# PHISHING

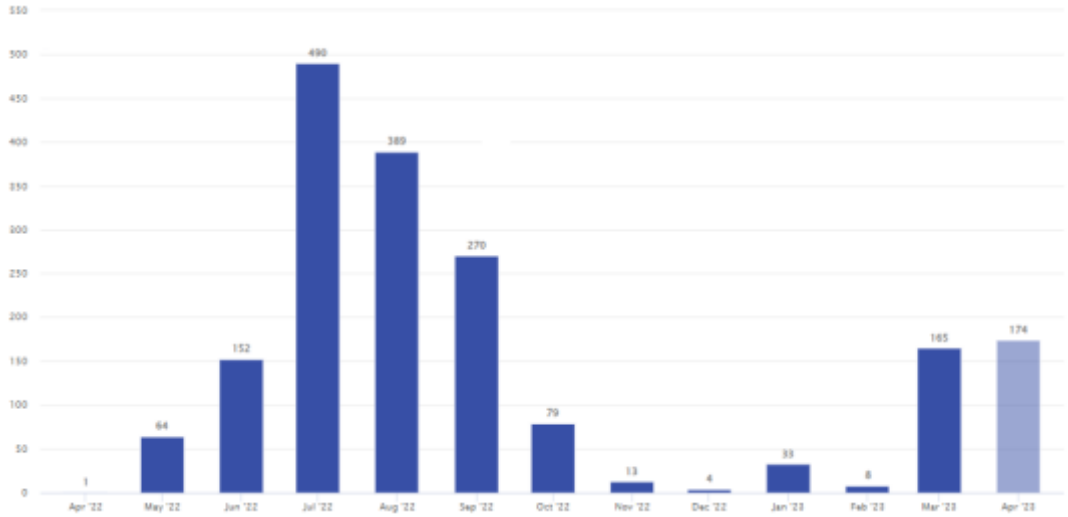
## STRIKING BACK

Joachim Kerschbaumer
CISO / bank99
(ISC)² / ISACA Conference 20.04.2023

# AUSGANGSLAGE....

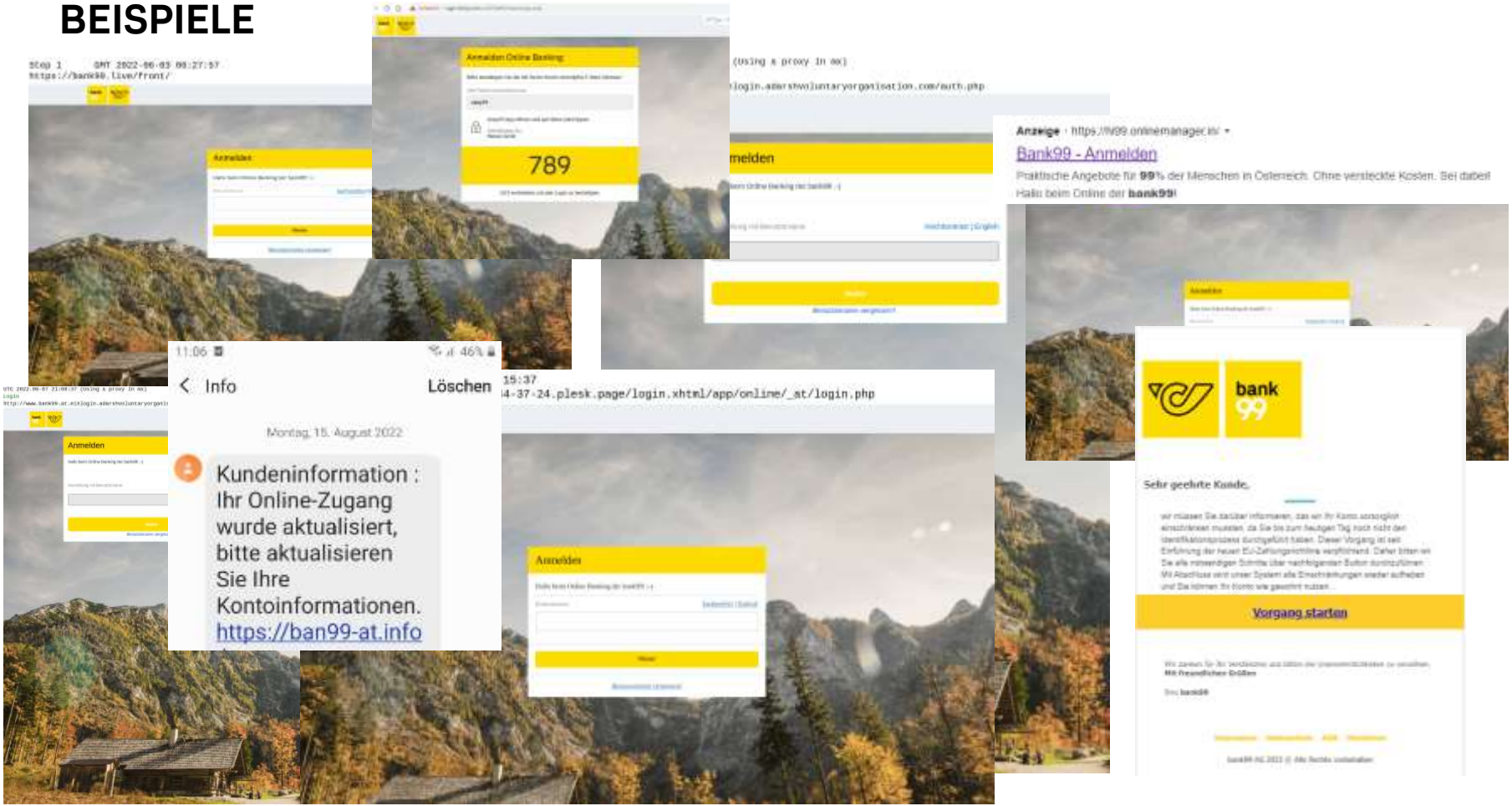
- bank99 startet als junge Bank 2020
- Übernahme von ING Österreich Ende 2021
- bank99 rutscht in den Fokus von Phishern mit Q2 2022

- **> 1000 unique phishing domains / pages**
- **hunderte neue Seiten pro Monat** (in Wellen)
- Bis zu **neue 25 Seiten täglich**




