ENISA Threat Landscape 2023

Threats Against Data

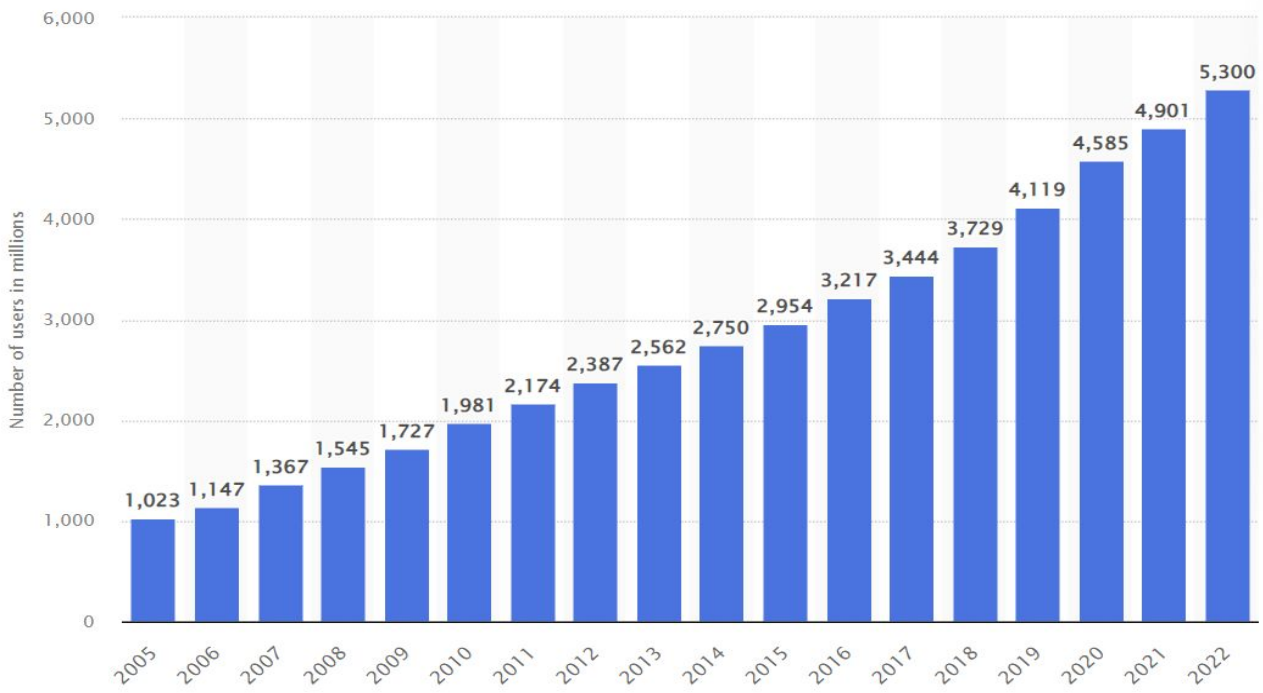
DIT172 | Project 2 | itp22104

Ψηφιακή εποχή και δεδομένα

- Διεύρυνση χρήσης του διαδικτύου
  - 63% του παγκόσμιου πληθυσμού το 2022 (5.3 δις)
  - Δημιουργία/αντιγραφή/κατανάλωση: 2022 (97 zetabytes) 2025 (181 zetabytes)
- Ψηφιακός μετασχηματισμός
  - 13% μέσος ετήσιος ρυθμός αύξησης market size
- Αύξηση του όγκου των δεδομένων στους διάφορους τομείς παραγωγής

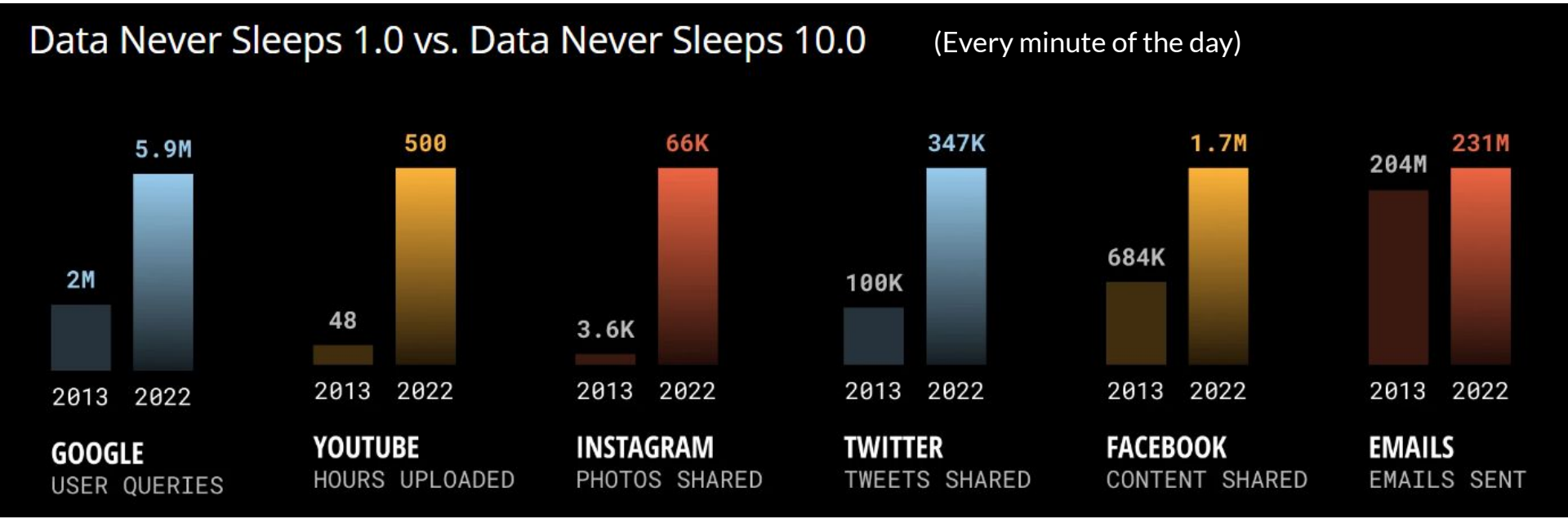
Compound Annual Growth Rate of Digital Transformation market size

