SecurityBrokers

GLOBAL CYBER DEFENSE & SECURITY SERVICES

GDPR, Cybercrime & Data Breaches

Raoul “Nobody” Chiesa

Il Relatore

- Presidente, fondatore **Security Brokers SCpA**
- Special Senior Advisor in tema di Cybercrime @ **UNICRI** (United Nations Interregional Crime & Justice Research Institute)
- Former PSG Member, **ENISA** (Permanent Stakeholders Group @ European Union Network & Information Security Agency) per i mandati 2010-2012 e 2013-2015
- Socio Fondatore, **CLUSIT** (Associazione Italiana per la Sicurezza Informatica)
- Comitato Direttivo, **AIIC** (Associazione Italiana Esperti Infrastrutture Critiche)
- Membro del Board, **ISECOM** (Institute for Security and Open Methodologies)
- Membro del Board, **OWASP**, Capitolo Italiano (Open Web Application Security Project)
- Cultural Attaché, Liaison Officer, **APWG** European Chapter
- Roster of Experts Member, **ITU** (International Telecomunication Union, Ginevra)
- Member of the Board, **TSTF** (Telecom Security Task Force)
- **Sostenitore di svariate comunità in tema di InfoSec**

Agenda

- Introduzione
- Rischi effettivi
- Casi di Studio Reali
- Conclusioni
- Q&A

Big Picture

Anti-DDoS,
(di base) Sicurezza
delle applicazioni

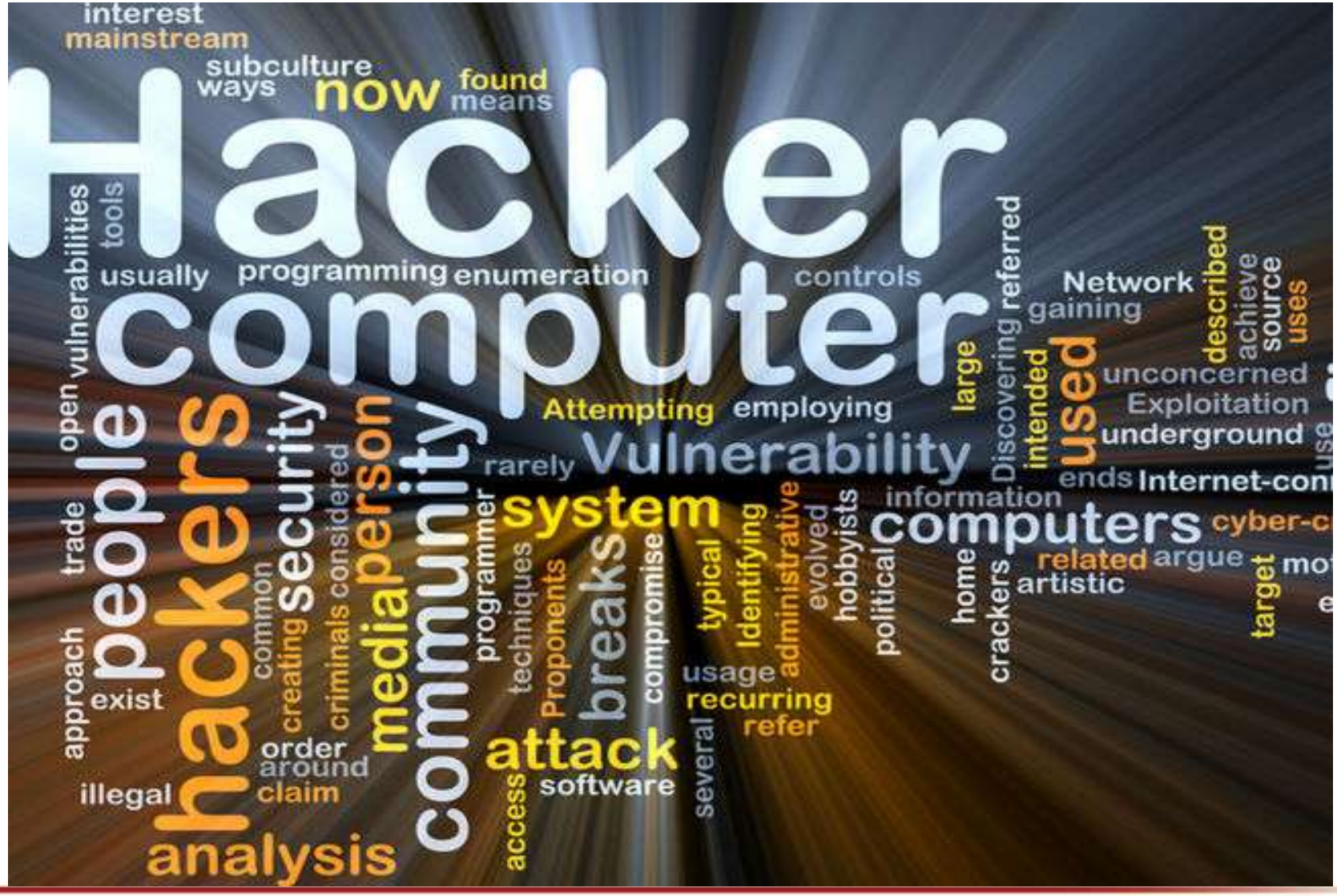
Cyber Intelligence,
Black Ops

Fattore umano, 0days

SCADA & Sicurezza sistemi di
automazione industriale,
Difesa - completa

Cybercrime Intelligence,
Conformità

Profilo degli insider,
DLP


interest
mainstream
subculture
ways
now
found
means
Hacker
computer
vulnerabilities
tools
usually
programming
enumeration
controls
Network
gaining
Discovering
referred
described
achieve
source
uses
unconcerned
Exploitation
underground
intended
used
large
open
people
hackers
security
person
community
Attempting
employing
Vulnerability
rarely
system
computers
information
ends
Internet-con
cyber-c
trade
approach
exist
common
creating
criminals
considered
media
programmer
techniques
Proponents
breaks
compromise
typical
Identifying
administrative
evolved
hobbyists
political
home
crackers
related
argue
artistic
target
usage
recurring
refer
several
order
around
claim
illegal
attack
software
access
analysis

Un assioma fondamentale

- La "merce universale di scambio" oggi è l'**informazione**.

Hai l'informazione, hai il potere.

(Quantomeno, nella **politica**, nel **mondo del business**, nelle **relazioni personali…**)

- Questo, semplicemente perché l'informazione è **immediatamente trasformabile** in:

1. **Vantaggio competitivo, strategico o politico**
2. **Informazione sensibile e/o critica**
3. **Denaro**
4. **Ricatto**