# Phishing Seiten / Monat

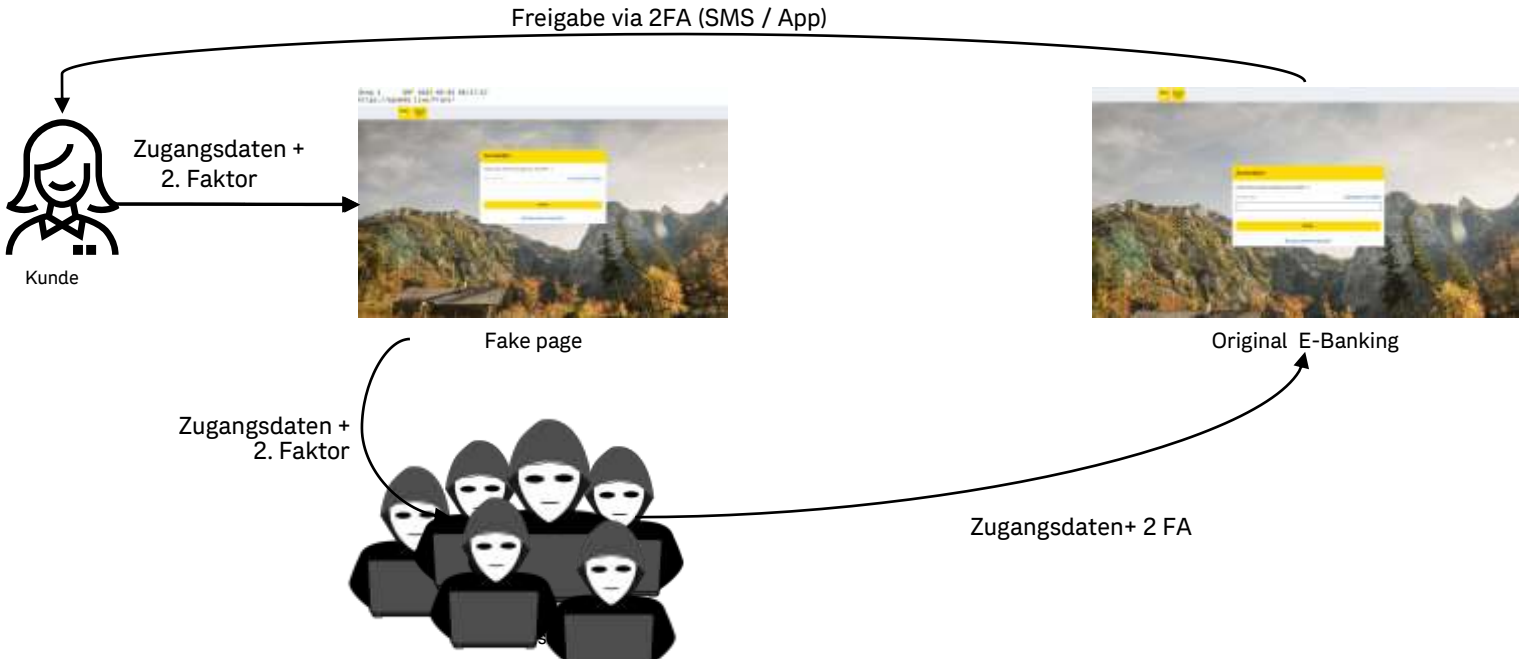
# BEISPIELE


Anmelden Online Banking
789
Anmelden
(using a proxy in ex)
login.adarshvoluntaryorganisation.com/auth.php
Anzeige · https://bk99.onlinemanager.io/
Bank99 - Anmelden
Praktische Angebote für 99% der Menschen in Österreich. Ohne versteckte Kosten. Bei dabei!
Halo beim Online der bank99!
11:06
46%
Info
Löschen
Montag, 15. August 2022
Kundeninformation : Ihr Online-Zugang wurde aktualisiert, bitte aktualisieren Sie Ihre Kontoinformationen.
https://ban99-at.info
15:37
4-37-24.plesk.page/login.xhtml/app/online/_at/login.php
Anmelden
bank 99
Sehr geehrte Kunde,
Vorgang starten

# 2-FAKTOR AUTHENTICATION SCHÜTZT VOR PHISHING?

## Umgehung 2-FA

- Faktor Mensch als Schwachstelle



# PHISHING – KANÄLE ZU DEN OPFERN

## 01 Email

- Kompromittierte Email Accounts (Freemail, Firmenkonten, ...)
- Falsch konfigurierte TLDs (e.g. bank99@kundenservice.at )
- Kommerzielle Marketing Mailer (kompromittierte Accounts)

## 02 SMS

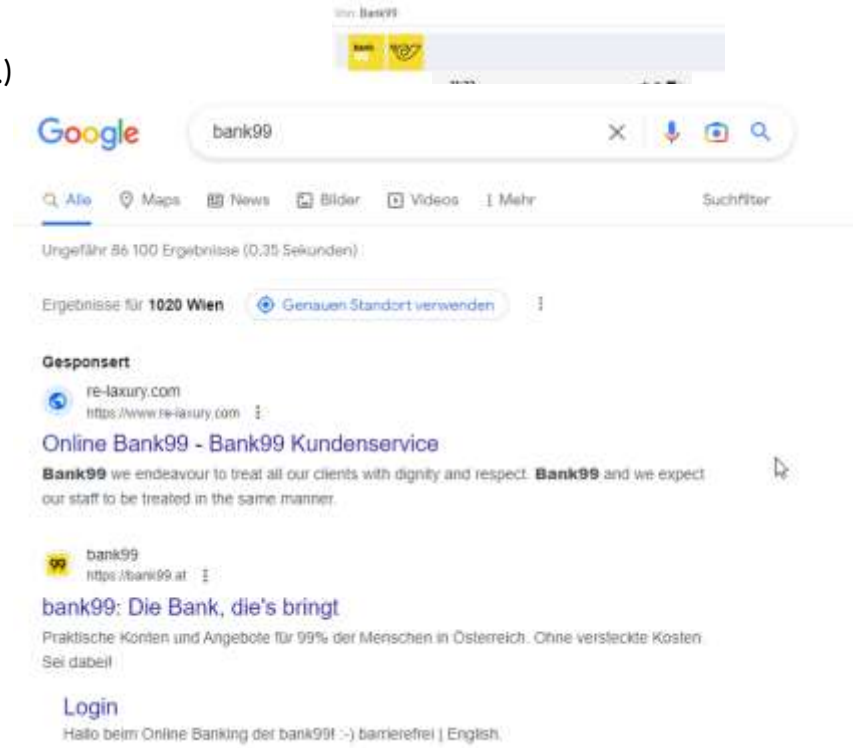
- Höhere Kosten für Phisher
- Gefälschte Absender
- **Extrem effektive** Methode

## 03 Social Media

- Fake Profile auf Facebook & Instagram
- Direkte Kontaktaufnahme mit Opfern

## 04 Search Engine Malvertising

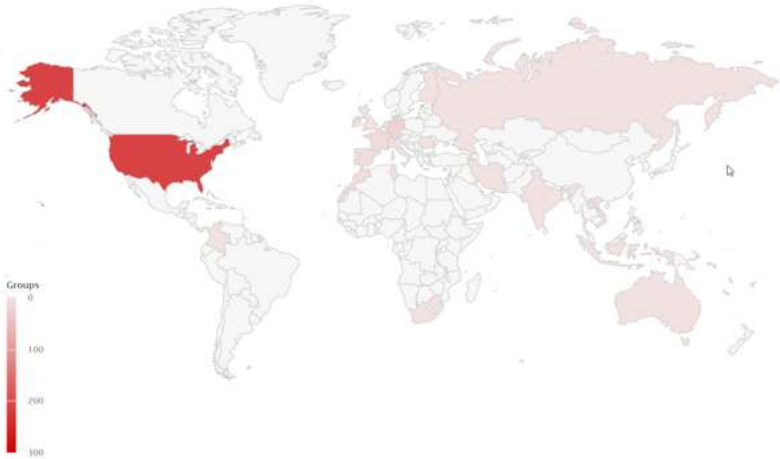
- Google Ads, Bing & andere Online Werbedienste
- **Zielgerichtete Werbung**



# PHISHING – WO/WIE?

**Wo und wie werden die Seiten gehostet?**

- **Top Level Domains**
  - e.g. https://bank99.pro , https://b99.pics , https://meine-bakn99-at.com , ...
- **Kostenlose Dynamic DNS provider**
  - e.g. https://meine99-bank.myvnc.com , https://bank99-at.ddns.net ...
- **Kostenlose Hosting services** (e.g. Google Firebase / Netlify / Blogger.com)
  - e.g. https://okay99-update-2022.web.app , https://meine-bank99.web.app , ...
- **Hacked websites**
  - e.g. https://pnkids.com/bank99/auth.php ,
  - https://dpi-bl.gov.la/bank99 , ...



