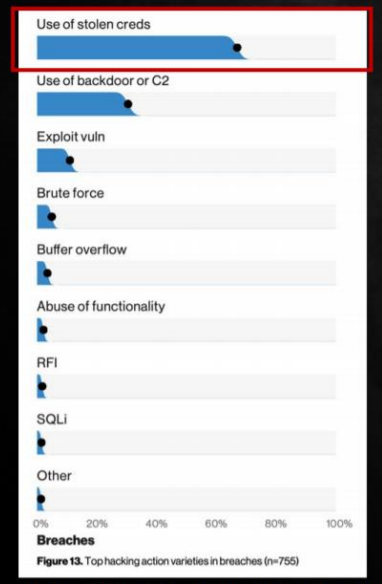
# Stolen Credentials = The Leading Attack Vector

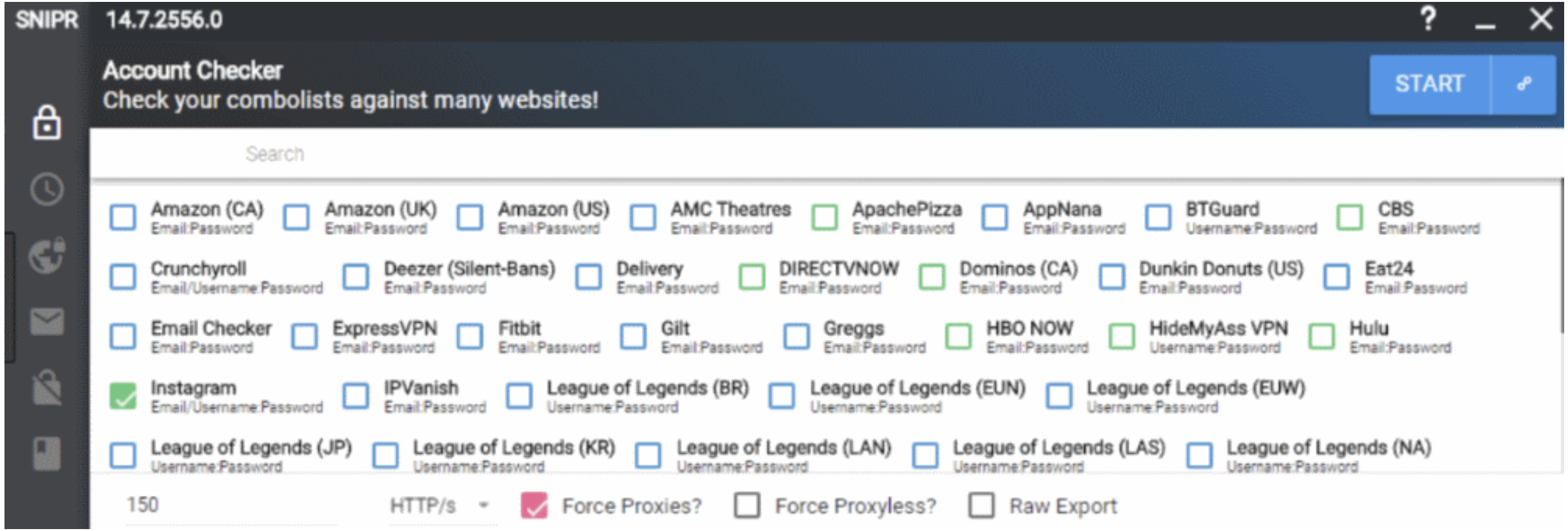



