Tobias Scheible, M.Eng.

Cyber Security Vortrag

Digitales Partner Forum

Zusatzfolie

Tobias Scheible, M.Eng.

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

- 1999 GeoCities Website, 2000 eigene Domain, 2001 erste Projekte
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter an der Hochschule Albstadt-Sigmaringen
  - BMBF gefördertes Forschungsprojekt SEKT (IT Security & Smart Textiles)
  - Aktuelle & ehemalige Lehrmodule (Auswahl):
    - Grundlagen der digitalen Forensik Masterstudiengang IT GRC Management
    - Digitale Forensik Bachelorstudiengang IT Security
    - Internet Grundlagen Masterstudiengang Digitale Forensik
    - IT Security 2 Bachelorstudiengang IT Security
    - Informationssicherheit Bachelorstudiengang Wirtschaftsinformatik
    - Internettechnologien Hochschulzertifikatsprogramm
    - Cloud Technologies and Cloud Security Architectures Masterstudiengang IT GRC

Agenda

- Cyber Security
  - Schadsoftware
  - Ransomware
  - Aktueller Vorfall
- Social Engineering
  - Gefängnisausbruch
  - Fallbeispiel Locky
  - SMS fälschen
- Passwortsicherheit
  - Faktor Mensch
  - Gehackte Accounts
  - Passwortlisten
- Zielgerichtete Angriffe
  - Problematische Hardware
  - Systeme suchen

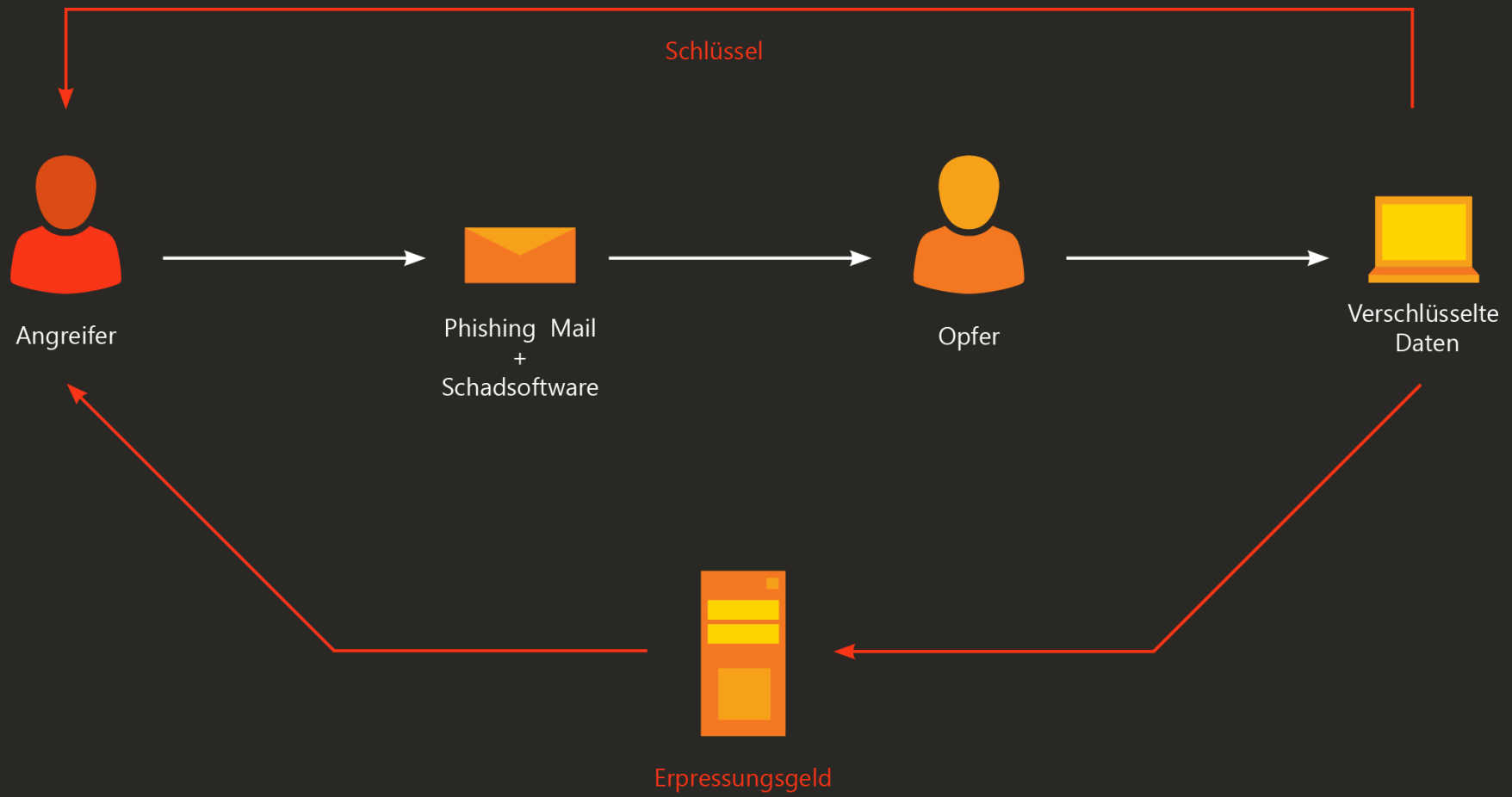
Cyber Security

Entwicklung der Schadsoftware

- **Nutzung von Standardfunktionen**
  - 80er Jahre: Der Begriff Computervirus wird zum ersten Mal verwendet
  - 1985: Über Computerviren wird in Deutschland berichtet
  - 1988: Zum ersten Mal wird das Konzept „Würmer“ bekannt
- **Ausnutzung von Schwachstellen**
  - 1997: Schadsoftware nutzt nun gezielt Schwachstellen aus
  - 2000: „I love you” Virus findet in Deutschland große Verbreitung
  - 2000: Erster Trojaner für mobile Endgeräte (PDAs)
- **Krimineller Hintergrund**
  - 2004: Schadsoftware wird von organisierten Kriminellen eingesetzt
  - 2005: „Wurm“ verbreitet sich automatisch auf Symbian Smartphones per MMS