# PHISHING – IDENTIFIKATION NEUER SEITEN?

## 01 Endkunden

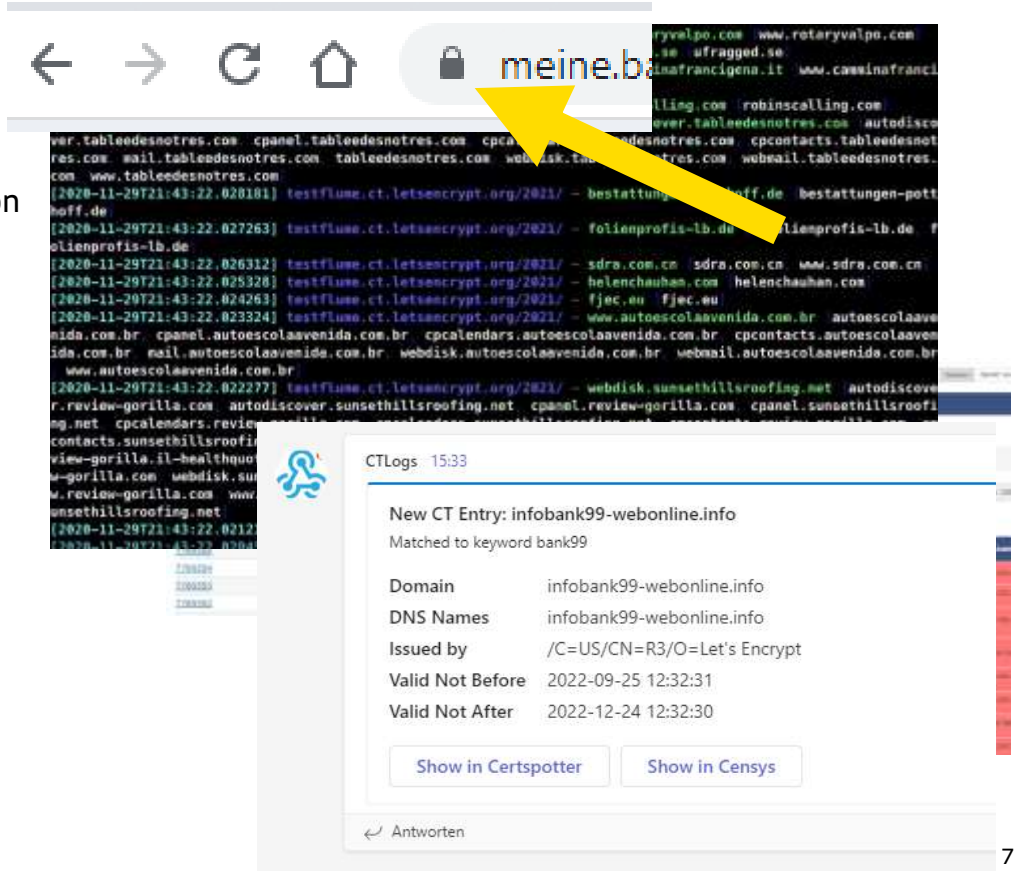
- via Kundendienst oder stop-phishing@
- Stark abhängig von **Awareness** & Kommunikation
- Meist **zu spät**

## 02 Threat Intelligence Provider

- **NetCraft**, Phishtank, …
- Umfangreichere Sicht als über Endkunden
- Verknüpft mit **Blocklisten**

## 03 Certificate Transparency Logs

- Nutzung von **CT-Logs für alle TLS Zertifikate**
- DNS-Twist Algorithmus, > 1500 Zeichenfolgen
- 20 Mio. TLS Zertifikate / Tag
- **Realtime**-Erkennung



# PHISHING – WAS DAGEGEN TUN?

## Block Lists

- Kurzfristige Blockade
- Alle modernen Browser & Mobilgeräte
- **Google SafeBrowsing**
- Microsoft SmartScreen, ESET / McAfee/ Kaspersky, …

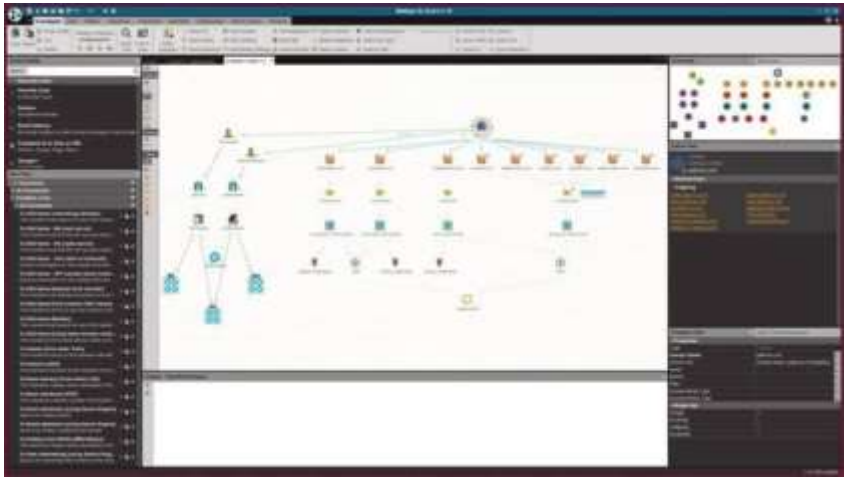

## Takedown

- Via Takedown Provider
  - Fire & Forget
  - „teuer“
- Manuell
  - **Lernprozess!**
  - Kontakt mit
    - Webseiten Betreiber
    - Hosting Provider
    - Domain Registrar
    - andere involvierten Parteien

# WER STECKT DAHINTER?

**Verfügbare Informationen**

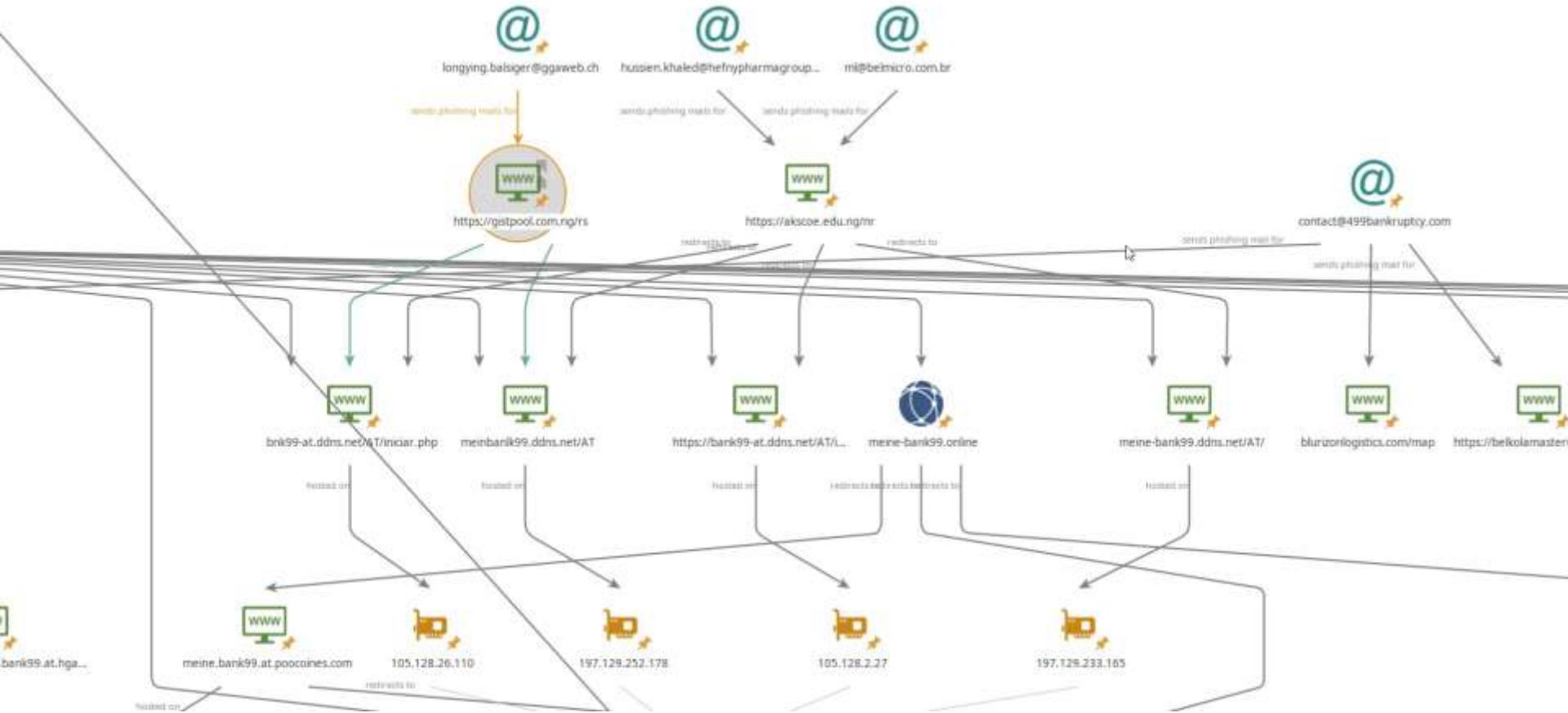
- Emails
- Absender-Adressen
- SMS
- Phishing Seiten
- Informationen zu Phishing Kits