Verizon 2019 Data Breach Investigations Report

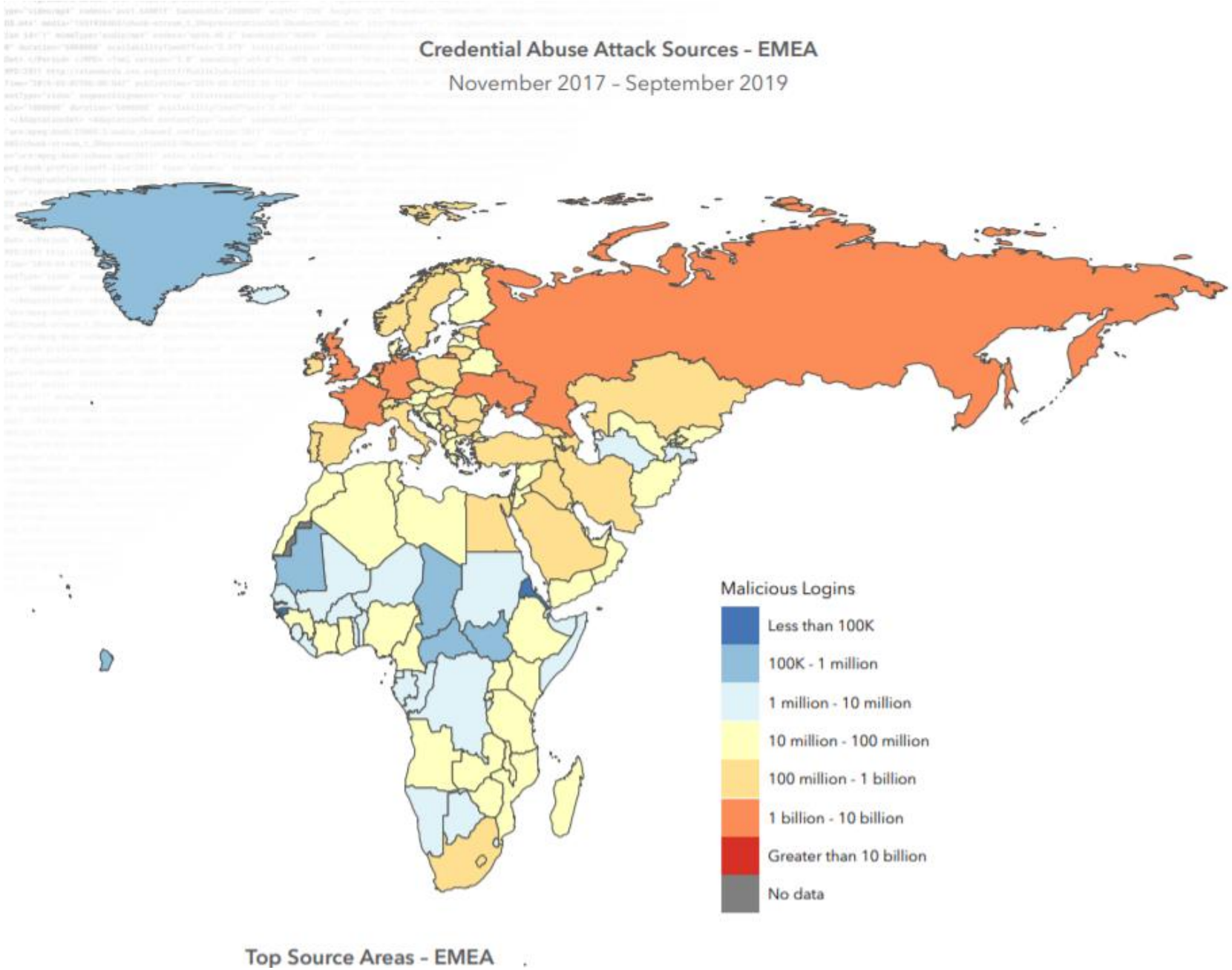

Palo Alto's Report "Credential-Based Attacks"

