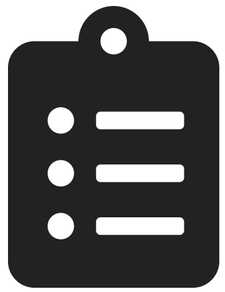
HONEYPOTOK

MÉZ MELLETT FULLÁNKOT IS TALÁLNI

miért

honeypot

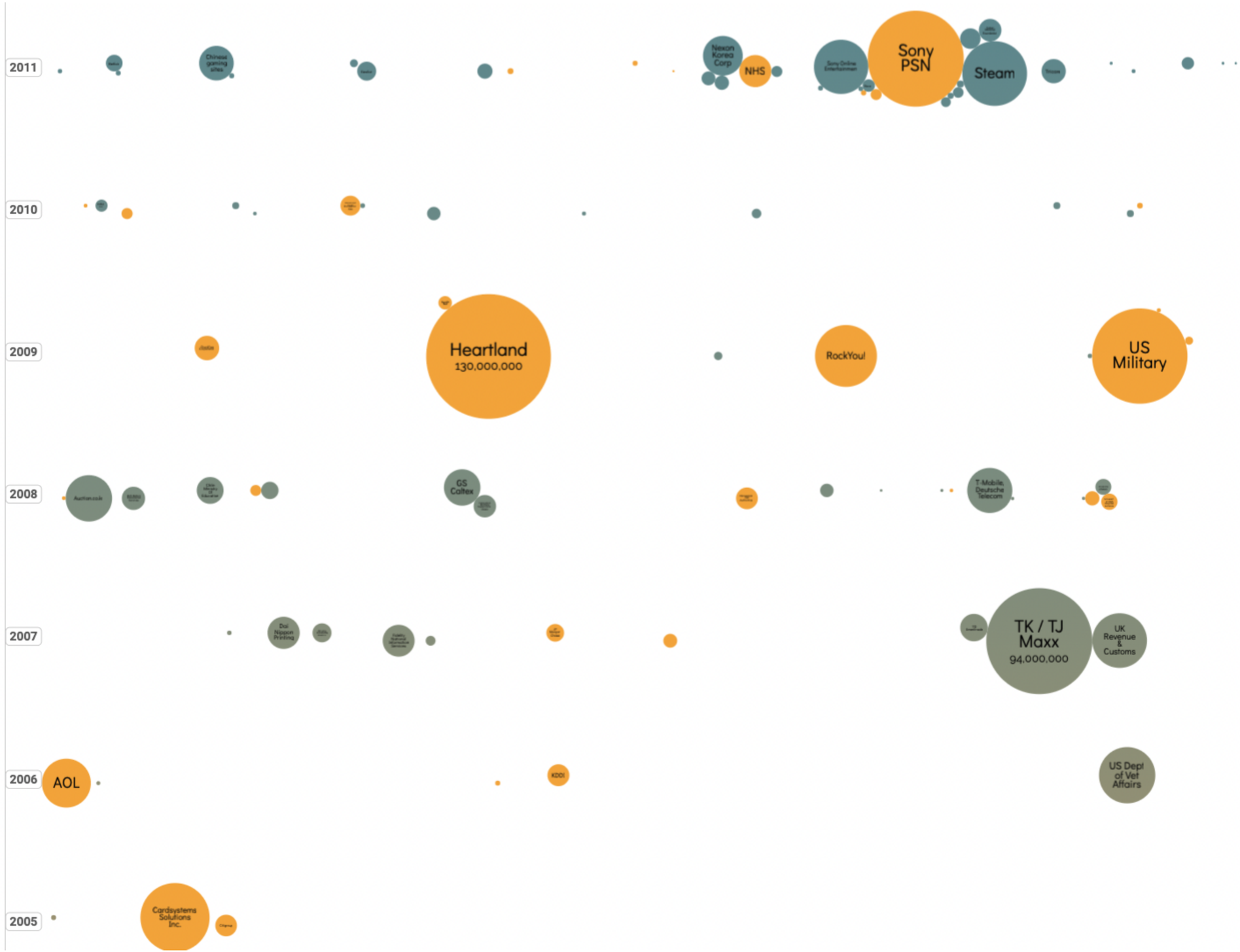


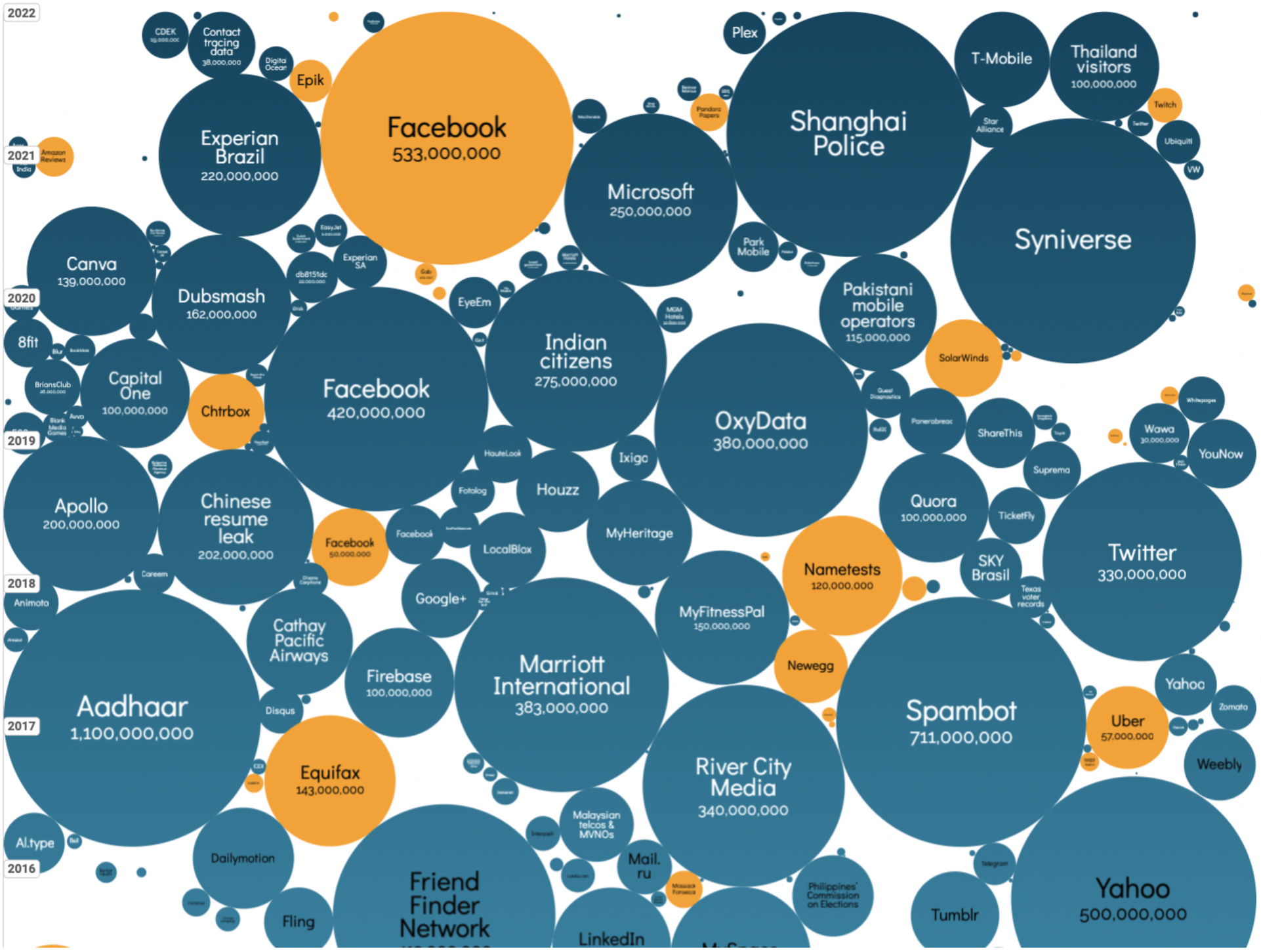
gyakorlatban

fejlesztés

AGENDA

MIÉRT?


2011
Chinese gaming sites
Nexon Korea Corp
NHS
Sony PSN
Steam
2010
2009
Heartland
130,000,000
RockYou!
US Military
2008
GS Caltex
T-Mobile, Deutsche Telecom
2007
Dai Nippon Printing
TK / TJ Maxx
94,000,000
UK Revenue & Customs
2006
AOL
KDDI
US Dept of Vet Affairs
2005
Cardsystems Solutions Inc.


2022
2021
2020
2019
2018
2017
2016
CDEK
Contact tracing data
38,000,000
Digital Ocean
Epik
Facebook
533,000,000
Plex
Shanghai Police
T-Mobile
Thailand visitors
100,000,000
Twitch
Twitter
Ubiquiti
VW
Star Alliance
Experian Brazil
220,000,000
Amazon Reviews
India
Pandora Papers
Microsoft
250,000,000
Park Mobile
Syniverse
Canva
139,000,000
Dubsmash
162,000,000
EasyJet
Experian SA
db8151dc
EyeEm
MGM Hotels
Pakistani mobile operators
115,000,000