- **Esempi** ? (ovviamente dove il **cyber*** è stato «protagonista»)
  - ✓ **Attacco BGP degli ultimi giorni a Cloudfare (1.1.1.1)**
  - ✓ **Massive Leak Twitter accounts**
  - ✓ **Stuxnet, Shamoon, etc..**
  - ✓ **LTT Lybia**
  - ✓ **Scandalo Telecom Italia/SISMI**
  - ✓ **Caso Vodafone Grecia**
  - ✓ **Regione Lazio**
  - ✓ **Caso Bisignani**
  - ✓ **Estonia**
  - ✓ **Ucraina**

Ma **non sono**

solo «hackers»

Key points del Cybercrime

- Il **Cybercrime**:
  - *"utilizzo di strumenti informatici e reti di telecomunicazione*
    - *per l'esecuzione di reati e crimini di diversa natura".*
- **L'assioma alla base dell'intero modello:**
  - *"acquisire diversi insiemi di dati (informazione), tramutabili in denaro."*
- **Punti salienti**:
  - **Virtuale** (modello "a piramide" ed anonimato, C&C, flessibili e scalabili, velocità di spostamento e rebuilding, utilizzo "cross" di prodotti e servizi in differenti scenari e modelli di business)
  - **Transnazionale**
  - Multi-mercato (**acquirenti**)
  - **Diversificazione** dei prodotti e dei servizi
  - **Bassa** "entry-fee"
  - **ROI** (per singola operazione, quindi esponenziale se industrializzato)
  - Tax & (cyber) Law **heaven**

Data Breach

- Con il termine **data breach** si intende un **incidente di sicurezza in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati** o **utilizzati** da un soggetto non autorizzato.

- Solitamente il data breach si realizza con una **divulgazione di dati riservati o confidenziali** all'interno di un ambiente privo di misure di sicurezze (da esempio, su web) in maniera involontaria o volontaria. Tale divulgazione può avvenire in seguito a:
  - **perdita accidentale**: ad esempio, data breach causato da smarrimento di una chiavetta USB contenente dati riservati
  - **furto**: ad esempio, data breach causato da furto di un notebook contenente dati confidenziali
  - **infedeltà aziendal**e: ad esempio, data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico
  - **accesso abusivo**: ad esempio, data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite

Esempi di “Violazione Data Breach”

- I **dati violati con un data breach** possono riguardare tutti gli ambiti (esempi reali):
  - **finanziario**, ad esempio dati di carte di credito, di conti correnti…
  - **sanitario**, ad esempio informazioni sulla salute personale, malattie…
  - **proprietà industriale**, ad esempio segreti commerciali, brevetti, documentazione riservata, lista clienti, progetti finalizzati ad esempio a pratiche di concorrenza sleale…
  - **personali**, ad esempio dati di documenti di identità, codici personali…