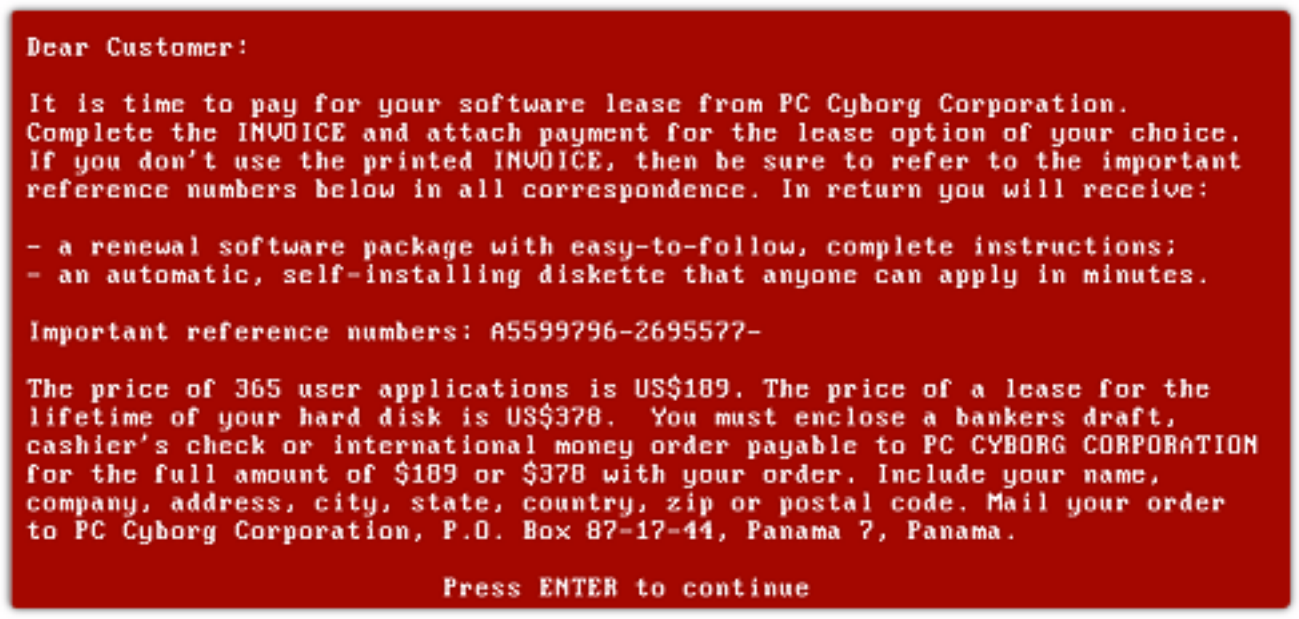
Quelle: gdata.de (1)

Ransomware



Ransomware - AIDS

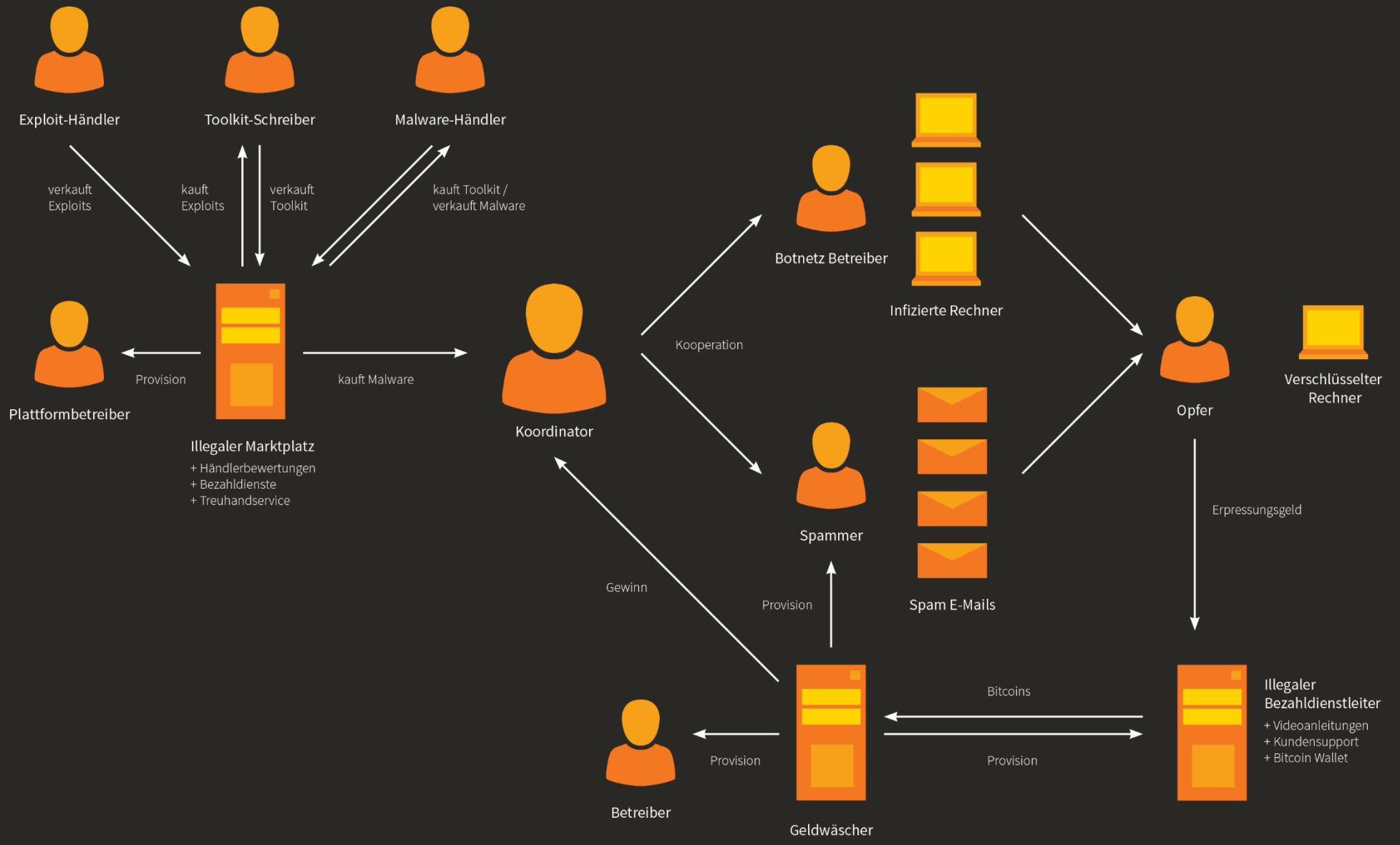
- Erste Angriffe mit Ransomware bereits 1989
- Schadsoftware wurde per 5,25“ Diskette mit der Post verschickt
- Nach 90 Starts wurden die Dateinamen verschlüsselt
  - Eine italienische AIDS Organisation verlor Forschungsergebnisse aus 10 Jahren
  - Ersteller der Ransomware wurde 1990 verhaftet



Quelle: wikipedia.org (2)

Zusatzfolie

Organisierte Kriminalität



Aktuelle Vorfälle

12. Februar 2021, 18:13 Uhr IT-Sicherheit

Wenn die Trinkwasserversorgung gehackt wird

Der Sheriff von Oldsmar bei seiner Pressekonferenz am Montag. (Foto: AP)

Hacker dringen ins System eines Wasserversorgers in Florida ein und erhöhen den Anteil von gefährlichem Ätznatron im Wasser. Dass dabei Menschen zu Schaden kommen konnten, stört die Angreifer offenbar nicht.