Χρήστες διαδικτύου

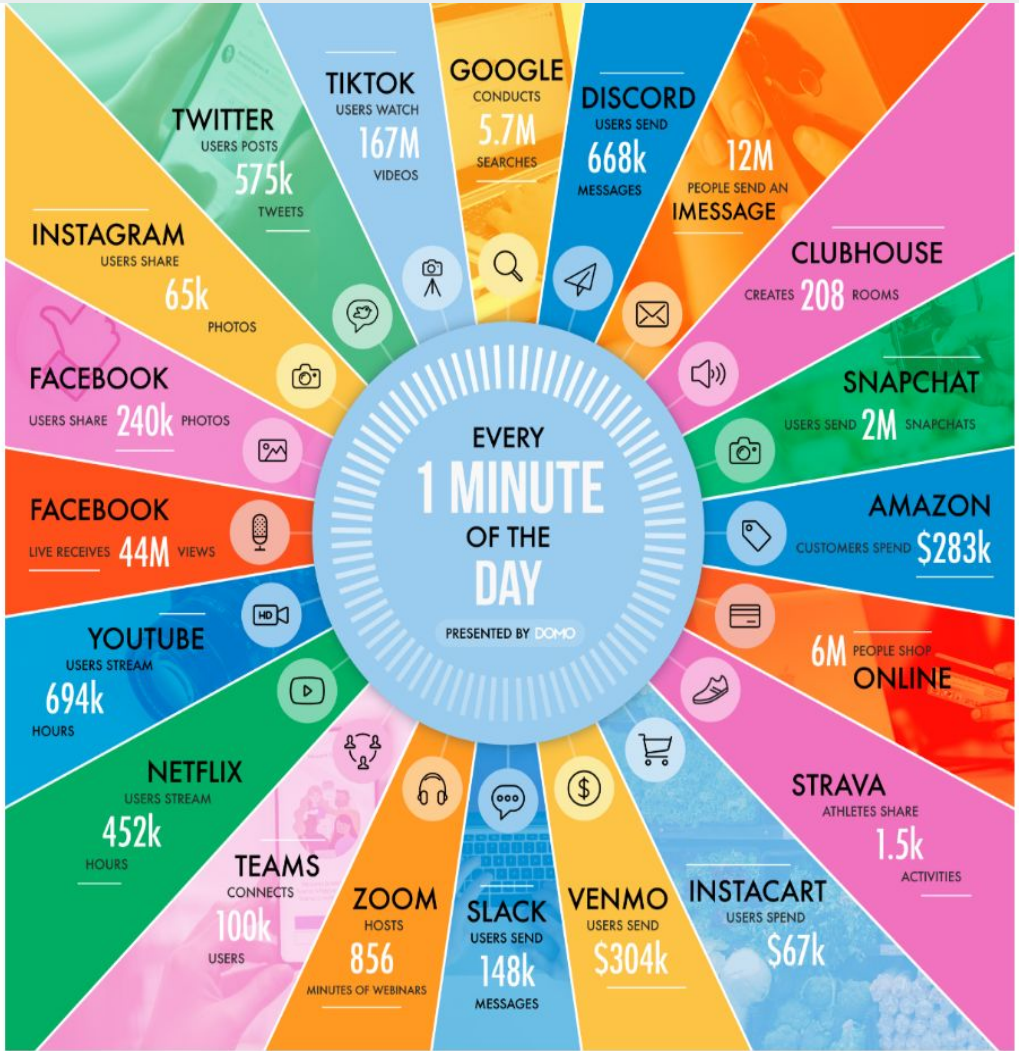


Additional Information

Show source


Data Never Sleeps 1.0 vs. Data Never Sleeps 10.0
(Every minute of the day)
2M
5.9M
2013
2022
GOOGLE
USER QUERIES
48
500
2013
2022
YOUTUBE
HOURS UPLOADED
3.6K
66K
2013
2022
INSTAGRAM
PHOTOS SHARED
100K
347K
2013
2022
TWITTER
TWEETS SHARED
684K
1.7M
2013
2022
FACEBOOK
CONTENT SHARED
204M
231M
2013
2022
EMAILS
EMAILS SENT

Data Never Sleeps 9.0 - 2021



Σημασία και κατανομή δεδομένων

- Clive Humby (Βρετανός μαθηματικός) το 2006 σε συνέδριο της Association of National Advertisers
  - *Data is the new oil*
- Economist 2017
  - *The world's most valuable resource is no longer oil, but data*
- Google, Amazon, Apple, Facebook, Microsoft: 2017 Q1 25δις συνολικό καθαρό κέρδος
- Η Amazon συγκεντρώνει μισό από το συνολικό ποσό σε δολάρια που ξοδεύεται online στην Αμερική
- Google και Facebook καρπώθηκαν σχεδόν τη συνολική αύξηση εσόδων (revenue growth) της ψηφιακής διαφήμισης στην Αμερική το 2016

Τα δεδομένα στο επίκεντρο - Παραβιάσεις 1

- GDPR: Κανονισμοί προστασίας
- *Data Breach*: Η ηθελημένη επίθεση προς έναν οργανισμό/υπηρεσία/εταιρία με σκοπό την απόκτηση πρόσβασης σε δεδομένα και κλοπής τους
  - ***Μάρτιος 2020****: Η CAM4 πάροχος περιεχομένου streaming όπου ο server της παραβιάστηκε εκθέτοντας 10.88 δισεκατομμύρια καταχωρήσεις.*
  - ***Οκτώβριος 2017****: Η Yahoo δέχθηκε επίθεση από χάκερς εκθέτοντας 3 δισεκατομμύρια λογαριασμούς.*
  - ***Μάρτιος 2018****: Στοιχεία όπως ονοματεπώνυμα, τραπεζικοί λογαριασμοί κ.α. 1.1 δισεκατομμυρίων ανθρώπων εκτέθηκαν από βάση βιομετρικών δεδομένων που διαχειριζόταν κρατική εταιρία στην Ινδία.*
  - ***Ιούλιος 2022****: Πάνω από 23 terabytes δεδομένων παραβιάστηκαν από τη βάση δεδομένων πελατών της Alibaba εκθέτοντας στοιχεία όπως ονοματεπώνυμα, κωδικοί χρηστών, τηλέφωνα, διευθύνσεις κ.ά.*

Τα δεδομένα στο επίκεντρο - Παραβιάσεις 2

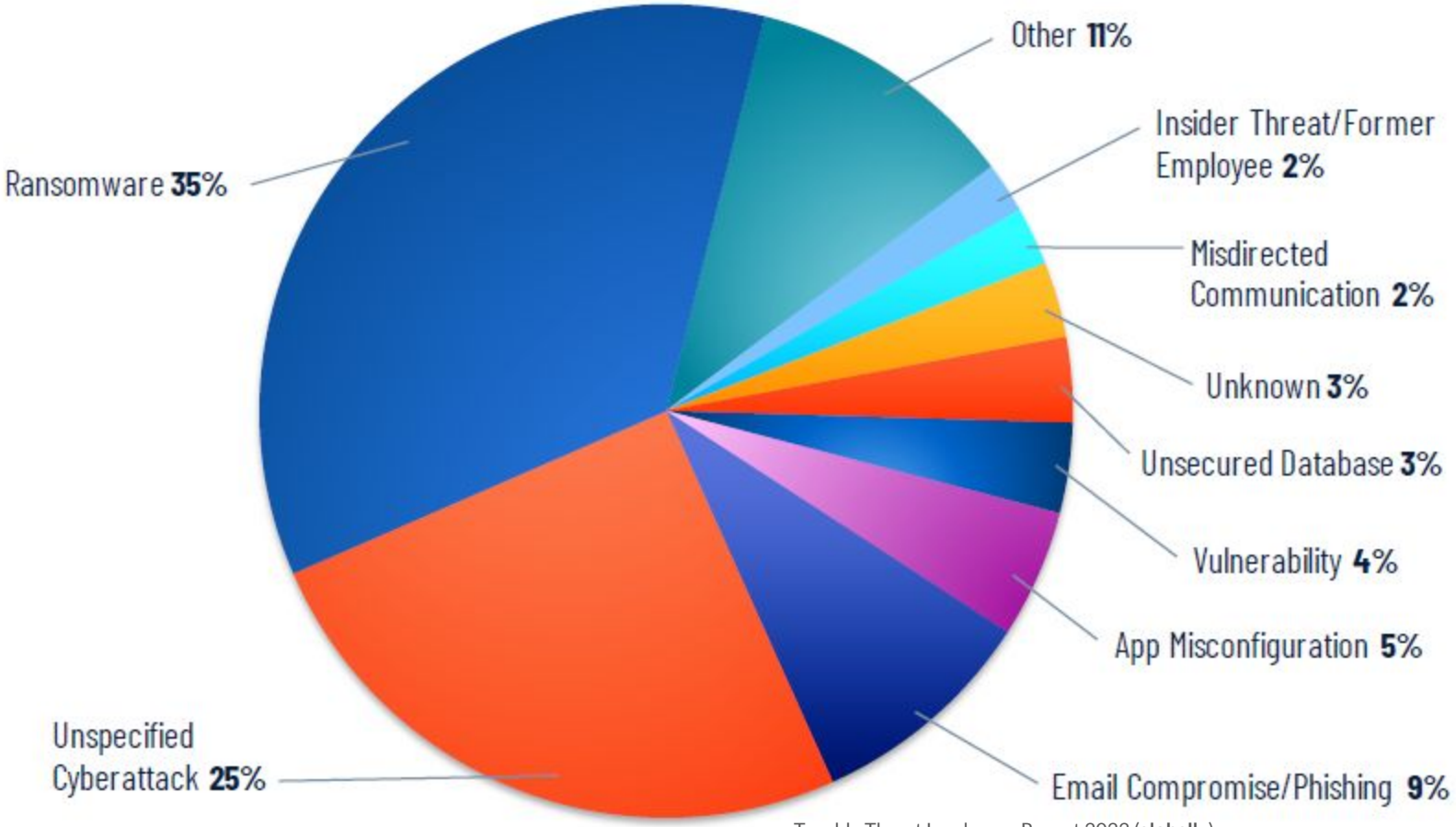
Data Leak: Η ηθελημένη επίθεση προς έναν οργανισμό/υπηρεσία/εταιρία με σκοπό την απόκτηση πρόσβασης σε δεδομένα και κλοπής τους

Microsoft Power Apps *(Εργαλεία δημουργίας και διαχείρισης εφαρμογών) data leak in 2021: Όπου κατέστη επιτρεπτή η δημόσια πρόσβαση σε δεδομένα που περιλάμβαναν προσωπικά στοιχεία πολιτών*