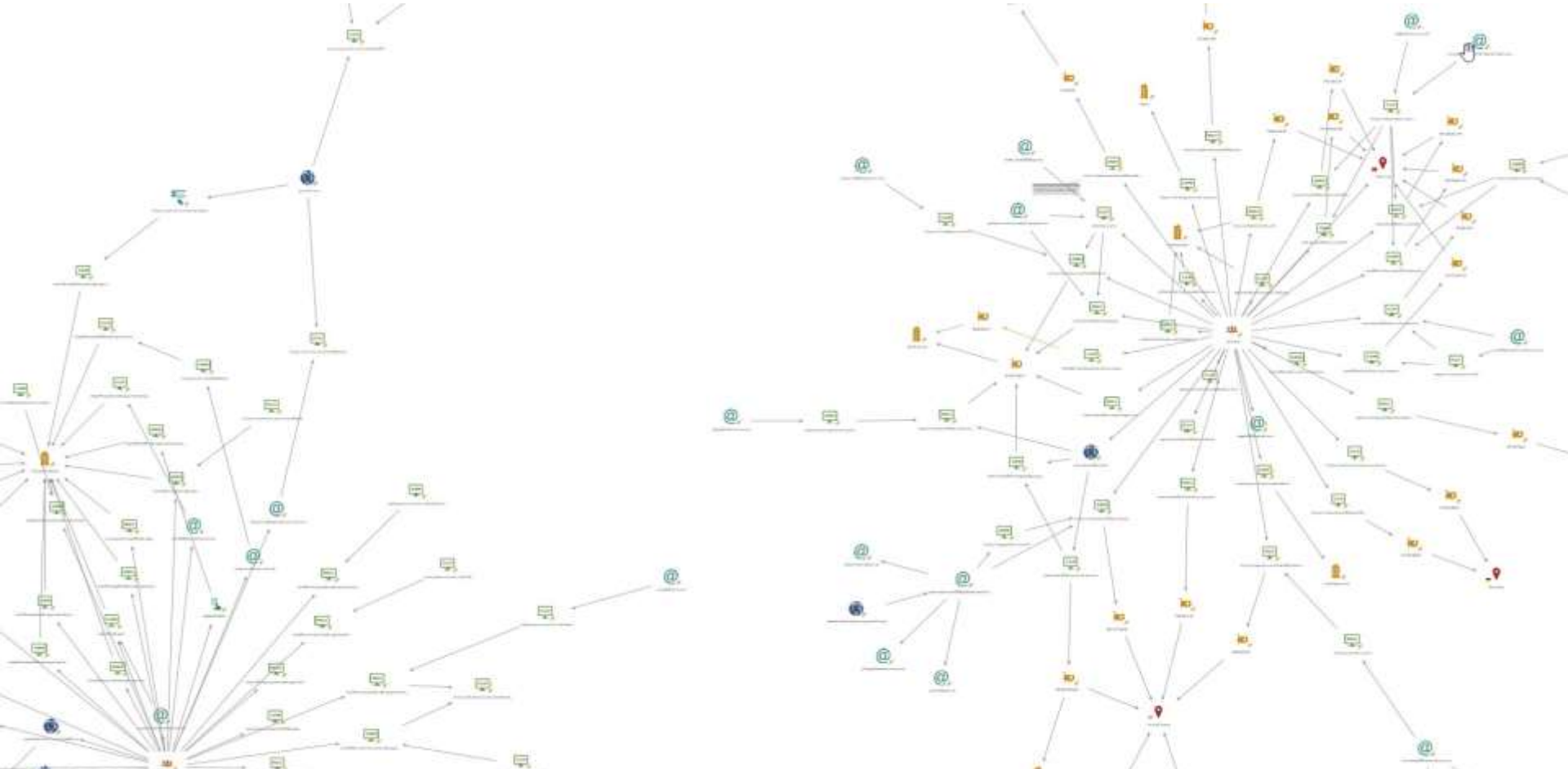
## Maltego

- Threat Graph
- Link Analysis
- Aggregation & Enrichtment
- Data Mining
- OSINT (Open Source Intelligence)

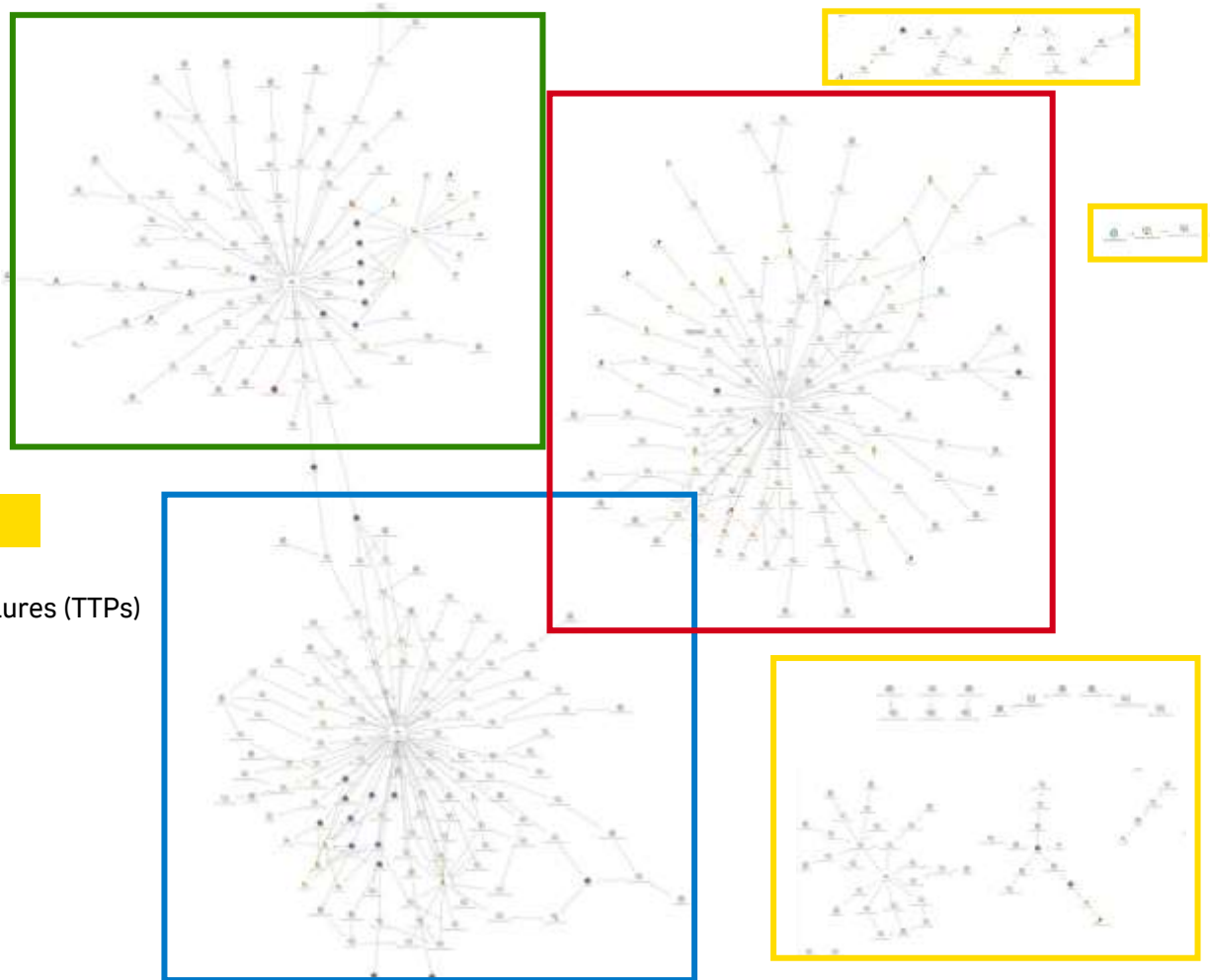
# WER STECKT DAHINTER?



