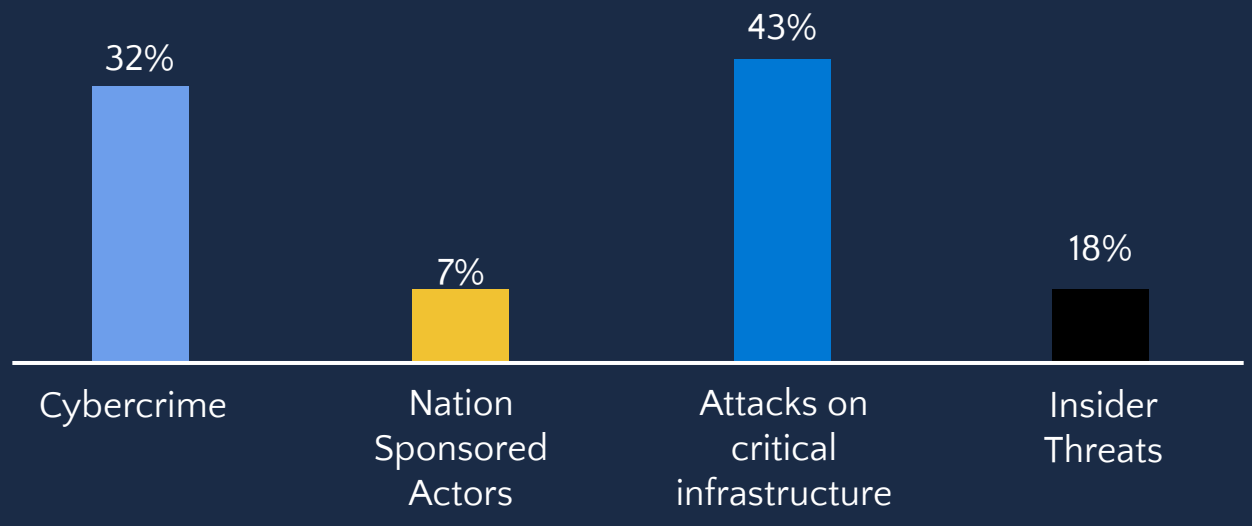
The changing threat landscape

Sarah Armstrong-Smith
Microsoft, Chief Security Advisor

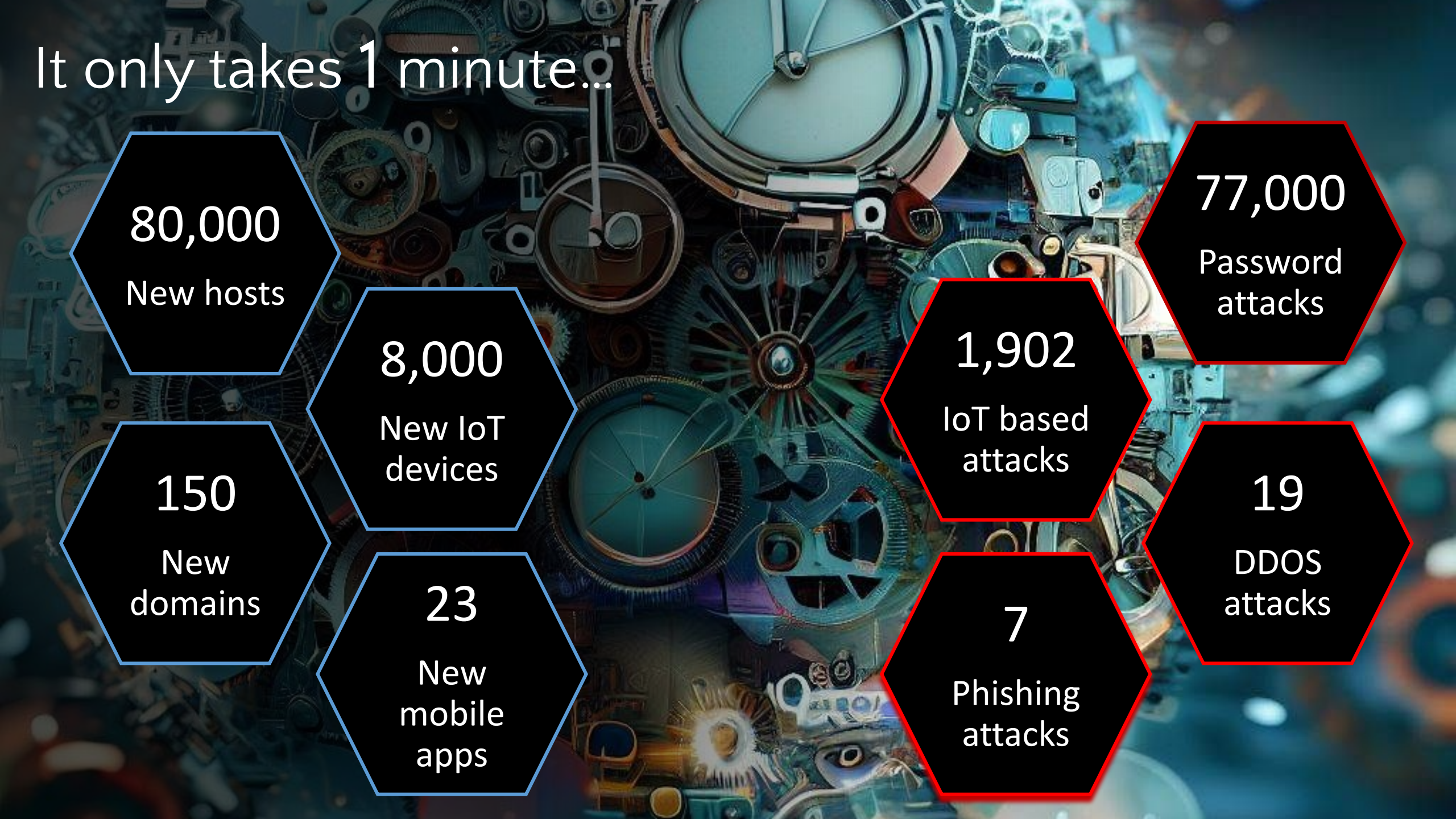
Poll 1: What are your biggest concerns today…