SolarWinds
8fit
BriansClub
Capital One
100,000,000
Chtrbox
Facebook
420,000,000
Indian citizens
275,000,000
OxyData
380,000,000
Quest Diagnostics
Panerabread
ShareThis
Suprema
Wawa
30,000,000
Whitepages
YouNow
Blank Media Games
Avvo
HauteLook
Houzz
Fotolog
Ixigo
Apollo
200,000,000
Chinese resume leak
202,000,000
Careem
Facebook
50,000,000
LocalBlox
MyHeritage
Google+
Quora
100,000,000
TicketFly
SKY Brasil
Texas voter records
Twitter
330,000,000
Nametests
120,000,000
Animoto
Cathay Pacific Airways
Firebase
100,000,000
Marriott International
383,000,000
MyFitnessPal
150,000,000
Newegg
Aadhaar
1,100,000,000
Disqus
Equifax
143,000,000
River City Media
340,000,000
Spambot
711,000,000
Uber
57,000,000
Yahoo
Zomata
Weebly
Al.type
Dailymotion
Fling
Friend Finder Network
Malaysian telcos & MVNOs
Mail. ru
Philippines' Commission on Elections
Tumblr
Yahoo
500,000,000
LinkedIn

ELTERJEDT VÉDELMI MEGOLDÁSOK

IDS

TŰZFAL

IPS

VPN

DMZ

FORGALOMELEMZÉS

MERRE INDULNÁTOK?

