

The background image shows a person's hands typing on a laptop keyboard. Overlaid on the scene is a complex digital interface with glowing blue lines and dots, resembling a circuit board. Various security-related icons are scattered across the interface, including padlocks, a document with a lock, an envelope with a lock, a laptop with a lock, and a shield with a lock. The overall color scheme is dark blue and black, with the glowing elements providing a high-tech, futuristic feel.

PERSONAL SECURITY IN A POST-PANDEMIC AGE

DEFCAMP 12

NOVEMBER 10TH, 2022

<https://youtu.be/KHMNPjkd5-0>



22. 28. 20

TUDOR DAMIAN

■ IT Advisor & Trainer

- Cloud Strategy & Governance
- IT Infrastructure & Operations
- Business Process Optimization
- Digital Transformation
- IT Risk Management
- Cybersecurity

■ Co-founder @ ITCamp

■ Contact: tudy.ro



SESSION OVERVIEW

■ **Post-pandemic industry trends**

- Nation State actors are more active than ever
- Cyber Influence Operations become increasingly sophisticated

■ **Common types of attacks on the rise**

- CaaS (Cybercrime-as-a-Service), Phishing & Malspam, Ransomware, BEC (Business Email Compromise), Cyber Extortion (Cy-X), Credential Stuffing, Password Spraying, MFA Bypass & MFA Fatigue, Vishing & Smishing, QR Code Exploits, Mobile Interception, IoT & OT attacks, Zero-Days, Synthetic Media

■ **Solutions & next steps**



LET'S START WITH A TABLE



HIVE SYSTEMS AND THEIR “PASSWORD TABLE”

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years



› Learn about our methodology at hivesystems.io/password

THE HIVE SYSTEMS METHODOLOGY (2022)



- Using **hashcat** and a **current-gen GPU** (RTX 3090)
- **Assumptions:**
 - Most sites still use MD5, with or without salt
 - BCRYPT and PBKDF2 SHA-256 (Password-Based Key Derivation Function) are seeing increased adoption
 - MFA is not used or has been bypassed via other means
 - Passwords are randomly generated (non-random password are easier to crack)
 - The password has not been a part of a past data breach
 - Metrics assume a finite "sample space" of 650 characters (ASCII lowercase, uppercase, numbers, symbols, Latin Set + Ext A-D, Cyrillic)
- **More info:** <https://www.hivesystems.io/password>

MD5 - RTX 2080

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	61tm years	100tn years	7qd years

MD5 - RTX 3090

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	3 secs
7	Instantly	Instantly	15 secs	51 secs	4 mins
8	Instantly	3 secs	13 mins	52 mins	5 hours
9	Instantly	1 mins	11 hours	2 days	2 weeks
10	Instantly	34 mins	3 weeks	5 months	3 years
11	1 sec	15 hours	3 years	24 years	300 years
12	14 secs	2 weeks	200 years	1k years	20k years
13	2 mins	1 year	9k years	91k years	2m years
14	24 mins	29 years	483k years	6m years	118m years
15	4 hours	800 years	25m years	251m y	9bn years
16	2 days	20k years	1bn years	22bn y	697bn years
17	2 weeks	518k years	68bn years	1tn years	54tn years
18	5 months	13m years	4tn years	84tn years	4qd years

MD5 - 8 X A100 GPUS (AMAZON EC2 P4D.24XLARGE)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	instant	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

BCRYPT - RTX 3090

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	5 secs	1 min	3 mins	1 min
5	1 sec	2 mins	1 hour	3 hours	8 hours
6	10 secs	53 mins	2 days	7 days	4 weeks
7	2 min	1 week	4 months	1 year	5 years
8	17 min	11 months	18 years	72 years	400 years
9	3 hours	2 years	900 years	4k years	31k years
10	1 day	46 years	47k years	275k years	2m years
11	2 weeks	1k years	2m years	17m years	185m years
12	4 months	31k years	128m years	1bn years	14bn years
13	3 years	813k years	180m years	66 bn years	1tn years
14	33 years	21m years	346bn years	4tn years	84tn years
15	300 years	550m years	18tn years	252tn years	6qdn years
16	3k years	14bn years	937tn years	6qdn years	500qdn years
17	33k years	372bn years	49qdn years	969qdn years	39qntn years
18	328k years	10tn years	3qntn years	60qntn years	3 sxtn years

BCRYPT - 8 X A100 GPUS (AMAZON EC2 P4D.24XLARGE)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	7 secs	14 secs	14 secs
5	Instantly	11 secs	6 mins	14 mins	42 mins
6	Instantly	5 mins	5 hours	15 hours	2 days
7	9 secs	2 hours	2 weeks	1 month	6 months
8	2 mins	2 days	2 years	6 years	36 years
9	15 mins	2 months	82 years	400 years	3k years
10	3 hours	4 years	4k years	25k years	215k years
11	1 day	100 years	221k years	2m years	17m years
12	2 weeks	3k years	11m years	95m years	1bn years
13	4 months	73k years	596m years	6bn years	98bn years
14	3 years	2m years	31bn years	364bn years	8tn years
15	29 years	49m years	2tn years	23tn years	582tn years
16	300 years	1bn years	84tn years	1qdn years	45qdn years
17	3k years	33bn years	4qdn years	87qdn years	3 qntn years
18	29k years	865bn years	227qdn years	5qntn years	266 qntn years

PBKDF2 SHA-256 - RTX 3090

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	2 secs	4 secs	4 secs
5	Instantly	3 secs	2 mins	4 mins	12 mins
6	Instantly	1 min	1 hour	4 hours	15 hours
7	3 secs	35 mins	3 days	2 weeks	2 months
8	26 secs	15 hours	5 months	2 years	10 years
9	4 mins	2 weeks	23 years	100 years	800 years
10	44 mins	1 year	1k years	7k years	61k years
11	7 hours	31 years	63k years	435k years	5m years
12	3 days	800 years	3m years	27m years	363m years
13	1 month	21k years	170m years	2bn years	28bn years
14	10 months	539k years	9bn years	104bn years	2tn years
15	8 years	14m years	460bn years	6tn years	166tn years
16	84 years	365m years	24tn years	399 tn years	13 qdn years
17	800 years	9bn years	1qdn years	25 qdn years	983 qdn years
18	8k years	246bn years	65 qdn years	2 qntn yrs	76qntn years

WHAT ABOUT STOLEN OR REUSED PASSWORDS?

- Rainbow tables
- Dictionary attacks
- Previously stolen hashes
 - Data Breach compilations/lists

Password reuse is still a common practice



WHAT ABOUT STOLEN OR REUSED PASSWORDS?

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	Instantly
9	Instantly	Instantly	Instantly	Instantly	Instantly
10	Instantly	Instantly	Instantly	Instantly	Instantly
11	Instantly	Instantly	Instantly	Instantly	Instantly
12	Instantly	Instantly	Instantly	Instantly	Instantly
13	Instantly	Instantly	Instantly	Instantly	Instantly
14	Instantly	Instantly	Instantly	Instantly	Instantly
15	Instantly	Instantly	Instantly	Instantly	Instantly
16	Instantly	Instantly	Instantly	Instantly	Instantly
17	Instantly	Instantly	Instantly	Instantly	Instantly
18	Instantly	Instantly	Instantly	Instantly	Instantly

PASSWORD HYGIENE IS STILL AN ISSUE

- **Commonly used passwords** are easy to guess
- 59% of people use their **name or birthdate in their password**
- 43% have **shared their password with someone** (20% have **shared their email password**)
- Only 45% would **change a password after a breach**
- 42% of organizations **rely on sticky notes for password management** (Ponemon Institute)
- Almost 2/3 of people use **the same password across multiple accounts**
- 42% **rely on memory for work passwords**
- 78% of people have had to **reset their passwords in the last 3 months**
- Employees use the **same password an average of 13 times** (Lastpass)
- MFA **blocks 99.9% of all attacks**
- Employees at **57% of business use MFA**
- 24% of people use a **Password Manager** (mobile apps helped with that)





THE STORY SO FAR



2020 – PANDEMIC, YEAR 1

- When business left the office in 2020, some left their security strategies behind as well
 - **IT lost control of the connectivity path** for employees
 - Cybersecurity controls and tools on internal network were **less effective**
- Business became **more reliant on public Cloud & SaaS applications**
 - A **rush into Digital Transformation**, with Security low on the priority list
 - Security had to deal with **infrastructures without perimeters**
 - **Your home Wi-Fi** became your IT department's edge network
- **Prevalent scams and fraud** (stimulus packages, news clickbait, etc.)
- **Teleconference hijacking** - disrupting video-teleconferencing (VTC) calls with hate and violent messages
- **Email attacks** increased by 64% in 2020
- 61% of companies experienced a **ransomware attack**

