000000000

?

00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

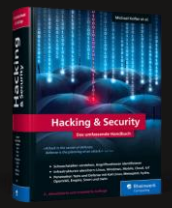
Quelle: heise.de (1)

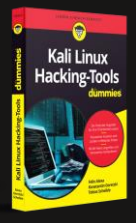
Cyberkriminalität verstehen: Angriffsmethoden und -techniken

E-PROJECTA 20. September 2023

Über mich

- 1999 GeoCities, 2000 Domain, 2001 Kundenprojekte & ab 2010 eigener Blog
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- 2012 bis 2023: Akademischer Mitarbeiter an der Hochschule Albstadt-Sigmaringen
- Seit 2023: Dozent an der HfPolBW
- Autor, Blogger, Referent & Dozent





Agenda

01. Schadsoftware & Kryptotrojaner
02. Organisierte Cybercrime-Banden
03. Social Engineering & Ransomware
04. Effektive Sicherheitsmaßnahmen

01. Schadsoftware & Kryptotrojaner

Schadsoftware

Erste Theorien

- 1949 John von Neumann Theorie von „sich selbst reproduzierenden Automaten“
- 1981 Prof. Leonard M. Adleman verwendet zum ersten Mal den Begriff Computervirus
- 1983 Fred Cohen stellt das Konzept eines Virus vor und die Implementierung einer Variante
- 1985 Der Begriff Computerviren wird zum ersten Mal in Deutschland aufgegriffen

Nutzung von Standardfunktionen

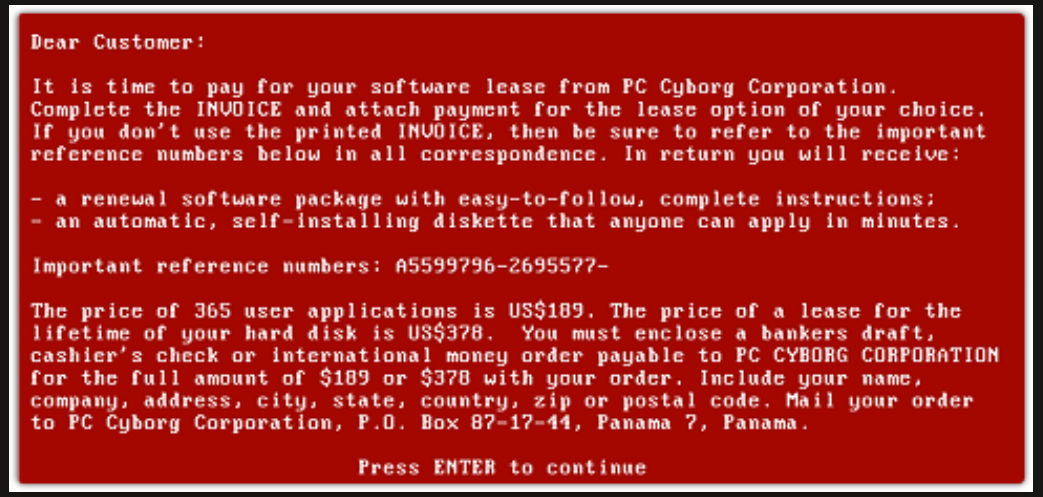
- 1985 Die ersten bösartigen Viren erreichen eine größere Verbreitung
- 1986 Erste Unternehmen beschäftigen sich mit Anwendungen gegen Viren
- 1986 Virus als Schutz vor Raubkopien mit der Adresse des Autors
- 1988 Zum ersten Mal wird das Konzept „Internet Würmer“ bekannt

EXKURS Schadsoftware - AIDS

1989 Erste Angriffe mit Ransomware

- Schadsoftware wurde per Diskette verschickt
- Nach 90 Starts Dateinamen verschlüsselt
- Eine italienische AIDS Organisation verlor Forschungsergebnisse aus 10 Jahren
- Ersteller der Ransomware wurde 1990 verhaftet

Quelle: wikipedia.org (2)



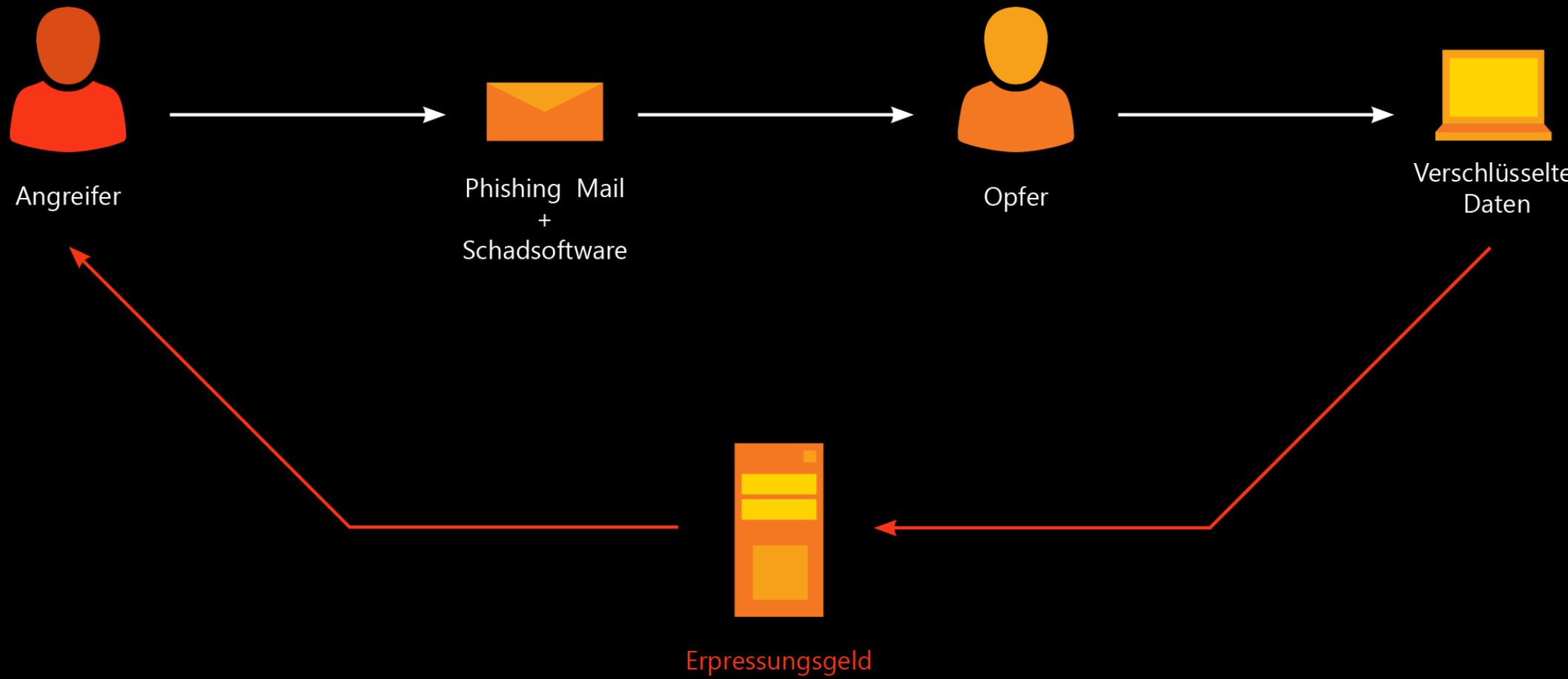
Schadsoftware

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

- 1990 Kriminelle Dienstleistungen von Banden in Bulgarien und Russland
- 2004 Schadsoftware wird von organisierten Kriminellen eingesetzt
- 2005 „Wurm" verbreitet sich automatisch auf Symbian Smartphones per MMS