# WER STECKT DAHINTER?



# WER STECKT DAHINTER?



## Threat Actors

- Diverse Gruppen
- Unterschiedliche Tactics, Techniques & Procedures (TTPs)
- Attribution
- Beweismaterial für Strafverfolgungsbehörden
- Threat Intelligence

Einiges initial **nicht eindeutig zuweisbar**!

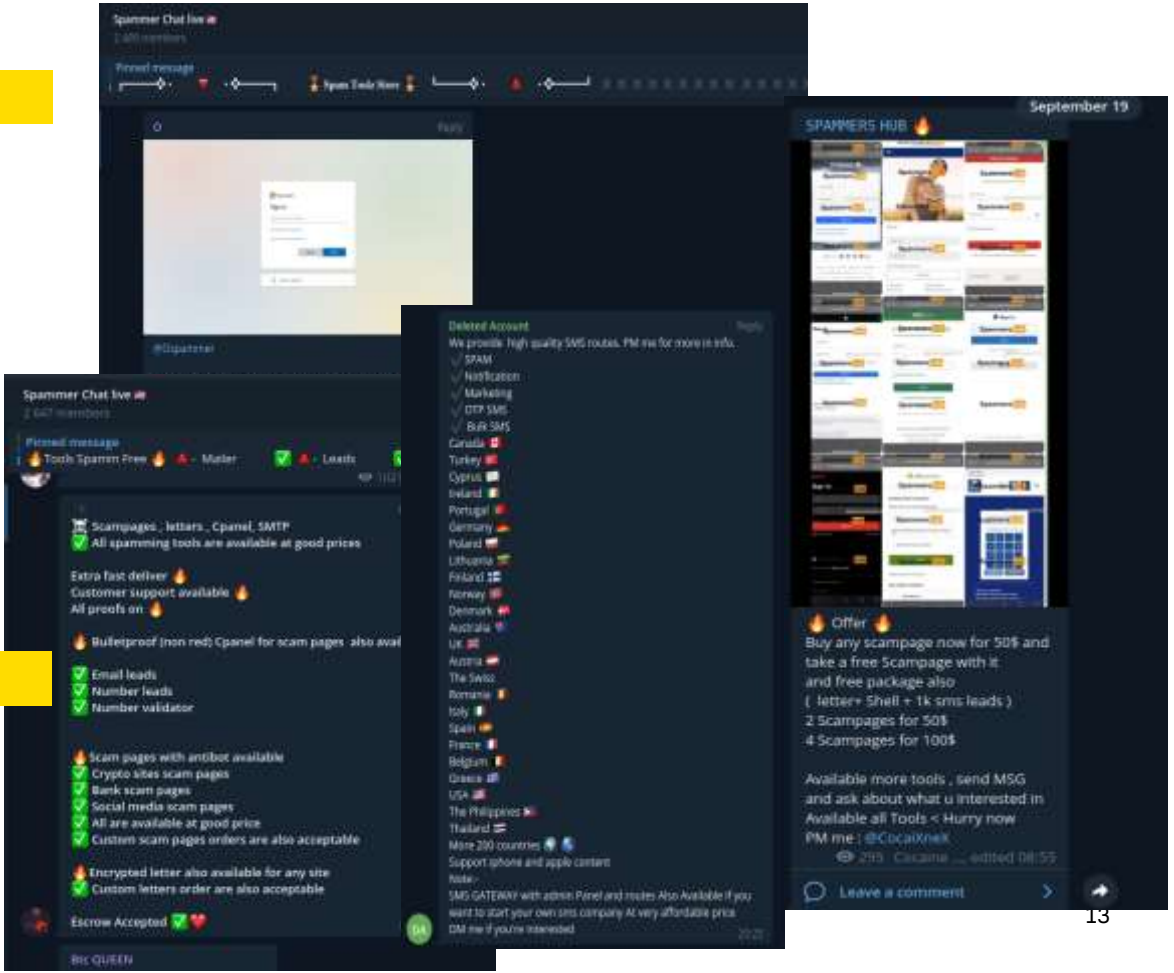
# PHISHER COMMUNITY

**Aktive weltweite community**

- **50+ Telegram-Channels**
  - Austausch zu neuen Opfern
  - Trainings / Seminars
  - Handel mit
    - Hosting
    - Zugriff auf kompromittierte Server, WebShells
    - Dienste
    - Gephishte Konten
    - Free Samples!
    - **Phishing Kits**

**Trusting a scammer?**

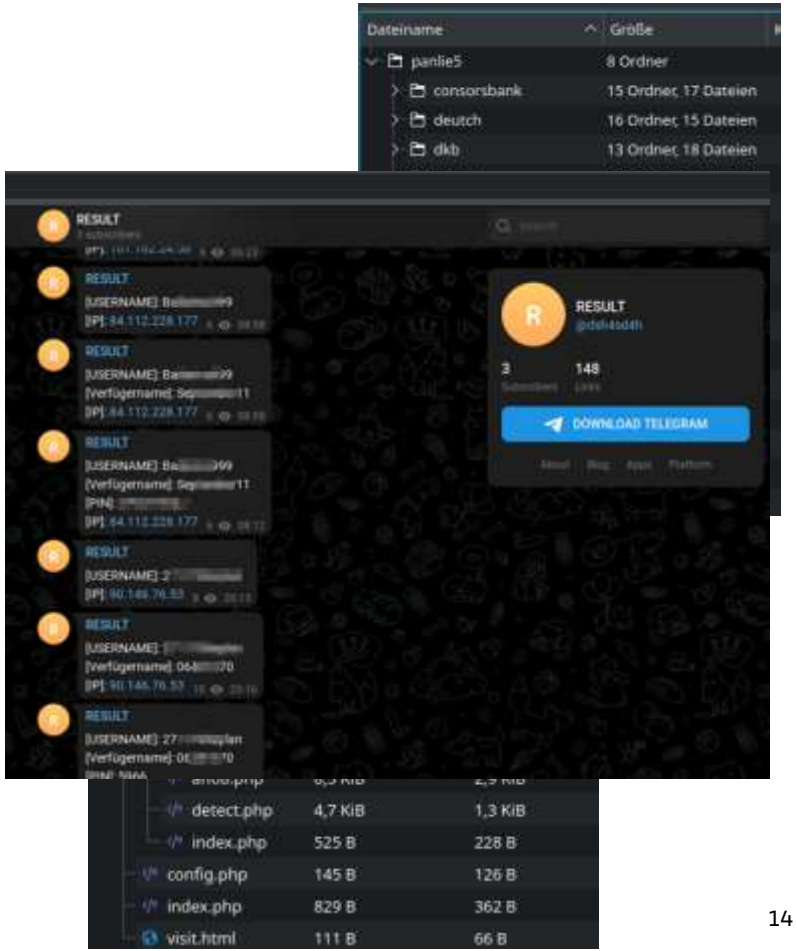
- Treuhänder-Services
- Betrüger werden rausgeworfen



# PHISHING KITS

## The software phishers use

- „von der Stange“ vs Customized
- Speichert/Überträgt Phishing Ergebnisse
  - Telegram
  - Email
  - Lokale Dateien
- **Schutzmaßnahmen**
  - Anti-Bot Detection
  - Geo-IP Blocking
  - Captchas & Blacklists
- Phisher „vergessen“ gelegentlich Phishing Kits (**mangelnde OpSec**)
  - **Schwachstellenanalyse** (100% PHP)
  - Zugriff auf wertvolle Informationen (IPs, Email Adressen, Social Media Informationen, **Telegram Bot Tokens**...)




