Sicherheit und Datenschutz: Ask me Anything

Prof. Dr. Dominik Herrmann

Privacy and Security in Information Systems Group
University of Bamberg
https://uni-bamberg.de/psi/

Slides: https://dhgo.to/ama19

FÜNF
BEISPIELE

#1

Einfacher Fall:

Mirai Botnet

How a Bunch of Hacked DVR Machines Took Down Twitter and Reddit

... and Spotify, and Github, and *The New York Times*

ROBINSON MEYER OCT 21, 2016

MIRAI-BOTNETZ

Drei US-Studenten bekennen sich schuldig

Also doch nicht Russland: Drei amerikanische Studenten haben vor einem US-Gericht zugegeben, im vergangenen Jahr mit Mirai eines der größten Botnetze der Internetgeschichte aufgebaut zu haben. Ihr Ziel sollen konkurrierende Minecraft-Server gewesen sein.

14. Dezember 2017, 12:07 Uhr , Jan Weisensee

Wer ist schuld?

Die drei Studenten

Die Besitzer der Kameras

Der Hersteller der Kameras

Ausbreitung durch Login mittels Standard-Passwörtern

Password	Device Type	Password	Device Type
123456	ACTi IP Camera	klv1234	HiSilicon IP Camera
anko	ANKO Products DVR	jvbzd	HiSilicon IP Camera
pass	Axis IP Camera	admin	IPX-DDK Network Camera
888888	Dahua DVR	system	IQinVision Cameras
666666	Dahua DVR	meinsm	Mobotix Network Camera
vizxv	Dahua IP Camera	54321	Packet8 VOIP Phone
7ujMko0vizxv	Dahua IP Camera	00000000	Panasonic Printer
7ujMko0admin	Dahua IP Camera	realtek	RealTek Routers
666666	Dahua IP Camera	1111111	Samsung IP Camera
dreambox	Dreambox TV Receiver	xmhdipc	Shenzhen Anran Camera
juantech	Guangzhou Juan Optical	smcadmin	SMC Routers
xc3511	H.264 Chinese DVR	ikwb	Toshiba Network Camera
OxhlwSG8	HiSilicon IP Camera	ubnt	Ubiquiti AirOS Router
cat1029	HiSilicon IP Camera	supervisor	VideoIQ
hi3518	HiSilicon IP Camera	<none>	Vivotek IP Camera
klv123	HiSilicon IP Camera		

M. Antonakakis et al. (2017): Understanding the Mirai Botnet. USENIX Security 2017.

#2

Nicht ganz so einfach:

ALDI-Kameras

Alert! 15.01.2016 10:49 Uhr | Security

IP-Kameras von Aldi als Sicherheits-GAU

Die Kameras IPC-10 AC, IPC-100 AC und IPC-20 C hat Aldi mit einer Firm-ware angeboten, die eine Nutzung des Fernzugriffs auch dann zulässt, **wenn der Nutzer bei der Inbetrieb-nahme kein Passwort gesetzt hat.** Das wird dem Nutzer schnell zum Verhängnis, **die Geräte ändern über UPnP nämlich selbstständig die Router-Konfiguration, wodurch sie über Port 80 aus dem Internet erreichbar sind**.

Ist kein Passwort gesetzt, kann fort-an jeder einen Blick durch die Ka-mera werfen. Da die Modelle IPC-10 AC und IPC-100 AC mit einem Mikro-fon ausgestattet sind, können Unbe-fugte sogar Gespräche belauschen. Ferner sind diese Geräte motorge-steuert schwenkbar, ein ungebe-tener Gast kann also den Bildaus-schnitt beliebig verändern. Alle drei Modelle können durch Infrarot-LED auch in der Dunkelheit sehen.