The expanding internet

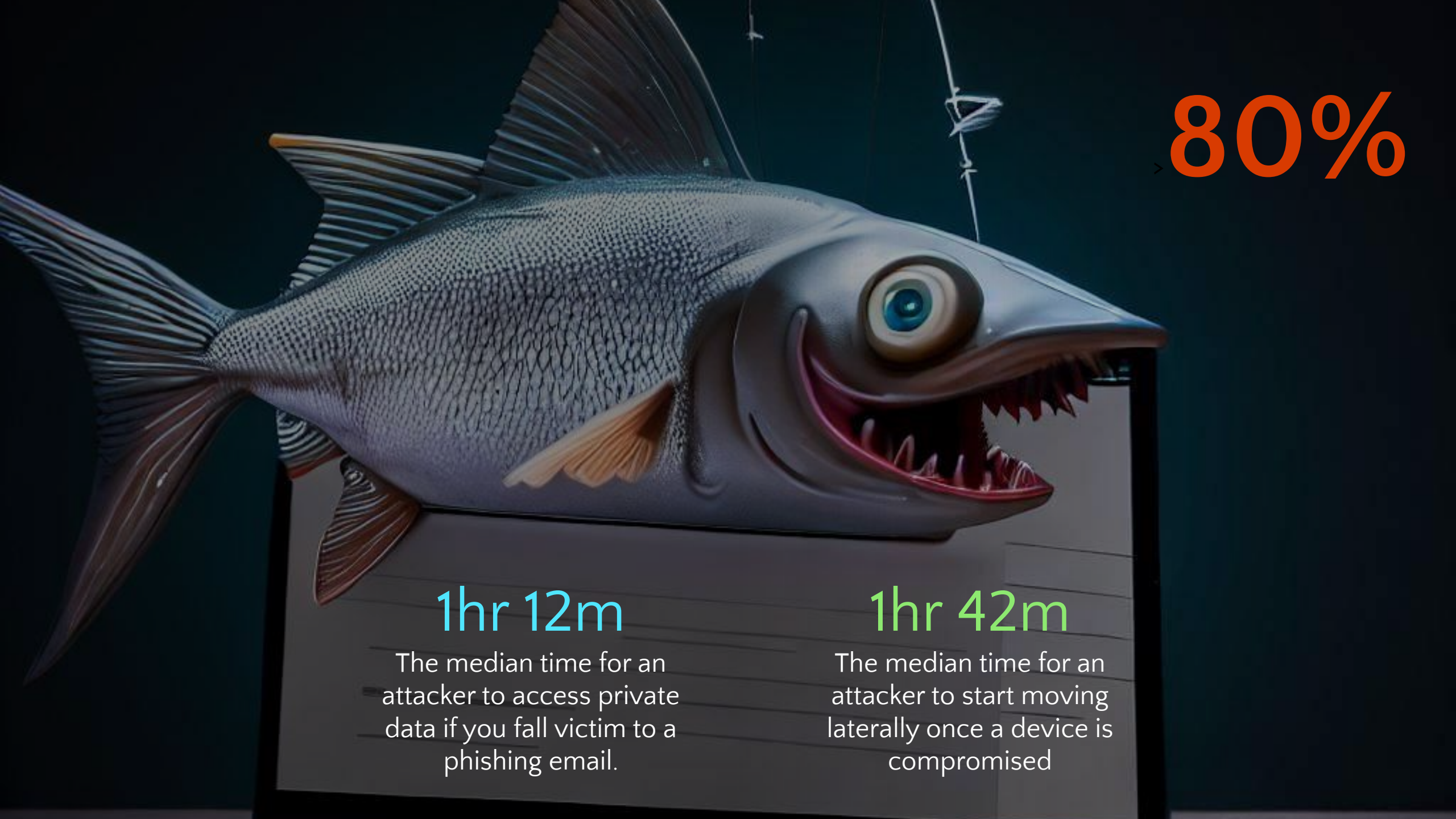
Cloud migration, new digital initiatives, and shadow IT increase the size of the attack surface.