Data Breach Intelligence

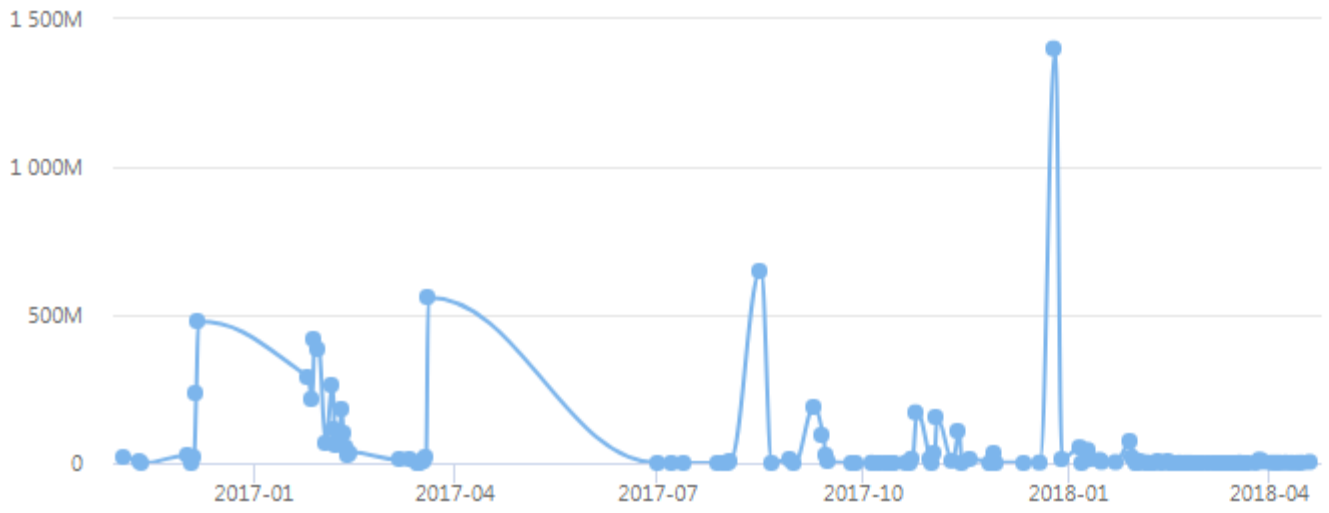
- Servizi che iniziano ad arrivare anche in Italia
- Avvisiamo i nostri Clienti in tempo reale se sono stati vittima di un Data Breach (Early Warning)

Data Breach Intelligence

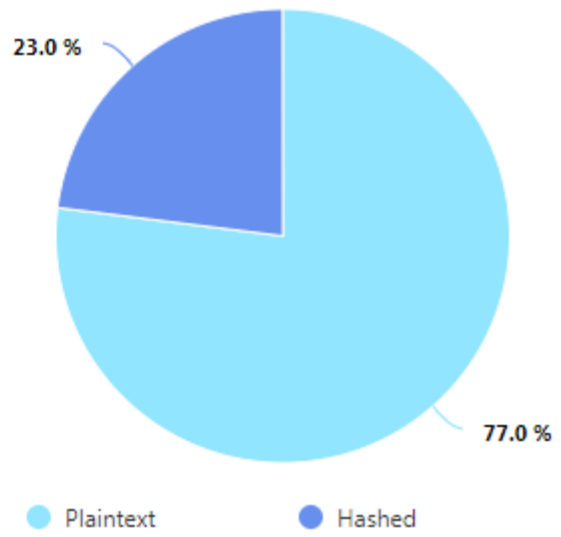
- Qualche numero…

Total records	Passwords (hashed)	Passwords (plaintext)	E-mails	Users names	IPs
6.95B	**1.53B**	**5.17B**	**6.25B**	**1.19B**	**123M**

