Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

CISO Sprechstunde

06.03.2024

Ihre Fragen?

Ihre Themen?

Informationssicherheit aktuelles

Darknet Footprint
- Russian Market
- Sind Passwörter noch zeitgemäß?
- Botnet @ FAU?

SOCRadar

Black Market | Botnet Data | PII Exposure | IM Content | Suspicious Content

Black Market ID	Source	Stealer Log Preview	Related Assets	Price	Status
Market-26927646	Russian Market	Open Preview	remote.cip.cs.fau.de, katalog.fau.de, ...	10.00 $	Action Waiting
Market-26927585	Russian Market	Open Preview	studon.fau.de, campo.fau.de	10.00 $	Action Waiting
Market-26927552	Russian Market	Open Preview	est.cs.fau.de	10.00 $	Action Waiting
Market-26927525	Russian Market	Open Preview	campo.fau.de	10.00 $	Action Waiting
Market-26786564	Russian Market	Open Preview	groupware.fau.de, campo.fau.de	9.00 $	Action Waiting
Market-26786537	Russian Market	Open Preview	campo.fau.de, faumail.fau.de	10.00 $	Action Waiting
Market-26786519	Russian Market	Open Preview	faumail.fau.de	10.00 $	Action Waiting
Market-26782780	Russian Market	Open Preview	adfs.fauad.fau.de, remote.cip.cs.fau.de, ...	5.00 $	Action Waiting

SOCRadar

Account kostet 100,- $

Infected Device - Accounts for "fau.de" were observed for sale on the Russian Market, On Jan 26, 2024

● Russian Market Bot - 2024 Jan 26 10:54 UTC

alibaba | platinum | india | net | android | ...


```
{
  "country": "IN",
  "date": "2024.01.23",
  "files": "archive.zip",
  "id": "14732690",
  "isp": "Bharti Airtel Ltd.",
  "links": [
    "flipkart.com",
    "joinindiannavy.gov.in",
    "idm.fau.de",
    "recruitment-portal.in",
    "flyclient.fvcorp.com",
    "...
```

4578 User/Passwörter Kombinationen mit FAU-Bezug

uni-erlangen.de und fau.de

	Source	Passworc
@fau.de	Hacker Forum	Flo15081
suad.fau.de	Hacker Forum	Anturredc
fau.de	Hacker Forum	xiaobao.(
v@fau.de	Hacker Forum	passworc
AUAD.FAU.DE	Hacker Forum	Faude@
ad.fau.de	Hacker Forum	Faude@
fau.de	Hacker Forum	Alepo933
fau.de	Hacker Forum	Alepo933
n@fau.de	Hacker Forum	[UNKNO
aei@fau.de	Hacker Forum	[UNKNO
aei@fau.de	Hacker Forum	JWKGU