It only takes 1 minute...



The State of Cybercrime

As cyber defenses improve and more organizations are taking a proactive approach to prevention, attackers are adapting their techniques.


80%
1hr 12m
The median time for an attacker to access private data if you fall victim to a phishing email.
1hr 42m
The median time for an attacker to start moving laterally once a device is compromised

A request via website contact us f...

File | Message | Tell me what you want to do...

Delete | Reply | Reply All | Forward | Create New | Move | Mark Unread | Categorize | Follow Up | Translate | Zoom

Delete | Respond | Quick Steps | Move | Tags | Editing | Zoom

@yahoo.com

Tue 11:59 AM

A request via website contact us form

Department

Group Dining, Meetings & Events

Name

Mel

Email

@yahoo.com

Phone

Address

Map It

Message

Hi

This is Melanie and I am a certified photographer

I was baffled, mildly speaking, when I saw my images at your web-site. If you use a copyrighted image without an owner's permission, you must be aware that you could be used by the copyright holder.

It's illegitimate to use stolen images and it's so low.

Check out this document with the links to my images you use at and my earlier publication to get the evidence of my copyrights

Download it right now and check this out for yourself.

https://sites.google.com/view

If you don't remove the images mentioned in the document above during the next couple of days. I'll file a complaint against you to you to your hosting provider stating that my copyrights have been severely infringed, and I am trying to protect my intellectual property.

And if it doesn't work, you may be pretty damn sure I am going to take legal action against you. And I will not bother myself to let you know of it in advance.

Hi, this is Melanie and I am a certified photographer

I was baffled, mildly speaking when I saw my images at your website.

If you use copyrighted images without an owner's permission, you must be aware that you can be sued by the copyright holder

It is illegitimate to use stolen images and it's so low.

Check out this document with the links to my images at XXX and my earlier publication to get my evidence of copyright.

Download it right now and check this out for yourself!

If you don't remove the images mentioned in the next couple of days, I'll file a complaint against you to your hosting provider stating that my copyrights have been severely infringed, and I am trying to protect my intellectual property