## Telegram

- Primäres Realtime-Kommunikationsmedium
- Erlaubt manuelles Eingreifen in **2-Faktor authentication**
- Automatisierung
  - Automation via „Bots“ (software robots)
  - **Bot configuration** Teil der Phishing Kits
  - Zugriff auf Echtzeit-Kommunikation der Phisher

# STRIKING BACK!

# SPEED MATTERS

- Welle von ca 30 Seiten nach immer selbem Schema / Naming Convention
- Immer der selbe Software-Stack / Phishing Kit
- Zugriff auf Phishing Seiten und „Rettung“ von 50+ Kunden

**Realtime Alert**
Neue Phishing Seite wird aufgesetzt


13:02

**OpSec**
Phisher lässt„phishing kit“ ein paar Minuten unbeaufsichtigt


13:07

**Analysis**
Source Code Review

13:30

**Access**
Admin Zugriff für bank99

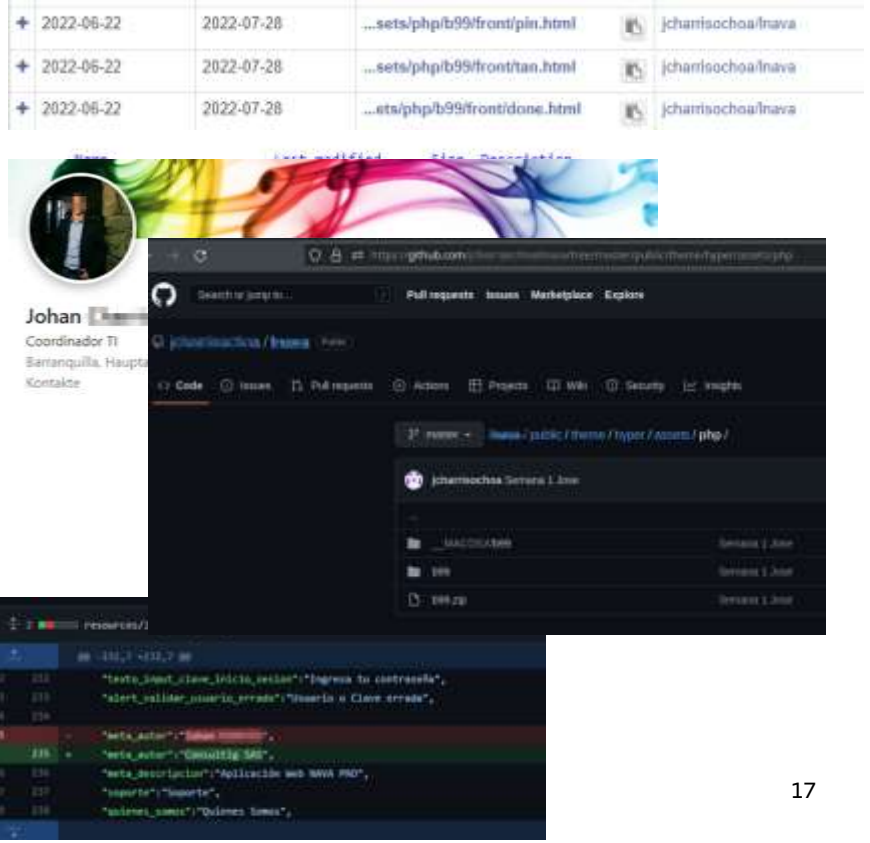
14:10

# PHISHER - OPSEC

- Gruppe „SadCockroach“.
  - Verantwortlich für >180 Phishing Seiten
  - Erste Seiten mit Attribution 03.06.2022
  - Phisher leaked/vergisst „Phishing Kit“ (zip)

- **Github Monitoring** findet Repository mit Code der zum Phishing Kit passt
  - Code wurde 6h später wieder „privat“ gestellt
  - Github Profil enthielt Name + Email Addresse
  - Mac User
  - IT Angestellter aus Baranquilla, Kolumbien

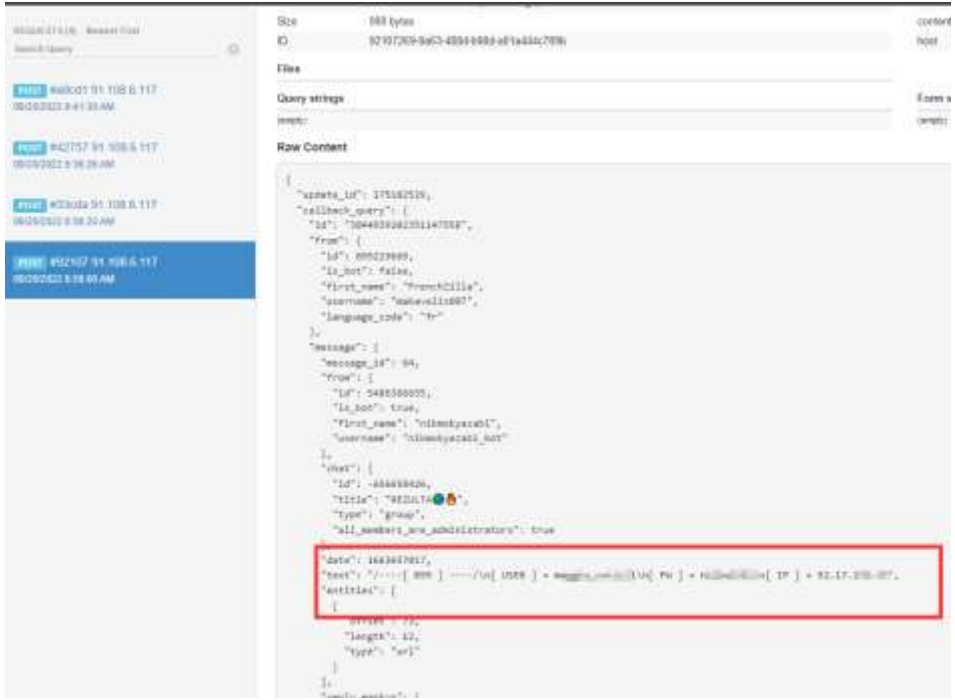
- **2 Wochen später:** Github Profil enthält wieder ein öffentliches Projekt für 2 Tage
  - Gewarteter Quellcode des Phishing Kits
  - Snapshot „b99_praktika.zip“ mit Erststand 21.05.2022
  - Telegram-Bot IDs wie auch auf den aktiven Phishing Seiten
  - Komplettes Repository & History gesichert



# GUERILLA APPROACH

**„Infiltration der Telegram Kanäle“**

- Nutzung von geleakten Telegram-Tokens um sich Zugang zu Phisher-Chats zu verschaffen 😎