Quelle: sueddeutsche.de (3)

Zusatzfolie

FAZIT Cyber Security

- Cyberkriminelle führen Angriffe aus, um Geld zu erbeuten.
- Die Akteure sind der organisierten Kriminalität zuzuordnen.
- Oft ist es ein loser Verbund aus verschiedenen Gruppierungen, die spezialisierte Aufgaben isoliert ausführen.
- Allerdings gibt es auch immer wieder Innentäter, die aus persönlichen Motiven wie Rache handeln.
- Diese setzen häufig alte Passwörter, die immer noch aktiv sind oder überall gleich sind, oder sehr simple Tools ein.

Social Engineering

Moderner Gefängnisausbruch

- Moderner Ausbruch aus einem britischen Gefängnis (März 2015)
- SocialEngineering Angriff auf das Gefängnis
  - Smartphone eingeschmuggelt
  - Domain reserviert, die dem zuständigen Gericht ähnelt
  - E-Mail Adresse mit dieser Domain eingerichtet
  - Hat sich als leitender Beamter ausgegeben
  - Anweisungen zu seiner Entlassung gegeben

►Gefangener kam frei

Quelle: heise.de (4)

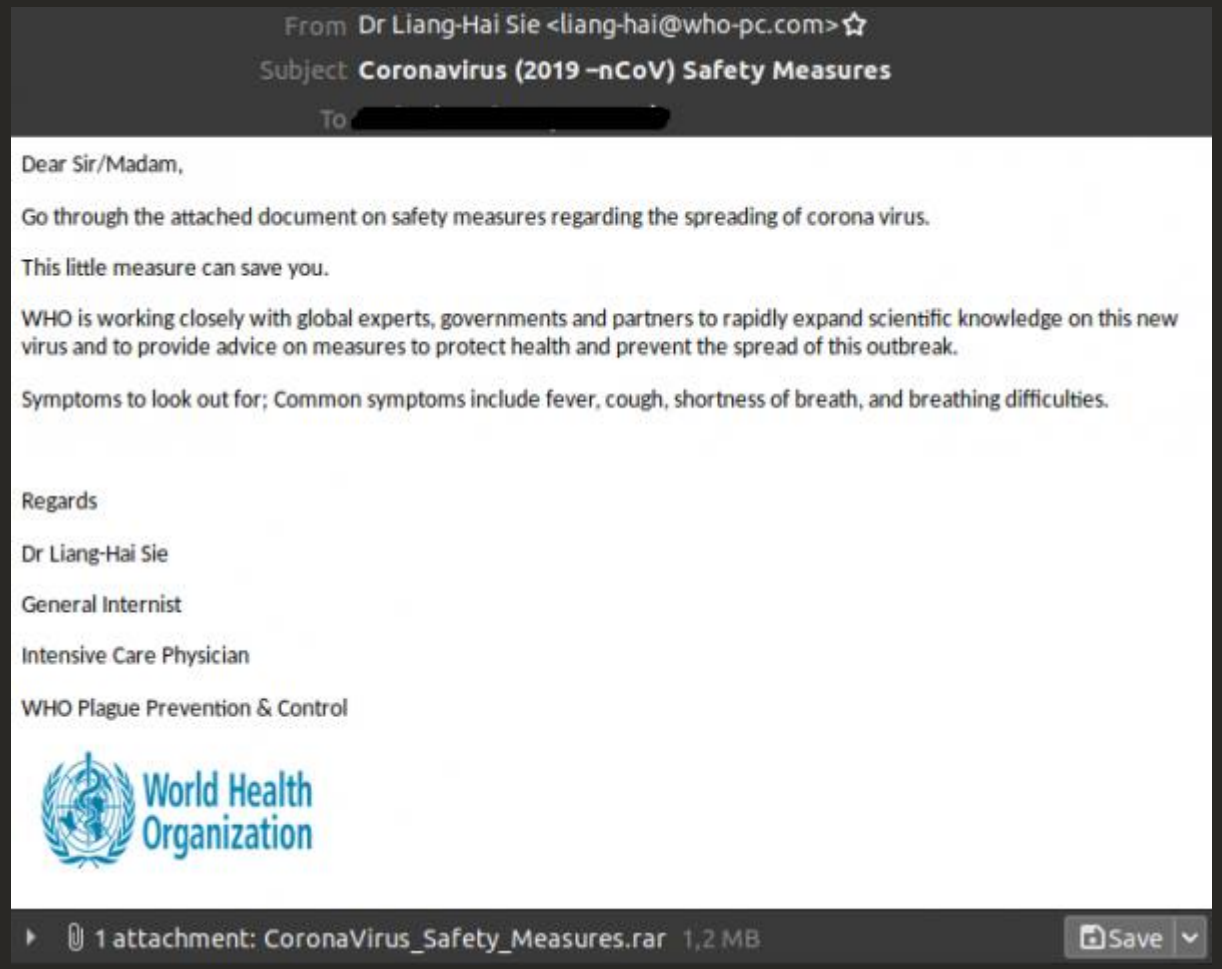
Fallbeispiel Locky

- Effektive Methode, um Geld zu ergaunern
- Auf deutsche Benutzer ausgerichtete Varianten
- Verschlüsselt alle Benutzerdateien, auch auf Netzwerklaufwerken

- Zeitlicher Ablauf:
  - 15.02.2016 Locky wird als Schläfer aktiviert (Makros)
  - 22.02.2016 Gefälschte Unternehmensrechnung (JScript)
  - 24.02.2016 Gefälschtes Sipgate Fax (JScript)
  - 26.02.2016 Neue Infektionstechnik mit Batch-Dateien
  - 02.03.2016 Gefälschte BKA E-Mail (EXE-Datei)

Quelle: wikipedia.org (5)

