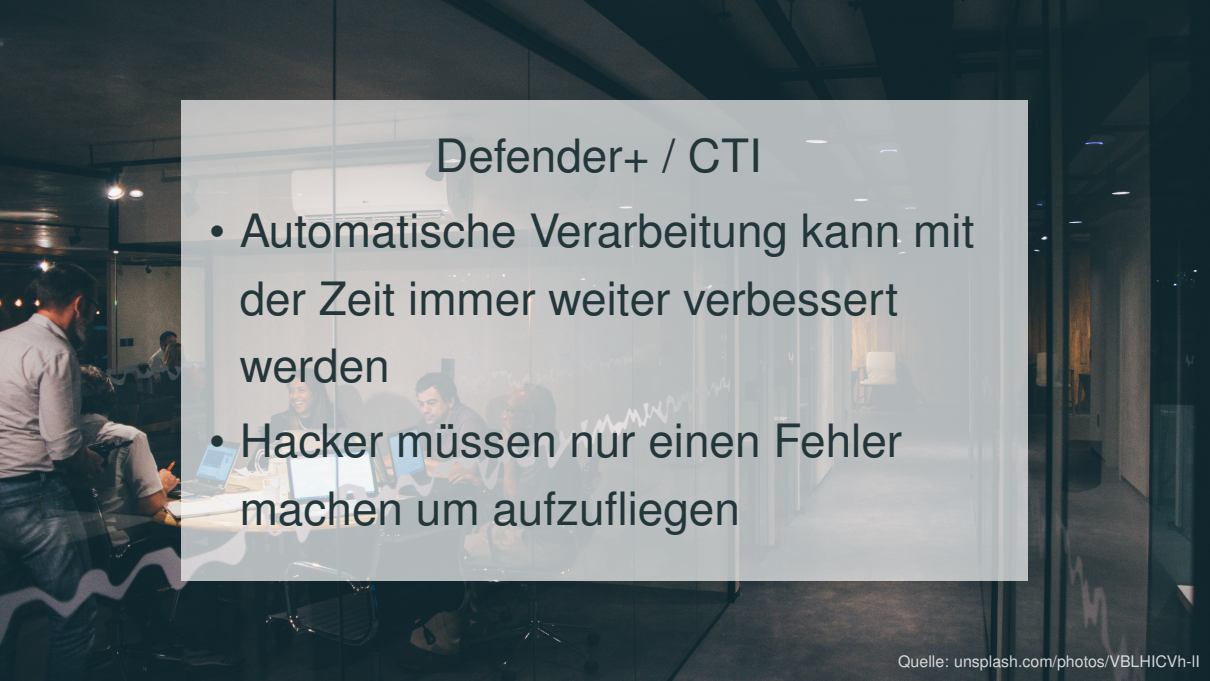
Beispielfälle

1. Trickbot $\Rightarrow$ Automatisch
2. WannaCry $\Rightarrow$ Dateien
3. Shamoon $\Rightarrow$ Metadaten

How to CTI at Home?

- Collection
  - Malware Sammlungen (VirusTotal, MalShare, MalwareBazaar, . . .)
  - Online Sandboxes (any.run, tria.ge, hybrid-analysis.com, . . .)
  - Organische Quellen (Spam E-Mails, Malvertising, Botnets, Honeypots, . . .)
  - . . .
- Verarbeitung
  - Generische Dateiformate (ZIP, E-Mails, Microsoft Office Dateien, . . .)
  - Generische Metadaten (PE Resources/Sections, E-Mail Absender, . . .)
  - Spezifische Dropper Malware Familien
  - . . .

- Hacker
  1. Proaktiv
  2. Ein Erfolg reicht
  3. Malware schreiben ist ”einfach”
- Defender
  1. Reaktiv
  2. Muss immer erfolgreich sein
  3. Malware analysieren dauert lang



Defender+ / CTI

- Automatische Verarbeitung kann mit der Zeit immer weiter verbessert werden
- Hacker müssen nur einen Fehler machen um aufzufliegen

Quelle: unsplash.com/photos/VBLHICVh-II

tl;dr

If you know the enemy and know yourself, you need not fear the result of a hundred battles

Sun Tzu

Lars A. Wallenborn

- lars@wallenborn.net
- @larsborn
- larsborn
- Armchair Investigators (mit Christian Dietrich)
- mal.re (mit Jesko Hüttenhain)
- github.com/binref (von Jesko Hüttenhain)