PII

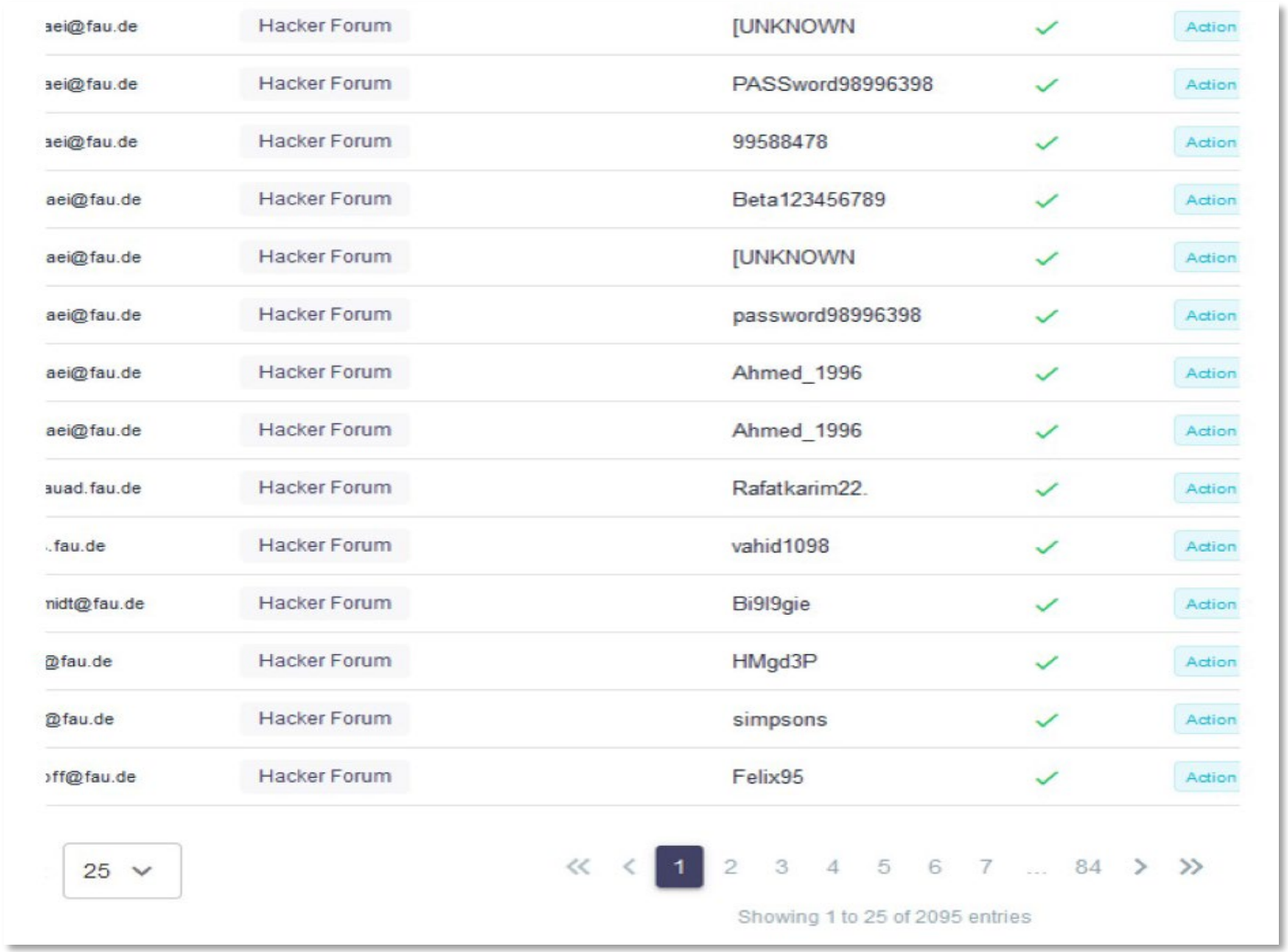
rum l2e3ra Action Waiting

1 2 3 4 5 6 7 ... 184

Showing 1 to 25 of 4578 entries

2095 User/Passwörter Kombinationen mit fau.de

fau.de



aei@fau.de	Hacker Forum	[UNKNOWN	✓	Action
aei@fau.de	Hacker Forum	PASSword98996398	✓	Action
aei@fau.de	Hacker Forum	99588478	✓	Action
aei@fau.de	Hacker Forum	Beta123456789	✓	Action
aei@fau.de	Hacker Forum	[UNKNOWN	✓	Action
aei@fau.de	Hacker Forum	password98996398	✓	Action
aei@fau.de	Hacker Forum	Ahmed_1996	✓	Action
aei@fau.de	Hacker Forum	Ahmed_1996	✓	Action
auad.fau.de	Hacker Forum	Rafatkarim22.	✓	Action
.fau.de	Hacker Forum	vahid1098	✓	Action
nidt@fau.de	Hacker Forum	Bi9l9gie	✓	Action
@fau.de	Hacker Forum	HMgd3P	✓	Action
@fau.de	Hacker Forum	simpsons	✓	Action
ɔff@fau.de	Hacker Forum	Felix95	✓	Action