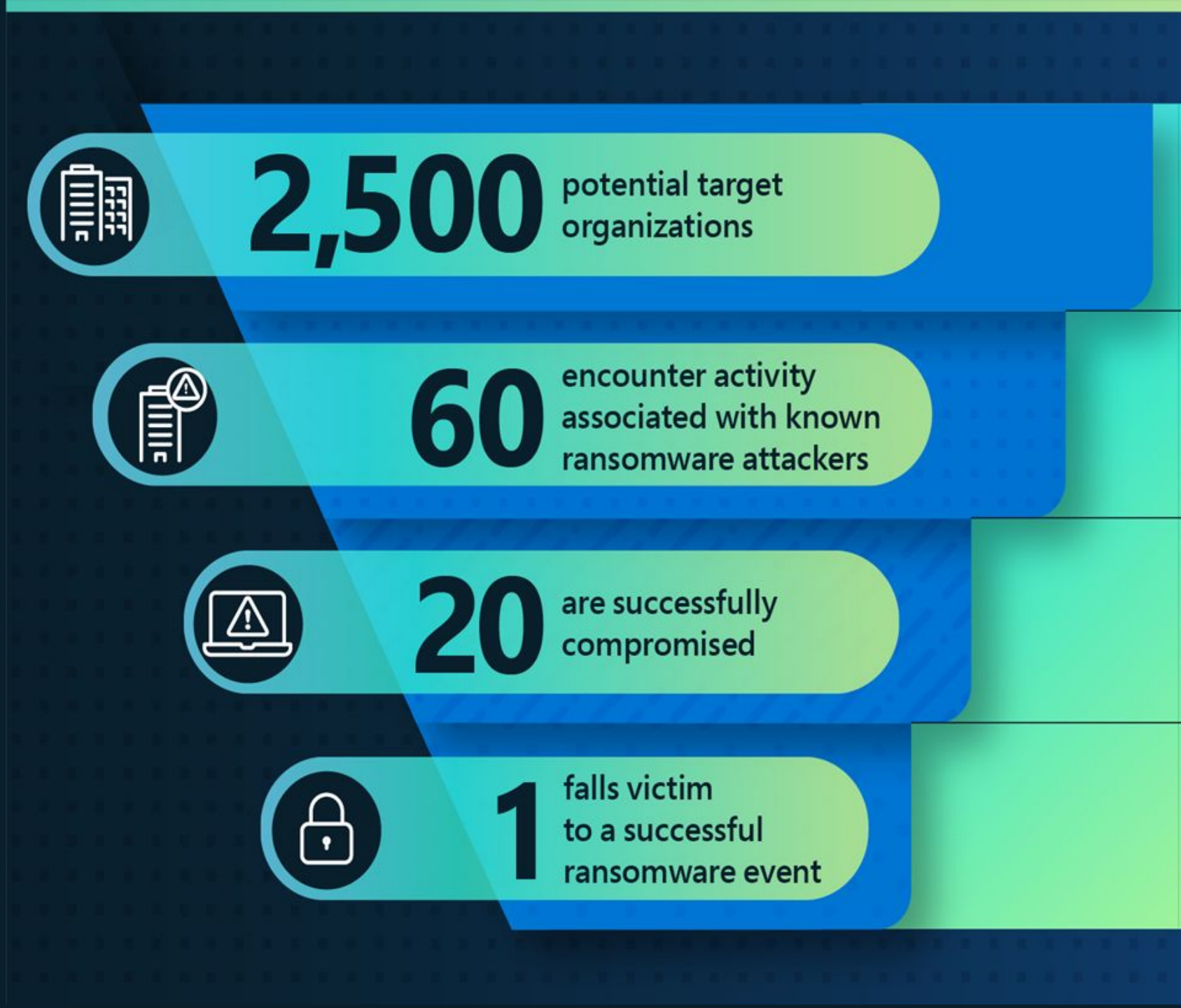
If it that doesn't work, you can be pretty sure I am going to take legal action against you. And I will not bother to let you known of it in advance!

‘Push bombing’

Attackers use a bot or script to trigger multiple access attempts with stolen or leaked credentials, to attempt to bypass MFA


156,000 per day
63%
Lure
15%
Payroll
redirection
8%
Invoice
fraud
4%
Business
information
5%
Gift card
scams
5%
Other
Business email compromise & impersonation – a $2.7bn business

Cybercrime as a service..



Watching your next move...

Deliberately triggering the crisis response to assess your level of confidence

Ransomware Trends

- Exfiltration without encryption
- Ransomware as a parting gift

Nation State Threats

Nation state actors are launching increasingly sophisticated cyberattacks to evade detection and further their strategic priorities.


The importance of moving fast
The need to move data across borders

The first shots fired were in cyberspace

23rd Feb 2022: The cyberwar started 10 hours before the physical invasion

24th Feb 2022: AcidRain wiper malware disables Viasat's KA-SAT satellite communication links, via a malicious firmware update on modems and broadband routers 1 hour before invasion.