2021 – PANDEMIC, YEAR 2

- **COMB21** (Compilation of Many Breaches) is made public
 - 3.28 billion passwords, 2.18 billion unique emails, 26 million email domains
 - 100GB in size, 1.5 million government emails & 625k government passwords
- \$40 million paid by an insurance company in 2021, in **one of the largest reported ransoms to date**
- **Data Breaches** increased in number and impact
 - Number of US data breaches for Q1-Q3 2021 exceeded all of 2020 by 17%
 - The **cost of a data breach** (downtime, recovery costs, insurance premiums) is **averaging at a little over \$4 million**, while mega-breaches could be 100x that

2022 – THE POST-PANDEMIC (?) AGE

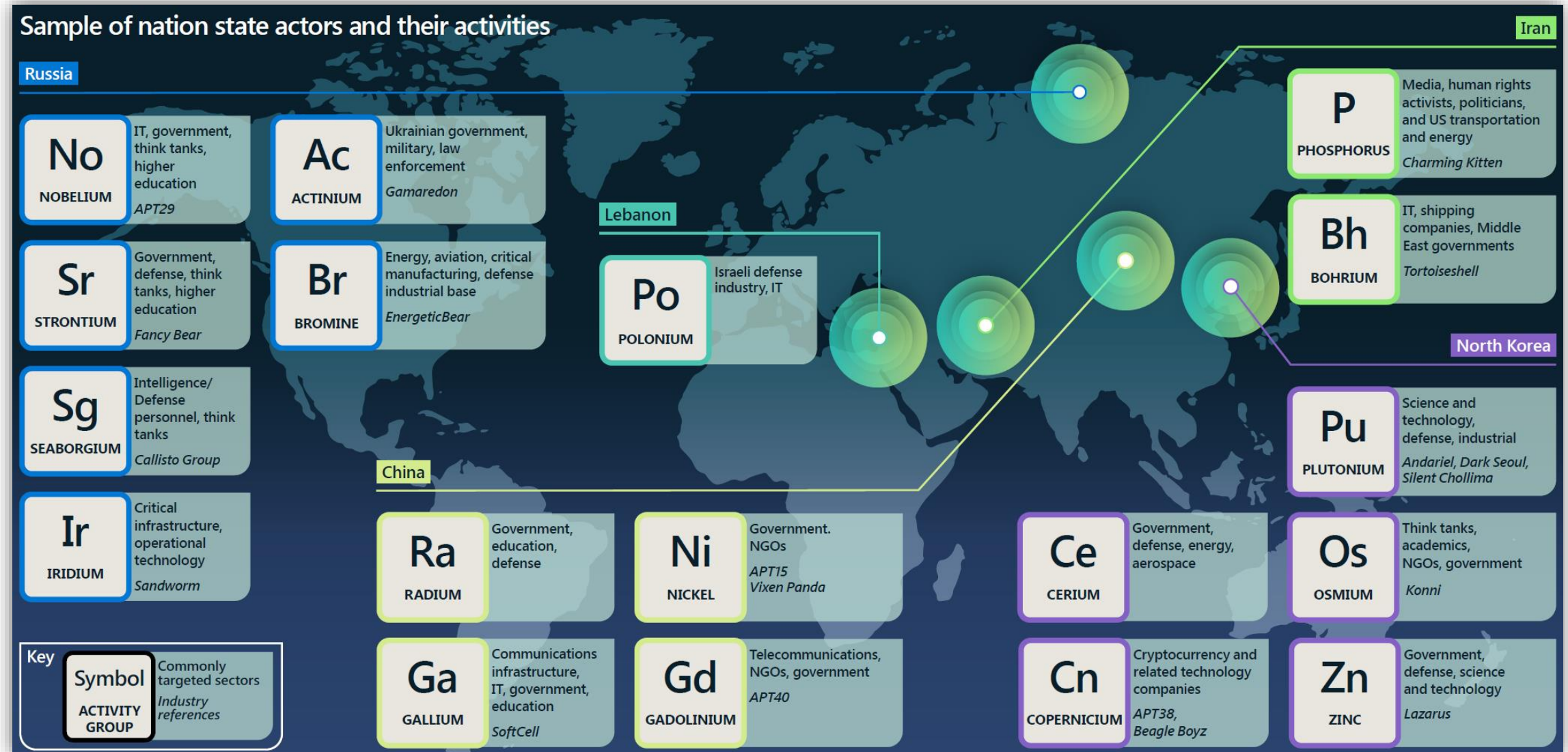
- Just in Q1 2022, ransomware **doubled the total 2021 volume**
- **Password Spraying** is on the rise
 - The result is not pretty: stolen shopping accounts, sensitive data (card numbers, private messages, pictures, documents), identity theft, sending phishing/spam, etc.
- **Volatile geopolitics** triggers new types of attacks
 - **State-sponsored, cybercrime, hacker-for-hire** and **hacktivists** remain prominent threat actors
- **High-profile hacks** occur more often
 - Just in March of 2022 – Ubisoft, NVIDIA, Samsung, Mercado Libre, Vodafone (& more) announced they were hacked
- July 2022 – Akamai mitigates what's probably the **largest European DDoS attack on record**
 - The target was attacked 75 times over 30 days, using UDP fragmentation, ICMP flood, RESET flood, SYN flood, TCP anomaly, TCP fragment, PSH ACK flood, FIN push flood, and PUSH flood, among others
 - The attack peaked at 853.7 Gbps / 659.6 Mpps
- **AI-enabled disinformation/misinformation**, deepfakes, and the rise of disinformation-as-a-service



Hackers take over 1.1 million accounts by trying reused passwords

Photo: January 6, 2022 by Peter Arndt

NATION STATE ACTORS



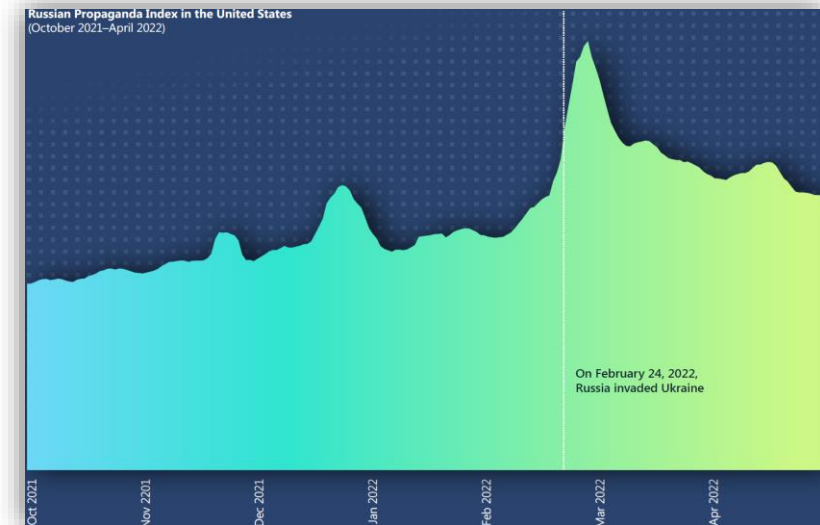
CYBER INFLUENCE OPERATIONS

- Nation States use **cyber-influence operations** to
 - Distribute **propaganda**
 - Impact **public opinion**, both domestically and internationally
 - Erode trust, increase polarization, **threaten democratic processes**
- They use **traditional media** as well as **Internet and social media**

Topics covered by top 10 most-viewed coronavirus stories on RT.com
(October 2021–April 2022)