VIEW
SETTINGS
CONTROL
POSITIONS
SETTINGS
Resolution: 640 x 480
Brightness: 3
Flip horizontally
Flip vertically
down left
1
2
3
HD
nachtmagazin

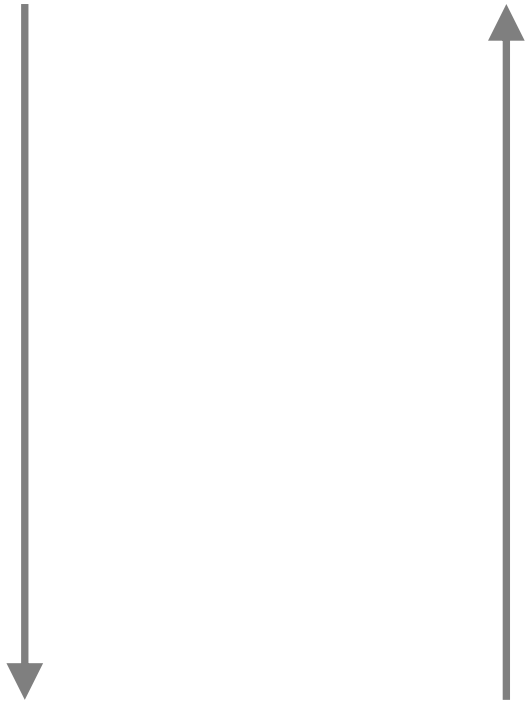
Wer ist schuld?

Die Besitzer der Kameras.

kein Passwort oder Default-Passwort ab Werk

kein Zwang zum Ändern des Passworts

Änderung der Router-Konfiguration ohne Rückfrage



Usability: Nutzer wünschen sich einfache Einrichtung!

Die Nutzer hätten nur das Handbuch lesen müssen!

Nutzer sind für Ihre Sicherheit selbst zuständig

Der Hersteller der Kameras

Wer ist schuld?

Die Umstände

Hersteller

Nutzer bezahlen nicht
für mehr Sicherheit!

Nutzer

Weil wir die Sicherheit
nicht überprüfen können!

Hersteller haben keinen Anreiz, Sicherheit einzubauen.

Folge: Market for Lemons

R. Anderson & T. Moore (2006), The Economics of Information Security. Science 314 (5799), pp. 610–613.

#3

Ein ungelöstes Problem:

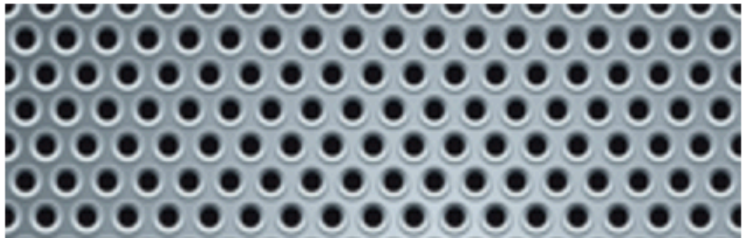
Sicherherheitslücken durch Programmierfehler