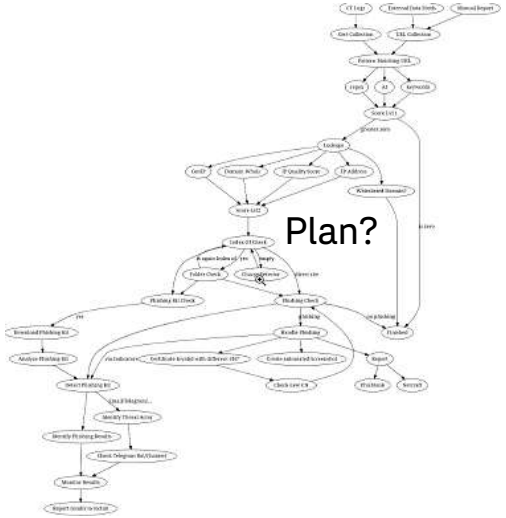

- Echtzeitmeldungen von gephishten Kunden
- Kommunikation zwischen Phishern
- Neue Phishing Seiten & neue Telegram Bots
- Phisher-Smalltalk (inkl. Sprachnachrichten und Fotos)

```
2022-09-05 23:05:46 : Voice voice/file_38.oga
2022-09-05 23:05:22 : Voice voice/file_39.oga
2022-09-05 23:03:06 : Hayad hadi
2022-09-05 22:27:05 : 3sar ghay sifat
2022-09-05 22:26:59 : Ok
2022-09-05 22:26:53 : Code
2022-09-05 22:26:52 : Kantsena
2022-09-05 22:26:49 : Norber
2022-09-05 22:26:45 : ????
2022-09-05 21:27:35 : Hhhhhhh
2022-09-05 21:23:49 : ta maloi ana programmer zbbk
2022-09-05 21:23:38 : chfiha bouton
2022-09-05 21:22:31 : Ma ghat khsar walou ana man 3amarch la kente kliyane
2022-09-05 21:21:44 : Haniaa
2022-09-05 21:19:18 : ??
2022-09-05 21:19:16 : Chi wahed ki bi3 listät nadiyine walou
2022-09-05 21:19:10 : yqlqh zejedt send
2022-09-05 21:19:05 : http://mtzion-ame.org/,eine/meine/
2022-09-05 21:18:55 : Ma jab Allah walou lioum
2022-09-05 19:28:21 : Okay
2022-09-05 19:23:03 : yalah gaditha
2022-09-05 19:21:39 : Alors ??
2022-09-05 19:21:06 : Ales
2022-09-04 18:56:48 : Ok
2022-09-04 18:56:28 : Bot
2022-09-04 18:48:46 : ???
2022-09-04 16:33:16 : I need money
2022-09-04 16:33:08 : Wewe
2022-09-03 23:59:33 : Nn
2022-09-03 23:59:11 : Log
2022-09-03 13:36:16 : Voice voice/file_1.oga
2022-09-03 12:25:52 : Wa 9lawi wa zabi
2022-09-03 12:24:19 : Wa si zab
2022-09-03 12:23:37 : Ma bolch ki waslak had zab
2022-09-03 08:49:06 : T'a9 sand
2022-09-03 08:49:00 : Bakbouki
2022-09-02 21:53:37 : ok
2022-09-02 21:53:32 : Hani jay hayed
2022-09-02 21:53:21 : oui
2022-09-02 21:53:10 : Kayne sand gmx Alor
```

# SCALING UP!

**Lassen sich derartige Steps skalieren?**

- **Annahmen:**
  - Phisher agieren global auf gleiche Weise
  - Erkennung von bank99 Phishing Seiten funktioniert auch für andere
  - Maßnahmen lassen sich **automatisieren**




**Validierung & Short Term Incentive**

- NetCraft als Benchmark
- **Gratis Tasse!**

The current list of prizes is as follows:

| Prize | Number of validated reports |
|---|---|
| Netcraft USB Flash Drive | 100 |
| Netcraft Branded Mug | 250 |
| Netcraft T-Shirt | 500 |
| Targus Laptop Backpack | 1000 |
| iPad | 5000 |

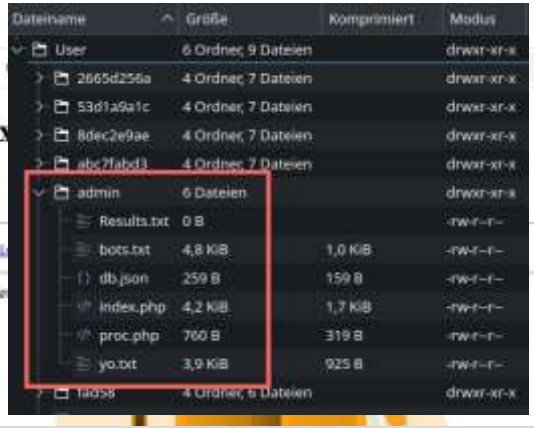
# GLOBAL SCOPE

**Do phishers act the same globally?**

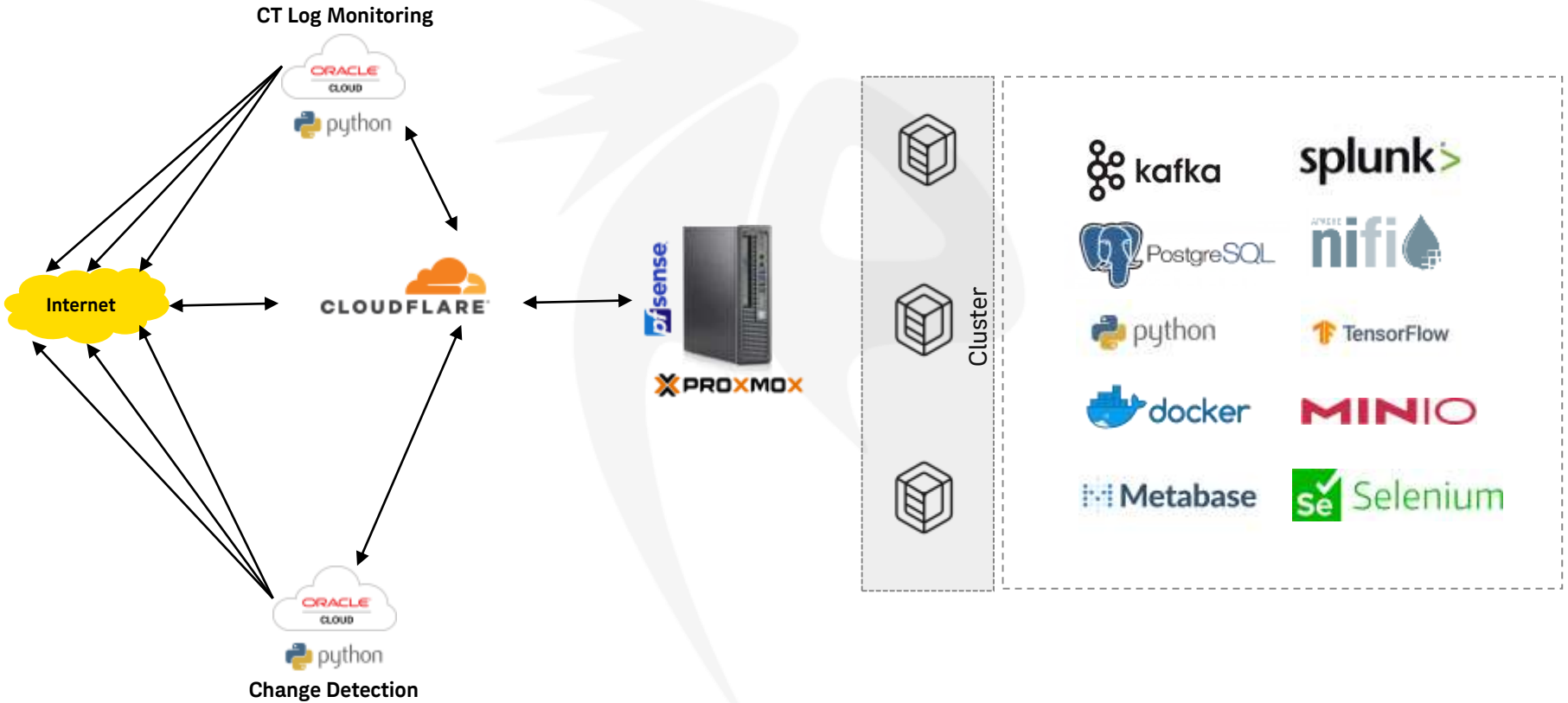
- OpSec bei Phishern allgemein schwach ausgeprägt
- autom. **Sammlung von Phishing Kits**
  - **> 1400 unique Kits** seit August
    - 50% US Banken
    - 30% Amazon, Netflix, Microsoft, Facebook, ...
    - 20% Rest (EU Banken, Post & Paketdienste), ...