Mails fälschen



From Dr Liang-Hai Sie <liang-hai@who-pc.com>☆
Subject **Coronavirus (2019 -nCoV) Safety Measures**
To [redacted]

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

Dr Liang-Hai Sie

General Internist

Intensive Care Physician

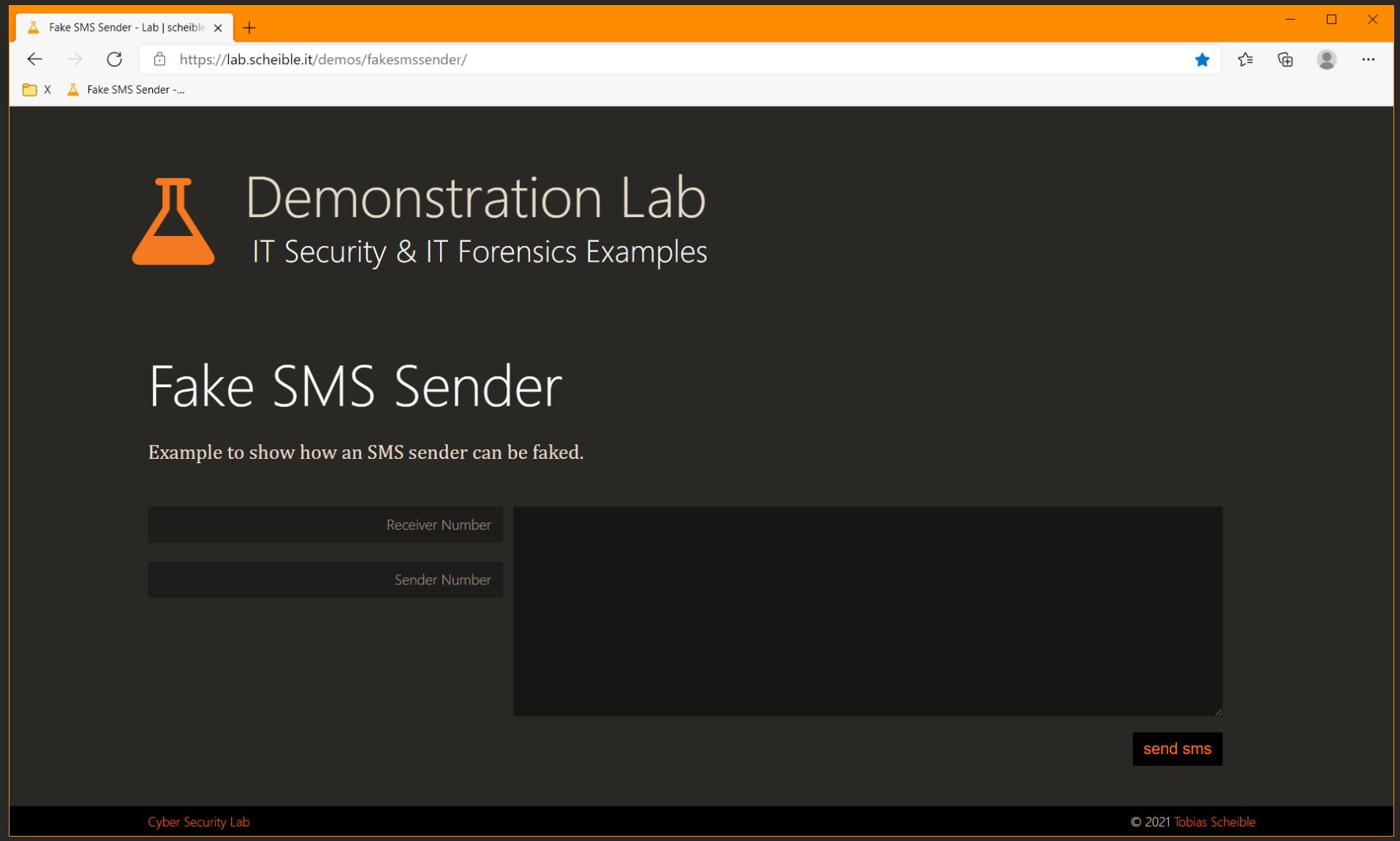
WHO Plague Prevention & Control

World Health Organization

1 attachment: CoronaVirus_Safety_Measures.rar 1,2 MB Save

Quelle: datensicherheit.de (6)

LIVE SMS fälschen



Zusatzfolie

FAZIT Social Engineering

- Informationen im Web, aber auch SMS-Nachrichten und Telefonnummern, können sehr einfach gefälscht werden.
- E-Mails können sehr einfach manipuliert werden und vorhandene Konversationen können von Angreifern aufgegriffen werden.
- Definierte Prozesse für alle Abteilungen, insbesondere mit Schnittstellen nach außen (Personalabteilung, Verkauf, etc.).
- Sensibilisierung der Mitarbeiter/innen mit Schulungen über Social Engineering-Strategien und –Methoden.

Passwortsicherheit

000000000

?

Quelle: heise.de (7)

00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Quelle: heise.de (7)