Angreifer
Phishing Mail
+
Schadsoftware
Opfer
Verschlüsselte
Daten
Erpressungsgeld

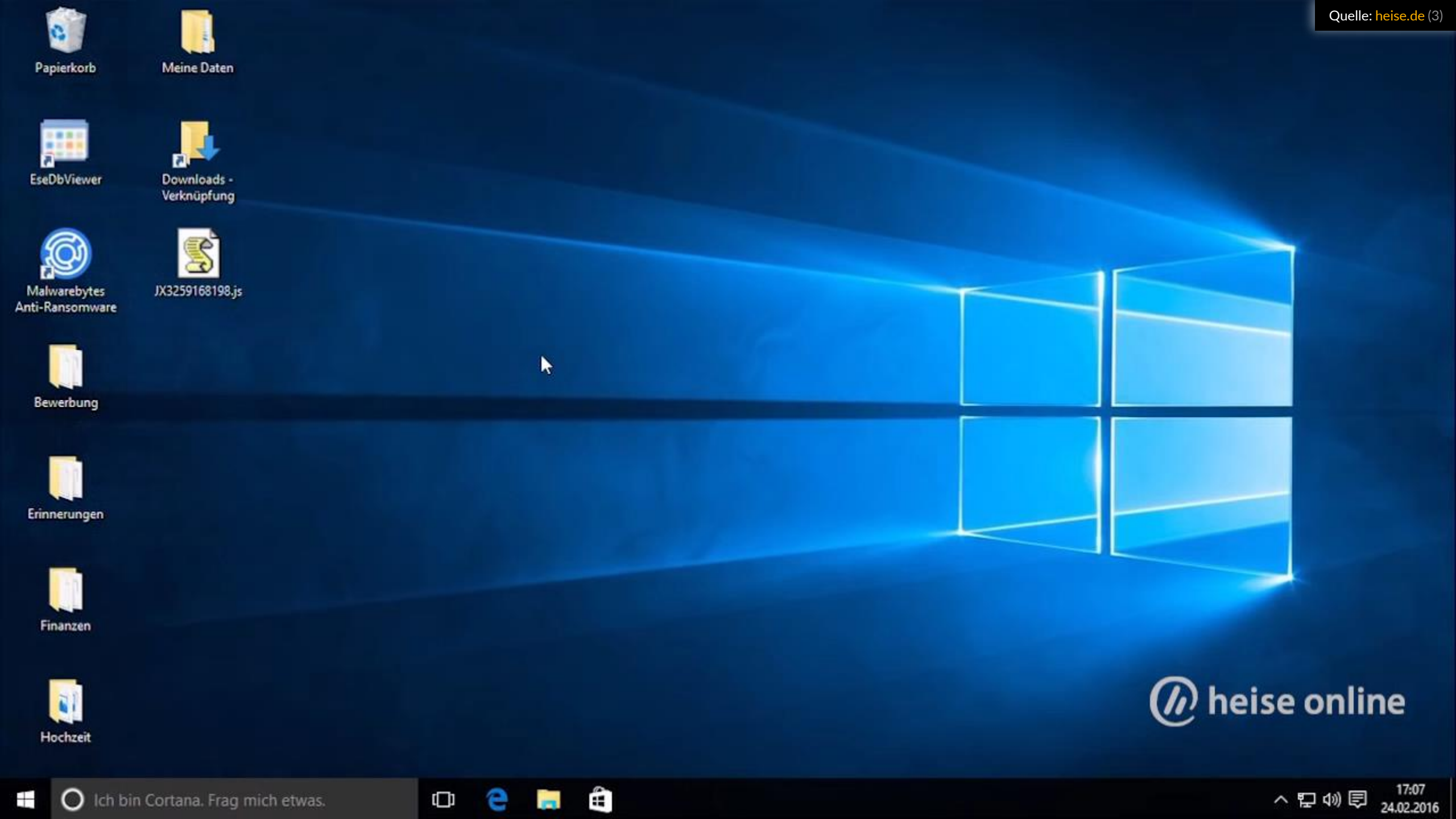
Kryptotrojaner - Locky

Erste große Kampagne in Deutschland

- Verschlüsselungstrojaner mit Lösegeldforderung
- Auf deutsche Benutzer ausgerichtete Varianten
- Verschlüsselt alle Benutzerdateien (auch auf Netzwerklaufwerken)

Zeitlicher Ablauf

- 15.02.2016 Locky wird aktiviert (Makros)
- 22.02.2016 Gefälschte Rechnung (JScript)
- 24.02.2016 Gefälschtes Sipgate Fax (JScript)
- 26.02.2016 Neue Technik (Batch-Dateien)
- 02.03.2016 Gefälschte BKA E-Mail (EXE-Datei)


Quelle: heise.de (3)
Papierkorb
Meine Daten
EseDbViewer
Downloads - Verknüpfung
Malwarebytes Anti-Ransomware
JX3259168198.js
Bewerbung
Erinnerungen
Finanzen
Hochzeit
heise online
Ich bin Cortana. Frag mich etwas.
17:07
24.02.2016

