



LEARNINGS FROM 2023 CYBER INCIDENTS

Presented by –

Jalaj Bhaskar

@ Null Delhi-Chapter

Airtel Centre Gurgaon

6 January'24



\$ whoami

- Blue Teamer
- Codes in C++, Python and GoLang
- Exploring the world of Threat Hunting
- Likes MMA and Bikes
- Connect with me on Telegram @senditfast

WHAT IS COVERED IN THIS PRESENTATION?

Top Cyber Incidents in 2023

Ransomware Group Activity in 2023

Targeted attacks on India in 2023

Attack Trends in 2023



Top Cyber Incidents in 2023



Royal Mail

- Hacked on January 2023
- British postal service
- Russia-linked LockBit Ransomware gang
- Double-extortion
- Ransomware
- Leaked Information on dark web
- Left the giant organization inoperable



3CX

- VoIP service
- 600,000 organizations
- Hacked by a subunit of Lazarus Group backed by North Korean
- Supply chain attack
- A malware-tainted version of the X_Trader financial software found on a 3CX employee's laptop.
- Actual number of victims still unknown



MOVEit Transfer

- Began in May when Progress Software disclosed a critical-rated zero-day vulnerability in MOVEit Transfer
- Clop gang to carry out mass hacks this year to steal the sensitive data of thousands of MOVEit Transfer customers
- Breach has so far claimed more than 2,600 victim organizations
- Personal data of almost 84 million individuals