MI AZ A HONEYPOT?

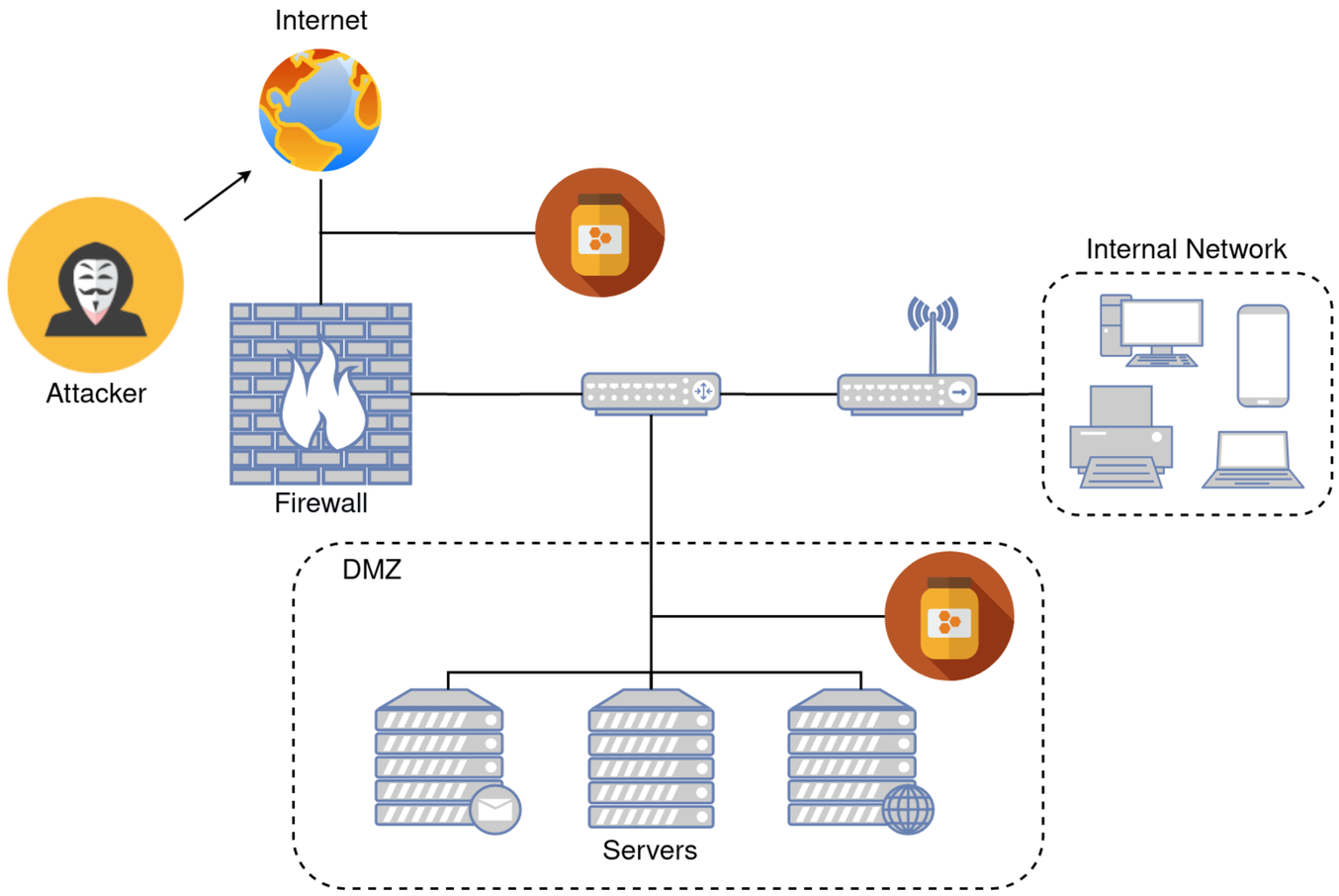
> IT biztonsági mechanizmus, amely az információs rendszerek illetéktelen használatára vonatkozó kísérletek észlelésére, elhárítására vagy valamilyen módon ellensúlyozására szolgál.

HONEYPOTOK ISMERTETÉSE

- szimulált szolgáltatások
- csapdarendszer
- sérülékenynek mutatja magát
- monitorozza a támadó tevékenységét

FELHASZNÁLÁSI LEHETŐSÉGEK

- Időhúzás
- Belső hálózat vizsgálata
- Fekete lista kialakítás
- IDS/IPS fejlesztése
- Security Informations and Event Management rendszer táplálása