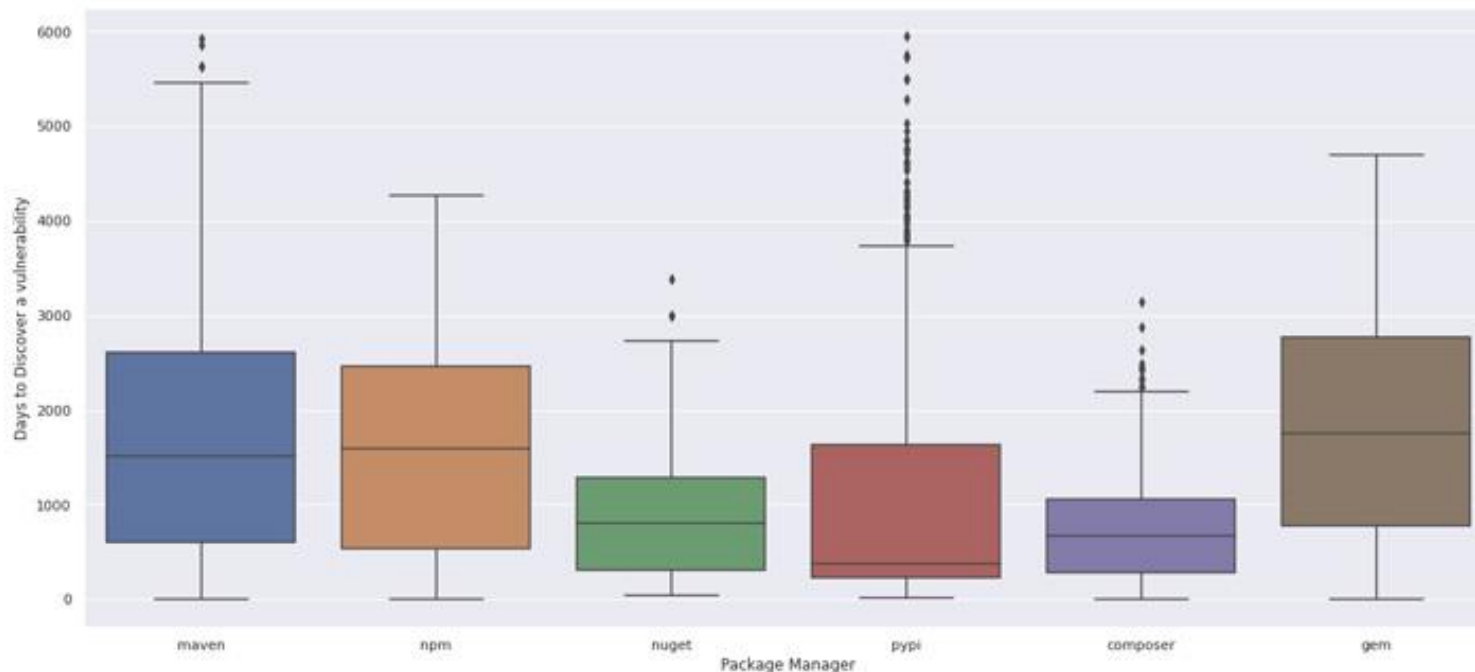
Anti-vaccine propaganda targets non-Russian readers

Russian (Translated below to English)	English
"Lockdowns and boosters prevent transmission"	"Vaccinations fail to curb transmission and are ineffective against new strains"
"Russian public figures are testing positive"	"Pfizer vaccine has dangerous side effects"
"Cases and deaths are increasing in Russia"	"Mass vaccination is politically motivated"
"The Sputnik V vaccine is highly effective"	"Pfizer and Moderna conduct unregulated trials"
"Vaccine proof needed on public transport"	



OPEN SOURCE, OPEN VULNERABILITIES

- A recent study by Emil Wåreus (Debricked) showed the **open-source community** isn't doing a great job on fixing security issues
 - On average, **it takes 800+ days to discover a security flaw** in open-source projects
 - 74% of security flaws stay **undiscovered for over a year**





ATTACKS ON THE RISE



CAAS (CYBERCRIME-AS-A-SERVICE)

■ **Phishing as a Service (PhaaS)**

- Hundreds of site templates/designs
- You provide an email address where you want to receive credentials
- Pay the PhaaS merchant in cryptocurrency

■ **DDoS on a subscription model**

- Outsource the creation and maintenance of the botnet
- You receive an encrypted service and one year of 24/7 support
- The subscription offers different architectures and attack methods, you just select a resource to attack and receive an array of compromised devices
- All this at just \$500 per year

PHISHING & MALSPAM

- Phishing is still **behind 90% of breaches** faced by organizations
 - Emails containing malicious links or attachments
 - Other forms of phishing (vishing, smishing) are included here
- Usually used for **credential theft**, in early stages of attacks
 - Spear Phishing campaigns are more and more common
- It's always been **more of a people problem**
 - Going after people makes it easy to circumvent technical measures

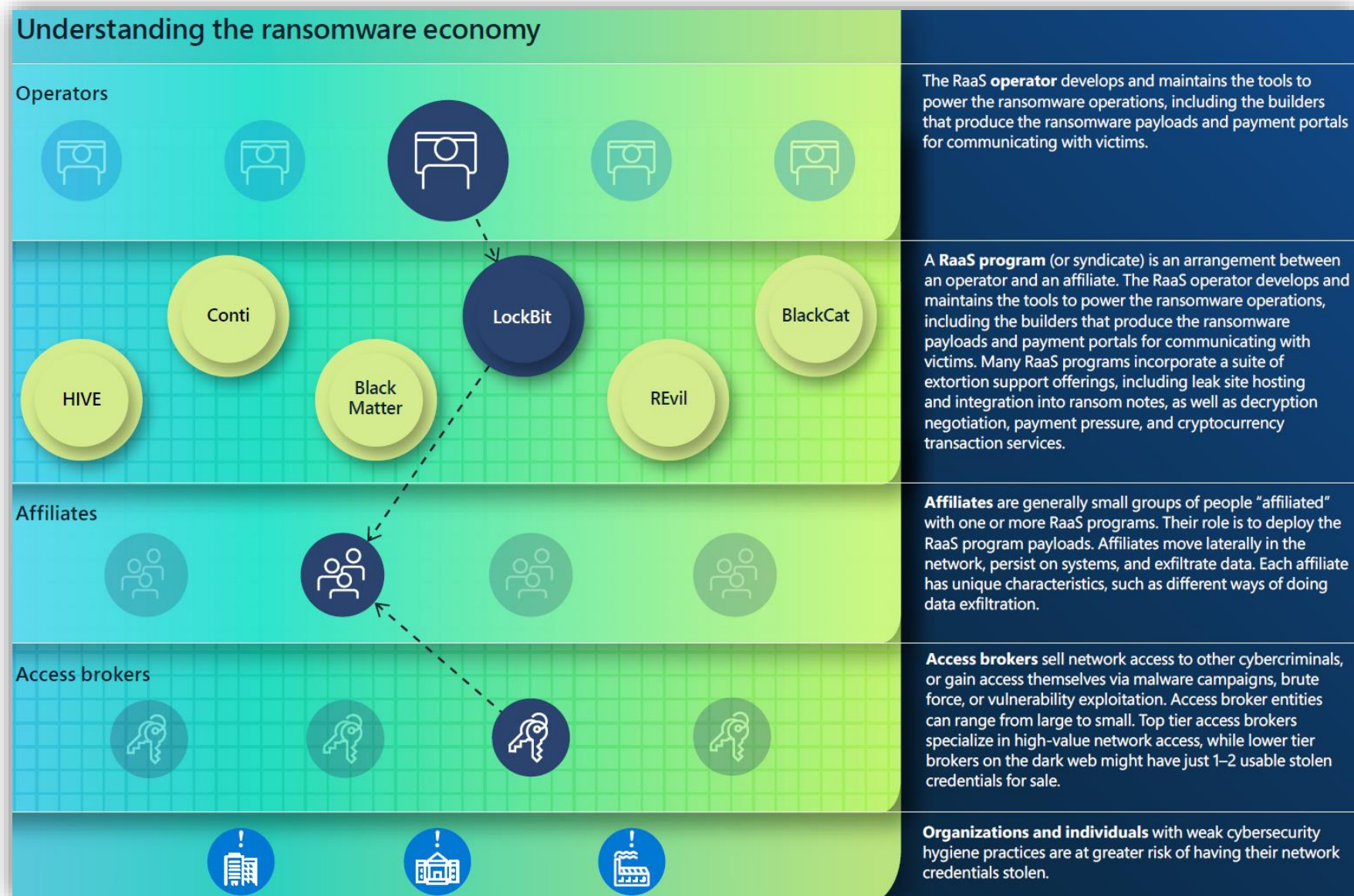


HUMAN-OPERATED RANSOMWARE

- A study on ransomware targeting and rate of success



UNDERSTANDING THE RANSOMWARE ECONOMY



BEC (BUSINESS EMAIL COMPROMISE) ATTACKS

- **Hacking and spoofing emails**, impersonating company staff or vendors
 - Thousands of such attacks occur every month
 - Usually using **homoglyph domains**
- **Identity-driven security** helps
 - Adaptive MFA, Single-Sign-On (SSO)
 - Properly set SPF, DKIM & DMARC records
 - In the end, the truth is **it's a people problem**
- Types of **BEC scams**:
 - Bogus invoice scheme
 - CEO fraud
 - Account compromise
 - Attorney impersonation
 - Data theft

Technique	% of domains showing homoglyph technique
sub l for I	25%
sub i for l	12%
sub q for g	7%
sub rn for m	6%
sub .cam for .com	6%
sub 0 for o	5%
sub ll for l	3%
sub ii for i	2%
sub vv for w	2%
sub l for ll	2%
sub e for a	2%
sub nn for m	1%
sub ll for l, sub l for i	1%
sub o for u	1%

Analysis of over 1,700 homoglyph domains between January–July 2022. While 170 homoglyph techniques were used, 75% of domains used just 14 techniques.