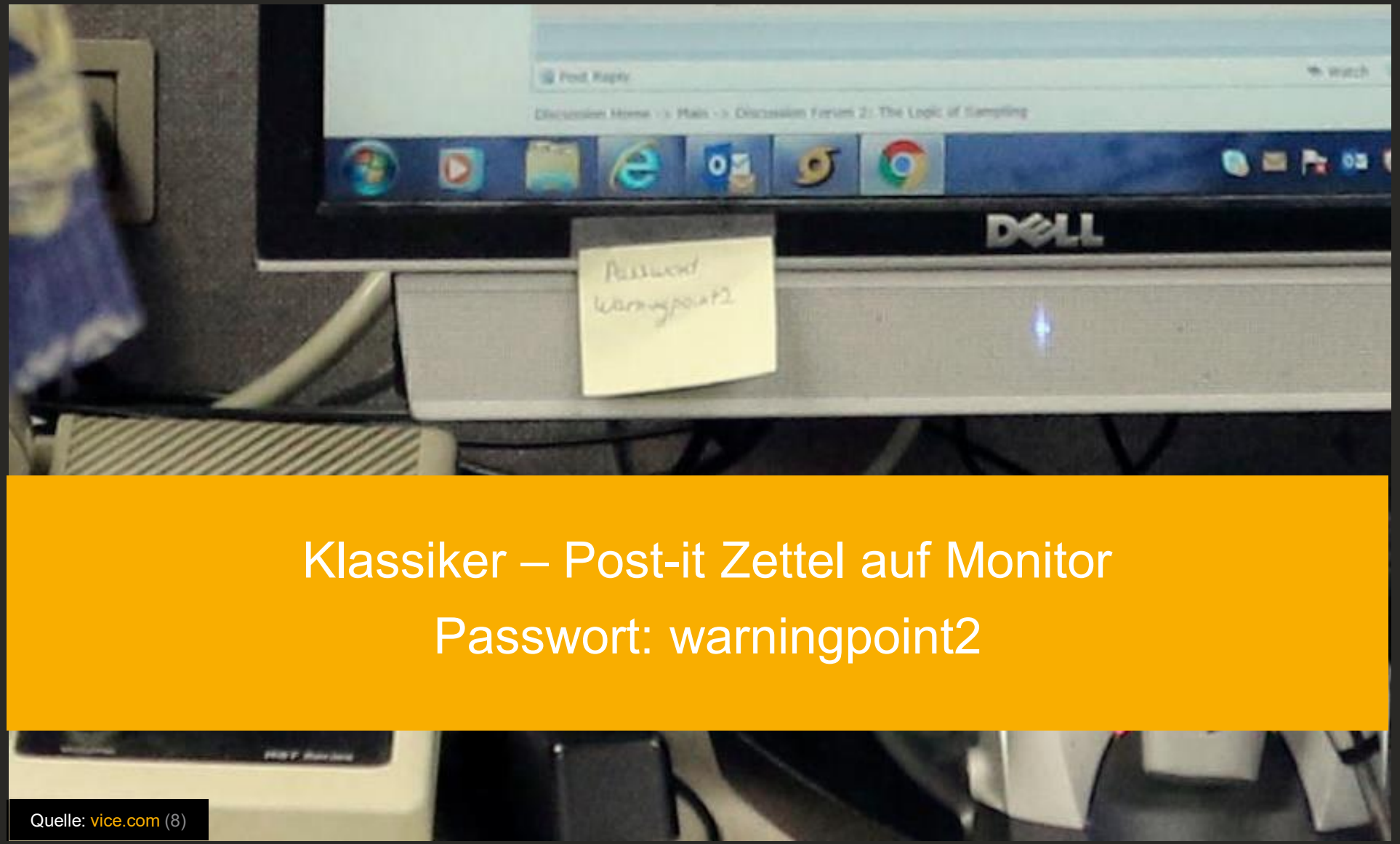
Zusatzfolie

Faktor Mensch

Quelle: vice.com (8)