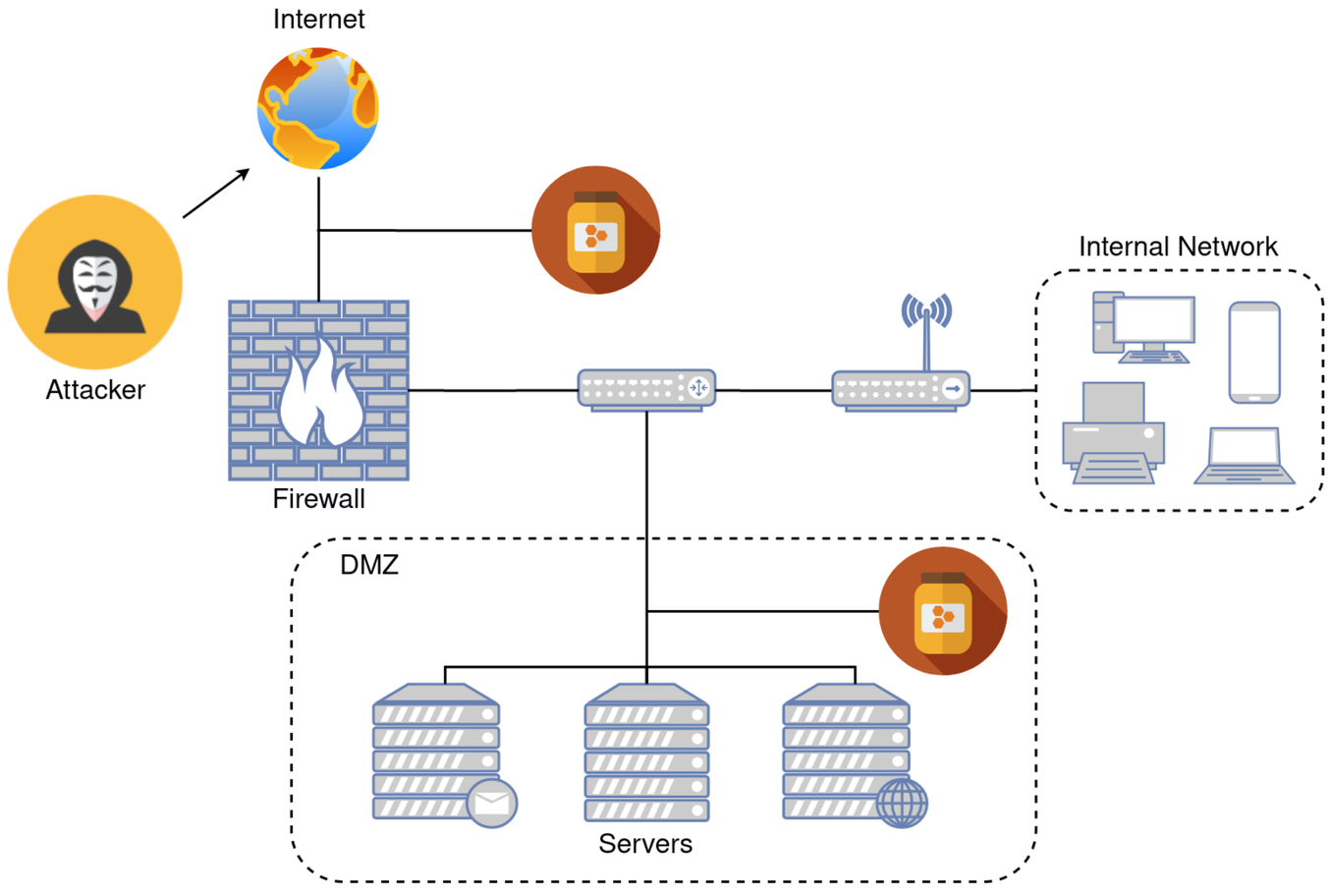
CSOPORTOSÍTÁSUK

CÉLJUK SZERINT

- Kutatási
- Vállalati - "*Production*"

INTERAKCIÓ SZERINT

- Alacsony
- Közepes
- Magas

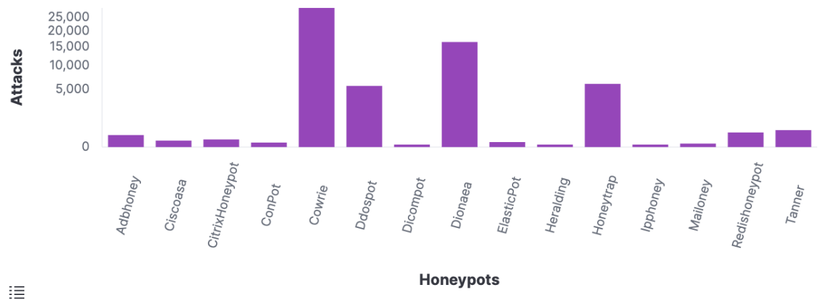


GYAKORLATBAN

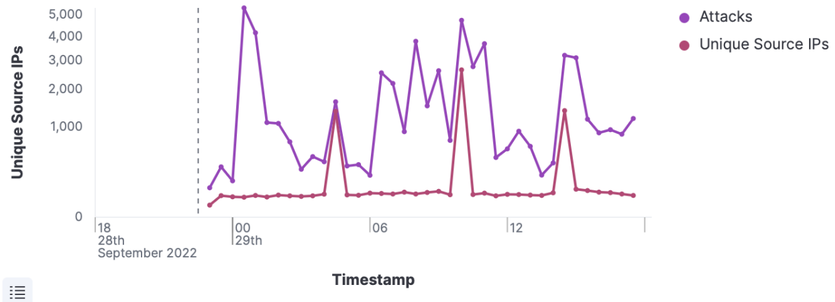
Honeypot Attacks - Top 10

28,721	16,378	5,924	5,551	426	316	214	86	62	37
Cowrie - Attacks	Dionaea - Attacks	Honeytrap - Attacks	Ddospot - Attacks	Tanner - Attacks	Redishoneypot - Attacks	Adbhoney - Attacks	CitrixHoneypot - Attacks	Ciscoasa - Attacks	ElasticPot - Attacks