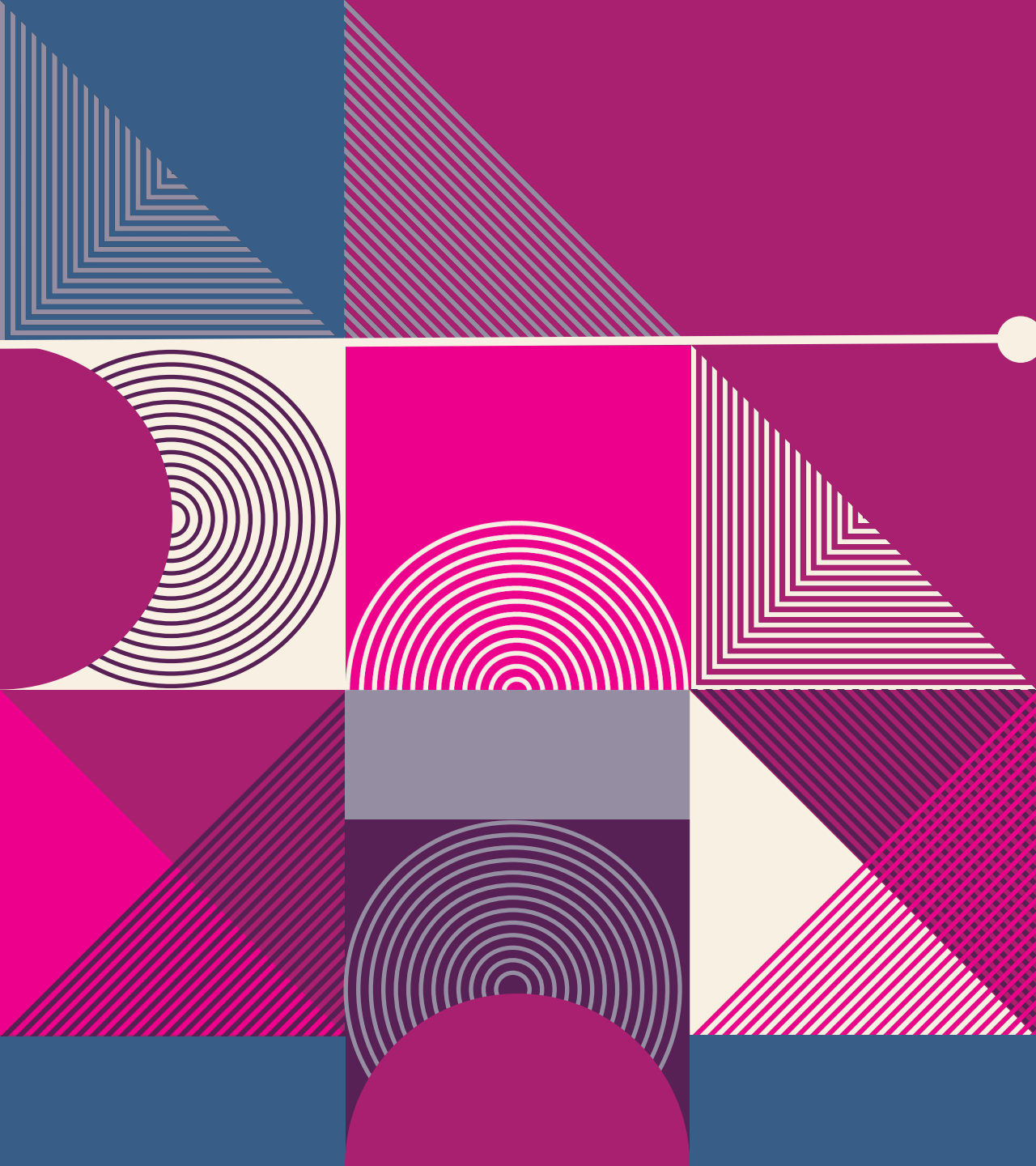


Microsoft

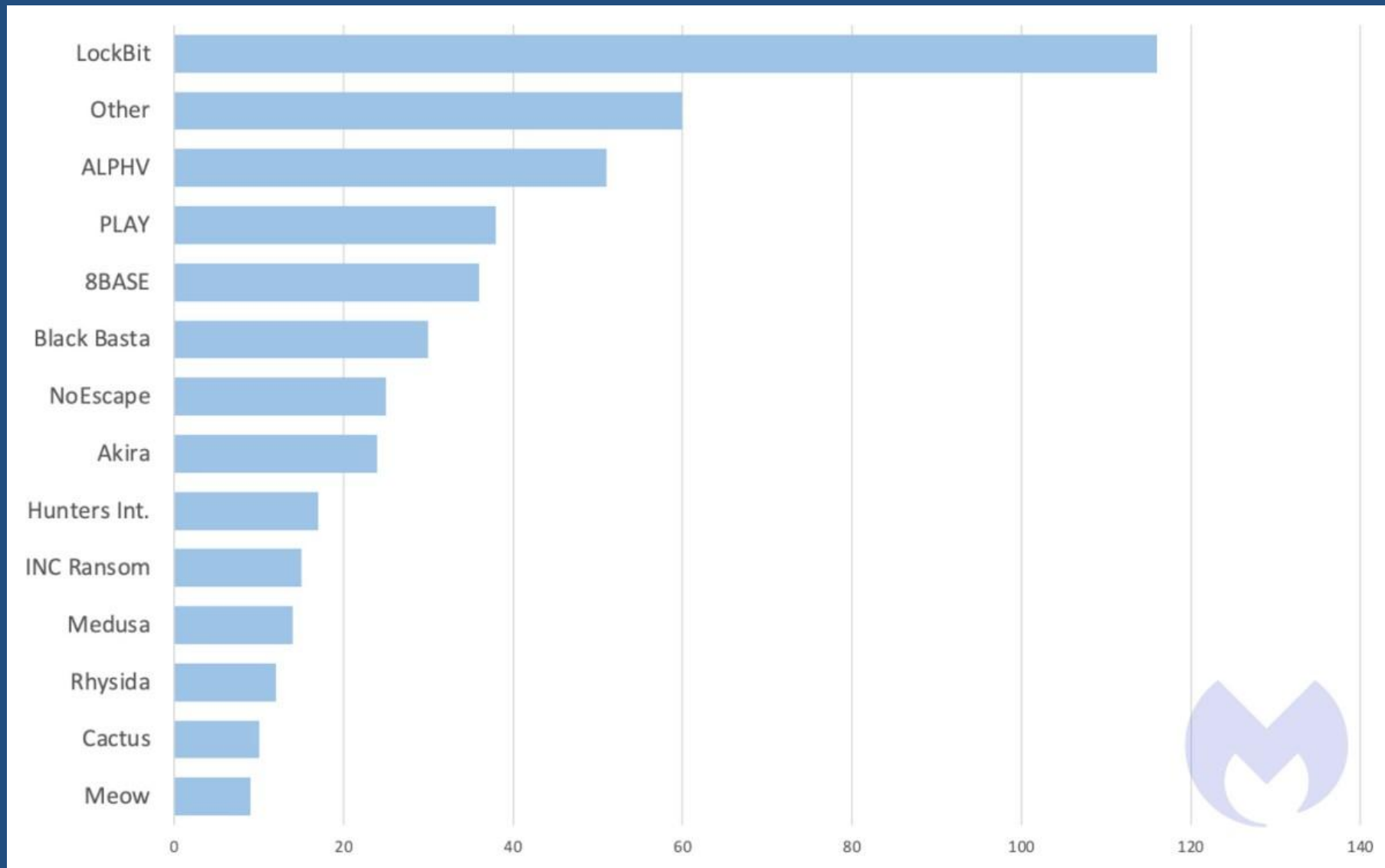
- In September, China-backed hackers (Storm-0558) obtained a highly sensitive Microsoft email signing key, which allowed the hackers to stealthily break into dozens of email inboxes
- Exfiltrated unclassified email data from these email accounts
- Microsoft said that it still does not have concrete evidence (or want to share) how these attackers initially broke in.