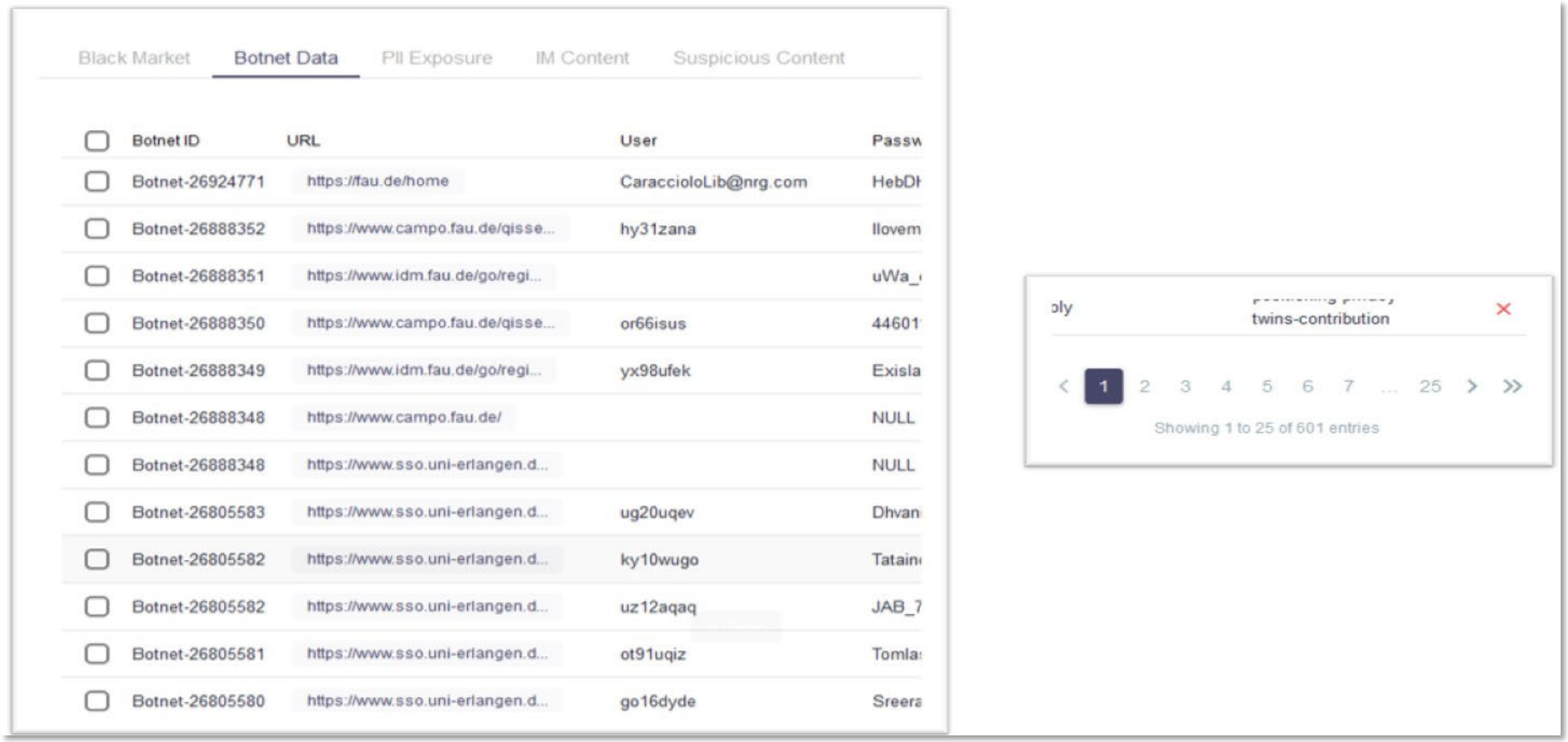
25 ⌄

« ‹ 1 2 3 4 5 6 7 ... 84 › »