Τα δεδομένα στο επίκεντρο - Παραβιάσεις 3 Μέθοδοι

- ***Phishing****:* Εξαπάτηση χρηστών ώστε να αποκαλύψουν ευαίσθητα προσωπικά δεδομένα μέσω emails ή ψεύτικων ιστότοπων
- ***Smishing****:* Εξαπάτηση χρηστών ώστε να αποκαλύψουν ευαίσθητα προσωπικά δεδομένα μέσω emails ή ψεύτικων ιστότοπων
- ***BEC (Business Email Compromise)****:* Οι επιτιθέμενοι υποδύονται πελάτες/υπαλλήλους ώστε να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα
- **Ransomware**:
    - **Ransom Denial of Service (RDoS)**: Μπλοκάρισμα πρόσβασης - απαίτηση πληρωμής
    - **Distributed Denial of Service (DDoS)**: Τεχνητή δημιουργία κίνησης - δυσλειτουργία

2022 Breaches by Root Cause



Tenable Threat Landscape Report 2022 (**globally**)

DATA POINT	2021	2022
Total records exposed	40,000,000,000	2,296,941,687
Total files exposed	1,800,000,000	389,127,450
Total data exposed	260 Terabytes	257 Terabytes

Region	Total records exposed	% of total
Asia-Pacific (APAC)	1,561,990,339	68.00%
North America (NAM)	405,954,391	17.67%
Europe, Middle East, and Africa (EMEA)	305,994,856	13.32%
Unknown/Global	22,540,901	0.98%
Latin America (LATAM)	461,200	0.02%
Totals	2,296,941,687	

Tenable Threat Landscape Report 2022

Figure 8 | *Compromises by Attack Vector*

	2022	2021	2020
Cyberattacks	1,595	1,613	878
Phishing/Smishing/BEC	461	537	383
Ransomware	276	352	158
Malware	70	141	104
Non-Secured Cloud Environment	9	24	50
Credential Stuffing	18	14	17
Unpatched Software Flaw	–	4	3
Zero Attack Day	8	4	1
Other	26	426	162
Not Specified	727	111	–
System & Human Errors	151	179	152
Failure to Configure Cloud Security	18	54	57
Correspondence (Email/Letter)	55	66	55
Misconfigured Firewall	30	13	4
Lost Device or Document	6	12	5
Other	23	34	31
Not Specified	19	–	–
Physical Attacks	46	51	78
Document Theft	7	9	15
Device Theft	21	17	30
Improper Disposal	5	5	11
Skimming Device	6	1	5
Other	6	19	17
Not Specified	1	–	–
Data Leaks	–	7	–
Unknown	10	12	–
Totals	**1,802**	**1,862**	**1,108**

Figure 9 | *Compromises by Industry*

	2022		2021		2020	
	Comp.	Victims	Comp.	Victims	Comp.	Victims
Education	100	1,745,226	125	1,687,192	42	974,054
Financial Services	268	27,146,354	279	19,978,108	138	2,687,084
Government	74	1,739,462	66	3,244,455	47	1,100,526
Healthcare	344	26,259,933	330	30,853,767	306	9,700,238
Hospitality	34	69,235,147	33	238,445	17	22,365,384
Manufacturing & Utilities	249	23,897,836	222	49,782,583	70	2,896,627
Non-Profit/ NGO	71	980,021	86	2,339,646	31	37,528
Professional Services	224	6,248,711	184	22,729,391	144	73,012,145
Retail	65	792,195	102	7,212,912	53	10,710,681
Technology	86	248,564,988	79	44,684,180	67	142,134,883
Transportation	36	3,991,847	44	569,684	21	1,208,292
Other	251	11,541,592	308	79,660,479	172	43,391,302
Unknown	–	–	4	35,232,664	–	–
Totals	**1,802**	**422,143,312**	**1,862**	**298,213,506**	**1,108**	**310,218,744**

ITRC Data Breach Report 2022 (**US**)