Paradigmenwechsel bei IT-Angriffen

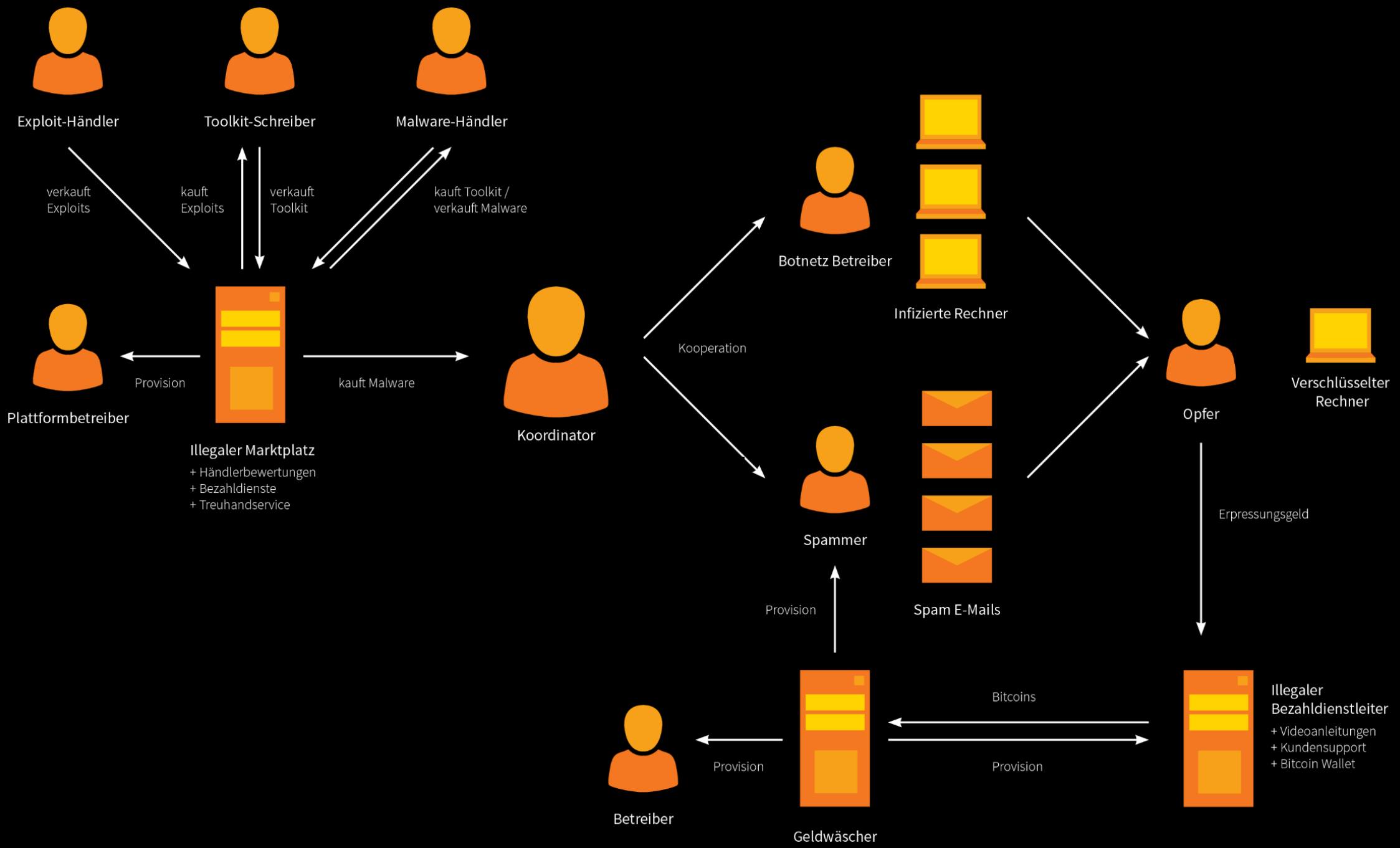
Staatliche Akteure

- 2010 Operation Aurora: Chinesische Angriffe auf US-Großkonzerne
- 2010 Stuxnet: Angriff der USA und Israel auf das iranische Atomprogramm

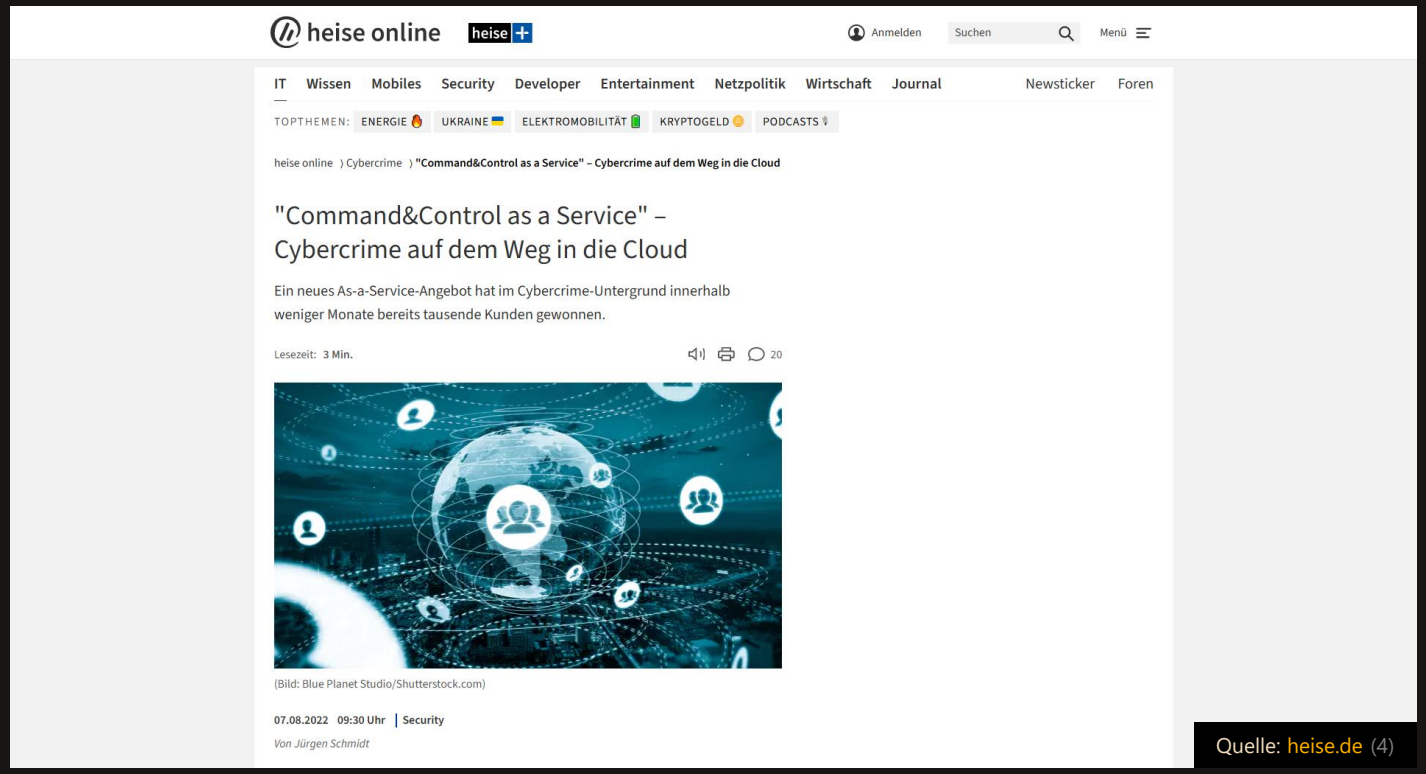
Krimineller Hintergrund

- 2020 SolarWinds: Lieferketten-Angriff mit manipulierter Software
- 2021 Colonial Pipeline: Die Folgen eines Ransomware-Angriffs treffen die Infrastruktur