CitrixBleed

- In October, security researcher6pointed0out exploration of critical vulnerability in Citrix NetScaler systems
- LockBit, the ransomware gang responsible for the attacks, claims to have compromised big-name firms
- Russia-linked gang to extract sensitive information, such as session cookies, usernames and passwords, from affected Citrix NetScaler systems, granting the hackers deeper access to vulnerable networks.
- Victims include Boeing, commercial bank of China, etc.



Ransomware Group Activity in 2023



Known ransomware attacks by gang, November 2023, Source :Malwarebytes



Targeted attacks on India in 2023



10:50 pm

Hacktivist Mayhem

India's G-20 Website Faced 16 Lakh Cyber Attacks Per Minute During 2023 Summit



<https://www.indiatoday.in> > technology > news > story > personal-data-of-815-cror...

81.5 crore Indians' personal data leaked, claims hacker

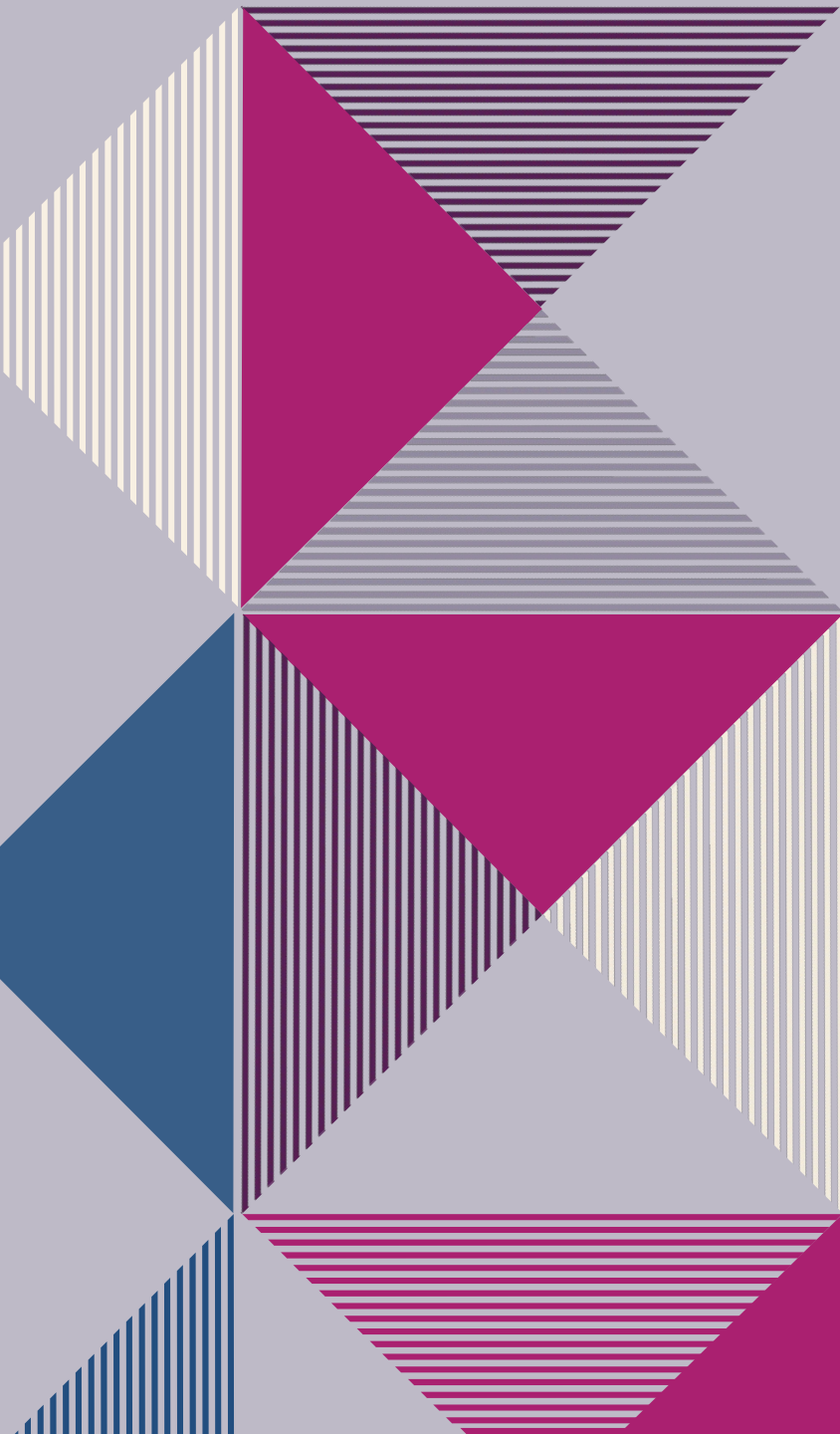
30 Oct 2023 · The Computer Emergency Response Team of India (CERT-In) has also alerted **ICMR** about the **breach**, according to a report by News18. The COVID-19 test information is scattered across various government bodies like the National Informatic...



<https://www.msn.com> > en-in > news > other > hacker-groups-from-malaysia-ind...

Hacker groups from Malaysia, Indonesia initiate cyber war against India ...

Jul 8, 2022 · "Hacker groups Dragonforce Malaysia and Hacktivist Indonesia belonging to Malaysia and Indonesia declared **cyber war** against **India**. We have done technical analysis and found out the IP addresses ...