Zusatzfolie

Faktor Mensch

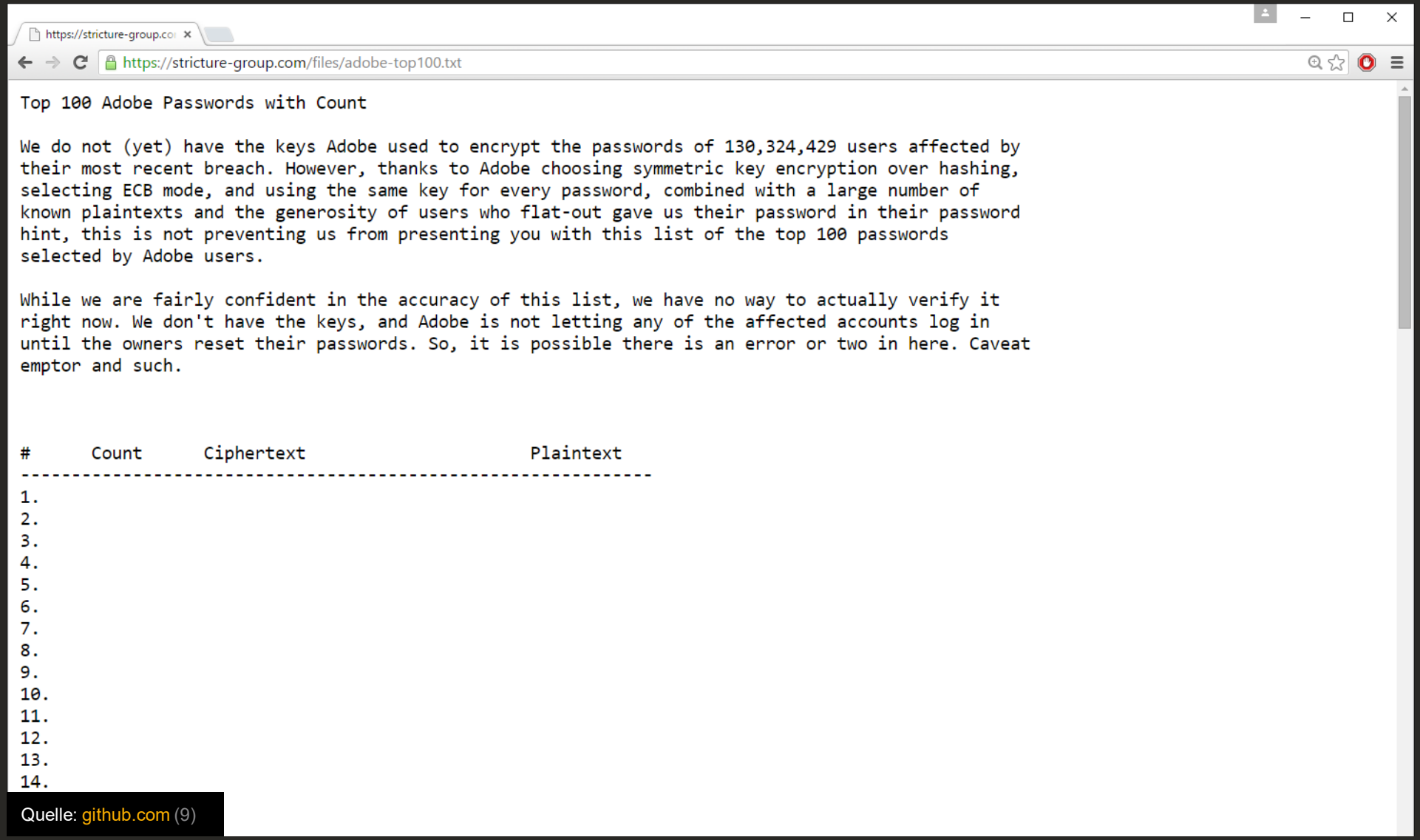


Klassiker – Post-it Zettel auf Monitor

Passwort: warningpoint2

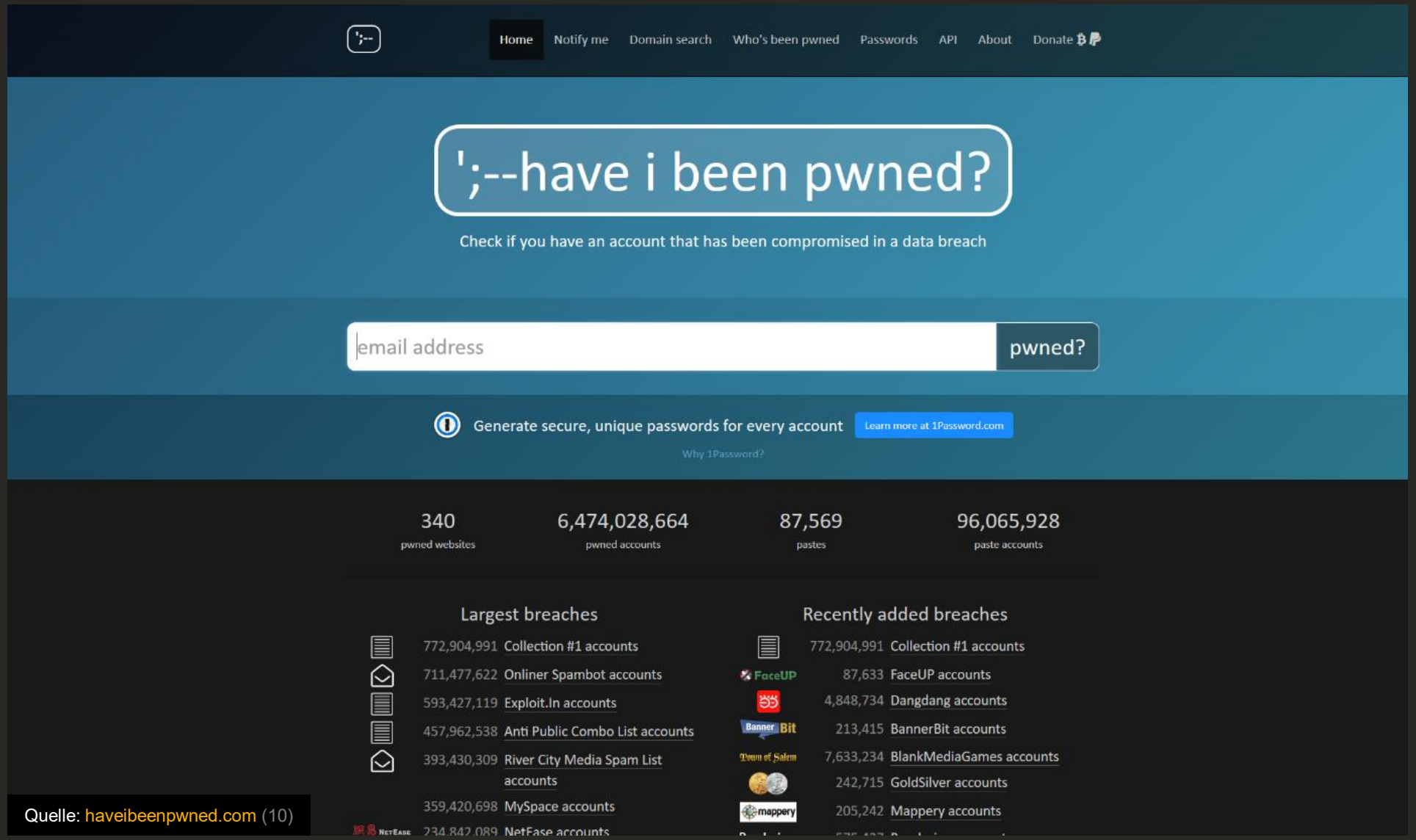
Quelle: vice.com (8)

Passwortlisten



Quelle: github.com (9)

LIVE Gehackte Accounts



Quelle: haveibeenpwned.com (10)

Zusatzfolie

Fazit Passwortsicherheit

- Die Länge eines Passwortes ist ein entscheidender Faktor. Lange Passwörter sind, pauschal gesagt, sicherer als kurze.
- Das Passwort darf nicht mit Ihrem persönlichen Umfeld in Verbindung stehen.
- Nutzen Sie für jeden Dienst verschiedene Passwörter, damit nach einem Angriff nicht auch andere Accounts von Ihnen betroffen sind.
- Nutzen Sie einen Passwortmanager, um die unterschiedlichen Passwörter sicher zu speichern.
- Nutzen Sie, wenn möglich, eine Zwei-Faktor-Authentifizierung.

Zielgerichtete Angriffe

Problematische Hardware

heise online

Anmelden Suchen Menü

IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft Journal Newsticker Foren

TOPTHEMEN: CES 2019 DSGVO WINDOWS 10 ANDROID AMAZON KI ANZEIGE: CLOUD SERVICES ZUKUNFTSMACHER

Security) 7-Tage-News | 01/2016) IP-Kameras von Aldi mit massiven Sicherheitslücken

Alert! 15.01.2016 10:49 Uhr | Security

IP-Kameras von Aldi als Sicherheits-GAU

Aldi hatte vergangenes Jahr mehrfach IP-Überwachungskameras mit denkbar schlechten Voreinstellungen verkauft. Die Geräte sind zu Hunderten fast ungeschützt über das Internet erreichbar.