Beispiel 1: **Fehlerhaft implementierte Verschlüsselung**

Ergebnisse eines Android-Sicherheitschecks erschrecken

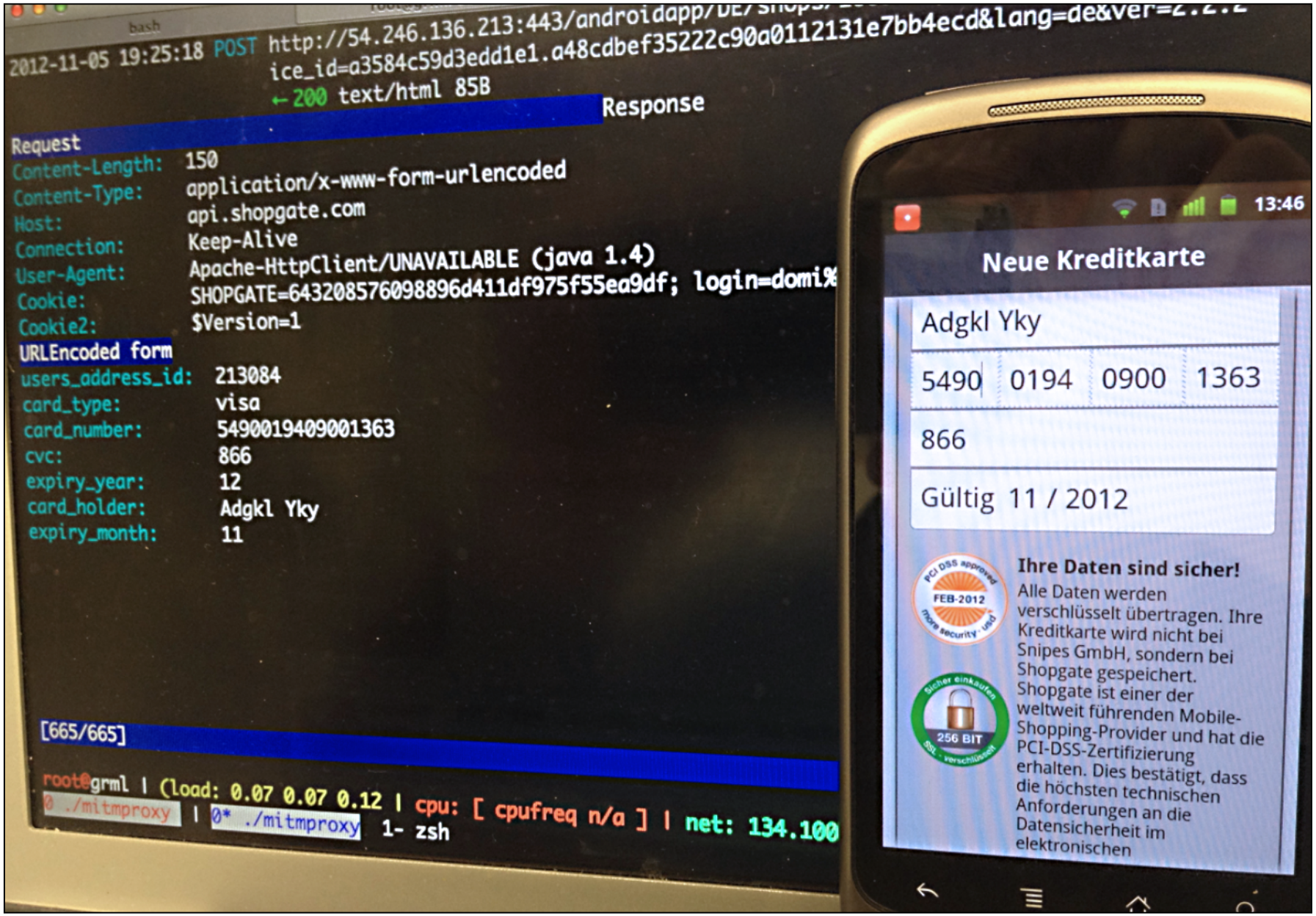
Ziemlich löchrig

Sascha Fahl



In über 90 Prozent der Fälle, in denen eine App-spezifische SSL-Zertifikats-validierung implementiert wurde, war das Resultat, dass die Zertifikats-validierung komplett ausgeschaltet wurde, so dass alle betroffenen Apps für die eben beschriebenen Man-In-The-Middle-Angriffe anfällig waren. […]

Von den 100 angegriffenen Apps, enthielten 41 ausnutzbare Schwach-stellen. Die Tester konnten erfolgreich Bankdaten, […], PayPal, […], Zugangs-daten zu Facebook, Email und Cloud-Speicherdiensten sowie Instant-Messaging-Anbietern abfangen und mitlesen. […] auch die Apps einiger namhafter Hersteller waren betroffen.



S Fahl et al. (2012). **Why Eve and Mallory Love Android: An Analysis of SSL (In)Security.** CCS 2012.

Wer ist schuld?

Entwickler

PCI-DSS-Zertifikat-Auditor

Software-Framework-Anbieter

Beispiel 2: **SQL-Injections wegen falscher Ratschläge**

Creating a very simple 1 username/password login in php

Ask Question

I want to make a single login for just 1 user without storing in a database but I can't seem to get this to work.

Eine der Antworten:

```php
if(!empty($_POST['submit'])){
    if(empty($_POST['username']))
        $error_msg='please enter username';
    if(empty($_POST['password']))
        $error_msg='please enter password';
    if(empty($error_msg)){
        $sql="SELECT*FROM users WHERE username='%s' AND password='%s'";
        $sql=sprintf($sql,$_POST['username'],md5($_POST['password']));
        $records=mysql_query($sql) or die(mysql_error());
```

https://stackoverflow.com/questions/19531044/creating-a-very-simple-1-username-password-login-in-php/19531260

Wie können wir die Umstände verbessern?

Dokumentation von Software-Frameworks verbessern

Möglichkeit zur unsicheren Nutzung von Software-Frameworks verhindern

Entwicklern Freiheit geben; erinnern, dass Sicherheit in ihre Verantwortung fällt

40% fühlten sich in einer Studie mit 124 Entwicklern nicht verantwortlich.