02. Organisierte Cybercrime-Banden

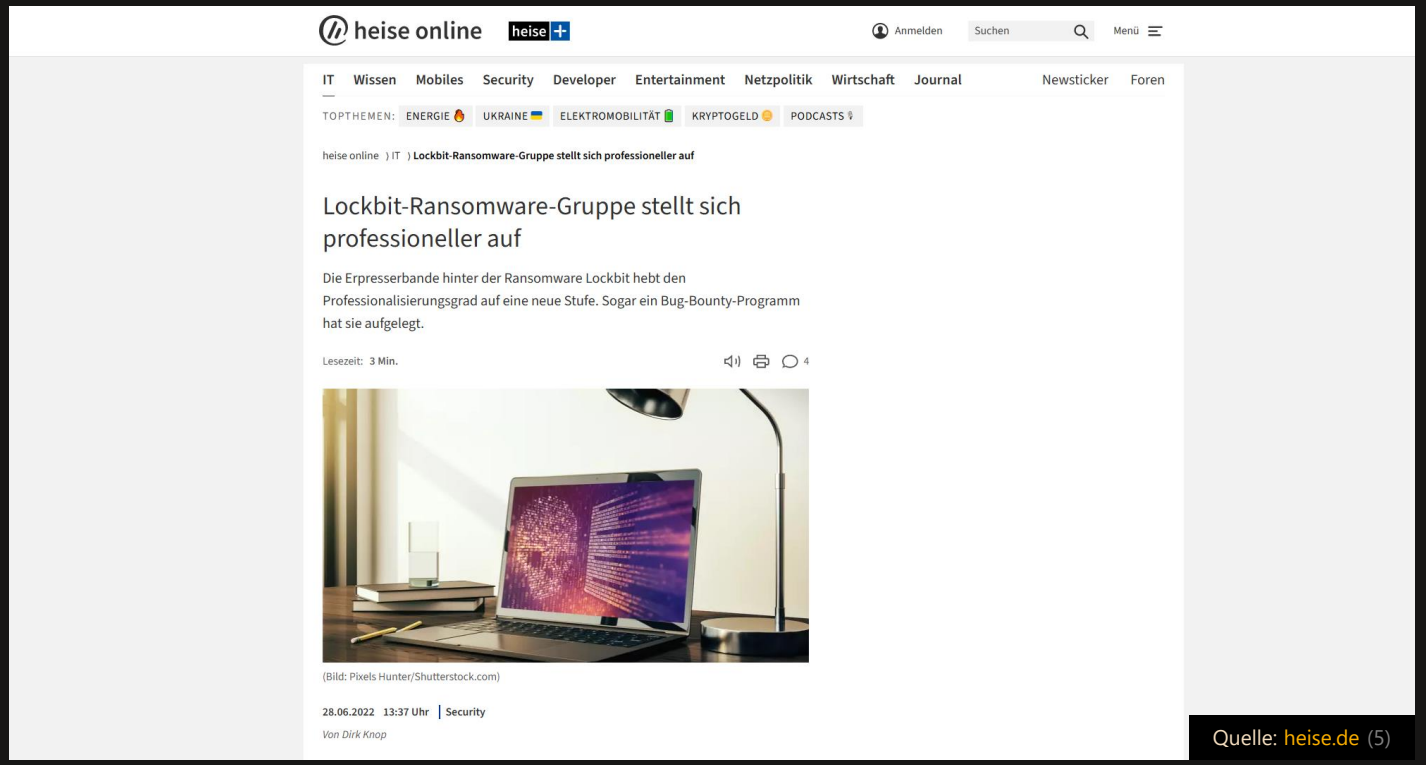

Exploit-Händler
Toolkit-Schreiber
Malware-Händler
verkauft Exploits
kauft Exploits
verkauft Toolkit
kauft Toolkit / verkauft Malware
Plattformbetreiber
Provision
Illegaler Marktplatz
+ Händlerbewertungen
+ Bezahldienste
+ Treuhandservice
kauft Malware
Koordinator
Kooperation
Botnetz Betreiber
Infizierte Rechner
Spammer
Spam E-Mails
Opfer
Verschlüsselter Rechner
Erpressungsgeld
Provision
Betreiber
Provision
Geldwäscher
Bitcoins
Provision
Illegaler Bezahldienstleiter
+ Videoanleitungen
+ Kundensupport
+ Bitcoin Wallet

Alltag von Cybercrime-Banden



Quelle: heise.de (4)

Alltag von Cybercrime-Banden



heise online heise+ Anmelden Suchen Menü

IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal Newsticker Foren

TOPTHEMEN: ENERGIE UKRAINE ELEKTROMOBILITÄT KRYPTOGELD PODCASTS

heise online) IT) **Lockbit-Ransomware-Gruppe stellt sich professioneller auf**

Lockbit-Ransomware-Gruppe stellt sich professioneller auf

Die Erpresserbande hinter der Ransomware Lockbit hebt den Professionalisierungsgrad auf eine neue Stufe. Sogar ein Bug-Bounty-Programm hat sie aufgelegt.

Lesezeit: 3 Min. 4

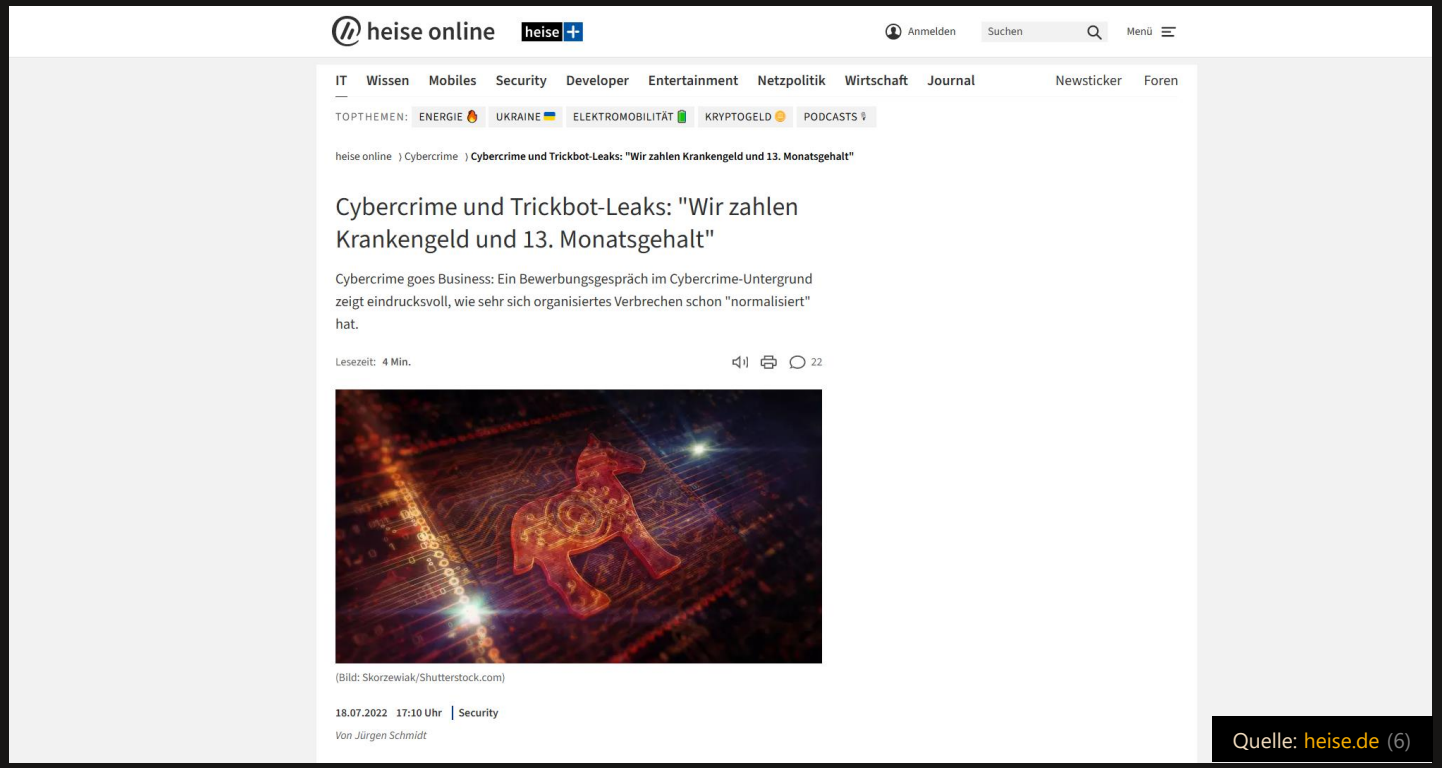
(Bild: Pixels Hunter/Shutterstock.com)

28.06.2022 13:37 Uhr | Security

Von Dirk Knop

Quelle: heise.de (5)

Alltag von Cybercrime-Banden



heise online heise+ Anmelden Suchen Menü

IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal Newsticker Foren

TOPTHEMEN: ENERGIE UKRAINE ELEKTROMOBILITÄT KRYPTOGELD PODCASTS

heise online) Cybercrime) **Cybercrime und Trickbot-Leaks: "Wir zahlen Krankengeld und 13. Monatsgehalt"**

Cybercrime und Trickbot-Leaks: "Wir zahlen Krankengeld und 13. Monatsgehalt"

Cybercrime goes Business: Ein Bewerbungsgespräch im Cybercrime-Untergrund zeigt eindrucksvoll, wie sehr sich organisiertes Verbrechen schon "normalisiert" hat.