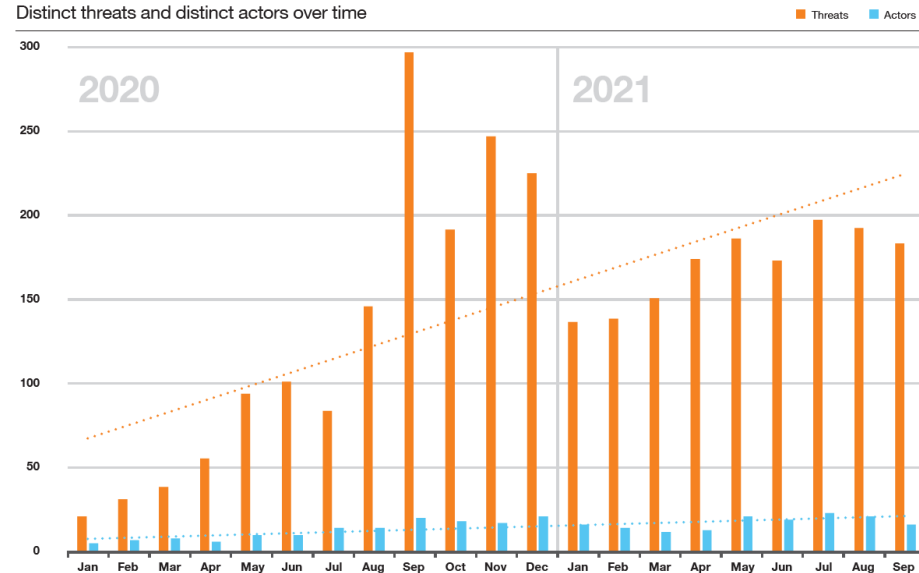


CYBER EXTORTION (CY-X)

- Also known as Double-Extortion
 - A unique form of cybercrime where criminals try to “**victim shame**” leak sites
- Attackers threat to leak stolen data

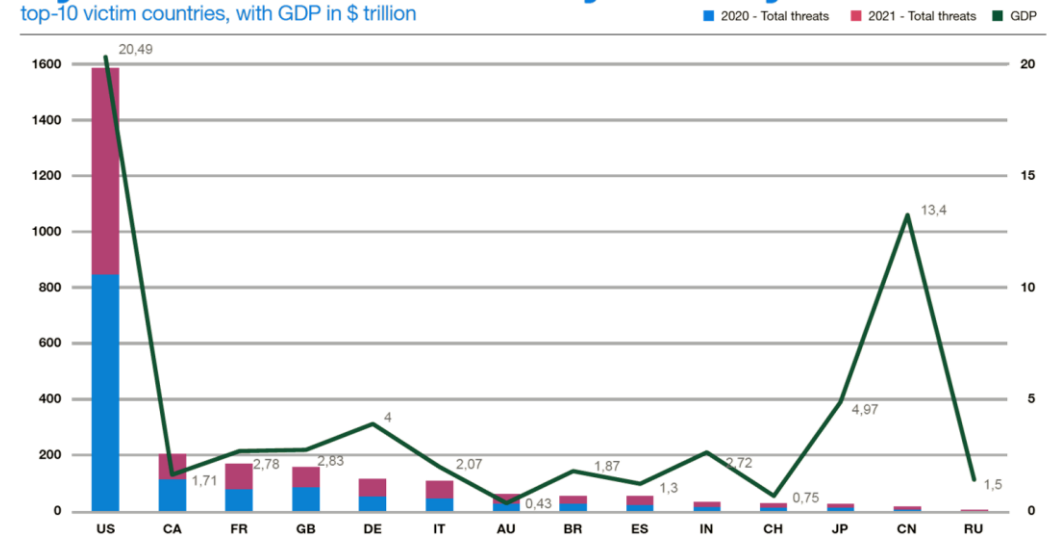
Threats and actors observed

Distinct threats and distinct actors over time



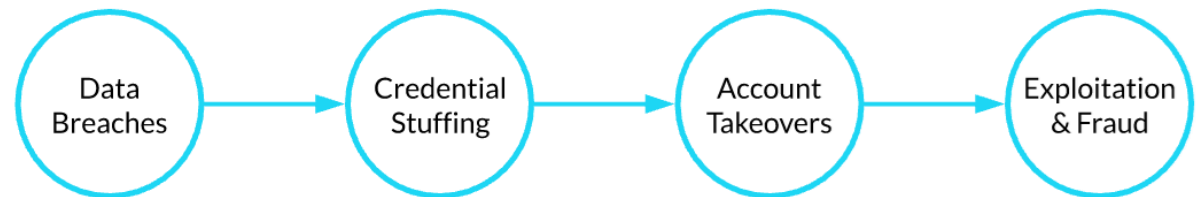
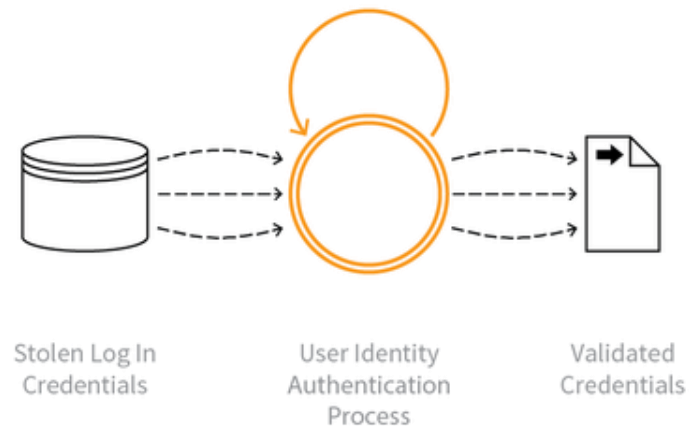
Cy-X leak threat victims by country

top-10 victim countries, with GDP in \$ trillion



CREDENTIAL STUFFING / REUSE

- **Reusing stolen credentials** to automate login requests
 - Uses lists of usernames and/or email addresses and the corresponding passwords, **often from a data breach**
- It's becoming a common occurrence, mainly because people **reuse the same passwords** for other platforms/sites



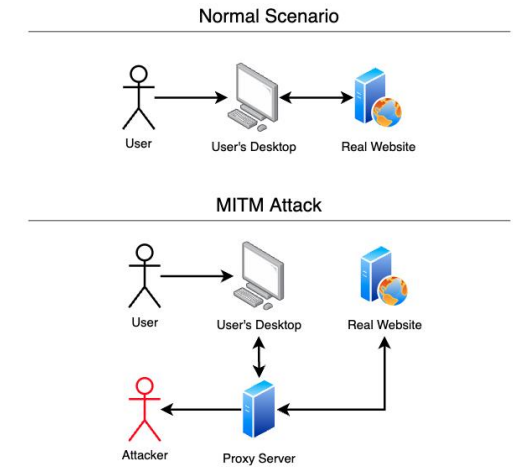
PASSWORD SPRAYING

- Usually, **lockout policies** prevent brute-forcing
- So, what if we try authenticating **against all accounts using just one password**, ideally a leaked, common or easily guessable one?
 - You still get a lot of failed logins, but none of them trigger the lockout
 - You might get lucky with a common password
 - SeasonYear, Company123, PasswordYear, PetnameYear, etc.
 - Wait until observation/lockout window ends, then repeat



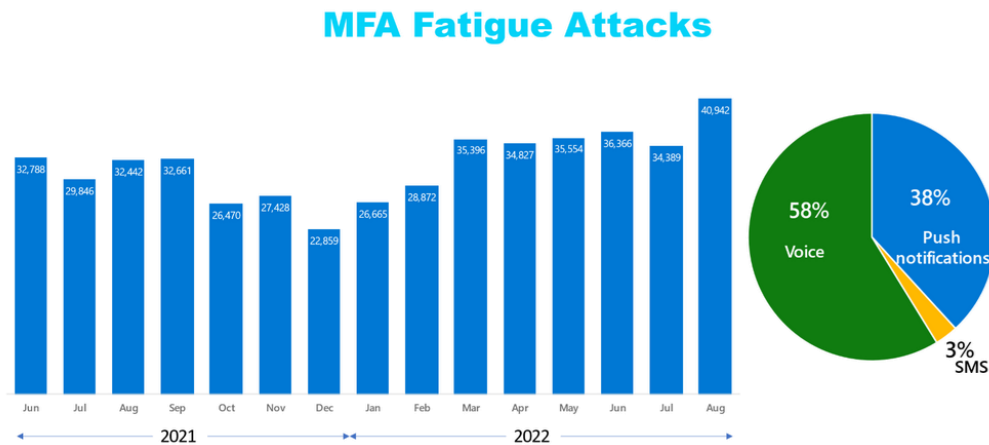
MFA BYPASS

- **Social Engineering** (e.g. cloned websites)
- **Session Hijacking** (e.g. cookie stealing)
- **Consent Phishing** (e.g. gaining OAuth access)
- **Breach Replay** (e.g. hacking a 3rd party with OAuth access)
- **Exploiting Generated Tokens** (e.g. "backup codes")
- **SIM hacking & intercepting OTP** (one-time-passwords)
- **Brute Force** (e.g. a temporary 4-digit PIN)