Figure 3 | *Compromises by Month, 2022*

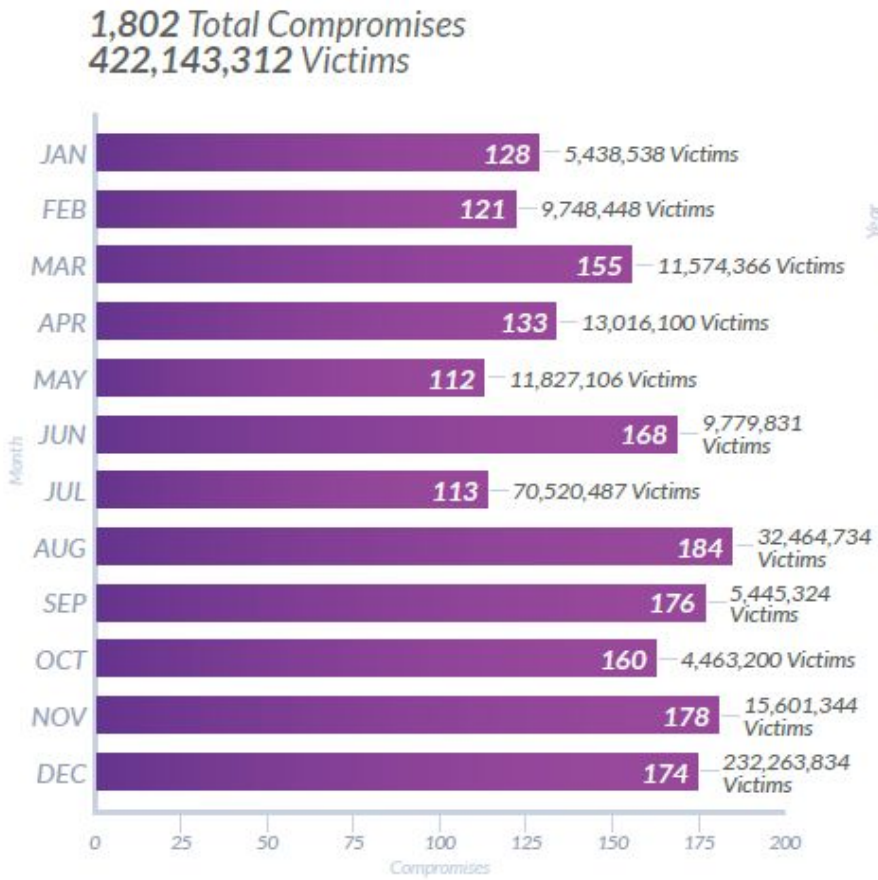
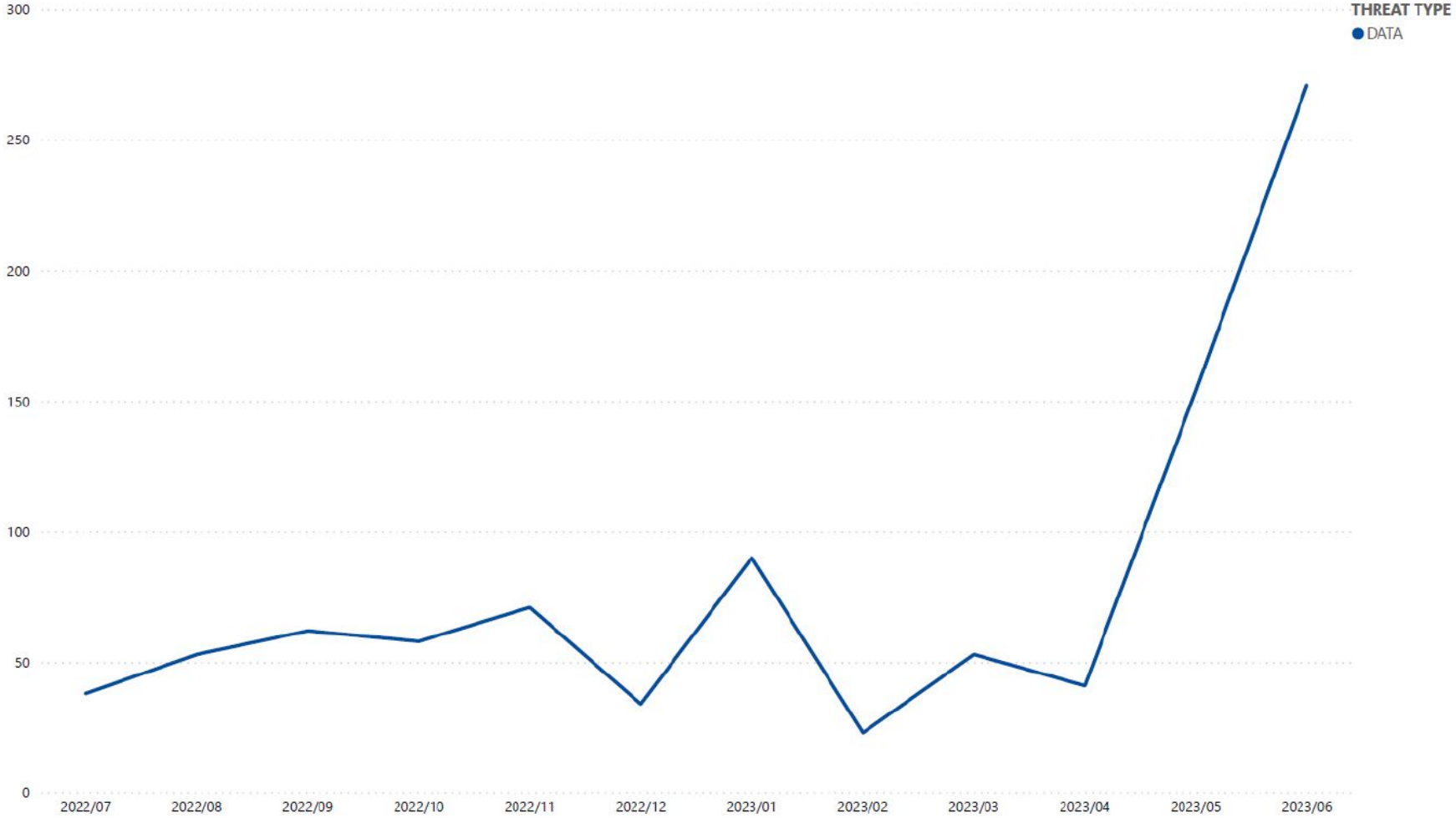
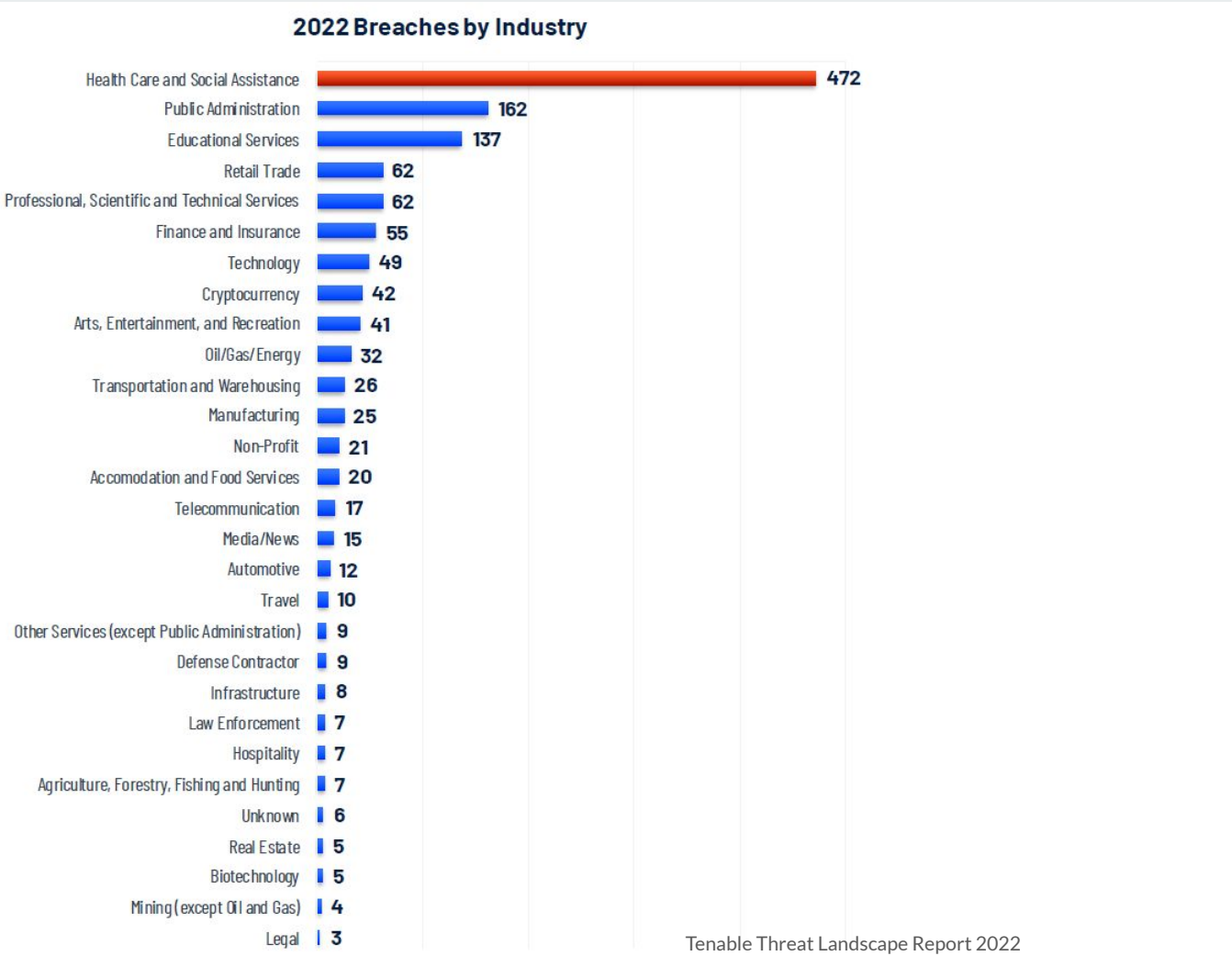


Figure 4 | *Total Compromises & Victims*

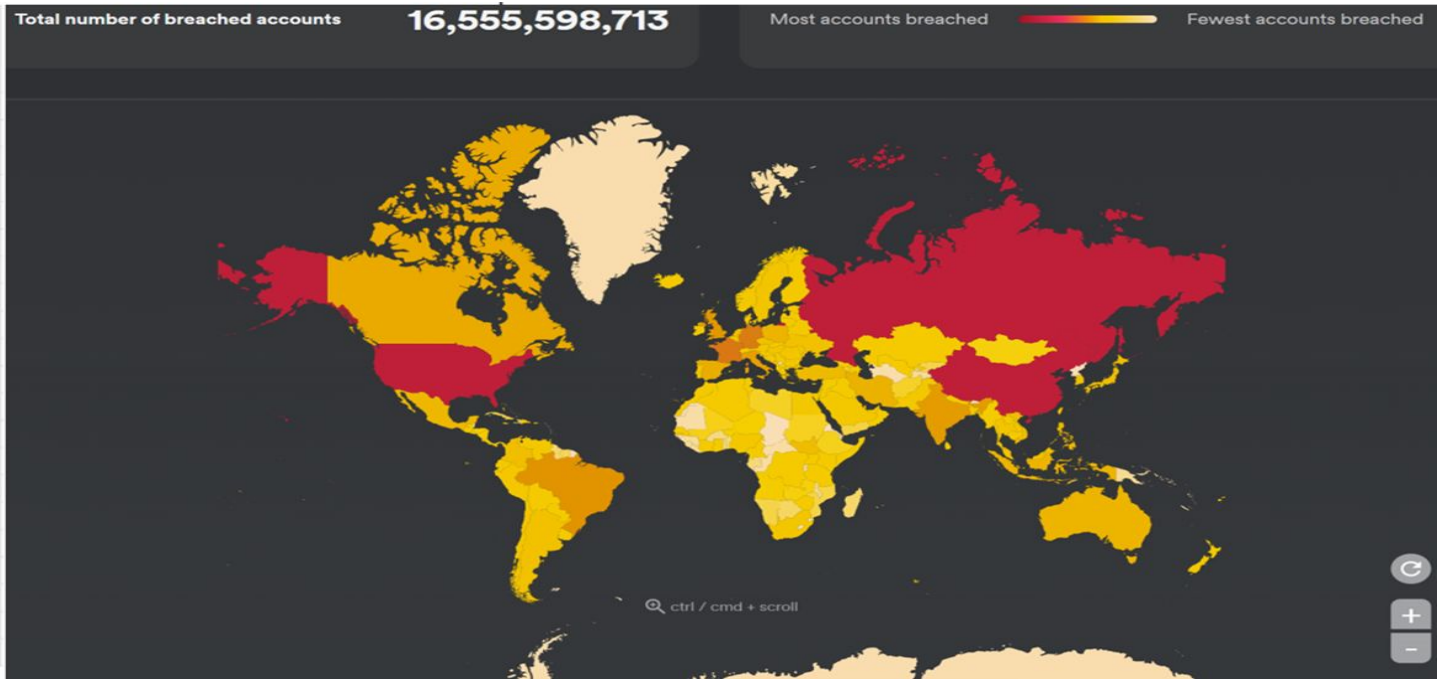
Figure 34: Time series of major incidents observed by ENISA (July 2022 - June 2023)