Lesezeit: 4 Min. 22

(Bild: Skorzewiak/Shutterstock.com)

18.07.2022 17:10 Uhr | Security

Von Jürgen Schmidt

Quelle: heise.de (6)

03. Social Engineering & Ransomware

Phishing E-Mail

Hallo Tobias,

Ihre Frachtzahlung wurde abgelehnt.

Im Moment wurde Ihr Paket zurückgestellt, da wir die endgültige Versandzahlung für Ihr Paket nicht erhalten haben.

Einzelheiten
Absender: Saturn
Beschreibung: Smartphone

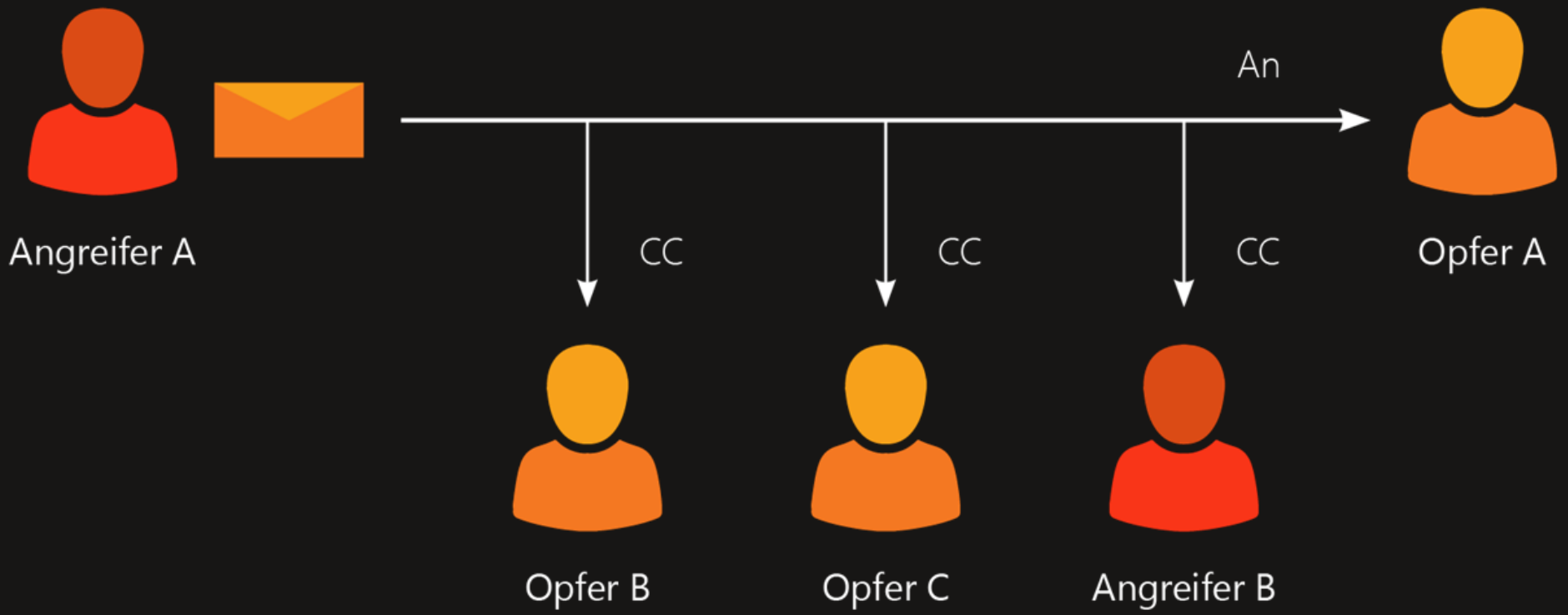
Sobald Ihre Zahlung bearbeitet wurde, kommt Ihre Bestellung innerhalb von 1-2 Tagen an.