ATTACK TRENDS IN 2023

January'24

Learnings from 2023 Cyber Incidents

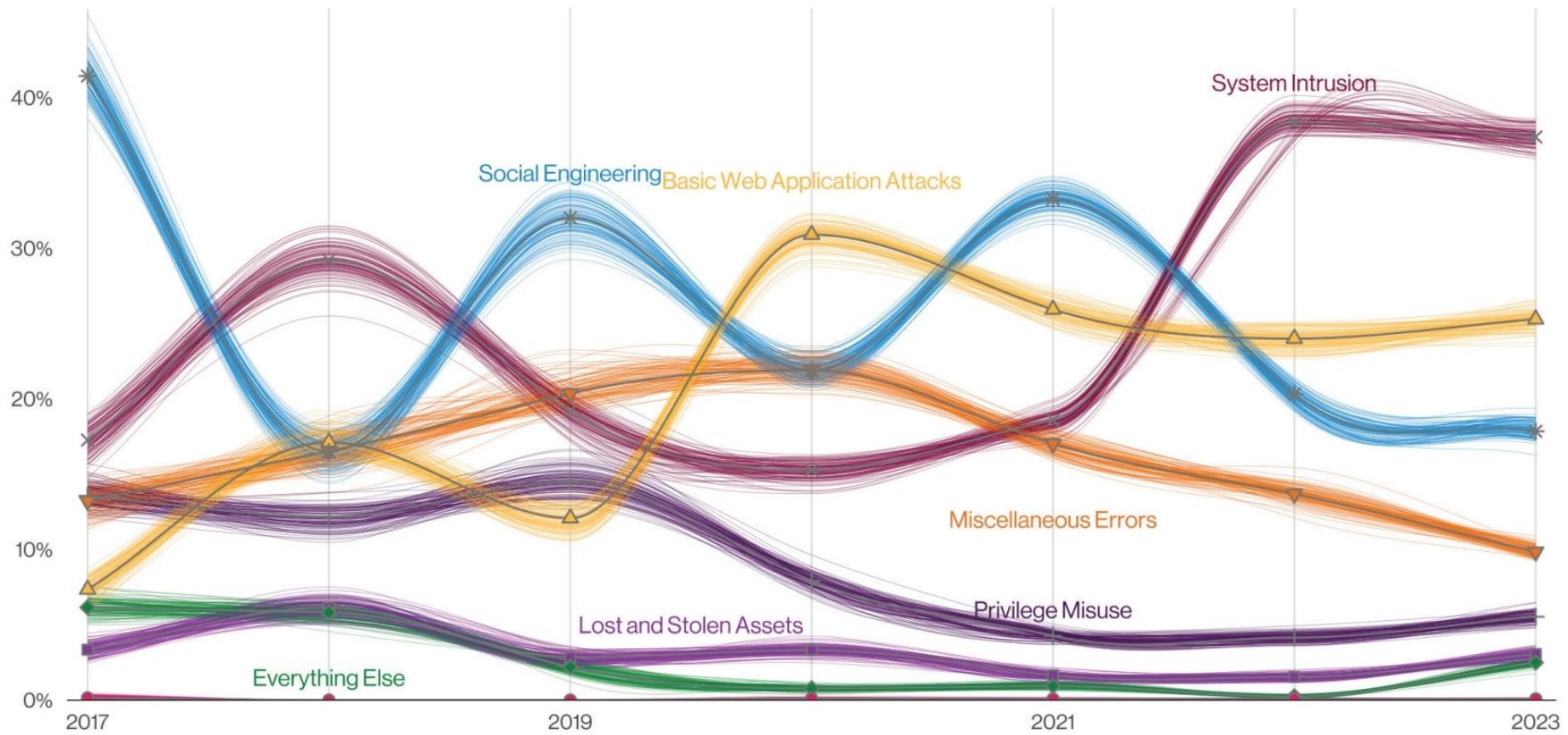
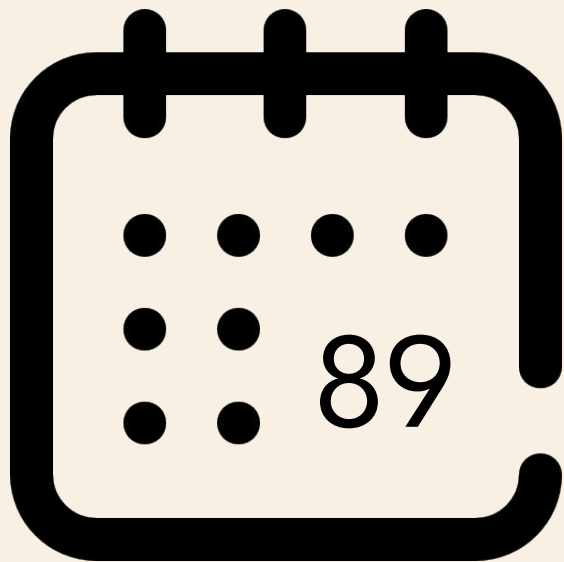