Tenable Threat Landscape Report 2022

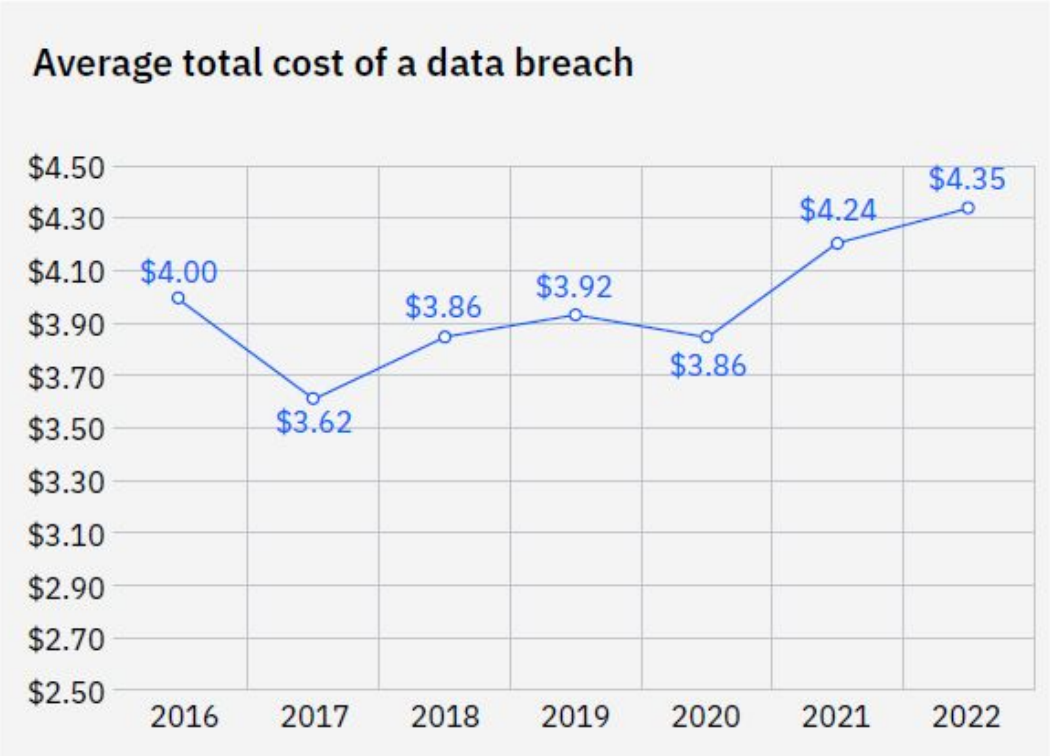
Global ranking by total breaches	Country/territory	Total breaches (leaked email addresses) since 2004
	Unknown	4801401259
1	US	2767381110
2	Russia	2332257266
3	China	1032311473
4	France	514216075
5	Germany	478482819
6	Brazil	346612565
7	UK	307958443
8	India	292915940
9	Italy	263493015
10	Canada	207682350
11	Spain	182821915
12	Iran	160264119
13	Indonesia	143742302
14	Poland	142666284
15	Australia	137039655
16	Micronesia	130041676
17	Philippines	123821843
18	Mexico	120647662
19	Turkey	104811849
20	Japan	92031863



Κατά μέσο όρο

- Μια μοναδική ηλεκτρονική διεύθυνση παραβιάζεται 3 φορές
- Για κάθε 100 άτομα 75 μοναδικές ηλεκτρονικές διευθύνσεις παραβιάζονται
- 207 λογαριασμοί παραβιάζονται ανά 100 άτομα

SurfShark Data Breach Monitoring



IBM Cost of Data Breach Report 2022
(**globally**)

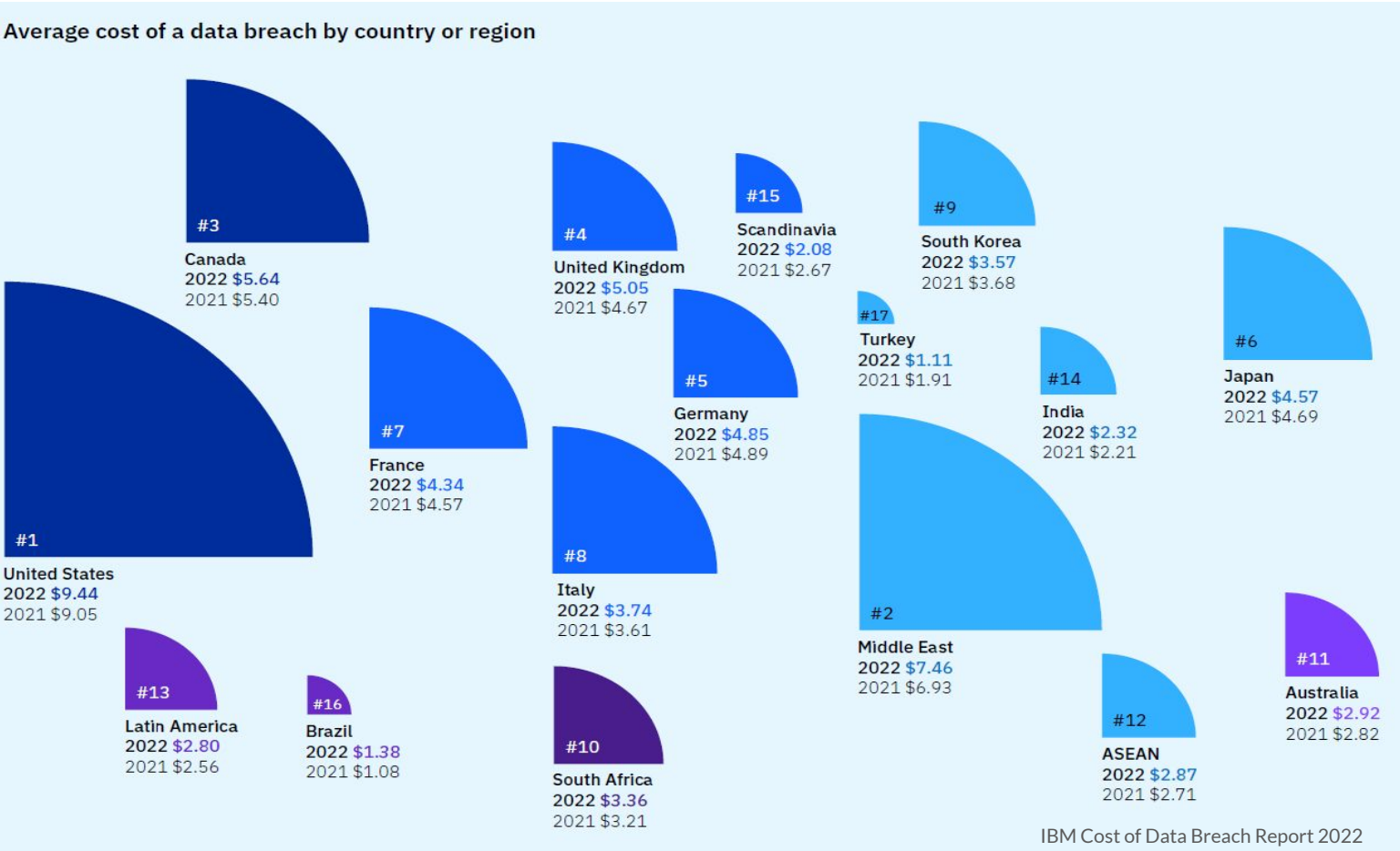


Figure 3: Measured in USD millions

Κίνητρα

- Οι περισσότερες επιθέσεις πραγματοποιούνται από επαγγελματίες που μετατρέπουν την πληροφορία σε κέρδος
- Υπάρχει σημαντική παρουσία του ακτιβισμού μέσω επιθέσεων σε μεγάλες επιχειρήσεις