47% sagten, sie bekämen nicht genug Freiheit und Autonomie für Sicherheit.

Y. Acar er al. (2017). Comparing the Usability of Cryptographic APIs. IEEE Security & Privacy 2017.
S. Spiekermann et al. (2018). Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers. Proc. IEEE (2018).

#4

Ein aktuelles Problem:

Datenlecks wegen schlecht gesicherter Nutzerkonten

Hackerangriffe

Unsichere Passwörter als größtes Einfalltor

Der aktuelle Datendiebstahl richtete sich gegen Prominente und Politiker. Das Problem könne aber jeden treffen, sagte Professor Christoph Meinel vom Potsdamer Hasso-Plattner-Institut im Dlf. Deshalb sollten Nutzer vor allem auf sichere Passwörter achten – und am besten für jeden Dienst ein eigenes anlegen.

Troy Hunt
@troyhunt

If someone creates a weak password and then reuses it across multiple services, do they have any responsibility if one of their accounts is then compromised via credential stuffing?

♡ 95 1:43 PM - Nov 7, 2018

84% Yes, some

16% No, none

4,929 votes • Final results

Wer ist schuld?

Hackerangriff aufgeklärt: Johannes S. klaute Date… weil er sich über sie ärgerte

Johannes S.

Nutzer

Anbieter

You are responsible for safeguarding your account, **so use a strong password and limit its use to this account**. We cannot and will not be liable for any loss or damage **arising from your failure to comply** with the above.

(Twitter ToS)

Wer ist schuld?

Die Umstände

Anbieter

Nutzer haben in den AGB zugestimmt, dass sie sich selbst um ihre Sicherheit kümmern

Unser Dienst ist kostenlos; wir haben keine Ressourcen; die Kunden honorieren es nicht (Market for Lemons)

Nutzer

Sind nicht bereit, sich mit Sicherheitsdetails zu beschäftigen

Unterliegen kognitiven Restriktionen

Systeme sind für normale Nutzer nicht zu durchschauen

Umstände verbessern: nicht so einfach

Passwort-Policy einführen:
Klein-/Großbuchstaben, Ziffern, Sonderzeichen

password => Password1!

lgg1PaINNentlang <= **überall dasselbe!**

Blacklist: einfache Passwörter und geleakte Passwörter sind nicht erlaubt!