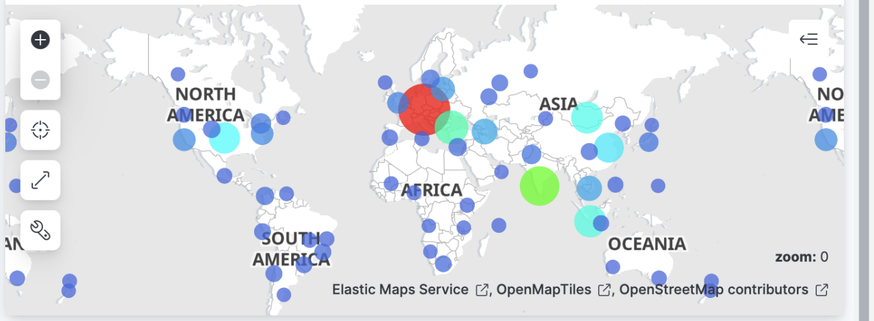
Honeypot Attacks Bar



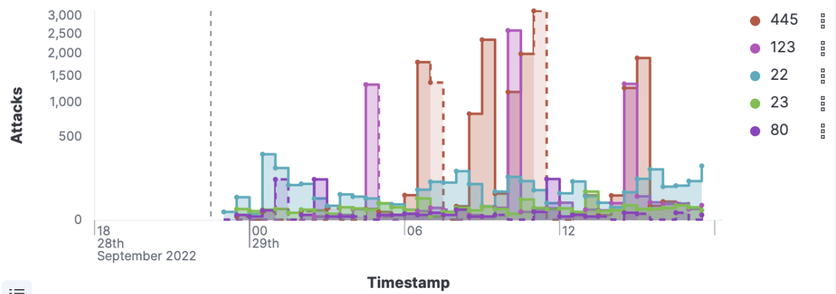
Honeypot Attacks Histogram



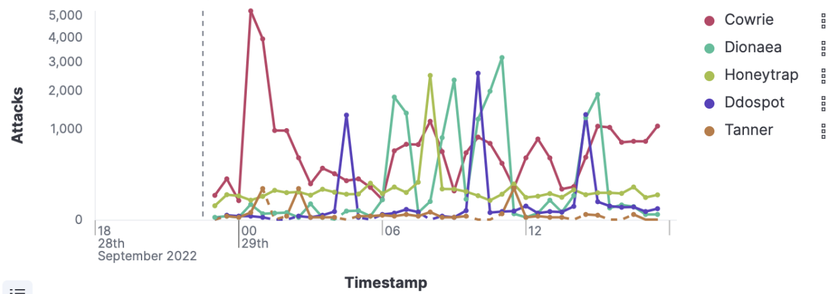
Attack Map - Dynamic



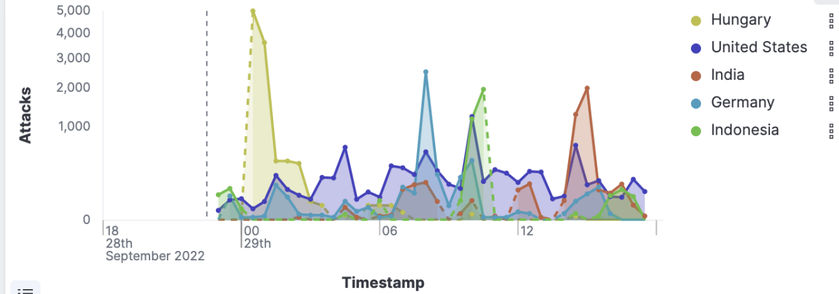
Attacks by Destination Port Histogram



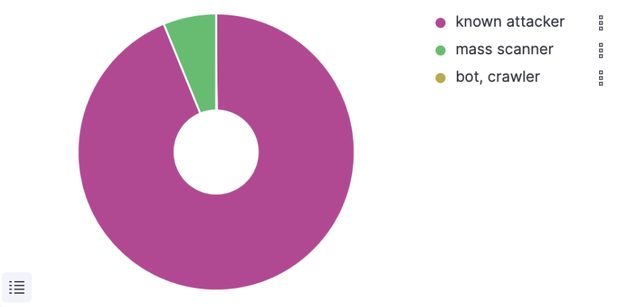
Attacks by Honeypot Histogram



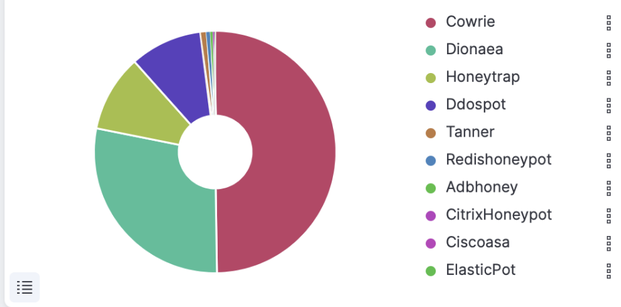
Attacks by Country Histogram