Russian government (Blizzard) entities responsible for cyberattacks

GRU

STRONTIUM (*Forest Blizzard*)
Data theft, phishing (military targets)

IRIDIUM (*Seashell Blizzard*)
Destruction: FoxBlade wiper;
CaddyWiper, Industroyer2

DEV-0586 (Cadet Blizzard)
Destruction: WhisperGate wiper,
data theft, influence operations

SVR

NOBELIUM (*Midnight Blizzard*)
Password spray, phishing
(Ukrainian and NATO member diplomatic targets)

FSB

ACTINIUM (*Aqua Blizzard*)
Phishing, data theft

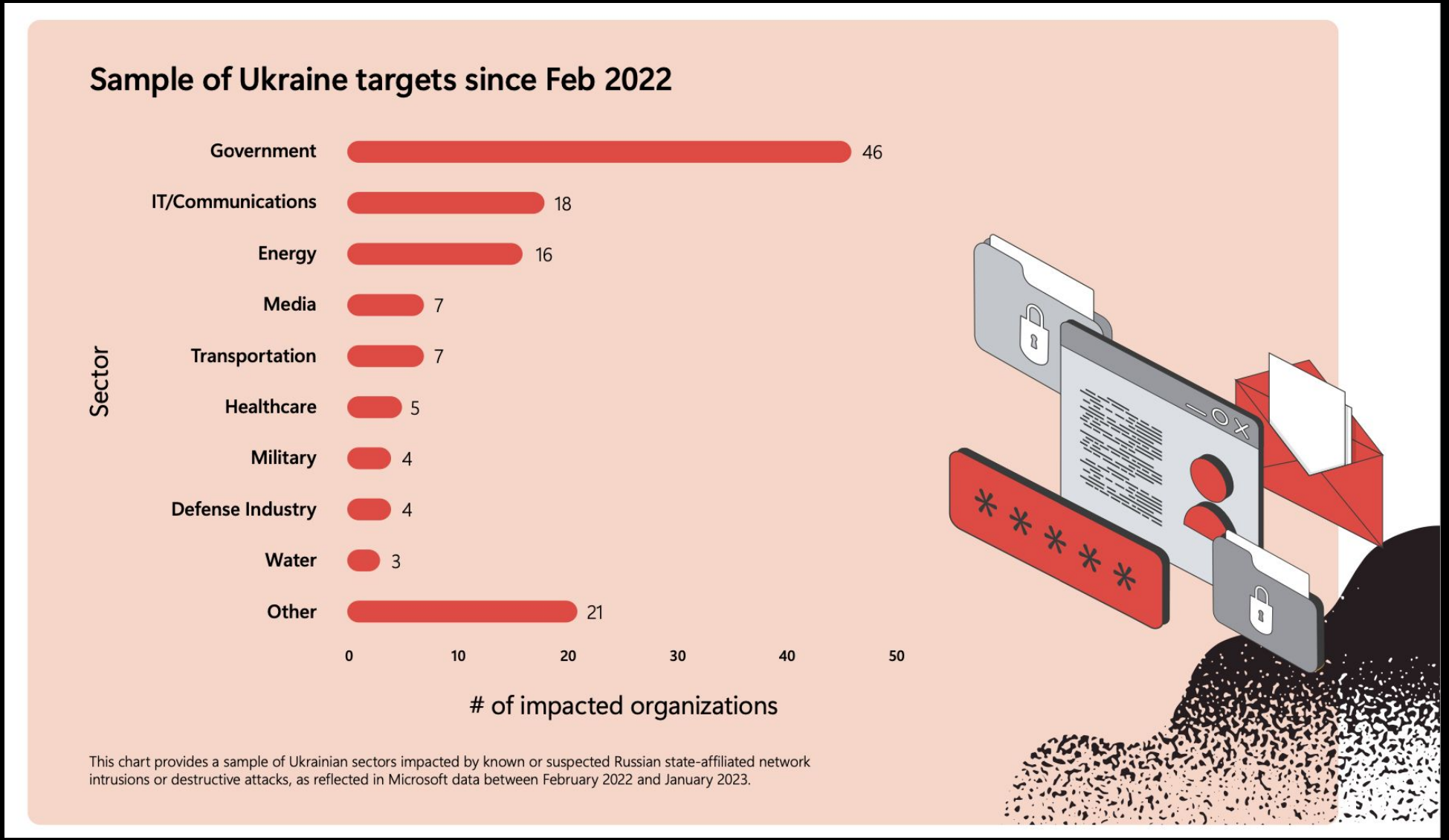
BROMINE (*Ghost Blizzard*)
Data theft

KRYPTON (*Secret Blizzard*)
Reconnaissance, phishing

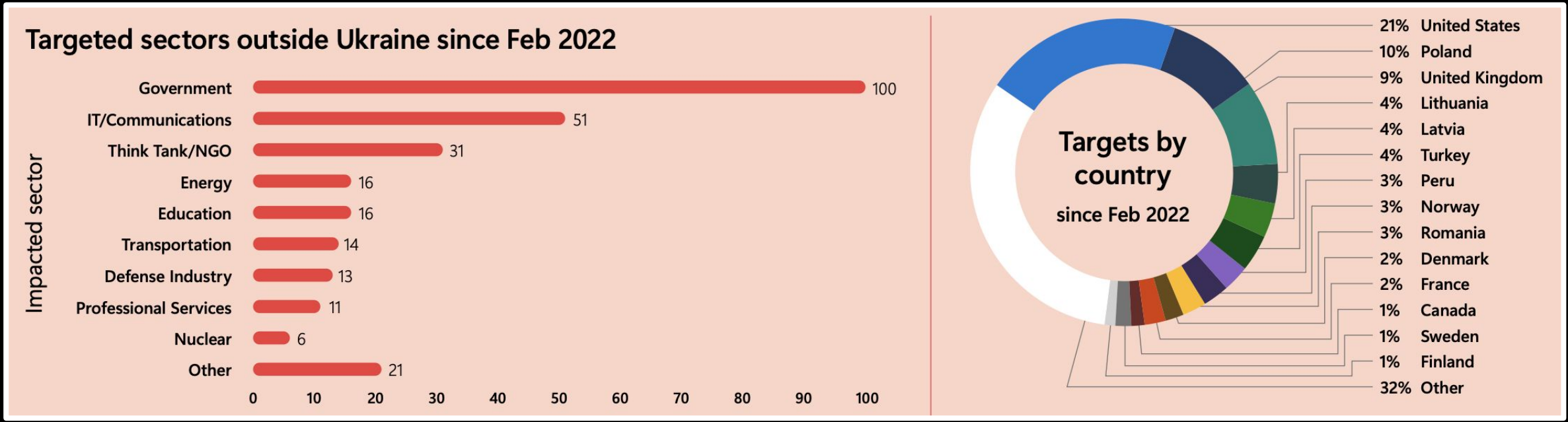
More disruptive operations took place in the first **four months** of the war than in the **eight years** before