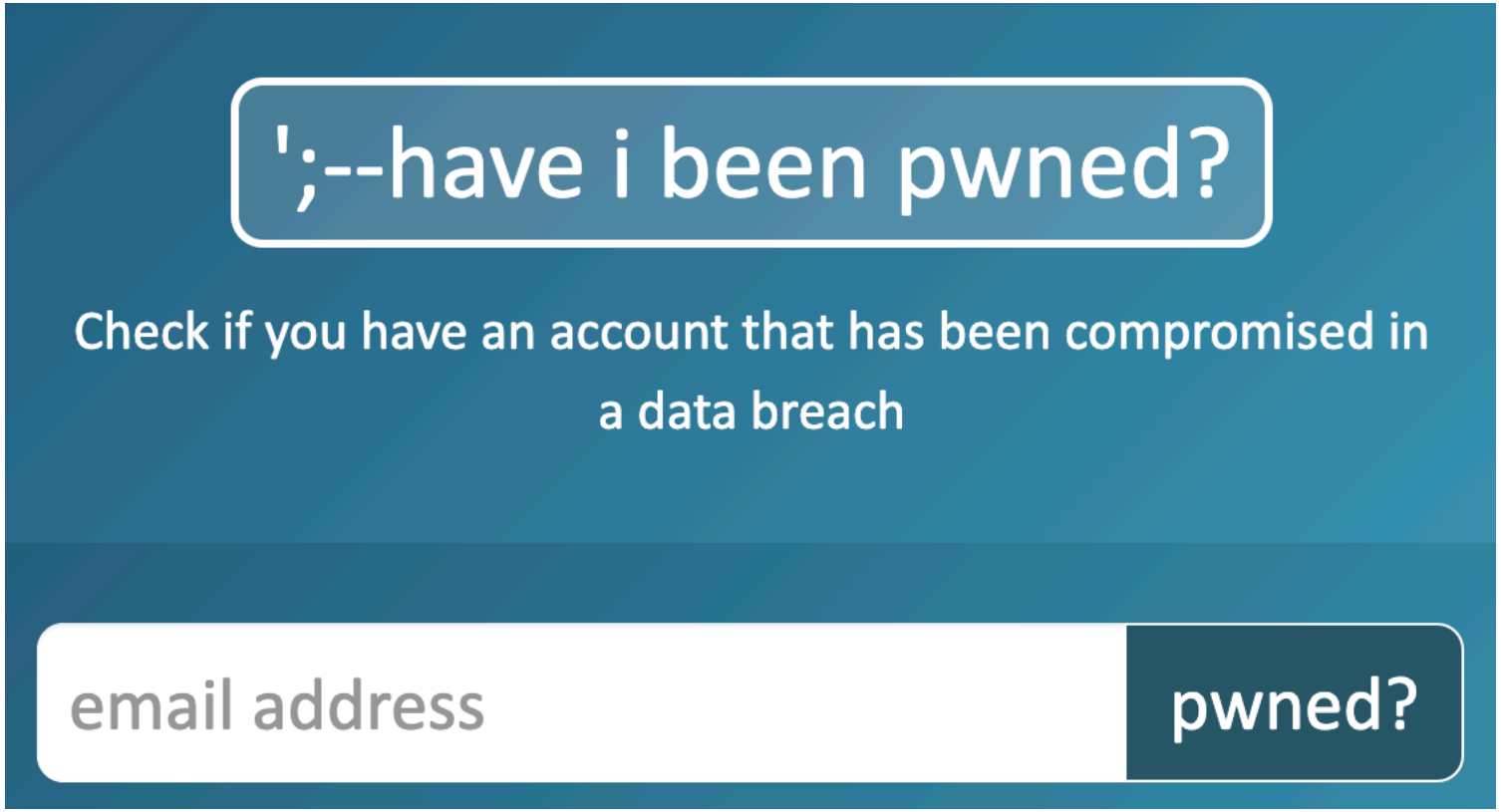
Beispiel Nextcloud-Freigaben:

Nutzer verzichten auf Passwörter

Forderung: Nutzer müssen doch nur Passwort-Manager und 2FA verwenden!

Welcher ist sicher und gut? (KeepassXC)

2FA birgt Verfügbarkeitsrisiken.



prüfen ob man von Leaks betroffen ist

https://sec.hpi.de/ilc/

https://haveibeenpwned.com/

lbi=zEd4

schlechter als

mehlbalkontisch

Warum?


Warum?

Wie viele Rate-Versuche?

(alle Möglichkeiten durchprobieren)