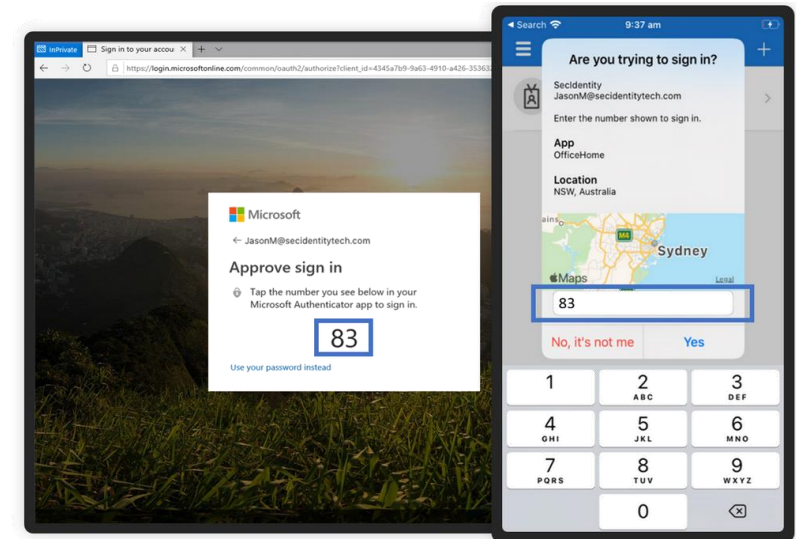


MFA FATIGUE

- Also known as **MFA Prompt Spamming**
 - Or **Push Notification Spamming** 😊
- If you call someone 100 times at 1am while they're trying to sleep, they'll likely accept the MFA prompt



Source: Azure AD Identity Protection sessions at high risk with multiple failed MFA attempts



VISHING & SMISHING

- **Vishing:** voice + phishing
 - During a phone call, attacker uses Social Engineering to get you to share personal information, financial details, account numbers, passwords, etc.
 - Usually, the caller claims to represent IT support, a government or medical institution, etc.
- **Smishing:** SMS + phishing
 - Similar technique, carried over text (SMS, Telegram, WhatsApp, etc.)
 - Often used to send out malware, or to make the user visit a malicious website



QR CODE EXPLOITS

- The “no-touch” / “low-touch” economy has changed things
 - When’s the last time you went to a restaurant and **scanned a QR code to check out the menu?**
- What if someone came in with a **QR code sticker and stuck it on top of the existing code?** The new code could now:
 - Open a pdf of the menu, but with a zero-day “bonus” on top
 - Take you to a malicious website
 - Divert a payment, make a request for money
 - Trigger a malicious action on your device



MOBILE INTERCEPTION

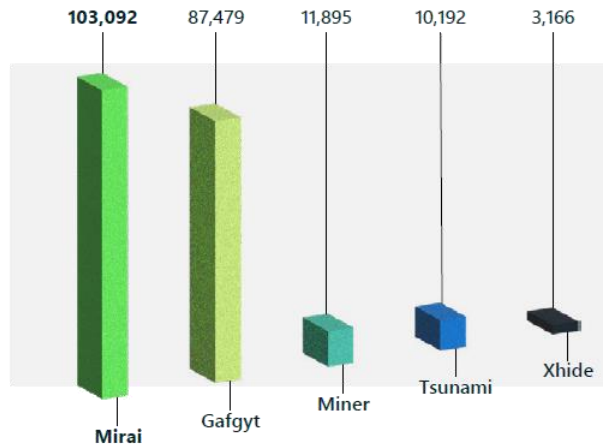
- When everything else fails, you go back to the basics 😊
- **Mobile interception** is the storage, recording, tracking, interception and deciphering of cellular communications such as phone calls, internet usage, SMS, and other text messaging forms
 - Legally, government and law enforcement can use mobile interception to gather info on terrorists and criminals
- Same techniques are used by said criminals
 - Regularly used in data theft or MFA bypass
- Bonus: **SIM Swapping Fraud**
 - ENISA: **50%+ of mobile operators in Europe** have experienced such attacks



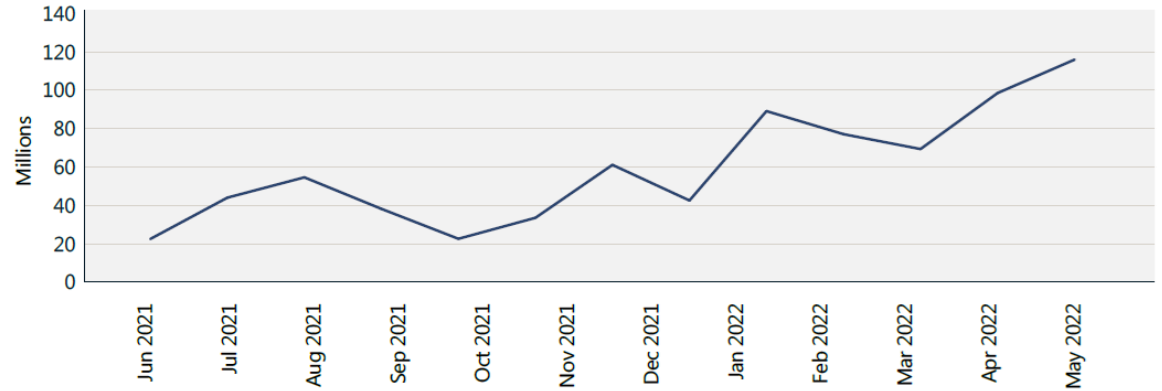
IOT & OT ATTACKS

- **IoT malware** targets multiple CPU architectures (ARM, MIPS, x86-64)
- **Operational Technology (OT)** is seeing attacks on many common industrial control system (ICS) protocols