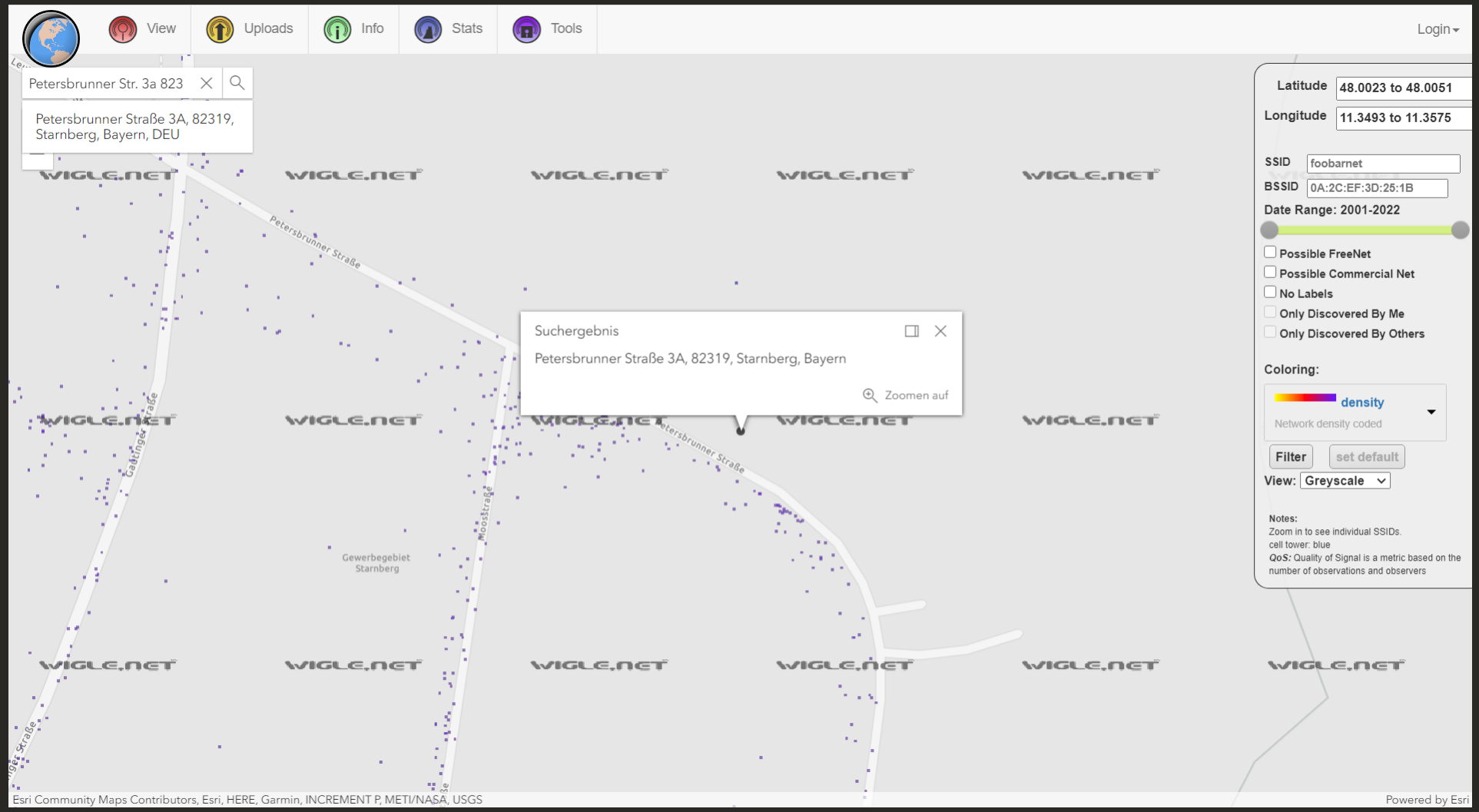
Von Ronald Eikenberg 411

Die bei Aldi verkauften IP-Überwachungskameras der Marke Maginon haben massive Sicherheitsprobleme: Unbefugte könnten über das Internet auf das Kamerabild zugreifen und sogar den Ton anzapfen. Zudem verraten die Geräte unter anderem die Passwörter für WLAN, E-Mail und FTP-Zugang ihres Besitzers. Hunderte Aldi-Kameras sind nahezu ungeschützt über das Internet erreichbar. Darauf hat uns der Zusammenschluss Digitale Gesellschaft aufmerksam gemacht.

Betroffen ist unter anderem die Außenkamera IPC-20 C. (Bild: Hersteller)

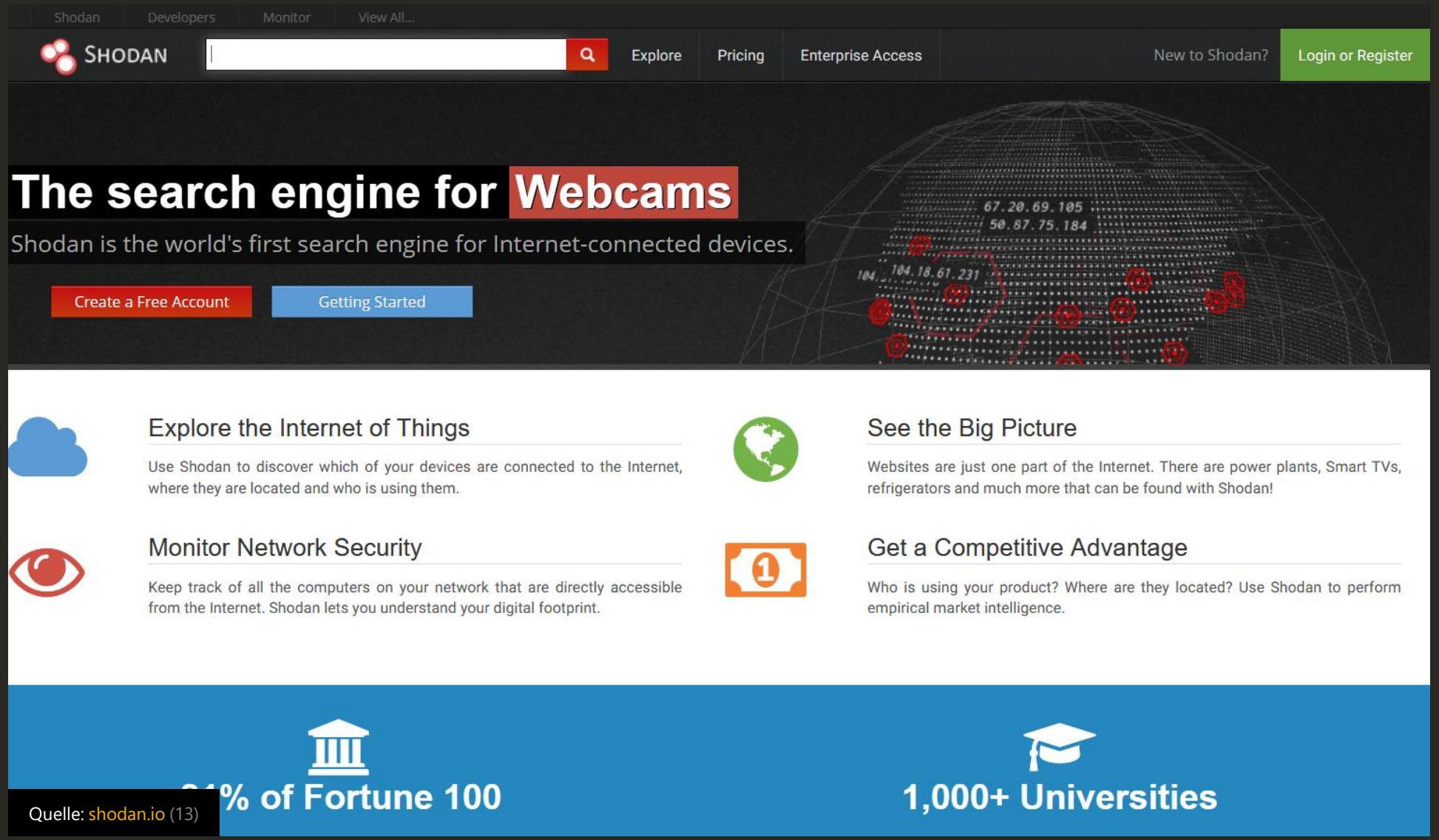
Quelle: heise.de (11)