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4
5 6 7 8 9 : ; < = > ? @ A B C D E F G H I
J K L M N O P Q R S T U V W X Y Z [ \ ] ^
_ ` a b c d e f g h i j k l m n o p q r s
t u v w x y z
```

90 Zeichen

lbi=zEd4 (8 Stellen)

4.304.672.100.000.000

Versuche (höchstens)

lbi=zEd4 (8 Stellen)

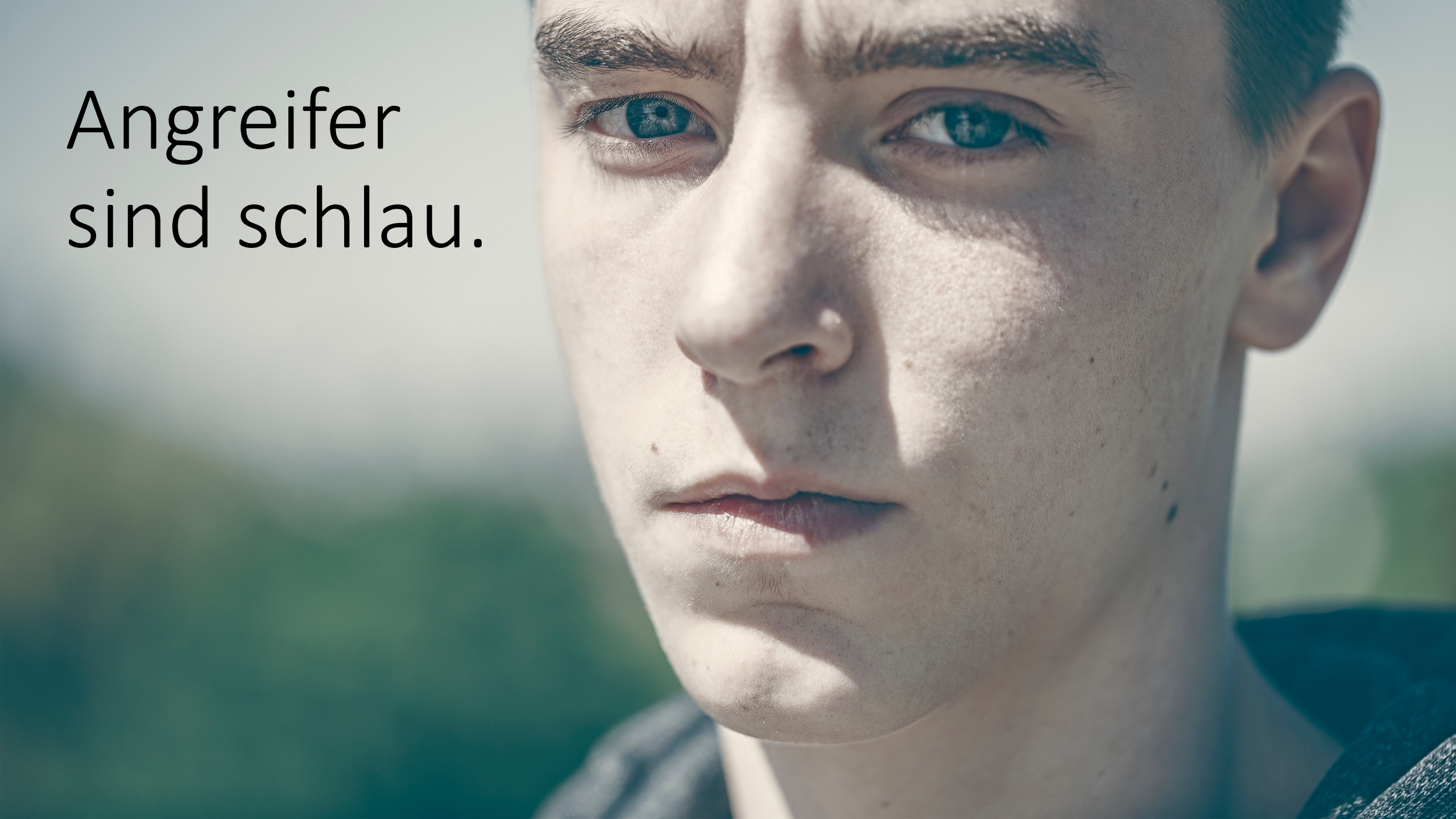
4.304.672.100.000.000

Versuche (höchstens)

mehlbalkontisch (15 Stellen)

1.677.259.342.285.725.925.376

Versuche (nur Kleinbuchstaben)


Angreifer
sind schlau.

aaaaaaaaaaaaaaa … aaaaaaaaaaaaaaab …

mehlbalkontisch … zzzzzzzzzzzzzzz

1.677.259.342.285.725.925.376 Versuche

aachenaachenaachen … aachenaachenaal …

mehlbalkontisch … zuziehenzuziehenzuziehen

125.000.000.000.000.000 Versuche

lbi=zEd4 4.304.672.100.000.000 Versuche

Leicht merkbare Passwörter?

Reime

rubinose keine taschenlampe deine