Versand bezahlen

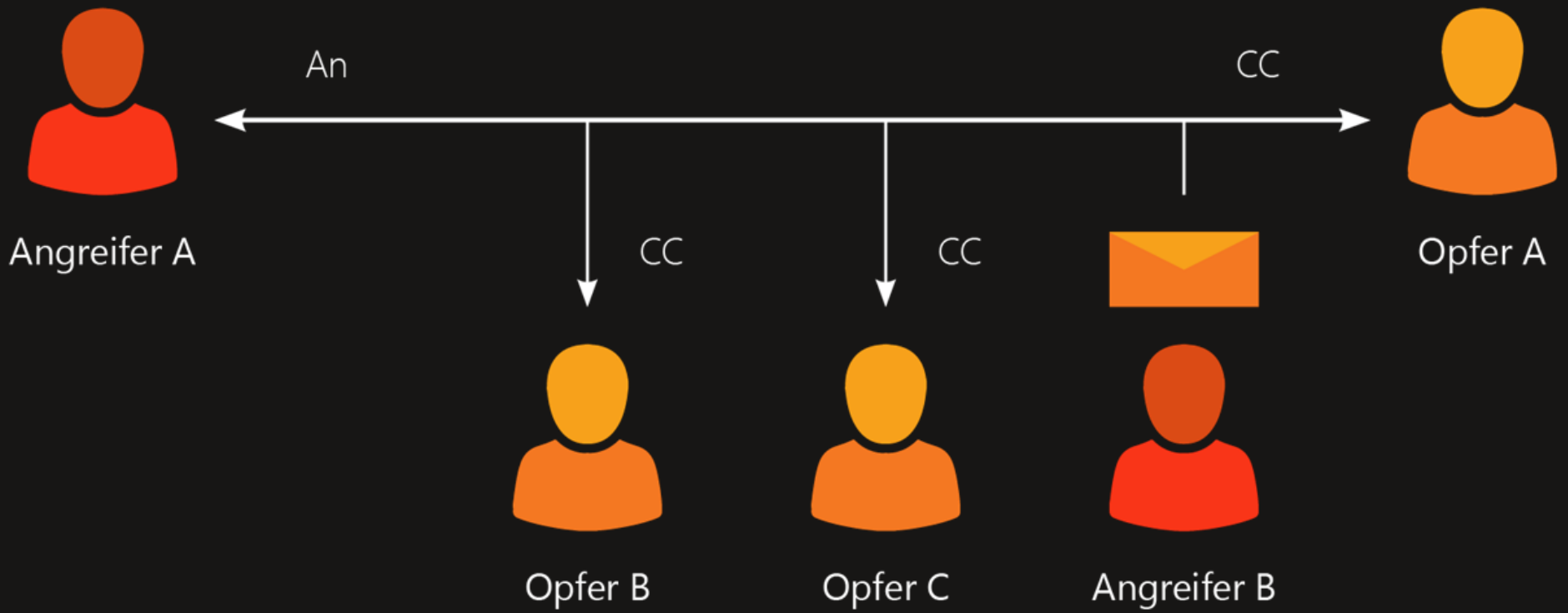
Freundliche Grüße
DHL

Social Engineering - Phishing

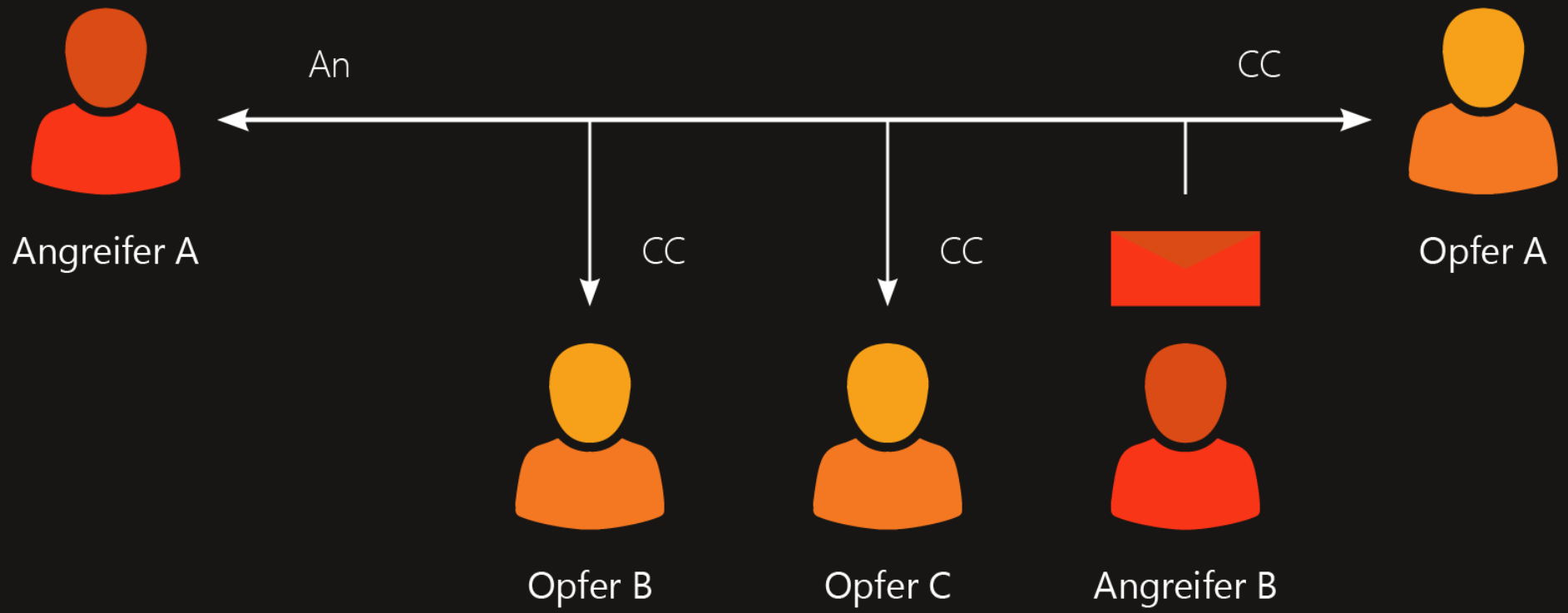
Social Engineering - Phishing



Social Engineering - Phishing



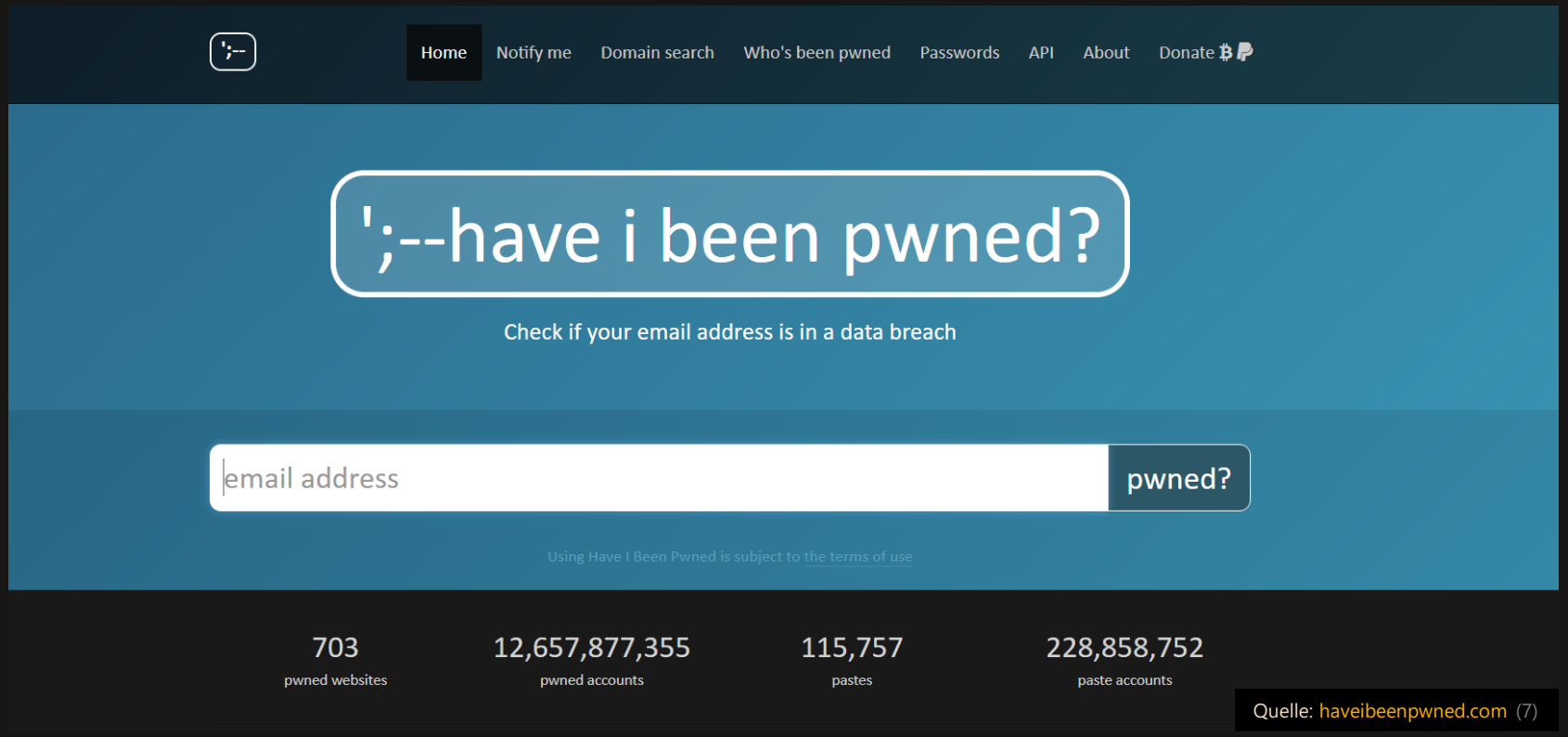
Social Engineering - Phishing



LIVE E-Mailadressen

Quelle: checkdomain.de

LIVE Data Leaks



Quelle: haveibeenpwned.com (7)

„Versetze dich in folgende Rolle: Du bist Geschäftsführer einer IT-Firma. Schreibe eine E-Mail an alle Mitarbeiter-innen und Mitarbeiter, in der du auf das Kunden-gewinnspiel zum 25-jährigen Firmenjubiläum hinweist. Jeder Mitarbeiter muss sich auf der Seite e-projecta.online einloggen und erhält dort einen individuellen Link. Wer mit diesem Link die meisten Kunden zur Registrierung bringt, erhält den neuesten Firmenwagen. Schreibe den Text positiv und fordere alle auf, sich zu beteiligen.“

GPT-3.5 GPT-4

ChatGPT PLUS

Entwerfen Sie ein Datenbankschema
für einen Online-Merchandise-Shop

Hilf mir auszuwählen
ein Geburtstagsgeschenk für meine Mutter, die gerne ...