Data Breaches Collected

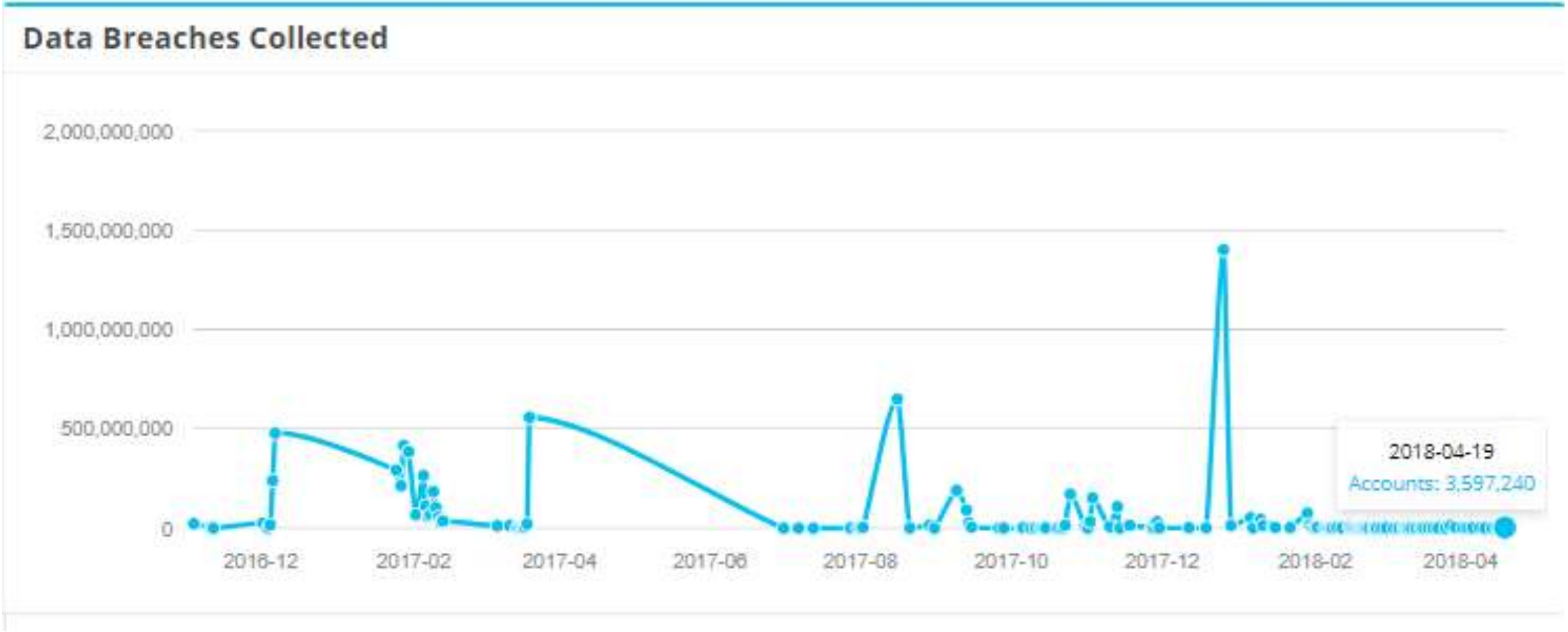


Password Type Distribution

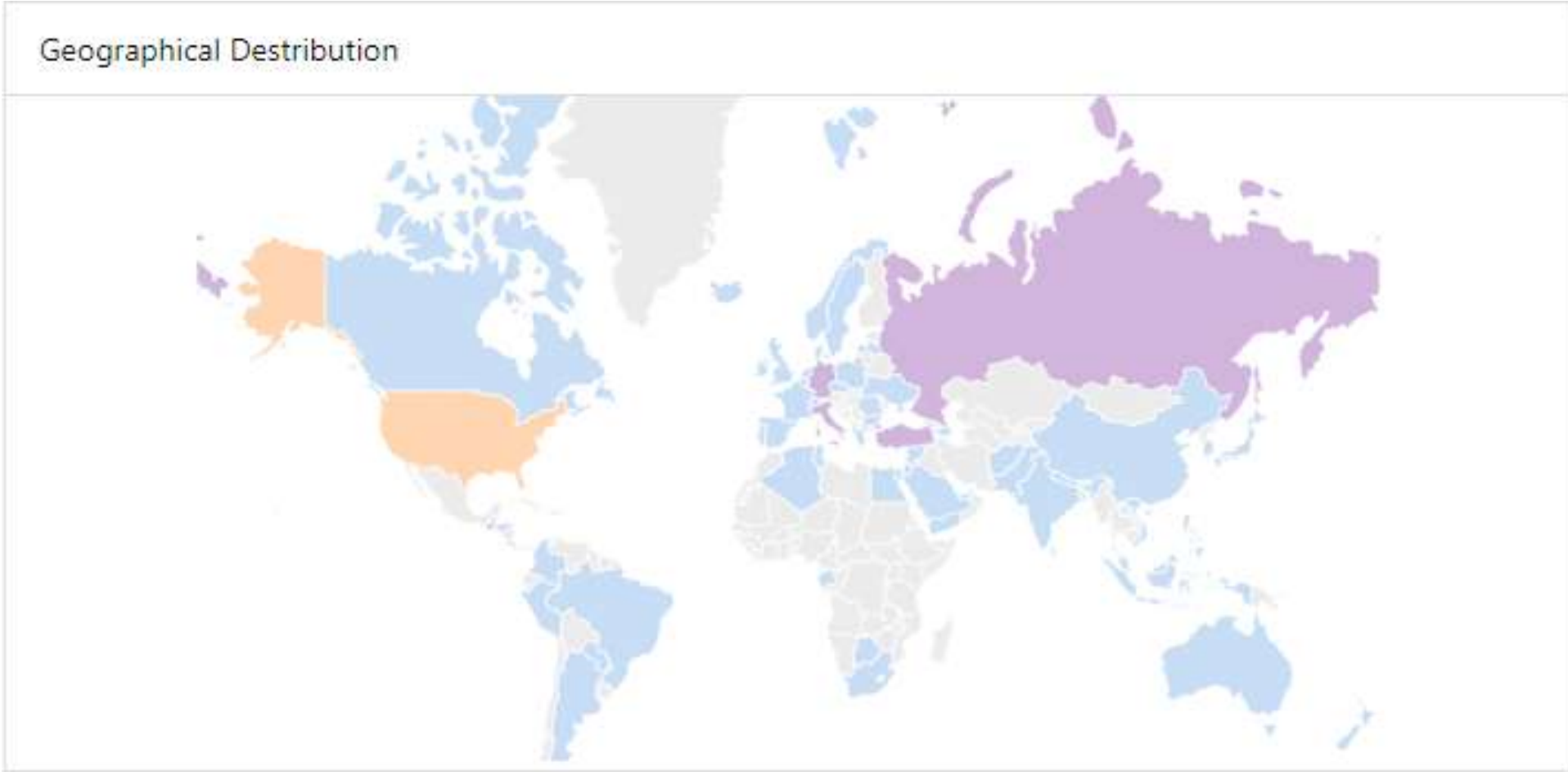


Data Breach Intelligence