Combined cyber & kinetic attacks provide paralysis

A Year of Hybrid War in Ukraine: Cyber Targets by Sector



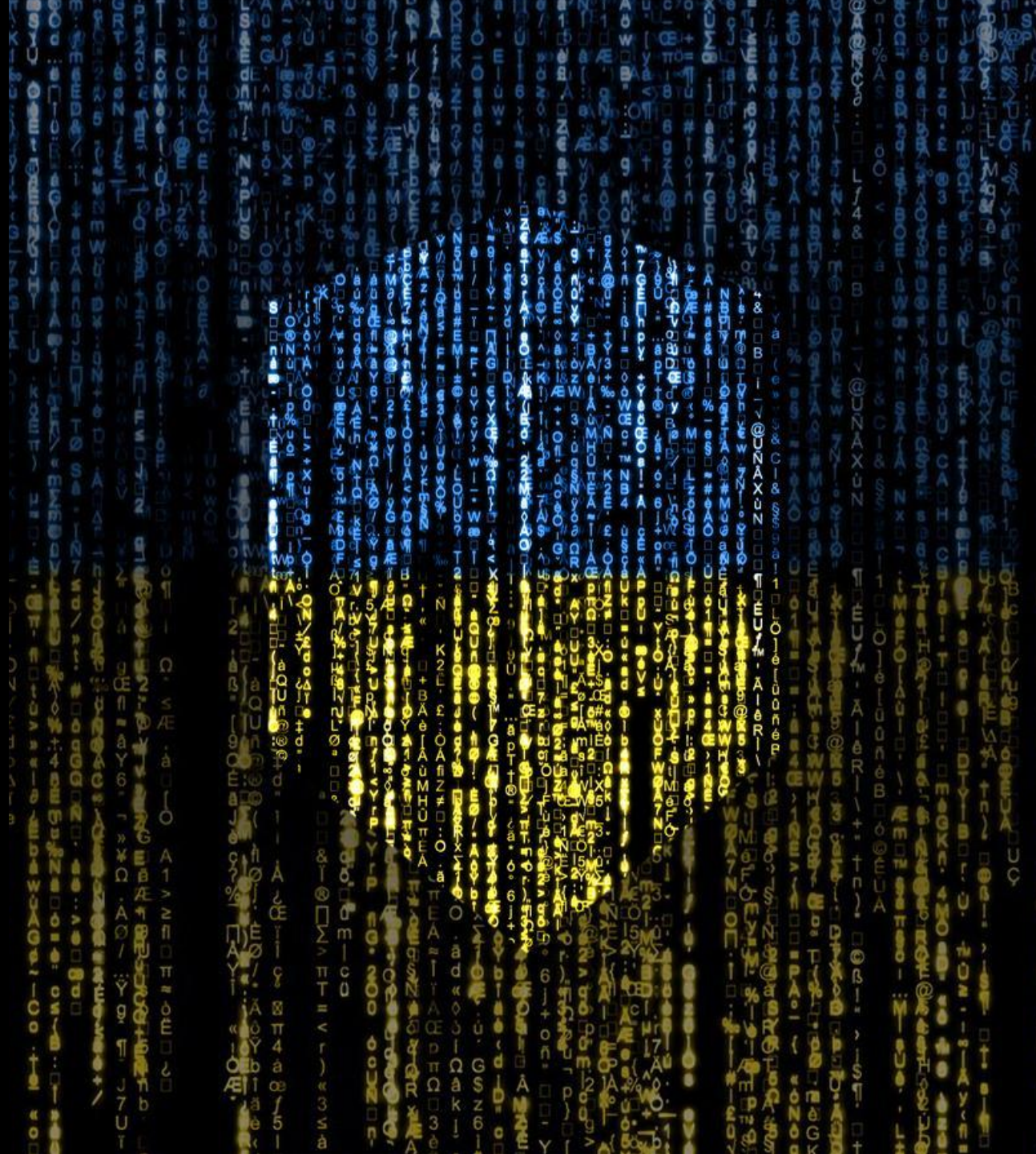
Targeted Sectors Outside Ukraine



- *Microsoft observed Russian activity against 74 countries, between Feb 23, 2022, and Feb 7, 2023*
- *Activities range from reconnaissance to data exfiltration.*
- *Russian threat actors most interested in government and IT sectors. Several actors compromise IT firms to exploit trusted technical relationships and gain access to those firms' clients in government, policy, and other sensitive organizations.*

Renewed campaigns

- **Oct 2022:** “Prestige” ransomware deployed in Ukraine & Poland transportation & logistics hub
- **Nov 2022**: “Sullivan” ransomware deployed against multiple Ukraine targets
- **Jan 2023**: Seashell Blizzard (*Iridium*) may be preparing for new offensive: reconnaissance, initial access campaigns and wiper deployments, reminiscent of early days – targeting defense, energy, media and regional government entities



Importance of foundations

Identify and remediate attack surface

Be accountable for your assets, particularly those that are public facing.

Adversaries will leverage the easiest path into your network. Prompt patching is a necessity.

Secure identities and gain visibility

A users' path is your threat actors' path.

Multi-factor authentication, implemented properly, is a must have for access vectors and applications.

Understand and secure trusted paths

Business-to-business relationships and access vectors are vulnerable to threat actors.

Actors *will* invest time to understand your business better than you.

A move to intelligence warfare?

Feb 2023:
Ukraine gives sign off on Delta situational awareness system, providing real-time data from drones, radar and sensors on a digital map, delivered anywhere, on any device.

A closer look at IoT and OT threats

IoT devices are outpacing IT in growth. The attack surface area has already grown **3x** in recent years and will continue to grow.

Critical infrastructure is becoming the battle ground in cyber warfare

ZDNet

NASA hacked because of unauthorized Raspberry Pi connected to its network

DARKReading SIGN UP FOR OUR NEWSLETTERS

Verkada Breach Demonstrates Danger of Overprivileged Users

In re-evaluating supply chains, companies should classify vendors with super admin privileges to devices or backdoors as a significant threat.

ZDNet

Hackers are attacking smart building access systems

More than 2,300 building access systems can be hijacked due to a severe vulnerability left without a fix.

ZDNet

Triton hackers return with new, covert industrial attack

Traces of a hacking group behind the destructive Triton malware have been found at a new infrastructure facility following an infamous attack in the Middle East.

Bloomberg

Hackers Breached Colonial Pipeline Using Compromised Password

The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant who responded to the attack.