SpyCloud

filter:max


SNIPR
14.7.2556.0
Account Checker
Check your combolists against many websites!
START
Search
Amazon (CA) Email:Password
Amazon (UK) Email:Password
Amazon (US) Email:Password
AMC Theatres Email:Password
ApachePizza Email:Password
AppNana Email:Password
BTGuard Username:Password
CBS Email:Password
Crunchyroll Email/Username:Password
Deezer (Silent-Bans) Email:Password
Delivery Email:Password
DIRECTVNOW Email:Password
Dominos (CA) Email:Password
Dunkin Donuts (US) Email:Password
Eat24 Email:Password
Email Checker Email:Password
ExpressVPN Email:Password
Fitbit Email:Password
Gilt Email:Password
Greggs Email:Password
HBO NOW Email:Password
HideMyAss VPN Username:Password
Hulu Email:Password
Instagram Email/Username:Password
IPVanish Email:Password
League of Legends (BR) Username:Password
League of Legends (EUN) Username:Password
League of Legends (EUW) Username:Password
League of Legends (JP) Username:Password
League of Legends (KR) Username:Password
League of Legends (LAN) Username:Password
League of Legends (LAS) Username:Password
League of Legends (NA) Username:Password
150
HTTP/s
Force Proxies?
Force Proxyless?
Raw Export

www.snipr.gg



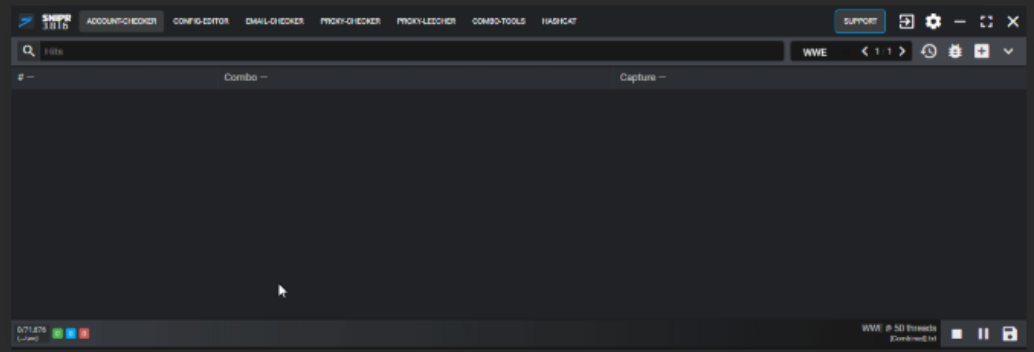

https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-a-year-in-review-report-2019.pdf

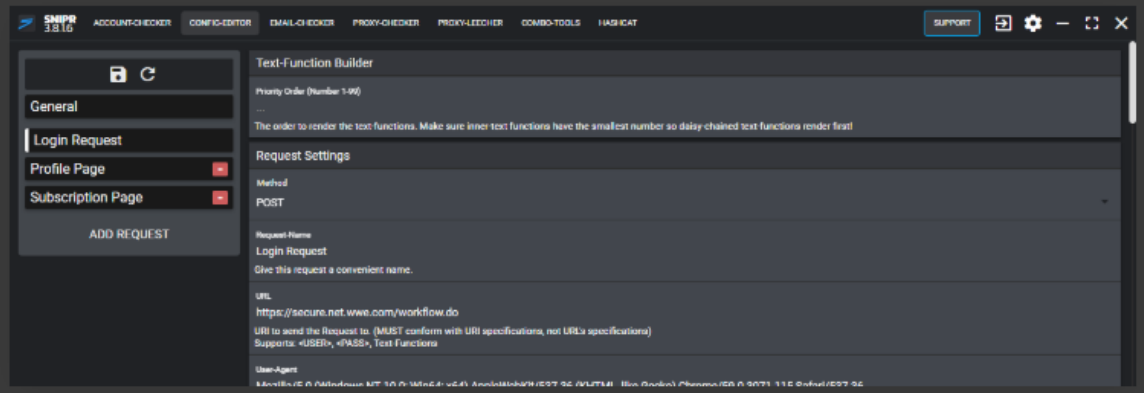
*„**43% of all logins seen by Akamai** were attempts to log in to an account using password guessing or **account details gathered** from elsewhere on the Internet.”*

https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf

# A Modern UI design focused on UX (User-Experience)

Every decision is made to make the experience better for the user. Design Language was originally using Material-Like design but has drifted to a more personal style. It uses the combined power of native JavaScript and AngularJS.