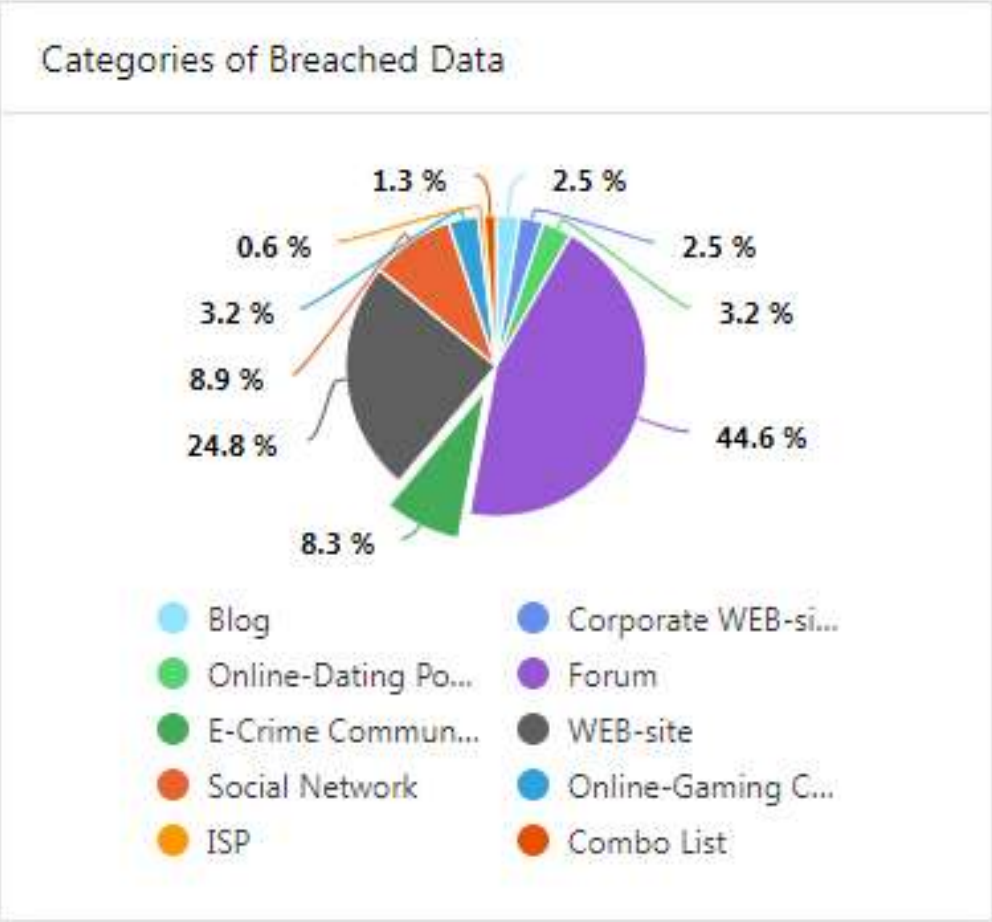
- Dati odierni

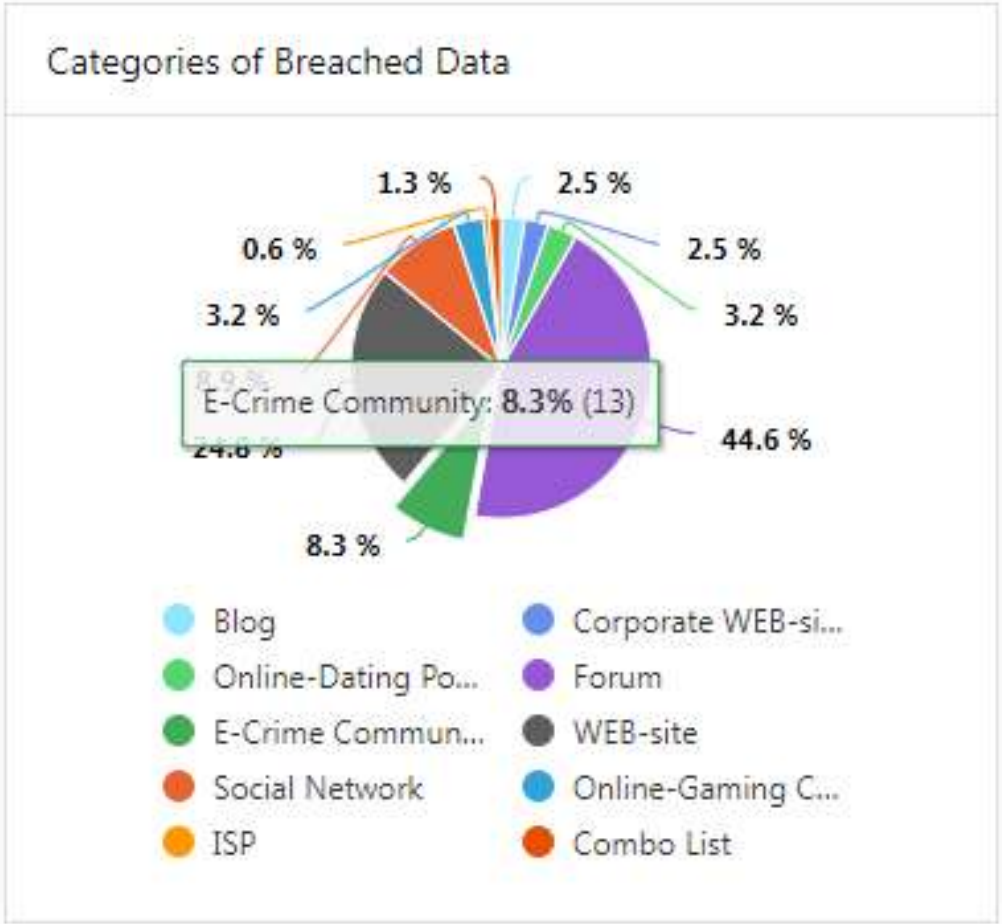


Data Breach Intelligence



Data Breach Intelligence