Top IoT malware detected in the wild

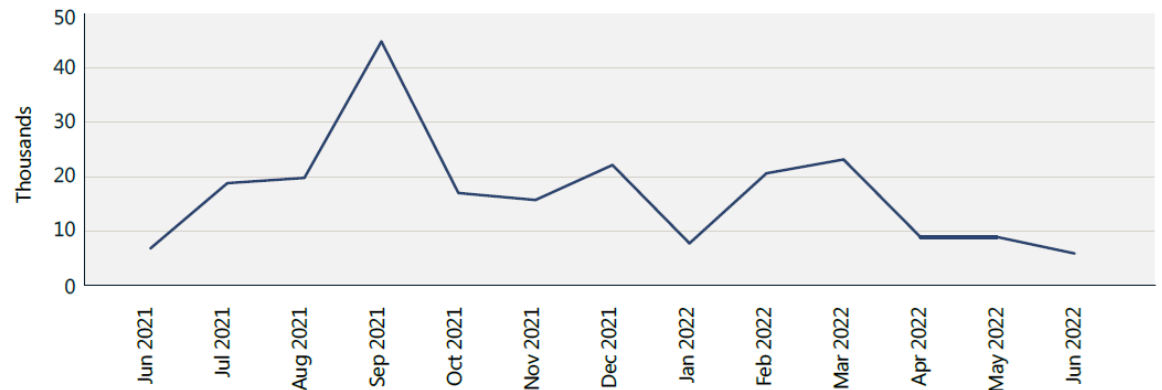


Attacks against remote management devices



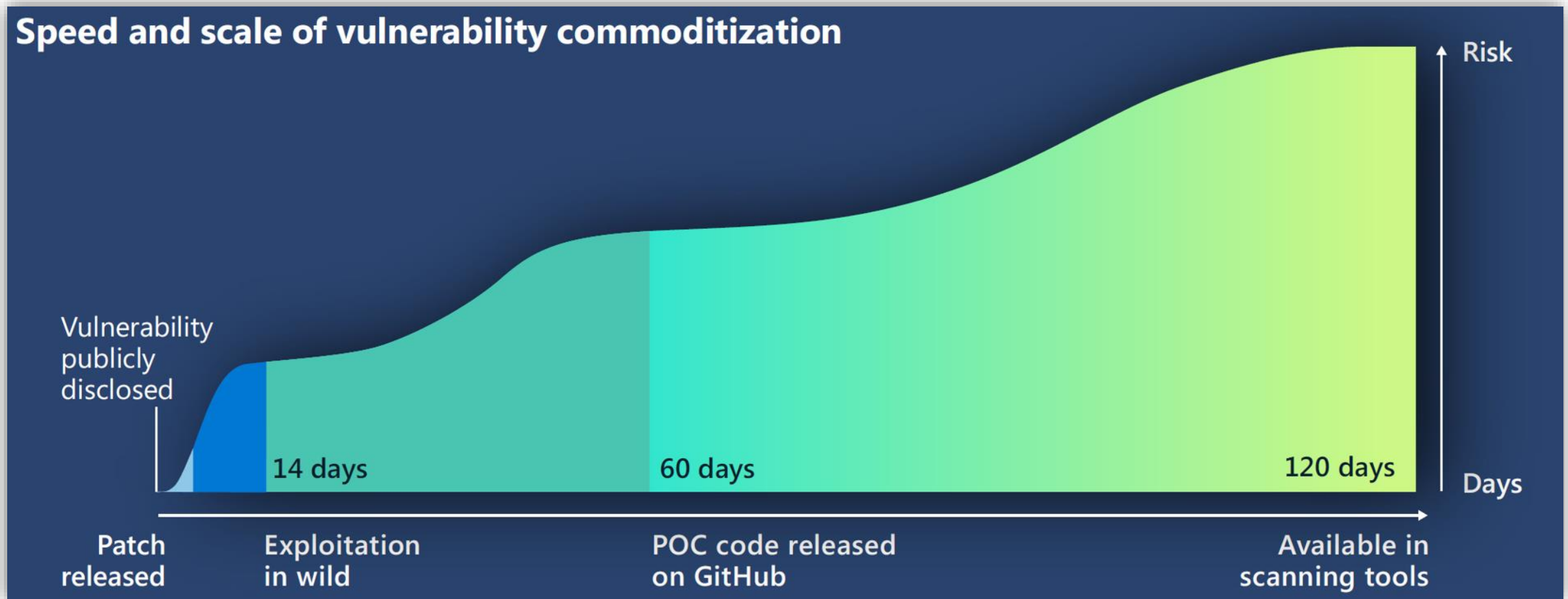
Increasing attacks on remote management ports over time, as seen through the MSTIC sensor network.

Web attacks against IoT and OT



Web attack volume over time, as seen through the MSTIC sensor network. As the number of devices directly connected to the web continues to drop, attackers might eventually be less likely to probe for them.

RAPID VULNERABILITY EXPLOITATION: ZERO DAYS, TODAY



SYNTHETIC MEDIA

- **Face swap (video, images)**

- Attempted blackmail of an individual, company, or institution
- Place individuals in embarrassing locations or situations

- **Puppeteering (video, images)**

- Using a video to animate a still image or second video
- This can make it appear an individual said something embarrassing or misleading

- **Generative adversarial networks (video, images)**

- A family of techniques for generating photorealistic imagery

- **Transformer models (video, images, text)**

- Creating rich imagery from text descriptions






- There's a **900% year-over-year increase in deepfakes** since 2019

- **Categories of attacks:**

- Market manipulation, payment fraud, vishing, impersonations, brand & reputational damage



THE SYNTHETIC MEDIA LANDSCAPE

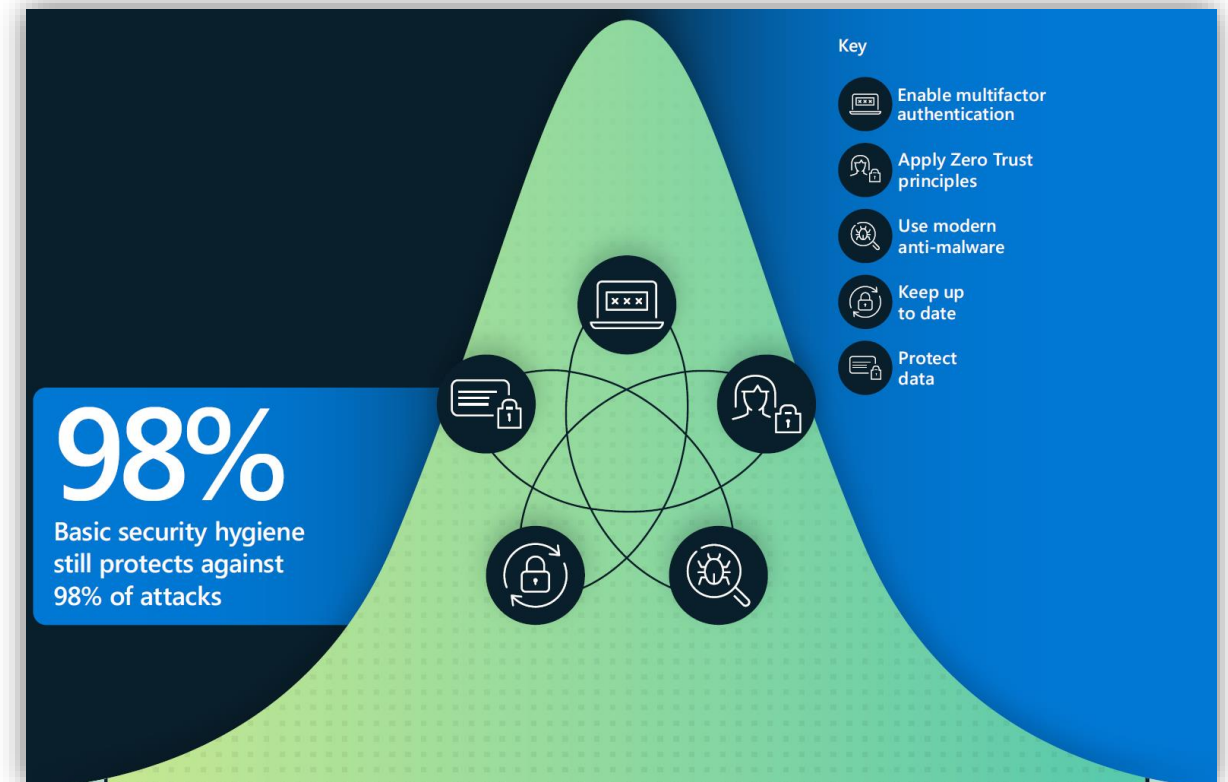
Synthetic media landscape				
 Factors Low barrier to entry	Easy-to-use tools	More sophisticated tools	Easy to distribute	
 Producers Good and harmful uses	Organizations and institutions	Individuals and consumers	Malicious actors to cause harm	
 Distribution Unprecedented speed	Social media amplification	Targeted emails and ads	Audio files via voice mail	Direct from the source
 Effects Erosion of trust	Damage to individual reputation	Fraud and other financial damage	Damage to organization or brand	Market manipulation
 Mitigation Promising solutions	Advanced AI systems for detection	Digital provenance	Cross-industry efforts	



SO, HOW DO WE “FIX” ALL OF THIS?