werwasweisskriegteinschokoeis

#5

Ein Evergreen:

Schadsoftware

https://www.computerworld.com/article/3197048/cybercrime-hacking/wannacry-sometimes-you-can-blame-the-victims.html

The Latest Ransomware Attack Shows Why You Shouldn't Ignore Those Annoying Software Updates

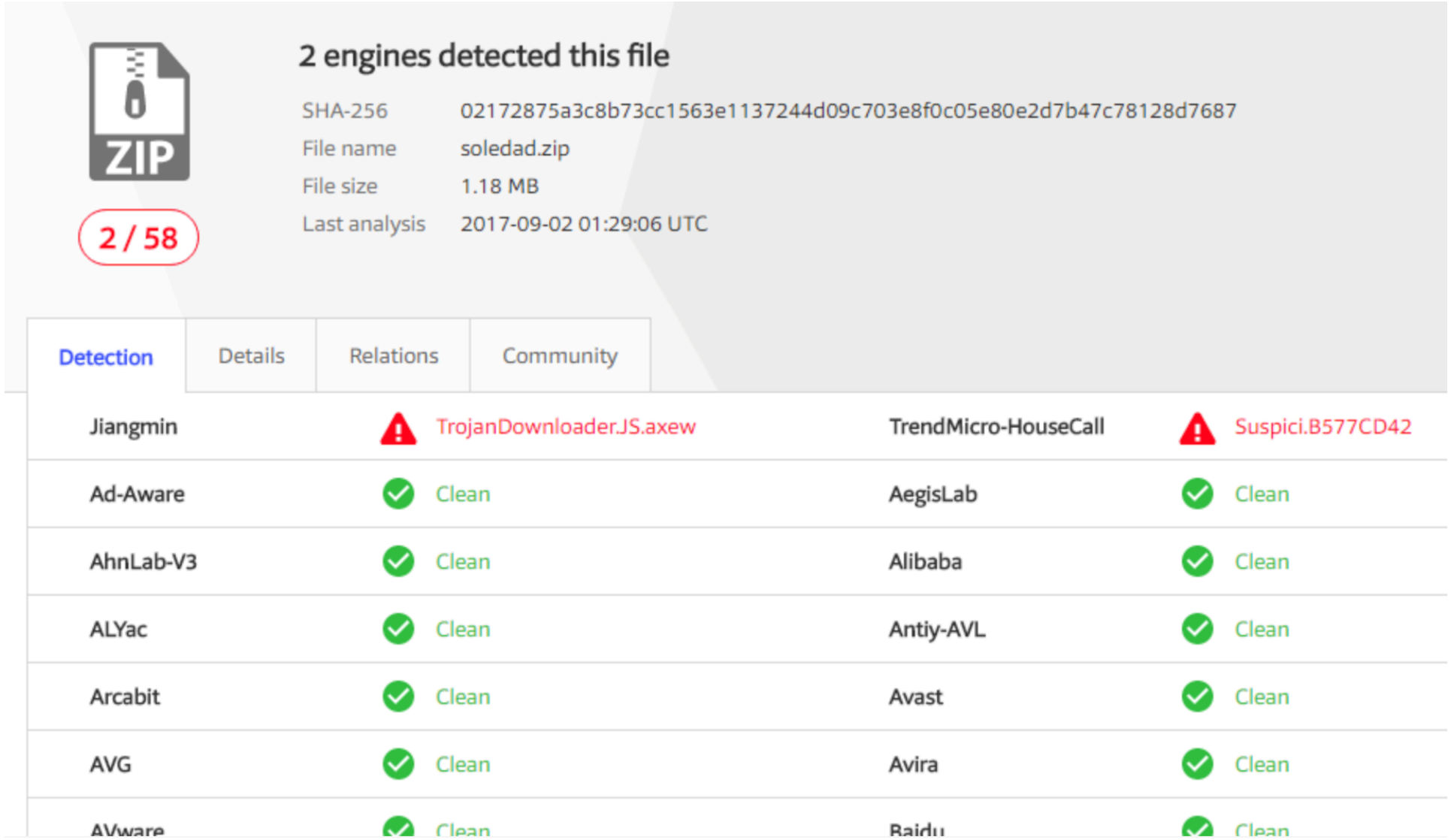
Ransomware uses a particularly nefarious technique that blocks the owner from accessing his or her files by encrypting them and demanding a ransom in order to have them recovered. The specific breed of ransomware that's been disrupting businesses, hospitals, and institutions around the world, referred to as "**WannaCry**" or "WannaCrypt," holds files hostage for a $300 fee. […] The attack stemmed from a **vulnerability found in Microsoft's Windows platform**, which the tech giant addressed in