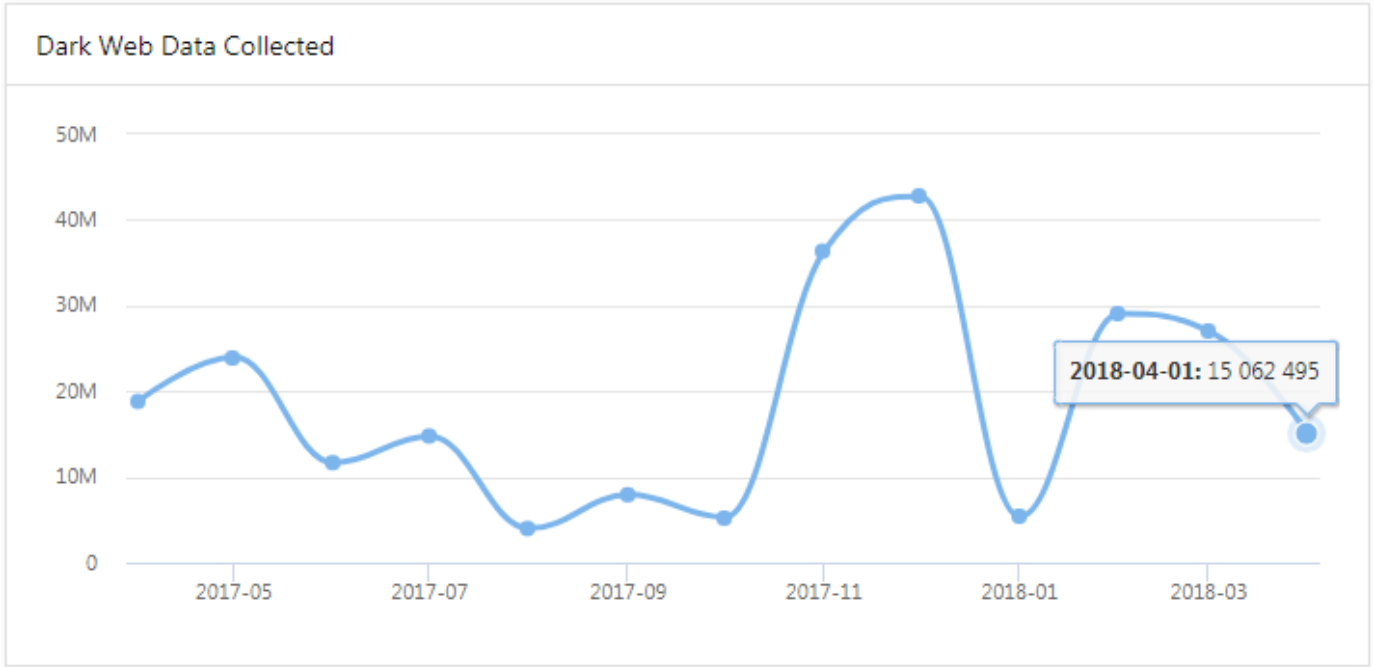


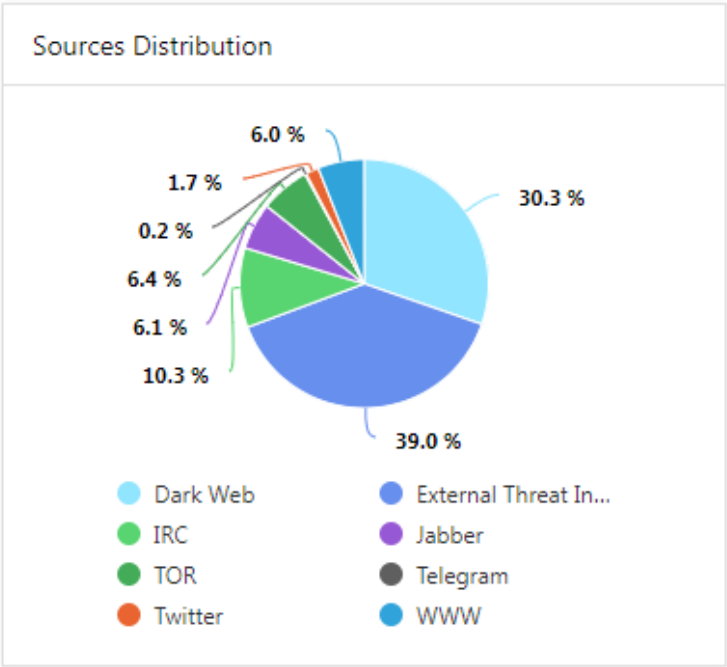
Da dove arrivano questi dati?

Cyber Threat Intelligence

- Dati reali

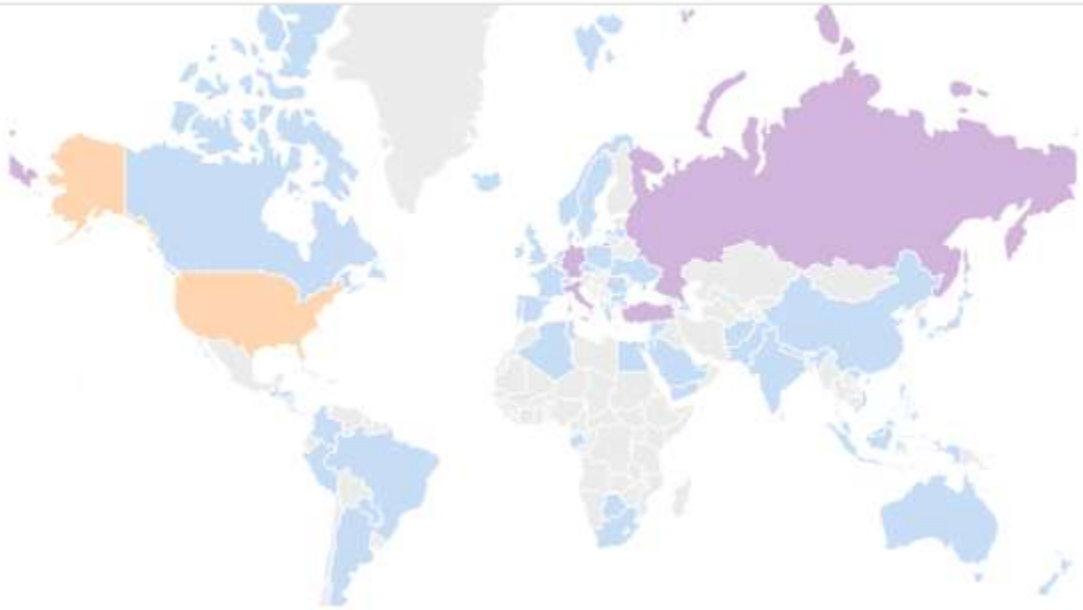
Total records	Data Collected, GBs	Security Incidents	Total Actors	Total Sources	Total IOCs
298M	**1146**	**1,825**	**9.2M**	**23,006**	**22.3M**