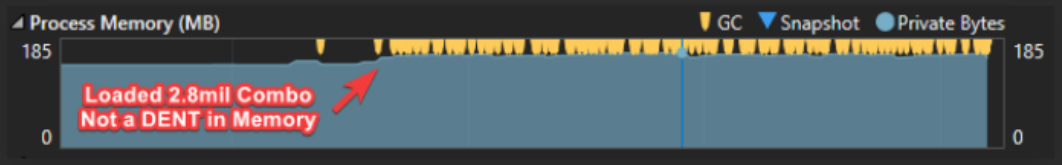




# Create or Edit Profile's in a snap

The Profile-Editor tab conveniently gives you a ton of tool's to quickly create a Profile with explanation's of each field present.

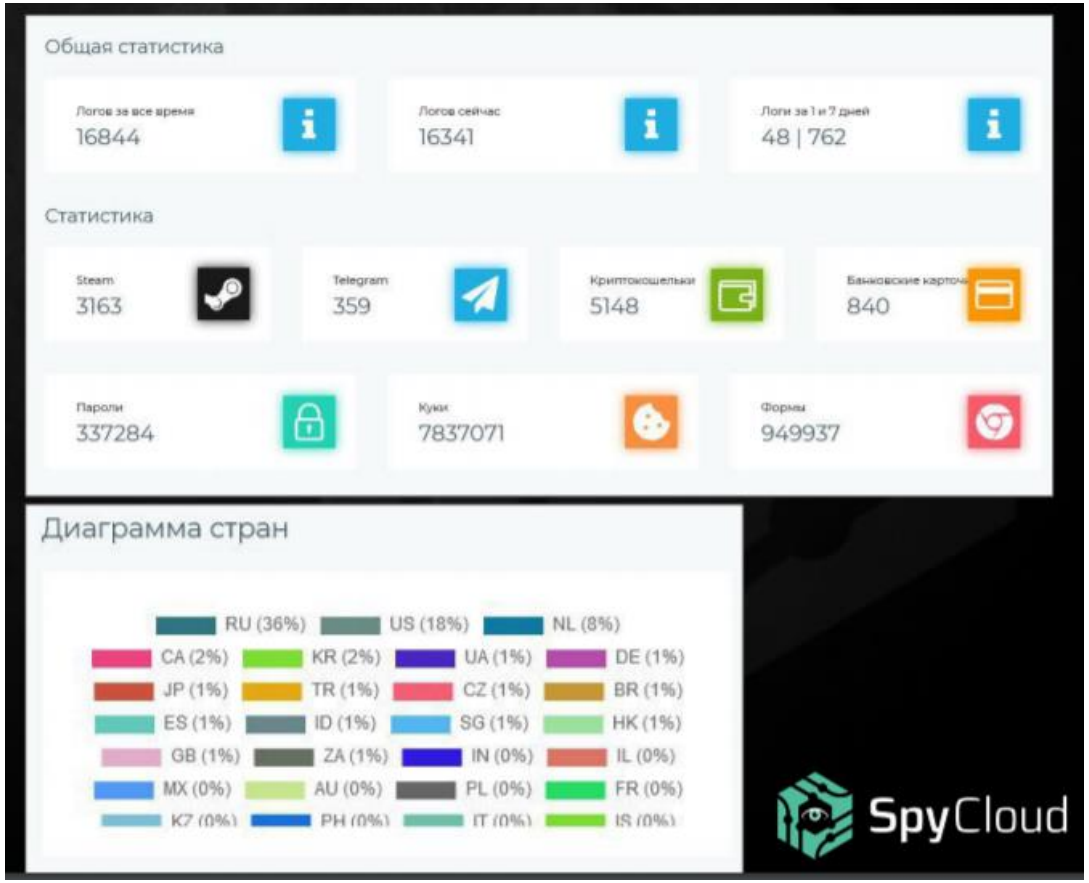
# Support for MASSIVE Combolist files

SNIPR read's Combo's from Combolist files as they are required instead of all at once unlike competitor software. This allows SNIPR to use very little memory when using even the biggest of files.