Figure 2. Patterns over time in breaches

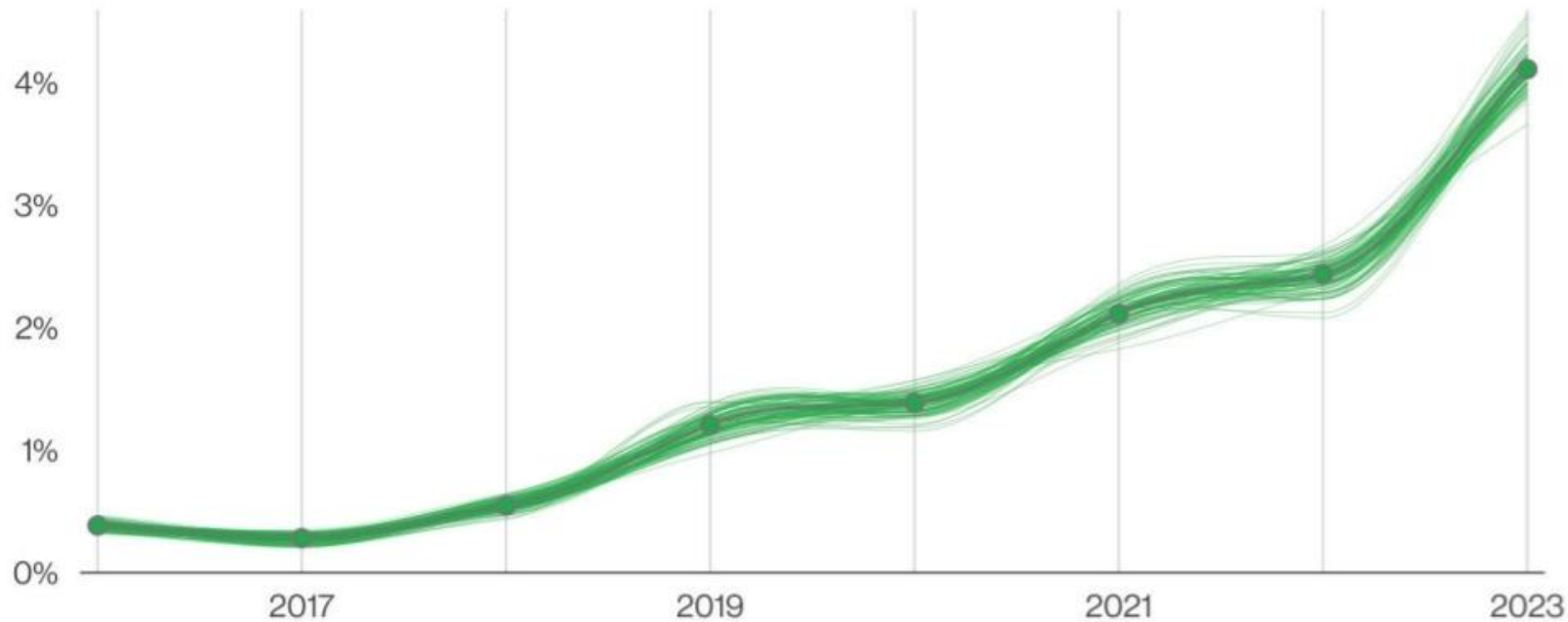
Source : DBIR REPORT 2023

Zero day Summer



0'days in 2023

Social Engineering Trend



Social Engineering attacks are often very effective and extremely lucrative for cybercriminals. Perhaps this is why why Business Email Compromise (BEC) attacks (which are in essence pretexting attacks) have almost doubled across our entire incident dataset, as can be seen in Figure 3, and now represent more than 50% of incidents within the Social Engineering pattern.

Figure 3. Pretexting incidents over time

Source : DBIR REPORT 2023



LEARNINGS

- Implement zero trust
- Backup often and test your backups
- Implement encryption
- Vulnerability assessment is critical
- Monitor identities
- Implement Defense in depth
- "If you are not upgrading yourself, you are dead"



Credits

- [Verizon DBIR report](#)
- [Ransomware review: December 2023](#)
- [The biggest data breaches of 2023](#)
- [Mandiant m-trend report](#)
- [SANS NewsBites](#)