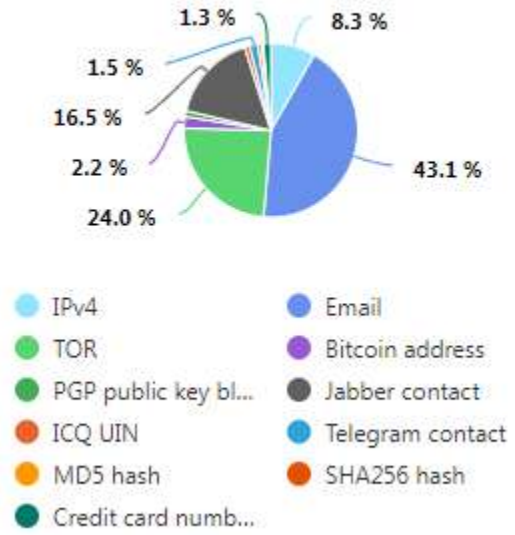


Cyber Threat Intelligence

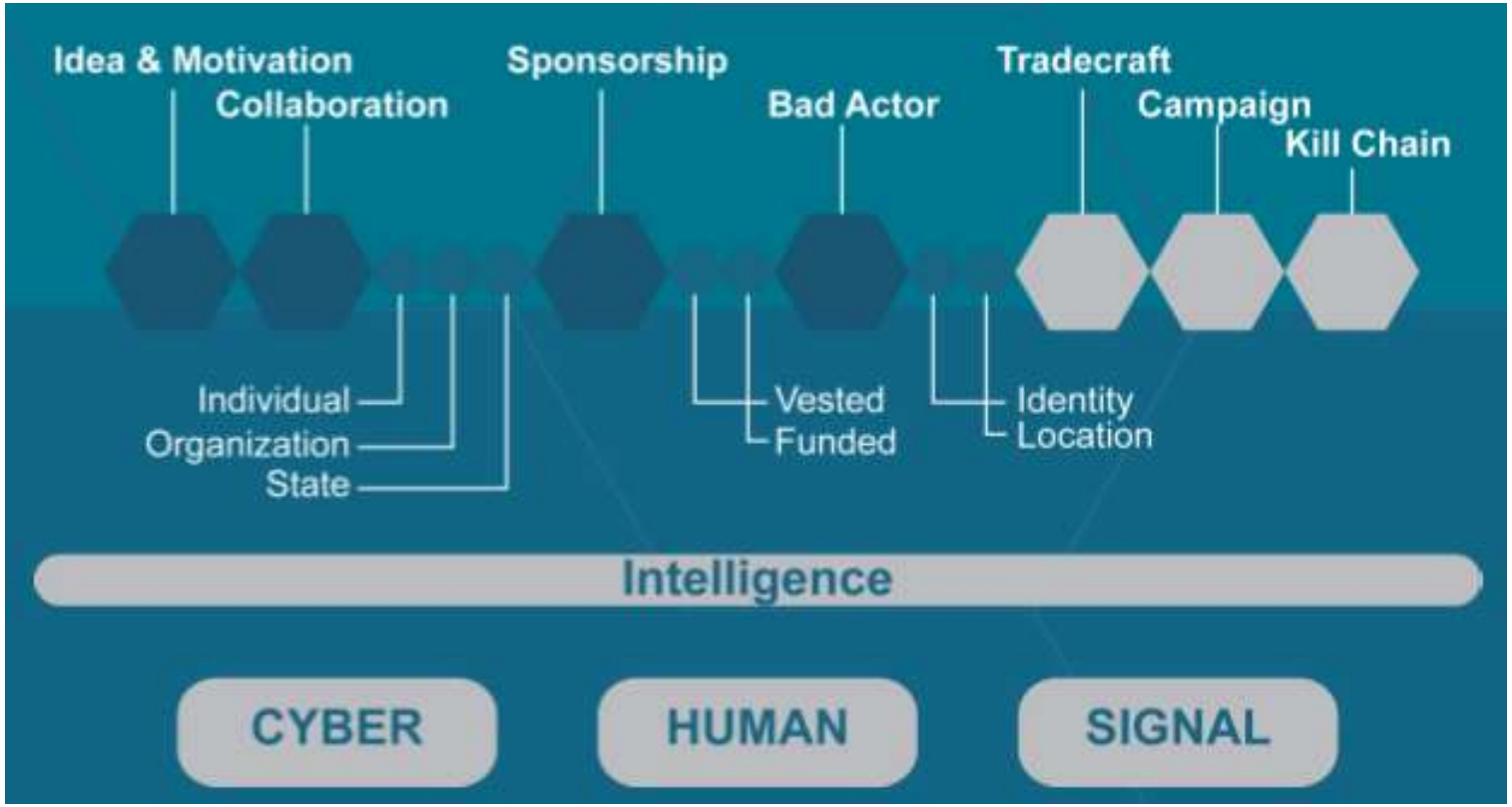
Geographical Destribution



Data Mining



Tipologie


Idea & Motivation
Collaboration
Sponsorship
Bad Actor
Tradecraft
Campaign
Kill Chain
Individual
Organization
State
Vested
Funded
Identity
Location
Intelligence
CYBER
HUMAN
SIGNAL

Riflessioni

- Differenti tipi di “black forums”
- Differenti Threat Actors (Anonymous diverso da LULZ; OC diverso dai “ragazzini”; etc…)
- Background, “pedigree” e Referenze, Storico del profilo sotto copertura
- Problematiche linguistiche
- I “peggiori bar di Caracas”
- Approccio “home made” interno:
  - Pericoloso
  - Non completo

Conclusioni

- **Educare gli utenti**
- **Dotarsi di strumenti all'avanguardia che non solo possono "aiutarci a capire se abbiamo ricevuto delle minacce"**
- Comprendere e prendere coscienza che ad oggi molte informazioni sono già all'esterno delle nostre organizzazioni
- Con noi potete sapere in tempo reale chi, cosa, perché e a quanto stanno vendendo i vostri dati!

Siamo entrati in una Nuova ERA dell'Information Security

ON-LINE TOUR

GRAZIE per l'attenzione!

Raoul "Nobody" Chiesa

rc [at] security-brokers [dot]com

SecurityBrokers

GLOBAL CYBER DEFENSE & SECURITY SERVICES

Security Brokers scpa

Via Appia Nuova, 96 - 00183 Rome Italy

Email: info@security-brokers.com - Website: http://www.security-brokers.com