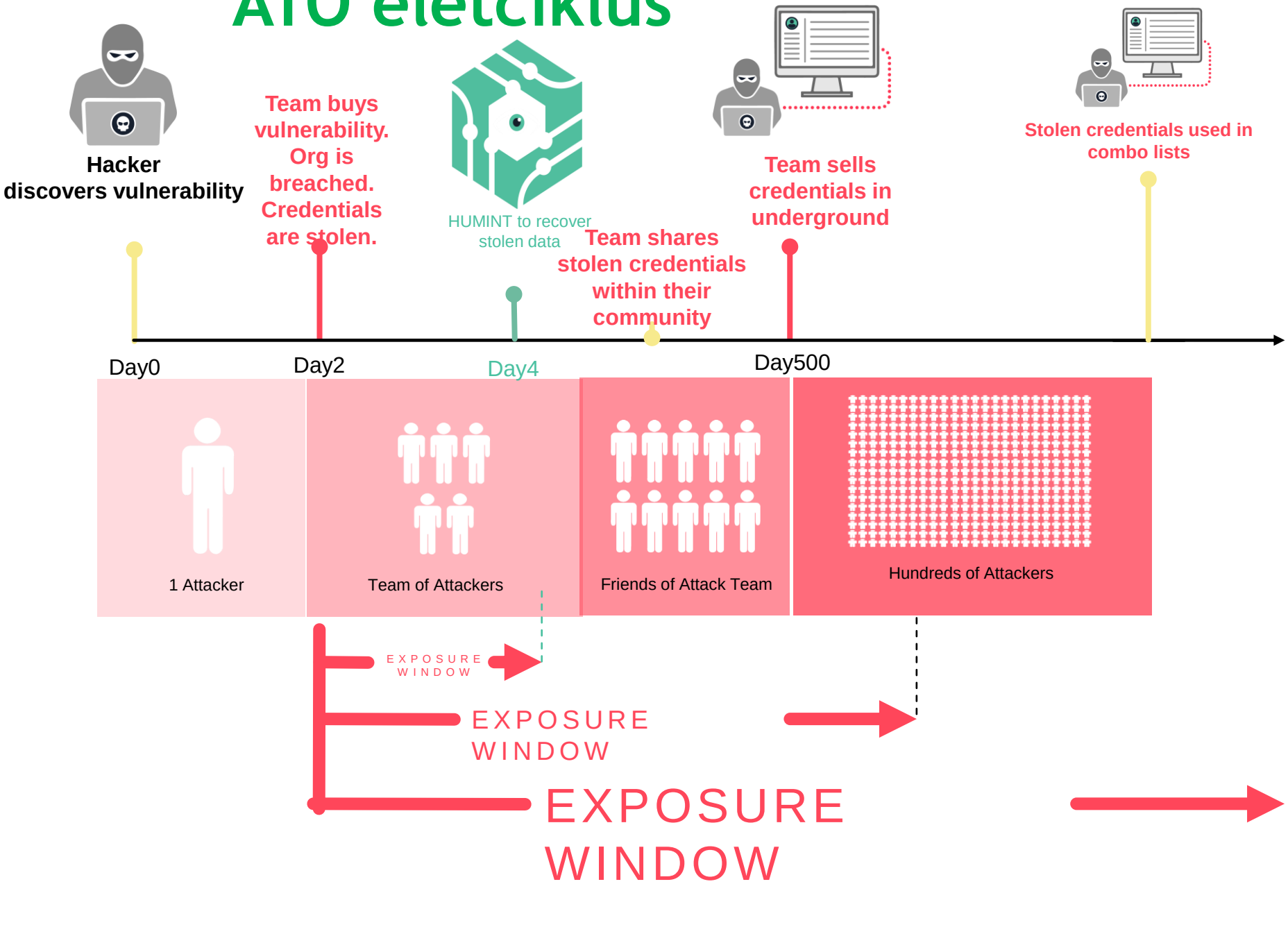


# Honnan szivárognak az accountok? - infected users

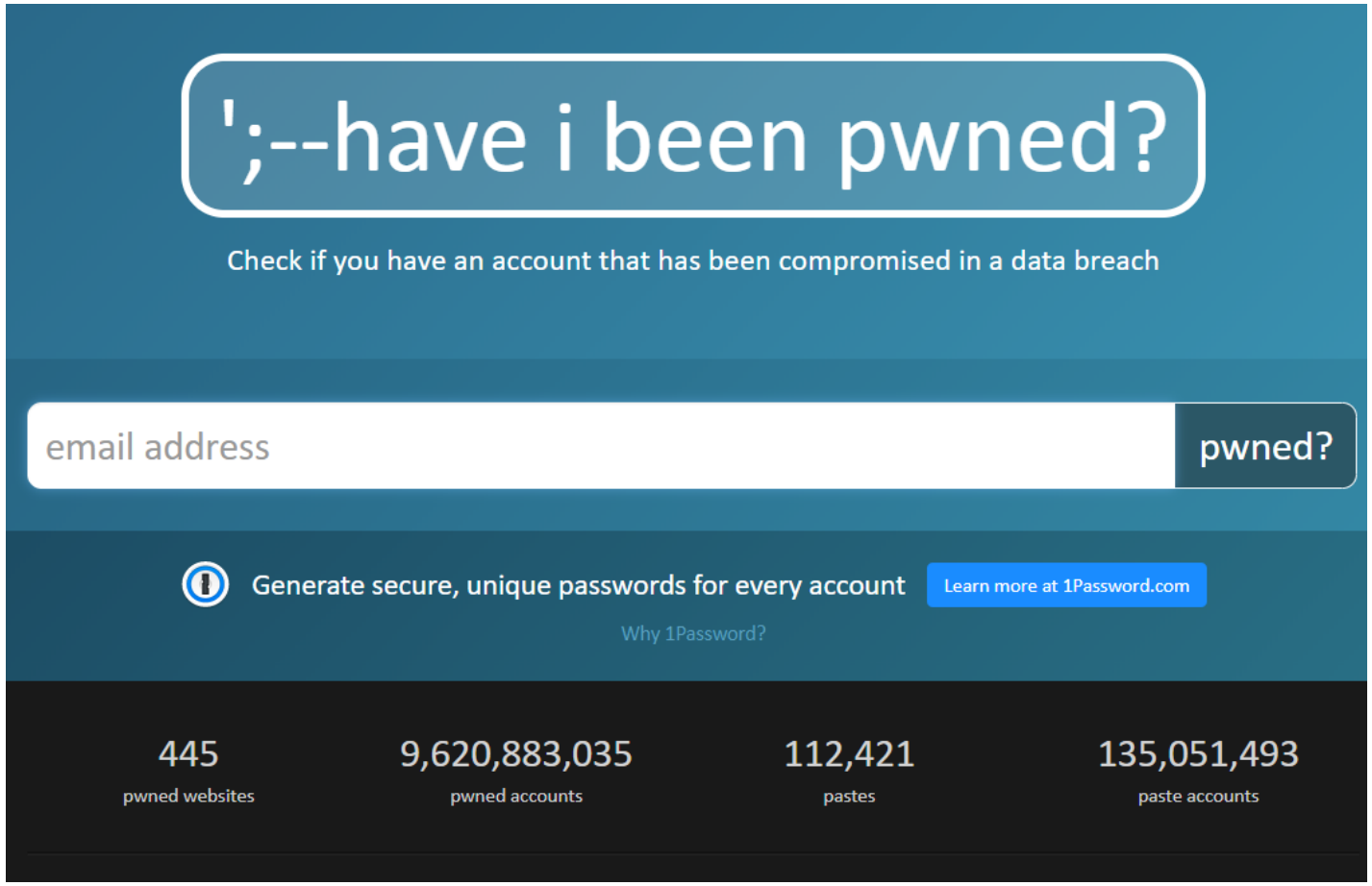
- *Predator stealer*
- Jelszvakra specializált malware
- 100-200 USD az ára
- Verzió frissítések
- GUI