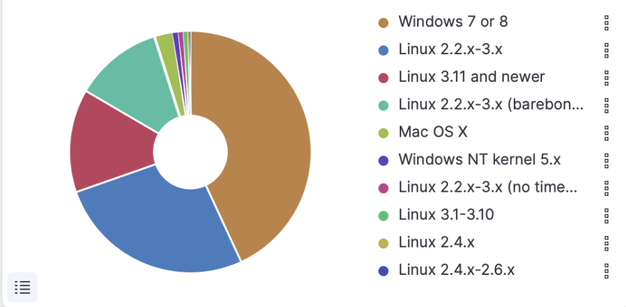
Attacker Src IP Reputation



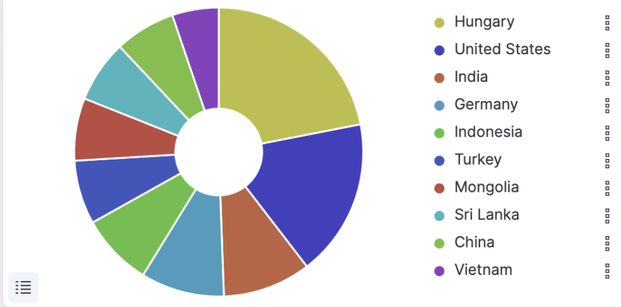
Attacks by Honeypot



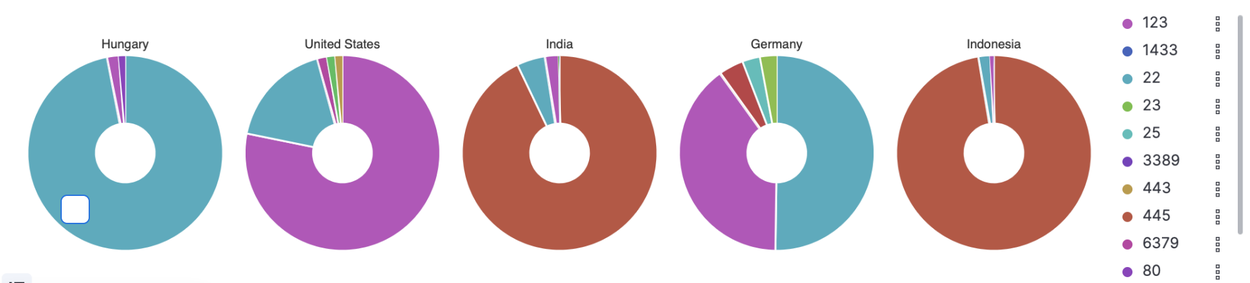
POf OS Distribution



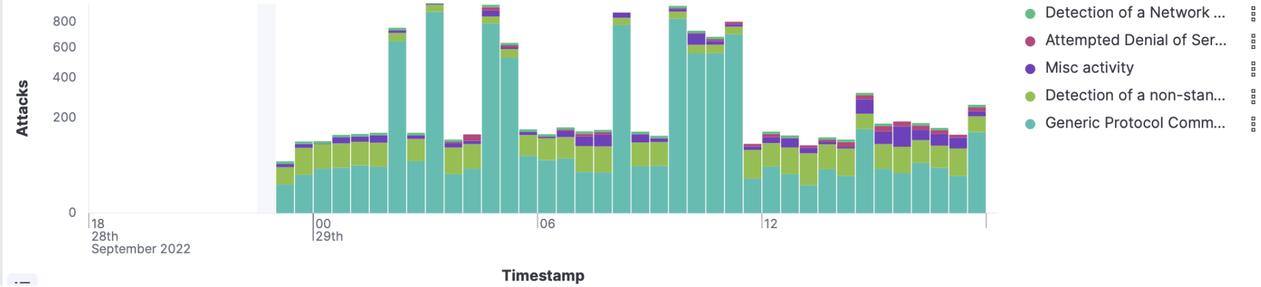
Attacks by Country



Attacks by Country and Port



Suricata Alert Category Histogram



Cowrie Attacks Bar

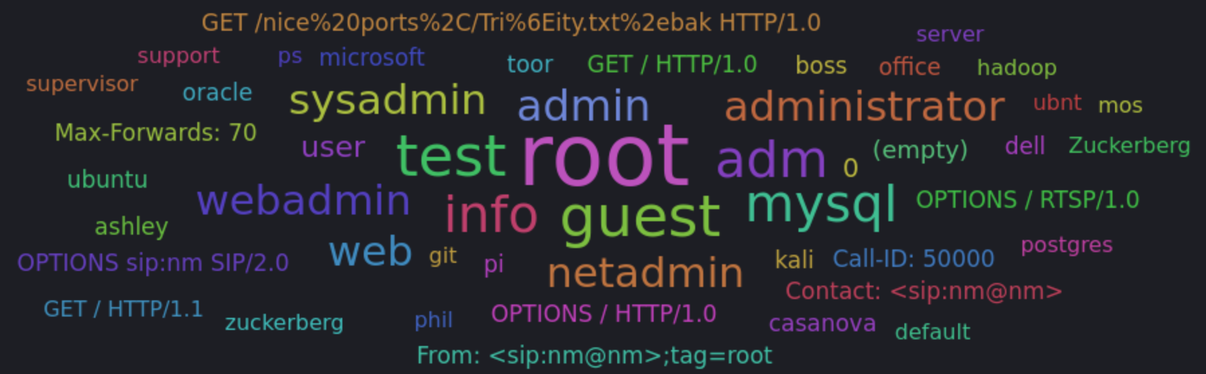
Cowrie Attacks

377,927
Attacks