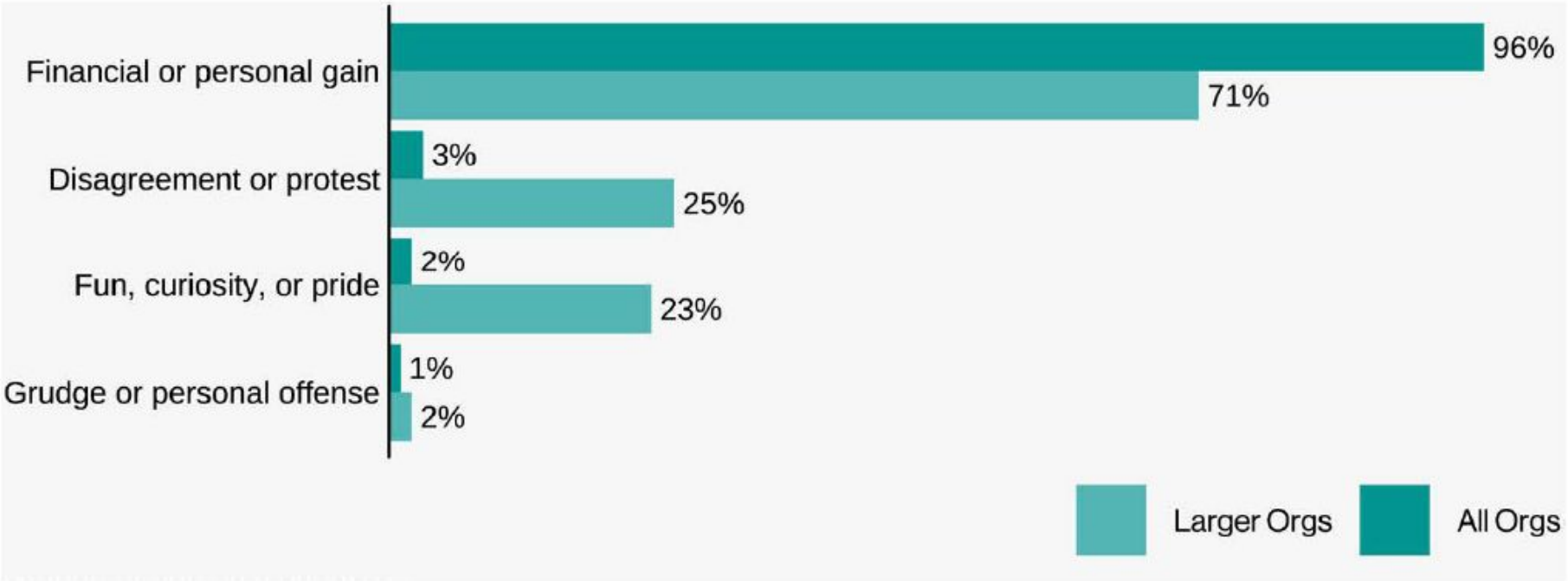


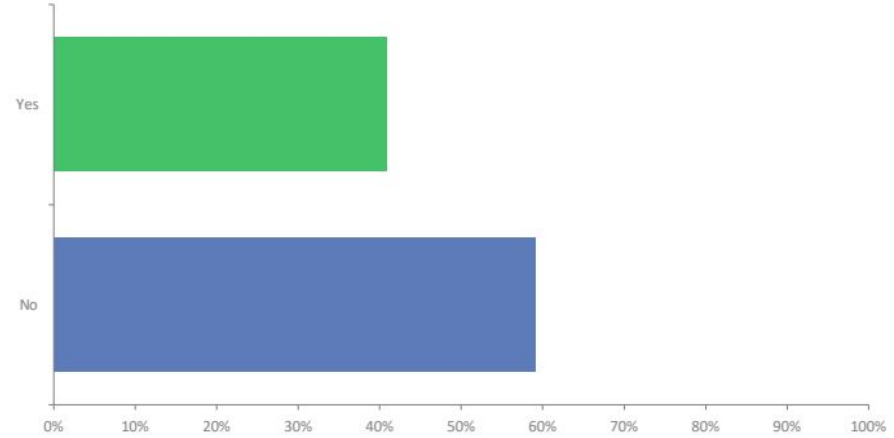
Figure 14. Motive in external agents by percent of breaches within external

Verison Data Breach investigations Report 2022

Κακόβουλη χρήση ταυτότητας

- **Misused Identity**: Υπάρχουν στοιχεία που καταδεικνύουν ότι τα προσωπικά δεδομένα κάποιου έχουν χρησιμοποιηθεί κακόβουλα
- **Compromised Identity**: Τα προσωπικά δεδομένα κάποιου έχουν εκτεθεί και ο κίνδυνος κακόβουλης χρήσης τους είναι υπαρκτός αλλά όχι αποδεδειγμένος
- **ITRC Trends in Identity Report 2022**
    - 40% των καταναλωτών αναφέρουν ότι προσωπικά τους δεδομένα έχουν κλαπεί ή χρησιμοποιηθεί κακόβουλα
    - Οι περισσότερες αναφορές το 2021 και το 2022 για compromised identity αφορούσαν την Google Voice (53% – 3.926 και 61% – 4.081 θύματα αντίστοιχα)
    - Στην κακόβουλη χρήση ταυτότητας μεσω υπάρχοντος λογαριασμού έναντι δημιουργίας νέου, πρώτα έρχονται τα κοινωνικά δίκτυα έναντι των πιστωτικών καρτών

1. Has your identity/personal information (SSN, DL, Login/ Password, account number, etc.) been stolen, compromised, or misused in the past 12 months as the result of a data breach or identity crime?



ANSWER CHOICES	RESPONSES	
Yes	40.92%	561
No	59.08%	810
TOTAL		1371


2022 Reported Identity Crimes
14,817
TOTAL CRIMES REPORTED
Less Than
1% Decrease
FROM 2021
COMPROMISED CREDENTIALS
55% – 8,199 CASES
MISUSED CREDENTIALS
40% – 5,961 CASES
REQUESTING PREVENTION
3% – 437 CASES
ATTEMPTED MISUSE
1% – 220 CASES
2022 Identity Misuse
61%
EXISTING ACCOUNT TAKEOVER (ATO)
32%
NEW ACCOUNT CREATION
IDENTITY MISUSE BY CATEGORY
Existing Account Takeover
New Account Creation
88% NON-GOVERNMENT, NON-FINANCIAL 12%
48% FINANCIAL 52%
62% FEDERAL 38%
30% STATE 70%
Number of Crimes Reported Per Victim in 2022
89% One Incident or Requesting Prevention
8% Two Incidences
2% Three Incidences
1% Four or More Incidences
2022 Identity Compromises
80%
COMPROMISES DUE TO A SCAM
3% Increase
FROM 2021
GOOGLE VOICE
61% – 4,081 VICTIMS

Figure 5 | *Top Three ATO by Account*

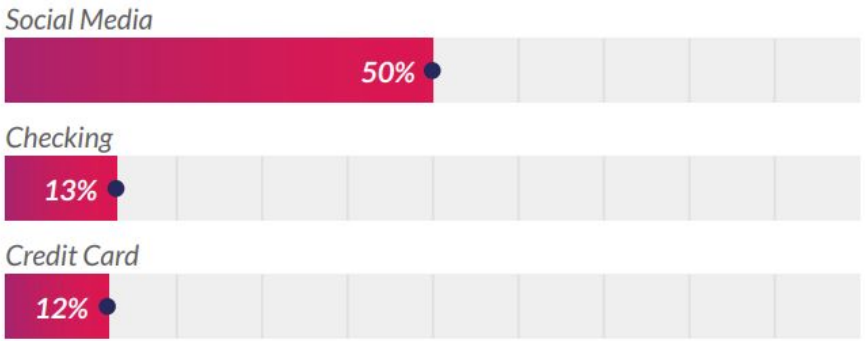
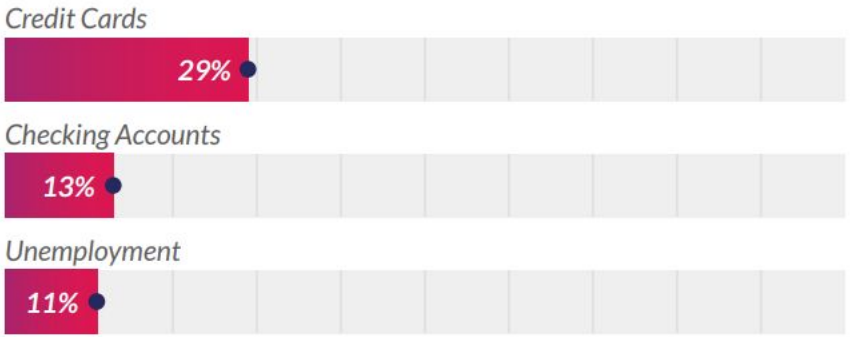


Figure 8 | *Top Three New Accounts Created by Account*



Καταγραφή επιθέσεων

- 2022 Αμερική: 34% των αναφορών έχει πληροφορίες για την επίθεση και το θύμα (χαμηλότερο 5ετίας)
- Ευάλωτοι πολίτες
- Αδυναμία αντιμετώπισης του φαινομένου
- IBM Cost of Data breach Report: Διάμεσος αριθμός μερών εντοπισμού της επίθεσης 207 ημέρες
- Αιτίες:
    - Αποφάσεις δικαστηρίων για ελάχιστη κατάθεση πληροφορίας
    - Απόκρυψη από εταιρίες (2022 Samsung σε έκθεση δεδομένων)
    - Εγγενής δυσκολία εντοπισμού λόγω όγκου επιθέσεων