Showing 1 to 25 of 2095 entries

601 FAU-Findings im Zusammenhang mit Botnets

uni-erlangen.de und fau.de



Actionable Threat Intelligence

120

alerts have been generated

Industry:
Country: Germany
API Integration: Active
Modules: AttackMapper | RiskPrime | ThreatFusion

Dark Web Findings

513
Mentions in Threat Actor Communication Channels

Malware-Bot Infection Threats

508
Bot-infected Users Posing a High Data Breach Risk

Phishing Intelligence

0
Potential Phishing Domains

Social Media Brand Reputation Threats

5
Impersonating Social Media Profiles

Leaked Employee Login Credentials

4543
Compromised Employee Login Credentials

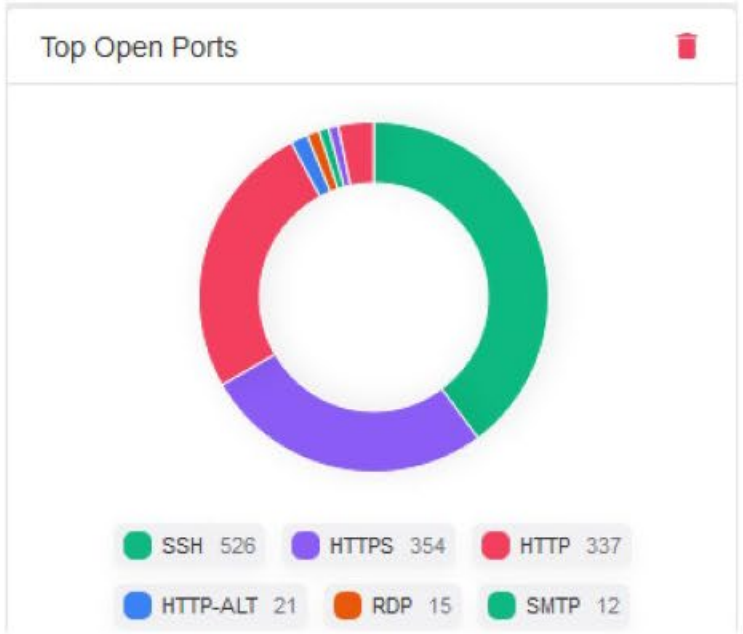
Critical Asset Exposure & Vulnerabilities