- **Analyse der Kits**
  - Admin-Panels oft mit default-Zugangsdaten
  - Phishing-Ergebnisse oft in Klartext-Files
  - Klassifikation / Fingerprinting der Kits

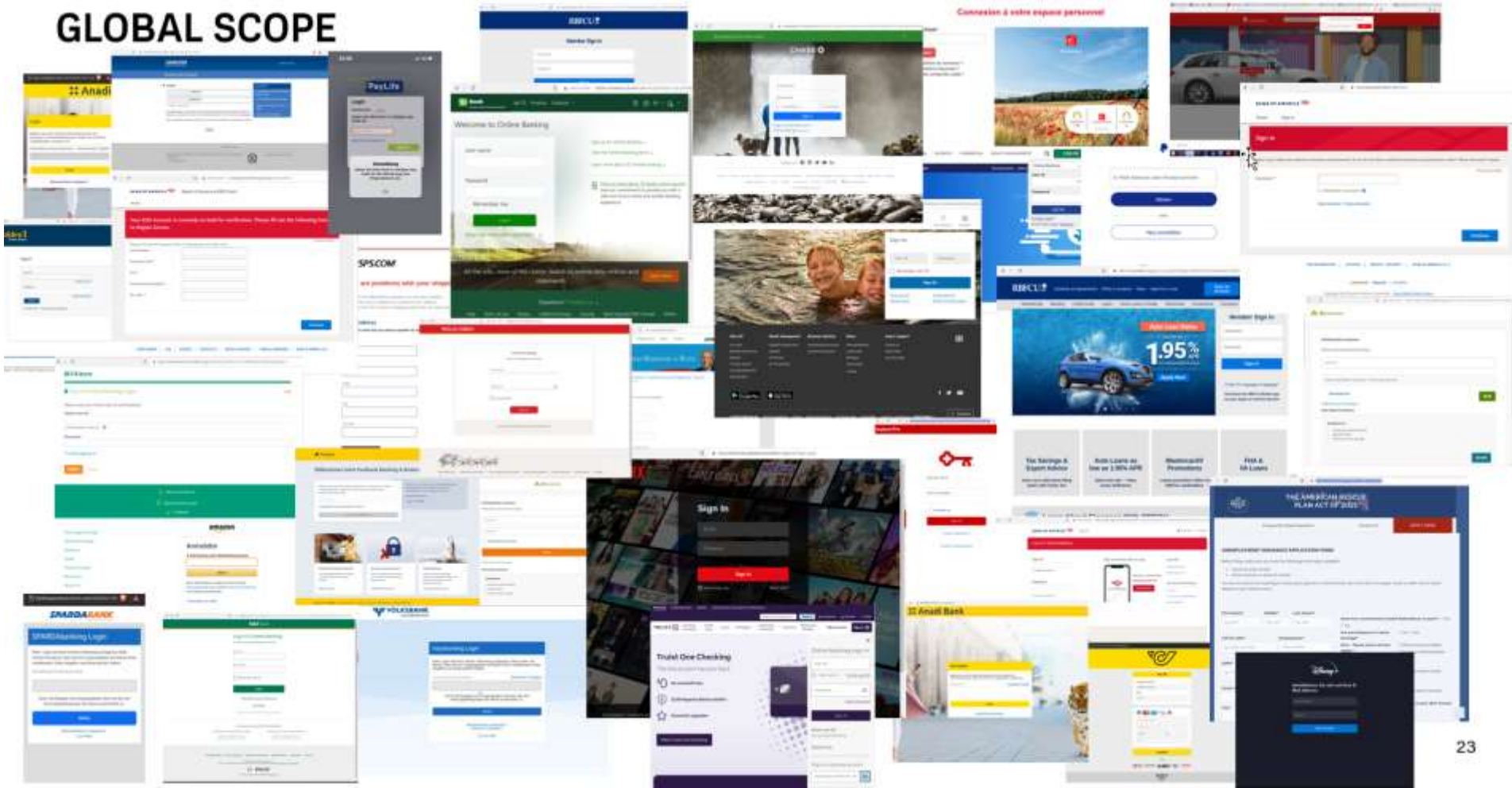
- **Abwehrmechanismen verstehen**
  - Eigene IP Reputation Services (VPN, Residential, ...)
  - Umgehung von Anti-Bot Maßnahmen oft einfach
  - Fake-Fehlermeldungen (HTTP 404, HTTP 500, Suspended, ..)



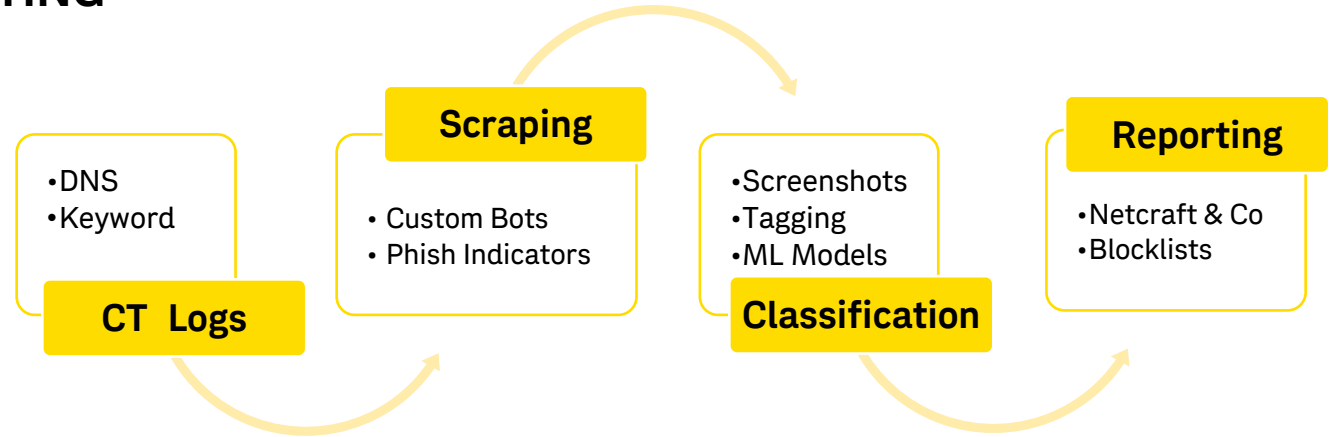

# DIY


CT Log Monitoring
ORACLE CLOUD
python
Internet
CLOUDFLARE
pfsense
PROXMOX
Cluster
kafka
splunk>
PostgreSQL
nifi
python
TensorFlow
docker
MINIO
Metabase
Selenium
ORACLE CLOUD
python
Change Detection

# GLOBAL SCOPE



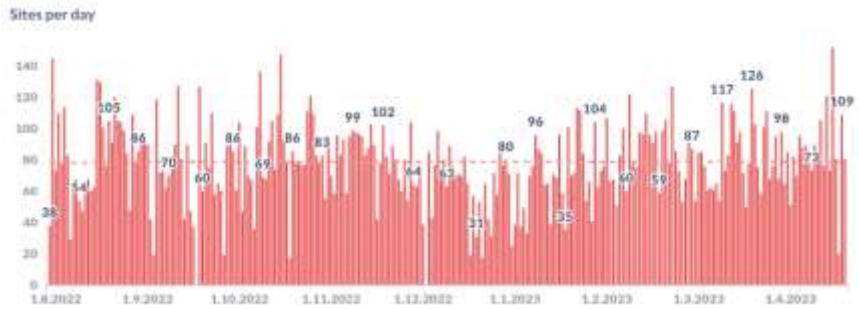
# AUTOMATING




**Proof of Concept – (seit August 2022)**

- **> 20.000** Malicious Sites
- 85 Phishing Seiten / Tag
- **> 10.000** Credited

- **17%** von Netcraft als **„No Threat“** identifiziert



# LESSONS LEARNED

## 01 Speed is king!

- Geschwindigkeit macht den Unterschied
- Near-Realtime Aktionen können Enduser retten
- Lebensdauer von Seiten oft < 24h

## 02 Improvise, Adapt, Overcome

- **Phisher ändern Taktik** sobald diese nicht mehr Effektiv
- Keine Garantie, dass Maßnahmen nachhaltig funktionieren

## 03 Asymmetric Warfare

- Phishing leicht umzusetzen
- Phishing Kits leicht verfügbar
- Phisher die aufrüsten (Automatisierung, DevOps, ..) – **Unstoppable**!

## 04 „Protect your Family“

- Home IP nach ca 3 Wochen nachhaltig in IP Blacklist der Phisher (d.h gesperrt)
- VPNs beinahe unbrauchbar
- Mobile / 4G als alternative

# Fragen