Figure 1 | *Notices with Attack Details*

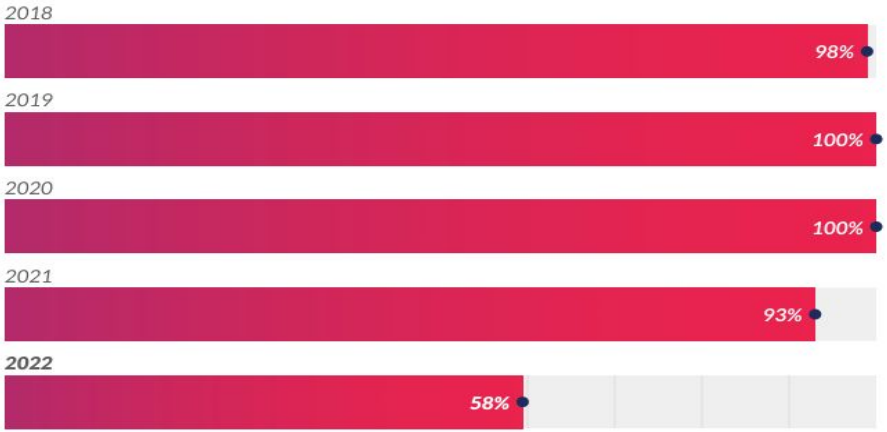


Figure 2 | *Notices with Attack & Victim Details*

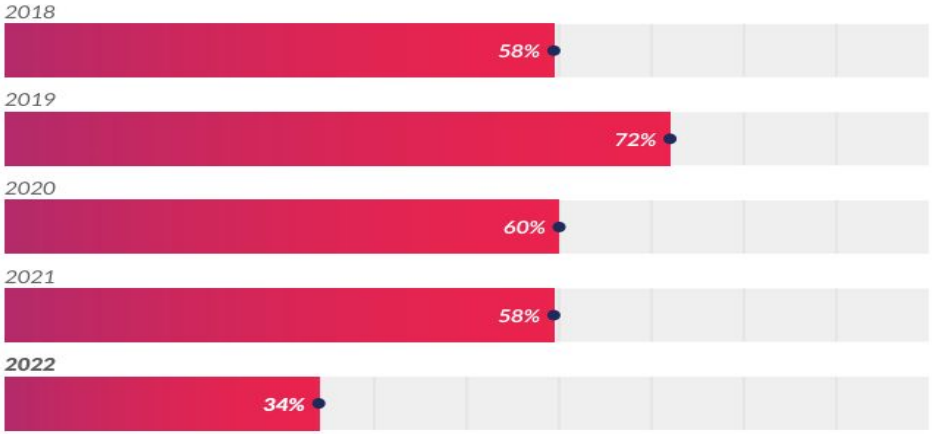


Figure 5 | *Data Breach Notices with Details*

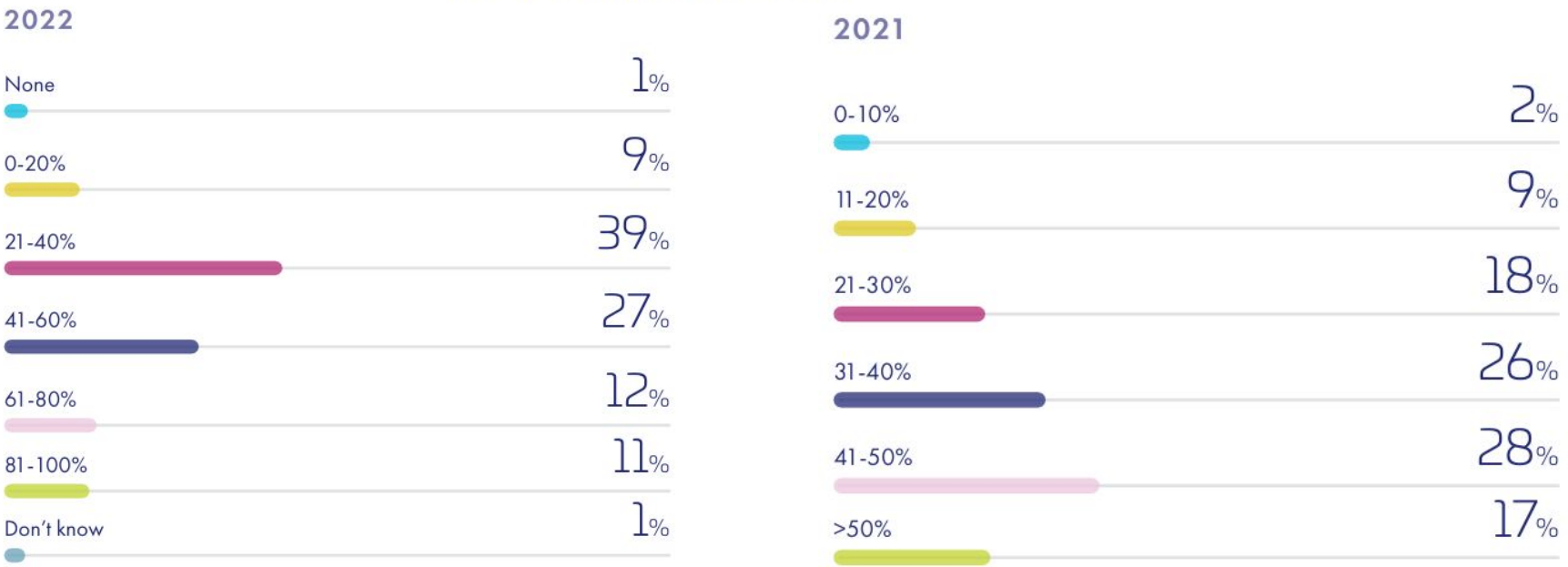
	2022	2021	2020	2019	2018
Compromises	**1,802**	1,862	1,108	1,279	1,175
Notices with Attack Vectors/Details	**1,045**	1,732	1,107	1,277	1,163
Percentage	**58%**	93%	~100%	~100%	99%
Notices with Victim Count & Attack Vectors/Details	**605**	1,075	663	917	681
Percentage	**34%**	58%	60%	72%	58%

Υπηρεσίες cloud

- Αύξηση χρήσης υπηρεσιών cloud
- Τα μέτρα ασφαλείας είναι χαμηλά
- Έλλειψη εξειδικευμένου προσωπικού σε θέματα ασφαλείας στο cloud
- Thales Data Threat report 2022
    - (Πολυπλοκότητα) 51% δυσκολία σε ασφαλεια cloud vs on-premise
    - (Πολλαπλοί πάροχοι) 79%
- Παραβίαση Microsoft Azure 2022: 2.4 terabytes 150.000 εταιρίες 123 χώρες
- Παραβίαση Amazon Prime 2022: 215 εκτμ εγγραφές με πληροφορίες συνδρομής/μετάδοσης

Encrypted Sensitive Data

WHAT PERCENTAGE OF YOUR SENSITIVE DATA IN THE CLOUD IS ENCRYPTED?



Source: 451 Research's 2021 and 2022 Data Threat custom survey

Μηχανική Μάθηση

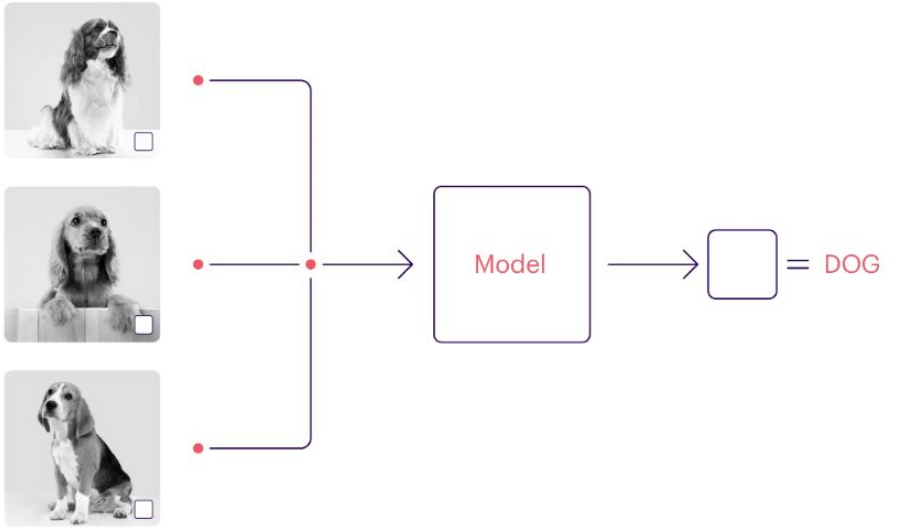
- Αυτοματοποίηση διαδικασιών
- Εντοπισμός μοτίβων
- Βελτιστοποίηση λήψης αποφάσεων
- Αύξηση παραγωγικότητας
- Μείωση κόστους