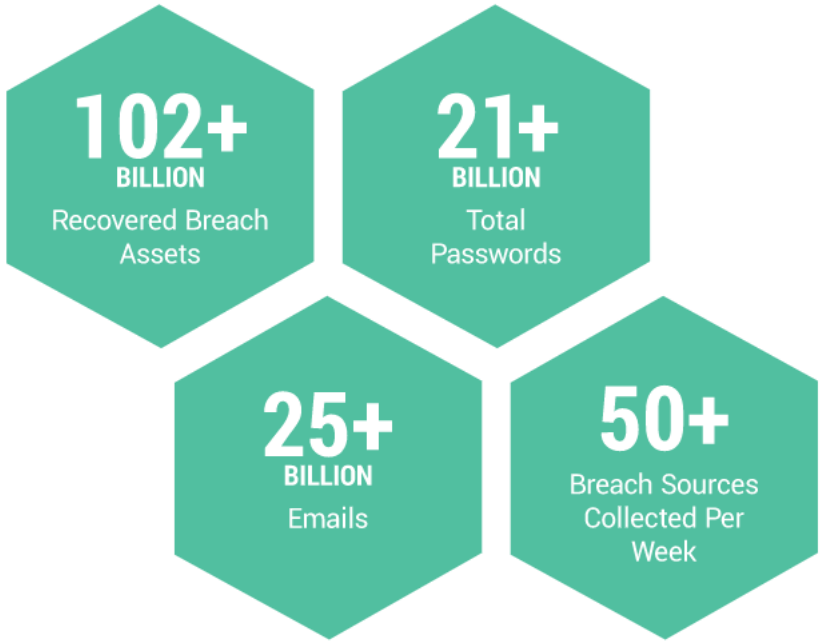


# ATO életciklus



# Spycloud vs publikus



# Mennyire aktuális?

Homeoffice =

- Cloud/SaaS szolgáltatások előretörése
- Felügyelet nélküli, patcheletlen gépek
- Megosztott gép használat
- Covid Phising

# Hogyan védekezzünk?

- 2FA
- Oktatás, szabályzatok, webes higiénia (Scirge?)
- Jelszó manager szoftverek, akár magán használatra is
- Proaktív ATO felderítés -> SpyCloud, Haweibeenpawned?
- Jelszó policy újra tervezése (90 nap, Priviliged Account Management?)

# Domain Breach Exposure Details

Domain: parlament.hu

**1,072**

Total Company Records Exposed

**3 Days**

Last Exposed

**0**

Potential Executive Credentials Exposed

https://spycloud.com/check-your-exposure/

filter:max

# A Big Data probléma

- Hasonló usernevek

  mrniceguy@gmail.com -> mrniceguy@yahoo.com

- Hasonló jelszavak (jelszó policy!)

  *Tutijelszo1234 -> Tut1j3lsz01234 -> tutijelszo4321*

- Azonos hostrol/IP-ről származó jelszavak

  *Titkos kérdés/válasz, azonos cím,*

  *azonos recovery email, telefonszám, nicknév*

- Stb. Stb. Stb. Stb -> korlátlan korreláció