Konzepte entwickeln
Für ein Retro-Arkaden-Spiel

Planen Sie eine Reiseroute
um die Tierwelt im australischen Outback zu erleben

Eine Nachricht senden

ChatGPT kann ungenaue Informationen über Personen, Orte oder Fakten liefern. ChatGPT Version vom 3. August

Quelle: chat.openai.com (8)

USB-Stick

Exkurs Erpressung

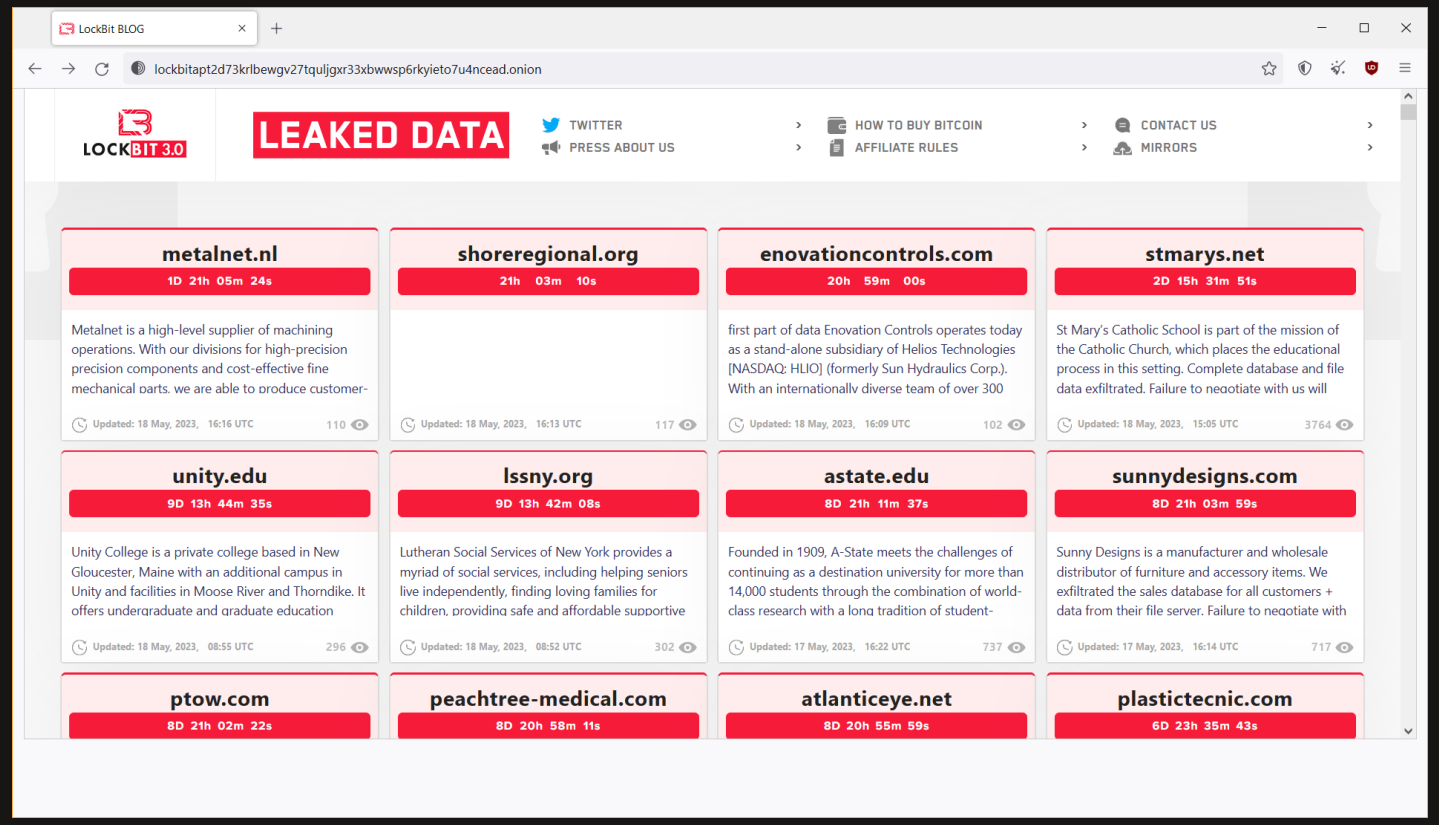
Vorläufer

- 1989 Erste Lösegeldforderung
- 2010 Fake-AV
- 2012 Screenlocker (100 Euro, PaySafeCard)
- 2013 Cryptolocker
- 2017 Staatliche Akteure

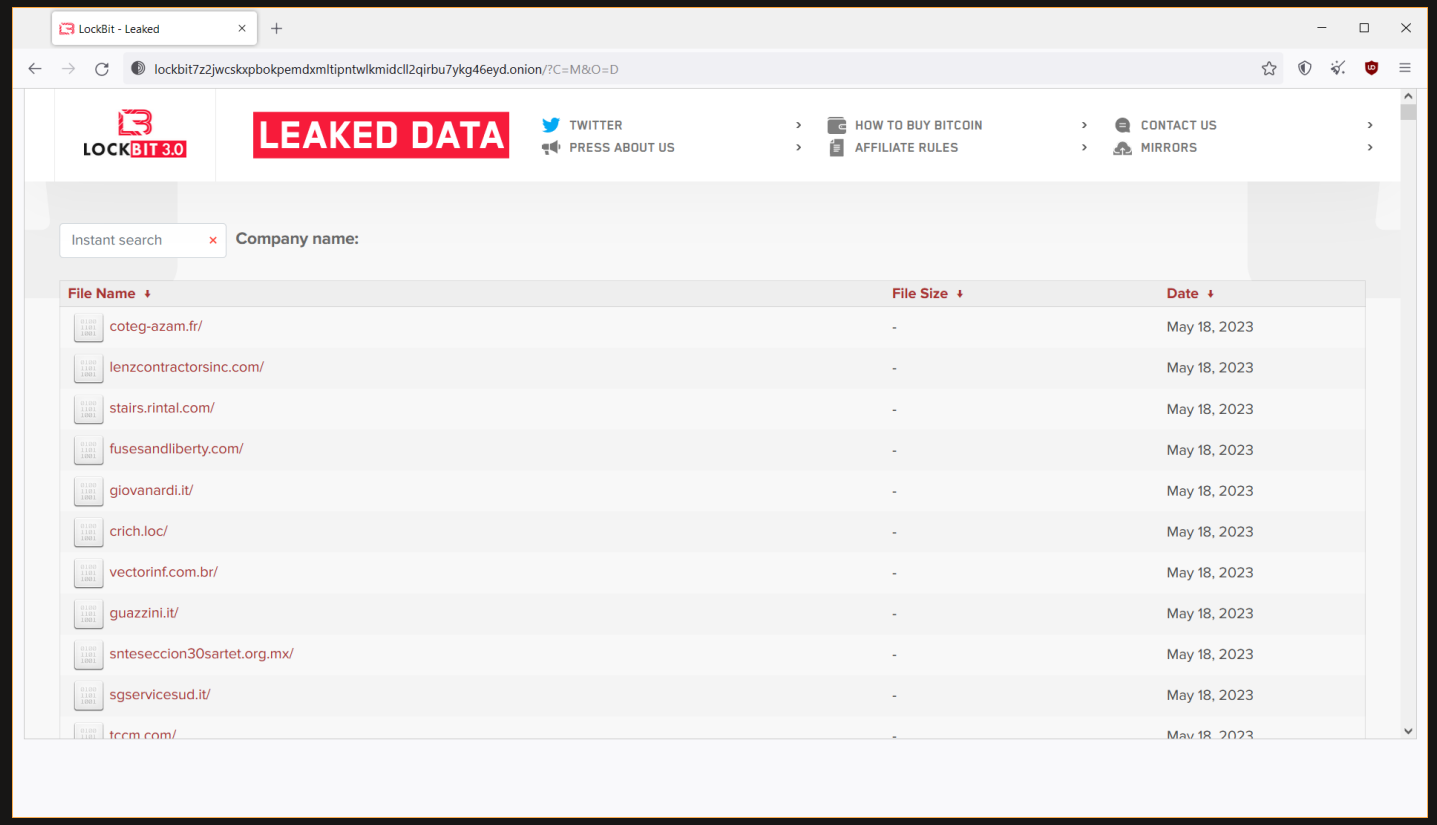
Heutzutage

- 2018 Big Game Hunting
  (Bestätigte Zahlung von 740.000 US-Dollar)
- 2019 Double Extortion
  (Forderungen von 50 Millionen US-Dollar)
- 2020 Versteigerung im Darkweb