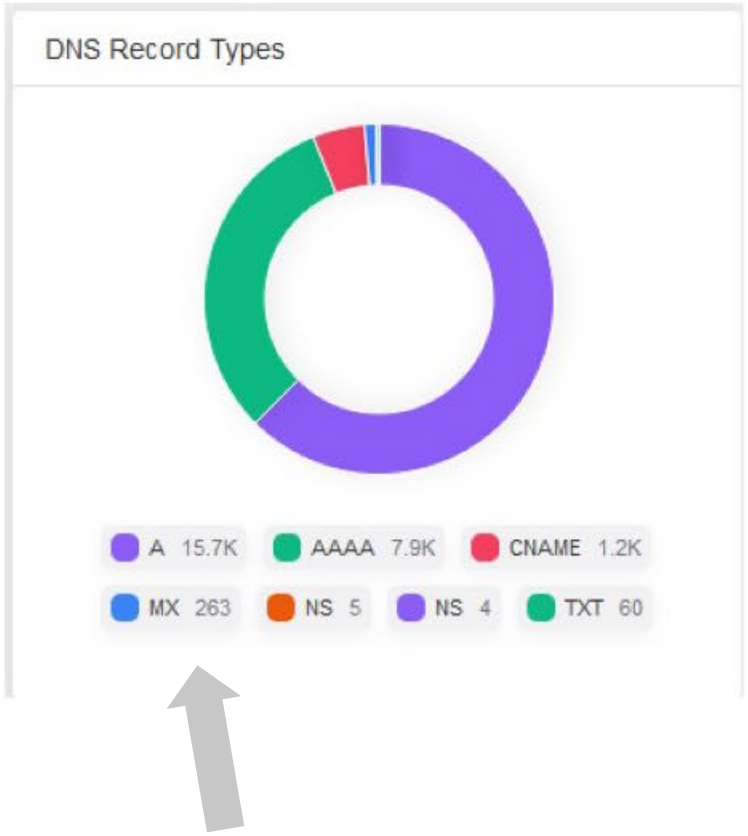
64201
External-Facing Digital Assets

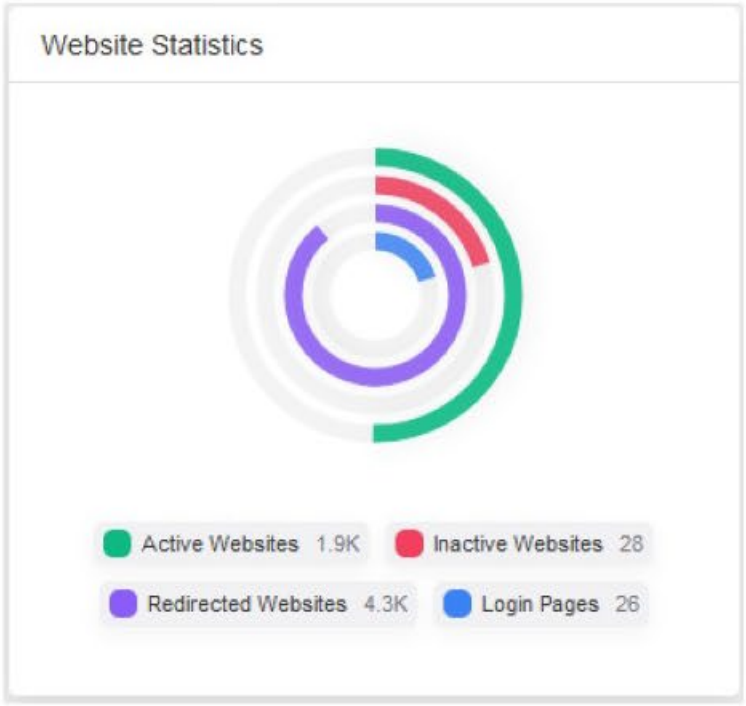
Mailserver

RDP

SOCRadar


Top Open Ports
SSH 526
HTTPS 354
HTTP 337
HTTP-ALT 21
RDP 15
SMTP 12


DNS Record Types
A 15.7K
AAAA 7.9K
CNAME 1.2K
MX 263
NS 5
NS 4
TXT 60


Website Statistics
Active Websites 1.9K
Inactive Websites 28
Redirected Websites 4.3K
Login Pages 26

MX Records

ffeekasse.iuk.fsi.uni-erlangen.de	131.188.40.90	443 80
-3.zuv.uni-erlangen.de	131.188.61.25	
nformatik.uni-erlangen.de	131.188.36.61	
.informatik.uni-erlangen.de	131.188.30.236	22
mmerfest.techfak.uni-erlangen.de	131.188.40.90	443 80
sik.uni-erlangen.de	131.188.16.206	443 80
l.biologie.uni-erlangen.de	131.188.171.53	
ubert-3.viro.med.uni-erlangen.de	131.188.178.56	
.biologie.uni-erlangen.de	131.188.170.165	
ngmt.rrze.uni-erlangen.de		
-pc.zew.uni-erlangen.de		
or-2.ltt.uni-erlangen.de	131.188.228.245	
npkins.webspace.rrze.uni-erlangen.de	131.188.16.201	80 443

InfoSec Richtlinie an der FAU - Teil 2

Informationssicherheit

Richtlinien und Regeln