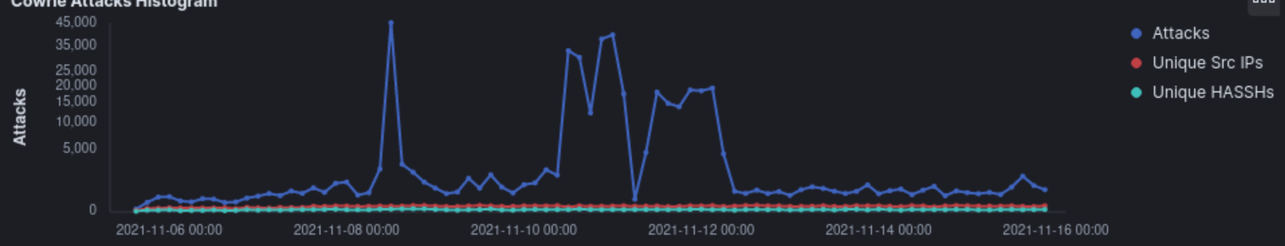
1,267
Unique Src IPs

41
Unique HASSHs

Cowrie Username Tagcloud

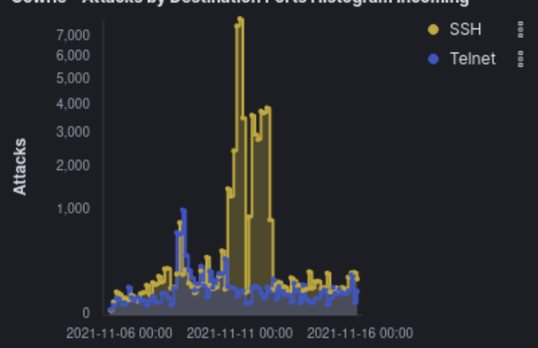


Cowrie Attacks Histogram

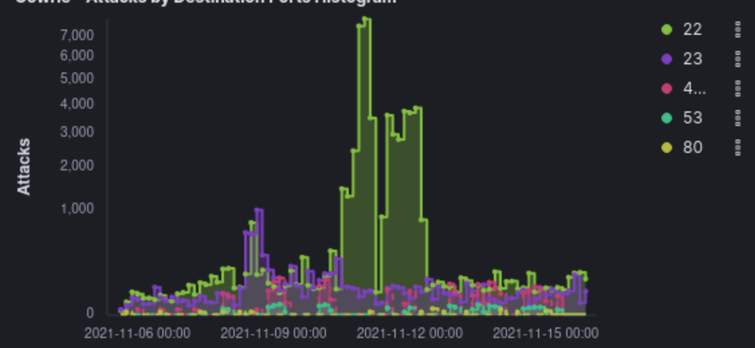


Cowrie Password Tagcloud

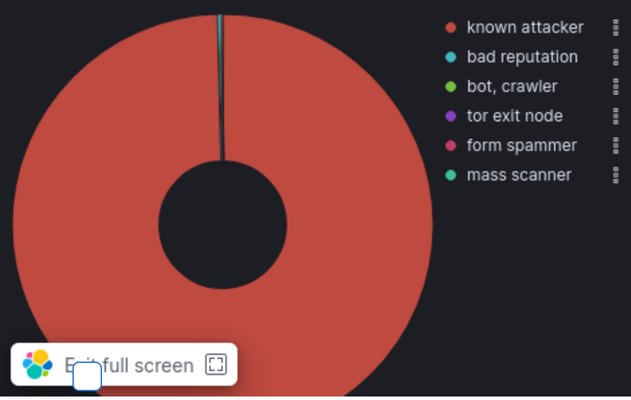
Cowrie - Attacks by Destination Ports Histogram Incoming



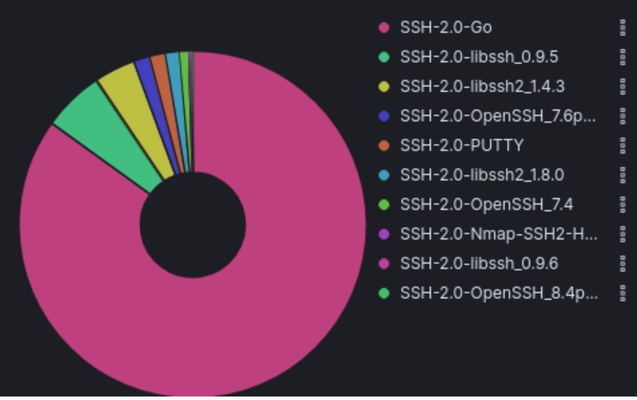
Cowrie - Attacks by Destination Ports Histogram