an update from March. But that fix was only available for systems it currently supports, meaning **older versions like Windows XP** were left susceptible.

http://time.com/4779750/wannacry-ransomware-patch-windows-cybersecurity/

Warum ist Ransomware eigentlich ein so großes Problem?

Backup…

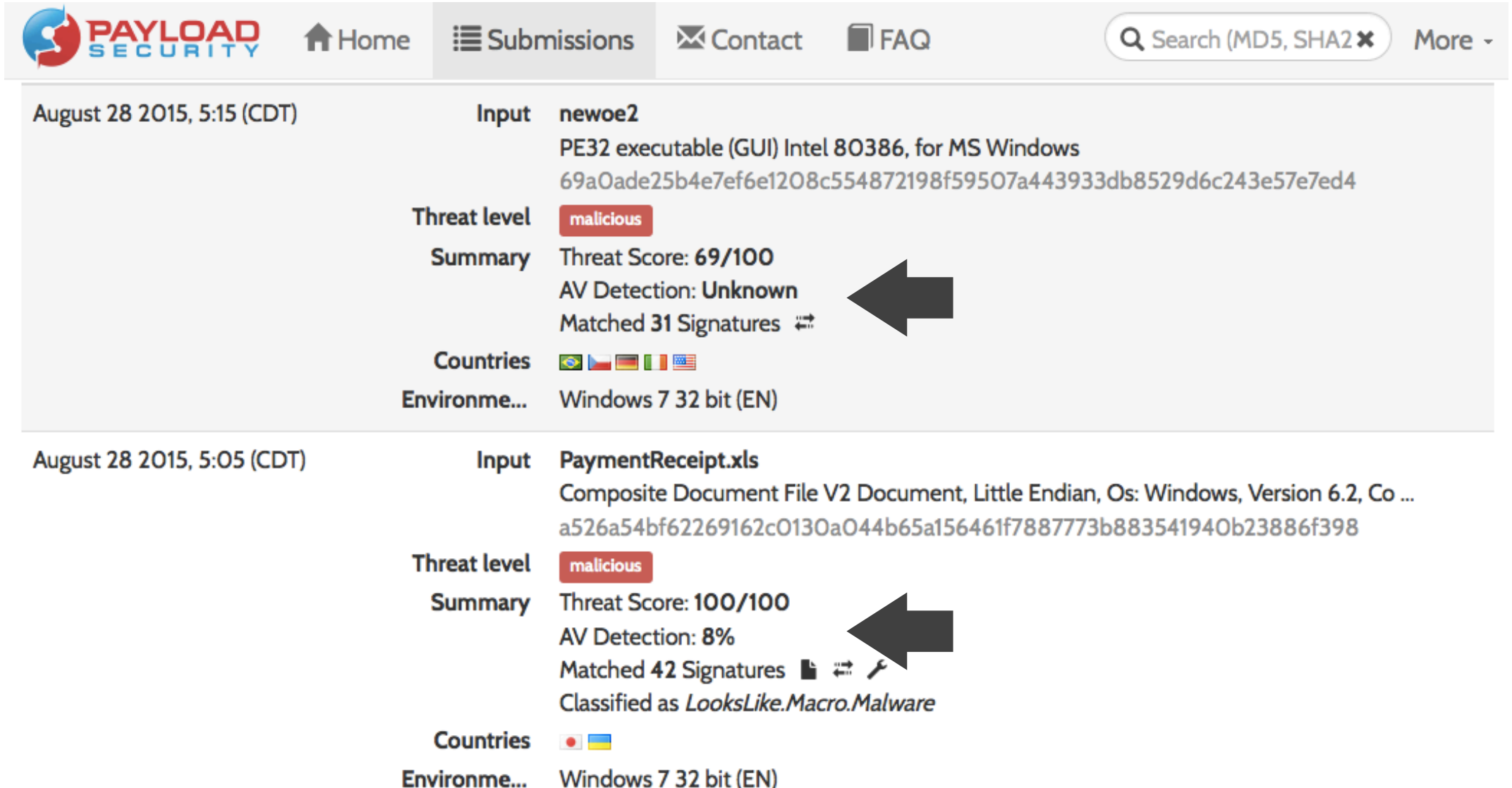
„aktuellen Virenscanner verwenden“



https://www.hybrid-analysis.com

Ausweg: cloudbasierte Sandbox

wenn Datenschutz gerade nicht wichtig ist …



https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf

Experten finden diese Maßnahmen wichtiger als Nicht-Experten

Sicherheit und Datenschutz: Ask me Anything

Prof. Dr. Dominik Herrmann

Privacy and Security in
Information Systems Group
University of Bamberg
https://uni-bamberg.de/psi//

@herdom auf Twitter

Slides: https://dhgo.to/ama19