Problematische Hardware



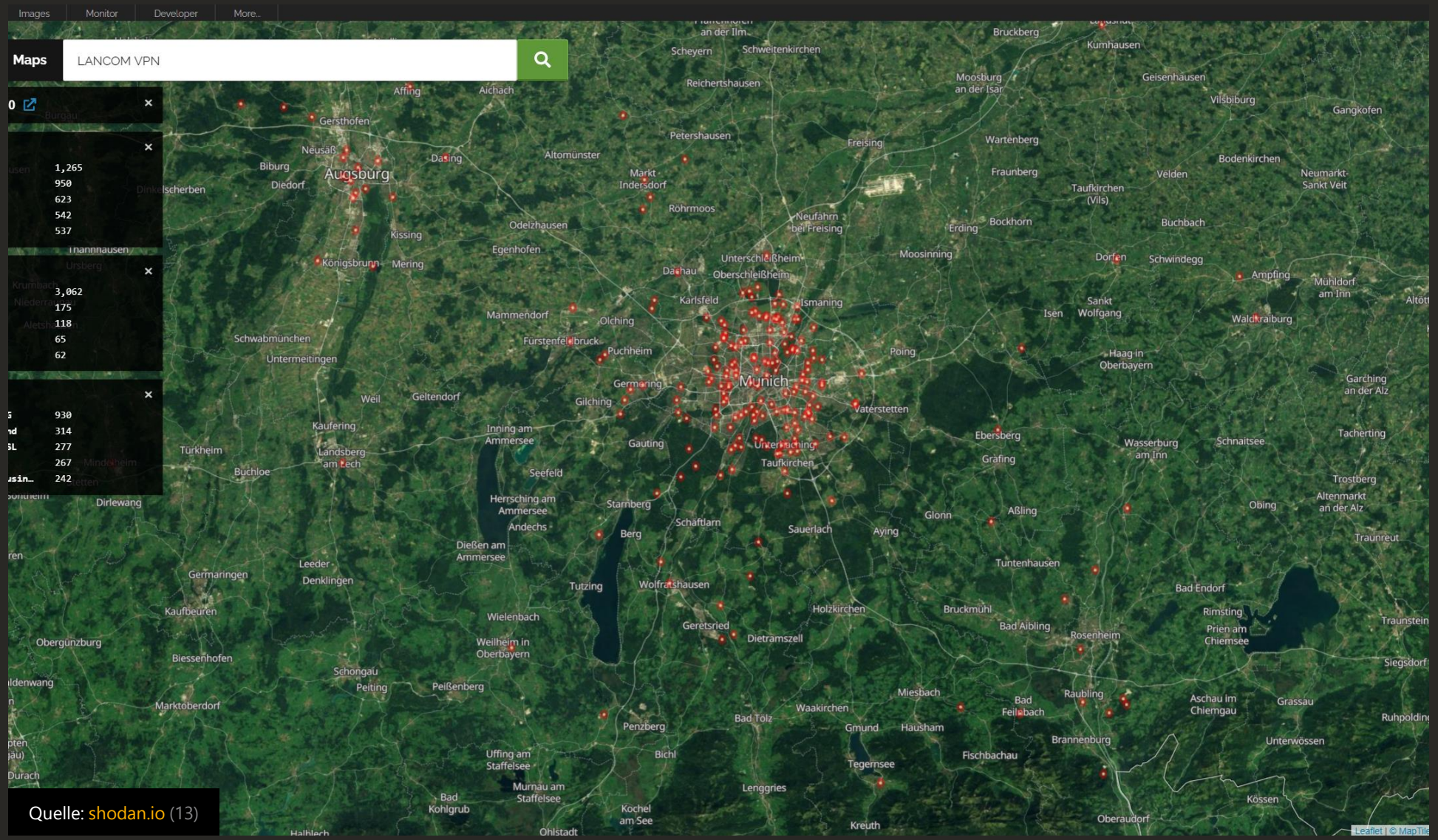
Quelle: wigle.net (12)

Systeme suchen



Quelle: shodan.io (13)

LIVE Systeme suchen



Quelle: shodan.io (13)

Zusatzfolie

FAZIT Zielgerichtete Angriffe

- Geräte oder Anwendungen, die im Internet sind, können nicht durch komplizierte Links oder weil die Adresse nirgendwo steht, geschützt werden.
- Die Standard-Passwörter von Geräten, die mit dem Internet verbunden sind, müssen immer geändert werden.
- Komponenten können sich auch selbstständig mit dem Internet verbinden, daher muss die Konfiguration immer geprüft werden.
- Alle Systeme, die online sind, werden von speziellen Suchmaschinen gefunden.

Vielen Dank

Fragen?

Quellen

1) https://www.gdata.de/ratgeber/was-ist-eigentlich-die-geschichte-der-malware
2) https://de.wikipedia.org/wiki/AIDS_(Schadprogramm)
3) https://www.sueddeutsche.de/digital/it-sicherheit-hacker-wasserwerk-florida-1.5205113
4) http://www.heise.de/newsticker/meldung/Gefaengnisausbruch-mittels-E-Mail-Betrug-2587303.html
5) https://de.wikipedia.org/wiki/Locky
6) https://www.datensicherheit.de/corona-virus-gefaehrliche-e-mails-virulent
7) http://www.heise.de/security/meldung/00000000-Passwort-fuer-US-Atomraketen-2060077.html
8) https://www.vice.com/en_us/article/qvwmx5/the-agency-that-messed-up-hawaiis-nuclear-alert-keeps-passwords-on-post-its-vgtrn
9) https://github.com/morontt/symfobrute/blob/master/adobe-top100.txt
10) https://haveibeenpwned.com
11) http://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html
12) https://wigle.net
13) https://shodan.io