Cowrie - Attacker Src IP Reputation



Cowrie Version Pie - Top 10

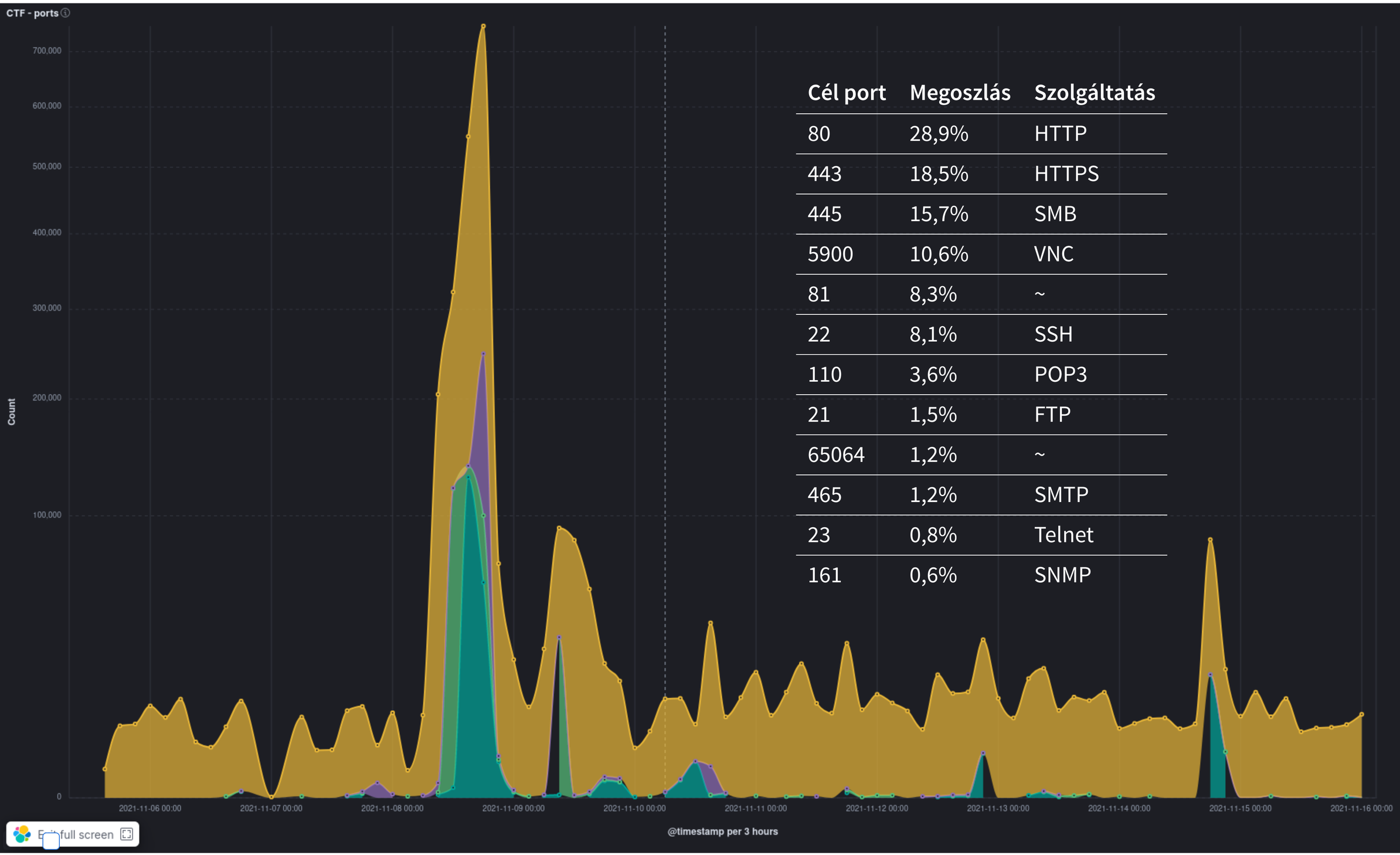


Cowrie - Attacker Src IP - Top 10

Source IP	Count
58.48.141.127	109,256
94.45.65.11	106,401
91.82.172.31	62,074
87.244.196.102	41,127
176.63.1.145	7,824
193.225.218.242	2,955
5.182.39.25	2,385
164.90.179.27	1,810
213.192.87.175	1,583
217.65.105.19	1,113

Cowrie Input - Top 10

Command Line Input	Count
shell	280
system	278
cd ..	253
ls -a	152
sh	138
enable	137
(empty)	126
/bin/busybox rm -rf .file .z .x	126
rm -rf .file .z .x	126
while read i	116



Cél port	Megoszlás	Szolgáltatás
80	28,9%	HTTP
443	18,5%	HTTPS
445	15,7%	SMB
5900	10,6%	VNC
81	8,3%	~
22	8,1%	SSH
110	3,6%	POP3
21	1,5%	FTP
65064	1,2%	~
465	1,2%	SMTP
23	0,8%	Telnet
161	0,6%	SNMP

TOVÁBBI LEHETŐSÉGEK

- Komplexitás
- Hatékonyság
- Megtévesztő képesség
- Minőség
- Támadó profilozás
- Biztonság

DINAMIKUS HONEYPOT

TÁMADÓ PROFILOZÁS

KÉRDÉS?

telekom-security/tpotce

Elasticsearch

Photo by Yulissa Tagle on Unsplash

Photo by Miłosz Klinowski on Unsplash

Photo by Aquaryus15 on Unsplash

Photo by Resource Database™ on Unsplash