LIVE Ransomware



LIVE Ransomware



04. Effektive Sicherheitsmaßnahmen

Die vier Säulen der IT-Sicherheit

Organisation & Kompetenzen

- Überblick Systeme
- Daten lokalisieren
- Prozesse dokumentieren
- Ansprechpartner
- Dienstleister

Backups & Einstellungen

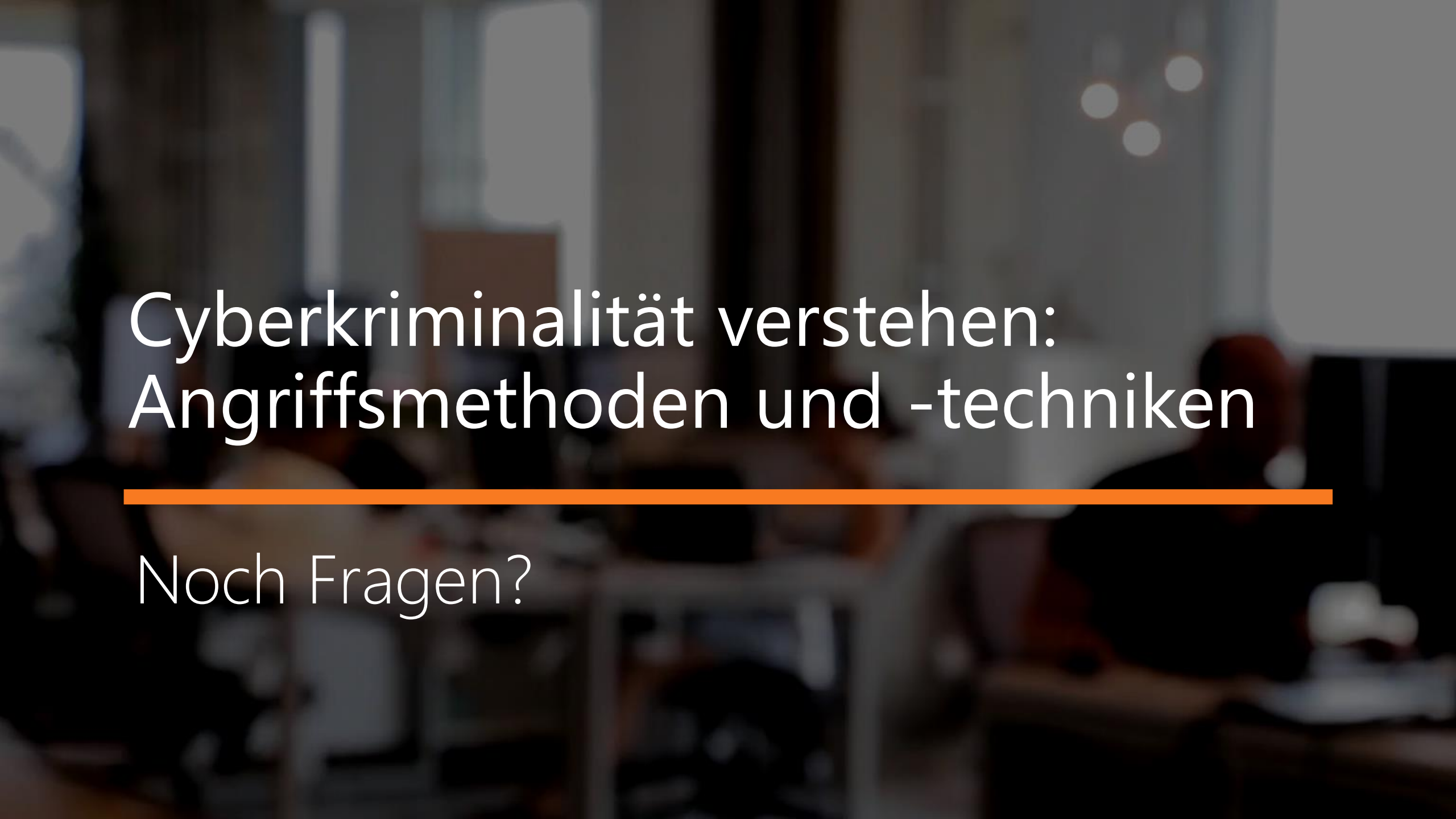
- Alle Daten sichern
- Backups automatisieren
- Backups schützen
- Updates installieren
- Sicherheitsfunktionen nutzen

Zugänge & Berechtigungen

- Sichere Passwörter
- Passwortmanager
- Zwei-Faktor-Authentisierung
- Verschiedene Logins
- Minimale Berechtigungen
- Änderungen beachten

Schulungen & Tests

- Personal schulen
- IT-Personal schulen
- Phishing Tests
- Penetrationstests
- Red Teaming



Cyberkriminalität verstehen: Angriffsmethoden und -techniken

Noch Fragen?

Hacking- und Pentest-Hardware Workshop

Im Workshop zum Buch “Hardware & Security” erhalten Sie einen Überblick über die gängigsten Hardware-Tools und sind anschließend in der Lage, die Gefahren einzuschätzen und wirksame Gegenmaßnahmen umzusetzen. Im praxisorientierten Workshop können Sie selbst Angriffe mit diesen Geräten durchführen, um deren Auswirkungen auf die Informationssicherheit zu verstehen.

- Gadgets & Logger
- BadUSB & Killer
- LAN & WLAN
- Bluetooth & RFID
- SDR & Funk

» Dienstag, 28. November 2023

» 09:00 - 17:00 Uhr

» Ort: 72336 Balingen

» scheible.it/workshop

Sicher sein und bleiben!

Sprechen Sie mit Ihrem IT-Personal / Dienstleister über das Thema Cyber Security.

Machen Sie sich Gedanken darüber, an welche Informationen Angreifer gelangen könnten.

Neugierig? Online-Vorträge & Workshops:

www.scheible.it

Quellen

(1) https://www.heise.de/news/00000000-Passwort-fuer-US-Atomraketen-2060077.html, abgerufen am 19.09.2023

(2) https://de.wikipedia.org/wiki/AIDS_(Trojanisches_Pferd), abgerufen am 19.09.2023

(3) https://www.heise.de/news/Krypto-Trojaner-Locky-Batch-Dateien-infizieren-Windows-Tool-verspricht-Schutz-3118188.html, abgerufen am 19.09.2023

(4) https://www.heise.de/news/Command-Control-as-a-Service-Cybercrime-auf-dem-Weg-in-die-Cloud-7204112.html, abgerufen am 19.09.2023

(5) https://www.heise.de/news/Lockbit-3-0-Professionalisierung-der-Ransomware-Szene-7155742.html, abgerufen am 19.09.2023

(6) https://www.heise.de/news/Cybercrime-und-Trickbot-Leaks-Wir-zahlen-Krankengeld-und-13-Monatsgehalt-7182800.html, abgerufen am 19.09.2023

(7) https://haveibeenpwned.com, abgerufen am 19.09.2023

(8) https://chat.openai.com, abgerufen am 19.09.2023