AI Attacks - Data manipulation

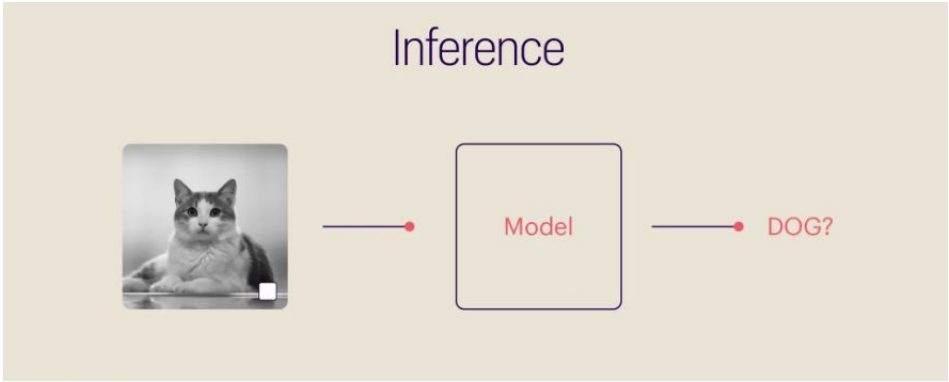
- **Data Poisoning**: Επιθέσεις κατά τις οποίες αλλοιώνονται τα δεδομένα εκπαίδευσης με σκοπό να επηρεάσουν την ακρίβεια των προβλέψεων των μοντέλων
- **Adversarial Attacks**: Επιθέσεις κατά τις οποίες αλλοιώνονται τα δεδομένα εισόδου κατά τη διαδικασία πρόβλεψης μοντέλων σε νέα δεδομένα.
- **Information Manipulation:** Συνίσταται στη δημιουργία σύγχυσης/ψευδών εντυπώσεων σε ομάδα ατόμων μέσω της διάδοσης διαστρεβλωμένης ή αλλοιωμένης πληροφορίας.

Data Poisoning

Training



Inference



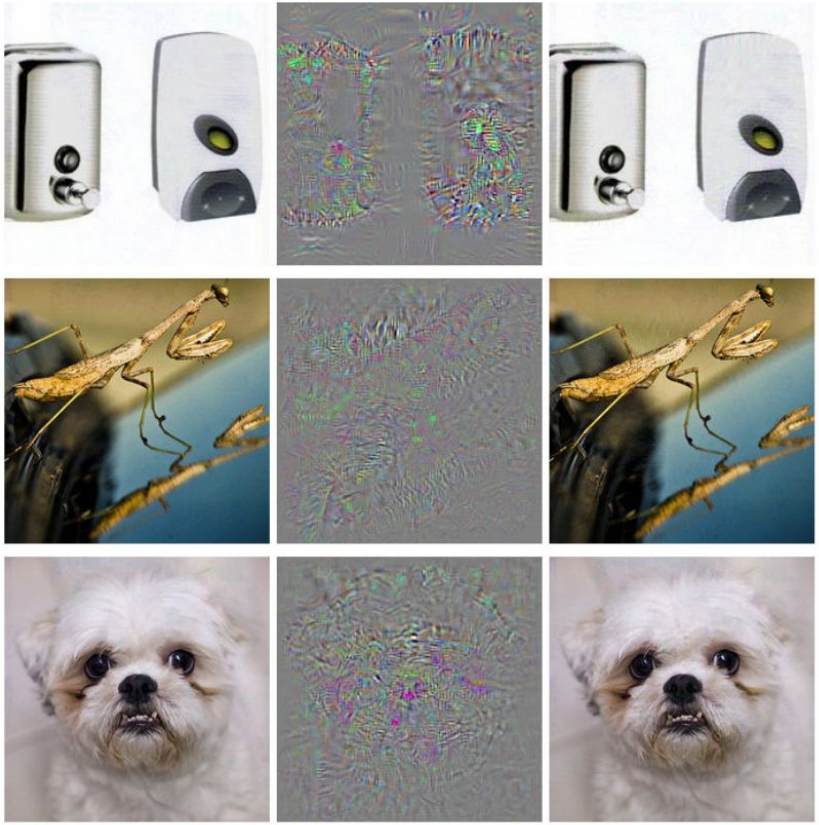


FIGURE 10.12: Adversarial examples for AlexNet by Szegedy et al. (2013). All images in the left column are correctly classified. The middle column shows the (magnified) error added to the images to produce the images in the right column all categorized (incorrectly) as “Ostrich”. “Intriguing properties of neural networks”, Figure 5 by Szegedy et al. CC-BY 3.0.

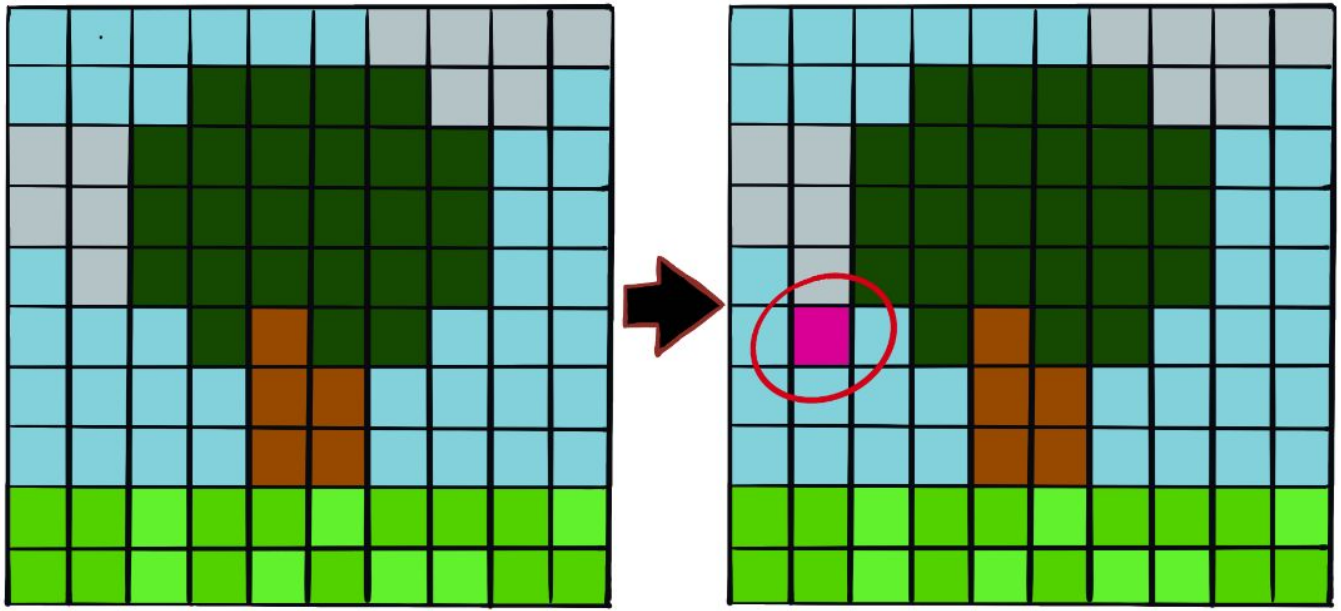


FIGURE 10.13: By intentionally changing a single pixel a neural network trained on ImageNet can be deceived to predict the wrong class instead of the original class.

Su, Jiawei, Danilo Vasconcellos Vargas, and Kouichi Sakurai. “One pixel attack for fooling deep neural networks.” IEEE Transactions on Evolutionary Computation (2019)

Information manipulation

Το πραγματικό πρόσωπο της παραλίας της Θεσσαλονίκης (efsyn 1/4/20)

Chatbots

- (Florian Tramèr): Δεδομένα εκπαίδευσης είναι ένα πολύ μεγάλο μέρος των δεδομένων όλου του διαδικτύου
- Επιθέσεις σε τέτοια μοντέλα
  - Δίνουν εν δυνάμει τεράστιο οικονομικό όφελος (πχ Bias in search engines)
  - Τεράστιος αντίκτυπος
  - 2023 έκθεση δεδομένων από ChatGPT λόγω bug