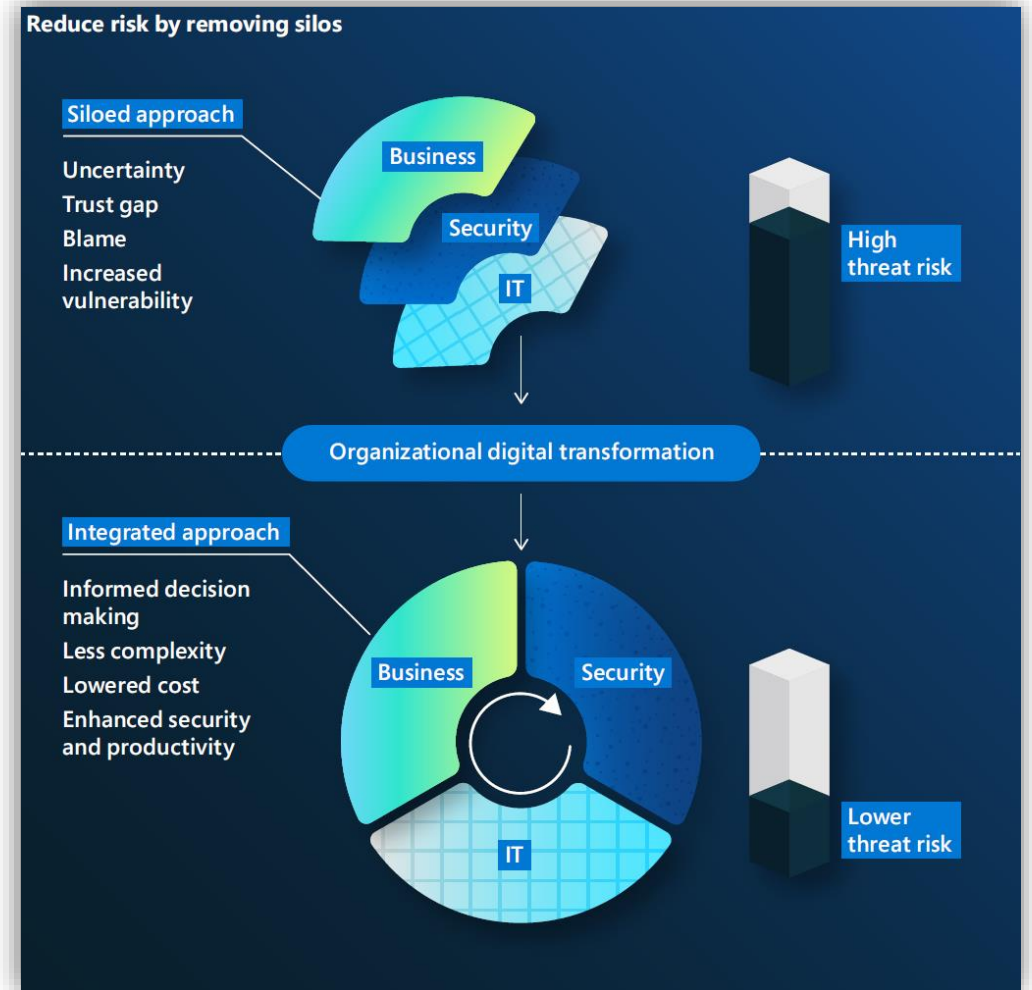
5 EASY STEPS

- Enable MFA
- Apply **Zero Trust** principles
- Use **modern Anti-Malware**
- **Keep up to date**
- **Protect your data**



KEEPING PROCESS/PEOPLE/TECHNOLOGY UP-TO-DATE

- Reduce risk by **removing silos**
- **Limit data access**
- **Update**, update, update
- **Backup**, backup, backup
- Maintain **cybersecurity awareness**



ZERO TRUST IS THE NEW “THING”

~~Big Data~~ / ~~Cloud~~ / **Zero Trust** is like teenage sex: everyone talks about it, nobody really knows how to do it, everyone thinks everyone else is doing it, so everyone claims they are doing it...



Dan Ariely ✓

January 6, 2013 · 🌐

Big data is like teenage sex: everyone talks about it, nobody really knows how to do it, everyone thinks everyone else is doing it, so everyone claims they are doing it...

2.5K Likes 124 Comments 1.2K Shares

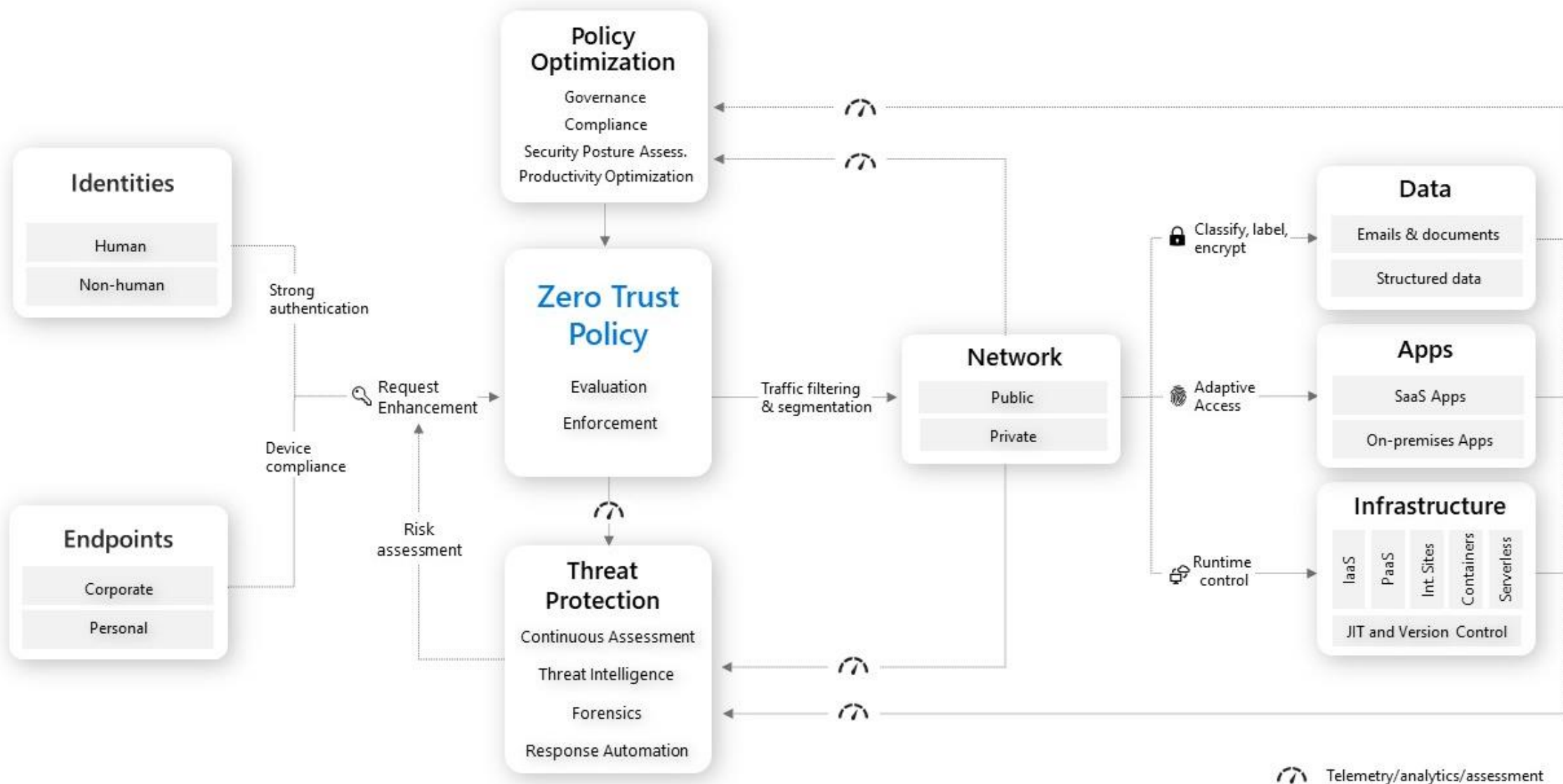
ZERO TRUST – HOW DO WE START?

"Hoping for the best, prepared for the worst, and unsurprised by anything in between"

- Start embracing a **Zero Trust (ZT)** approach
 - **Verify explicitly** (use all data points – identity, location, device health, service/workload, data classification, anomalies)
 - **Use least privileged access** (Just-In-Time/Just-Enough-Access, Risk-based adaptive policies)
 - **Assume Breach** (segment access, encryption, analytics & threat detection)
- Traditional **"castle-and-moat" security** is dead



ZERO TRUST, VISUALIZED



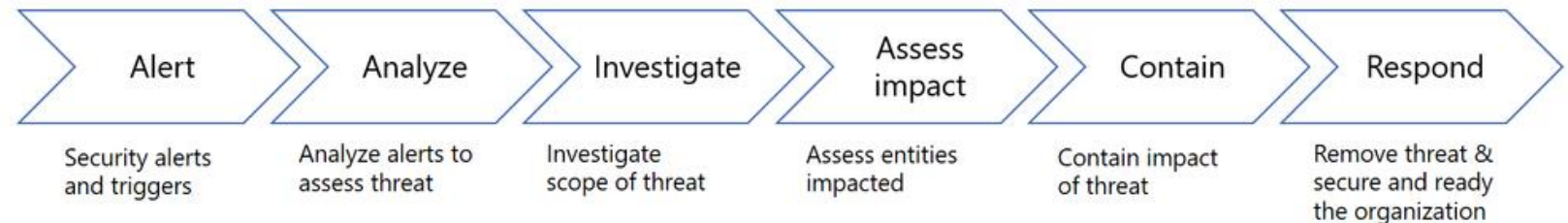
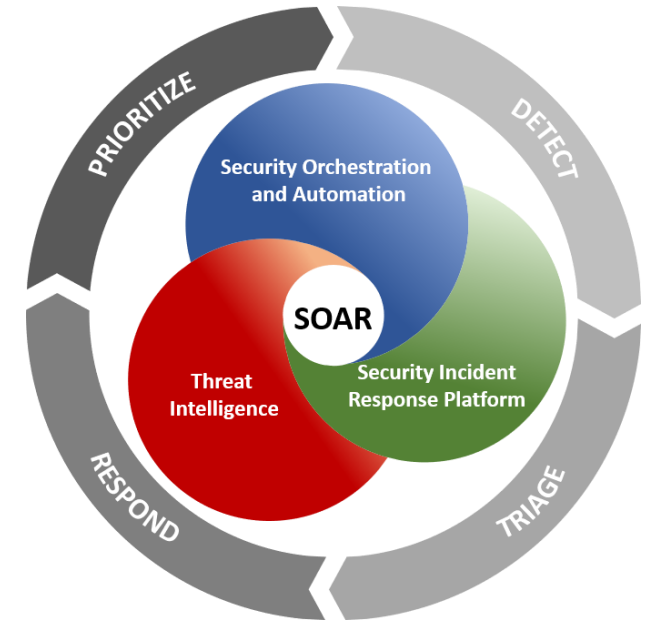
SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE

- Implement **automatic detection and response**

- Force MFA
- Force password resets
- Minimal access mode
- Breached password detection

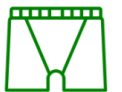
- Use **response playbooks**

- Notification
- Blocking
- Automation



PASSWORD HYGIENE, REVISITED

- Choose **strong, unique passwords**
- **Never reuse** the same or similar passwords
- Use a **Password Manager**
 - Set a **strong password/passphrase** and remember it
- **Treat passwords like you treat your underwear**
 - Change them regularly, don't leave them lying around, don't share them
- **Use 2FA/MFA** where possible
 - Combine that with FIDO, passkeys, passwordless
 - Managing multiple MFA tokens is the next challenge
- Sign up for **data breach notifications**
 - Change your password after a data breach
- Watch out for **phishing emails and sites**
- **Monitor your accounts**



SOME THINGS YOU COULD LOOK AT TODAY

■ Password Managers

- LastPass/1Password/Keeper/etc.

■ MFA management & tools

- Authy (compatible with Google Authenticator)
- Yubikey (FIDO U2F compatible physical keys)

■ Have I Been Pwned - haveibeenpwned.com

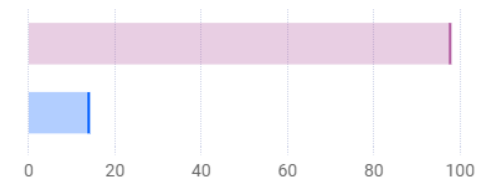
- Public breach monitoring and alerts

■ BitDefender Digital Identity Protection

- Multiple identities, breach checklists, etc.
- Impersonation tracking

■ Just good ol' **Critical Thinking** 😊

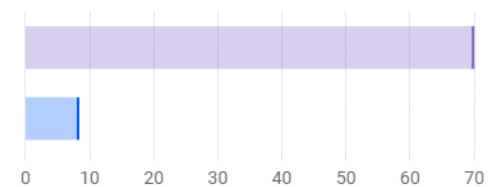
YOU VS. COMMUNITY



+590.1 %

more personal data found on the web about you versus our community average.

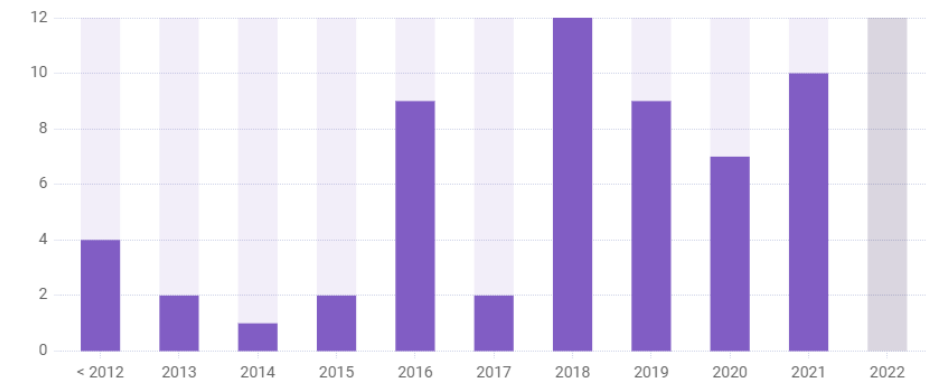
YOU VS. COMMUNITY



+733.3 %

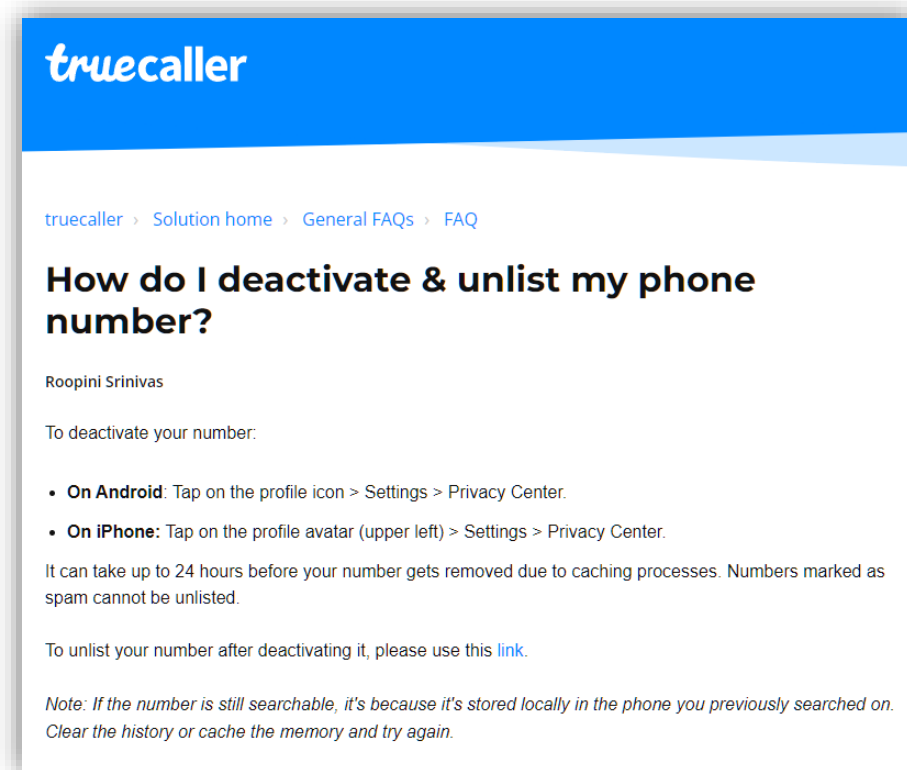
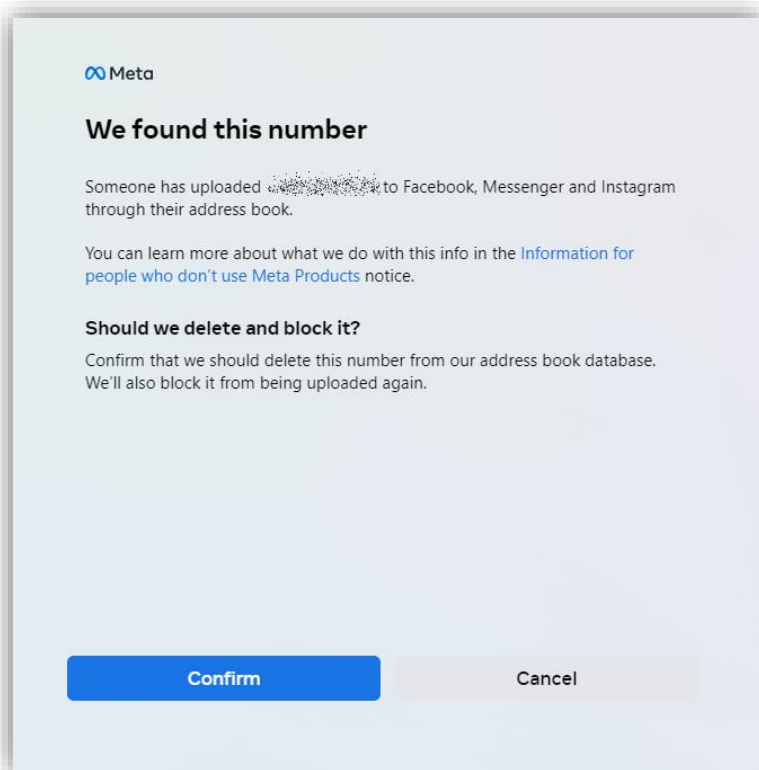
more affected by recent data breaches versus our community average

YOUR DATA BREACH HISTORY



KEEP YOUR DATA OFF THE WEB – E.G. META, TRUECALLER, ETC.

- <https://www.facebook.com/contacts/removal>
 - ...buried inside a [Help Center](#) page
- <https://www.truecaller.com/unlisting>





THANK YOU!

CONTACT ME: [TUDY.RO](https://tudy.ro)