The New York Times

'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town

Hackers remotely accessed the water treatment plant of a small Florida city last week and briefly changed the levels of lye in the drinking water, in the kind of critical infrastructure intrusion that cybersecurity experts have long warned about.

OT Security is one of the greatest risks to the global economy

Financial

Destructive malware shuts down factories worldwide, causing billion of dollars in losses (WannaCry, NotPetya, LockerGoga)

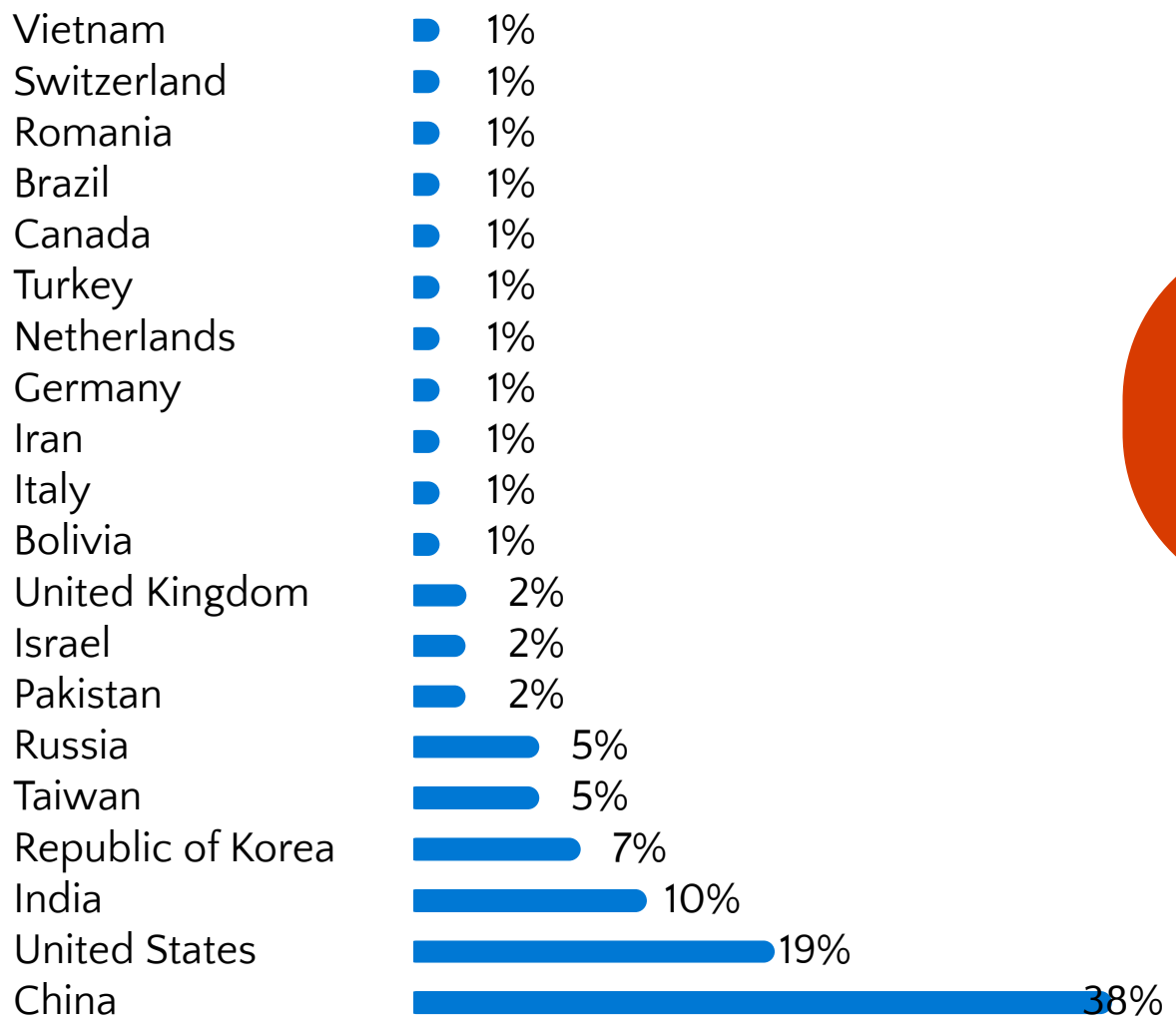
IP Theft

Manufacturers are 8x more likely to be attacked for theft of IP like proprietary formulas and designs than other verticals

Safety

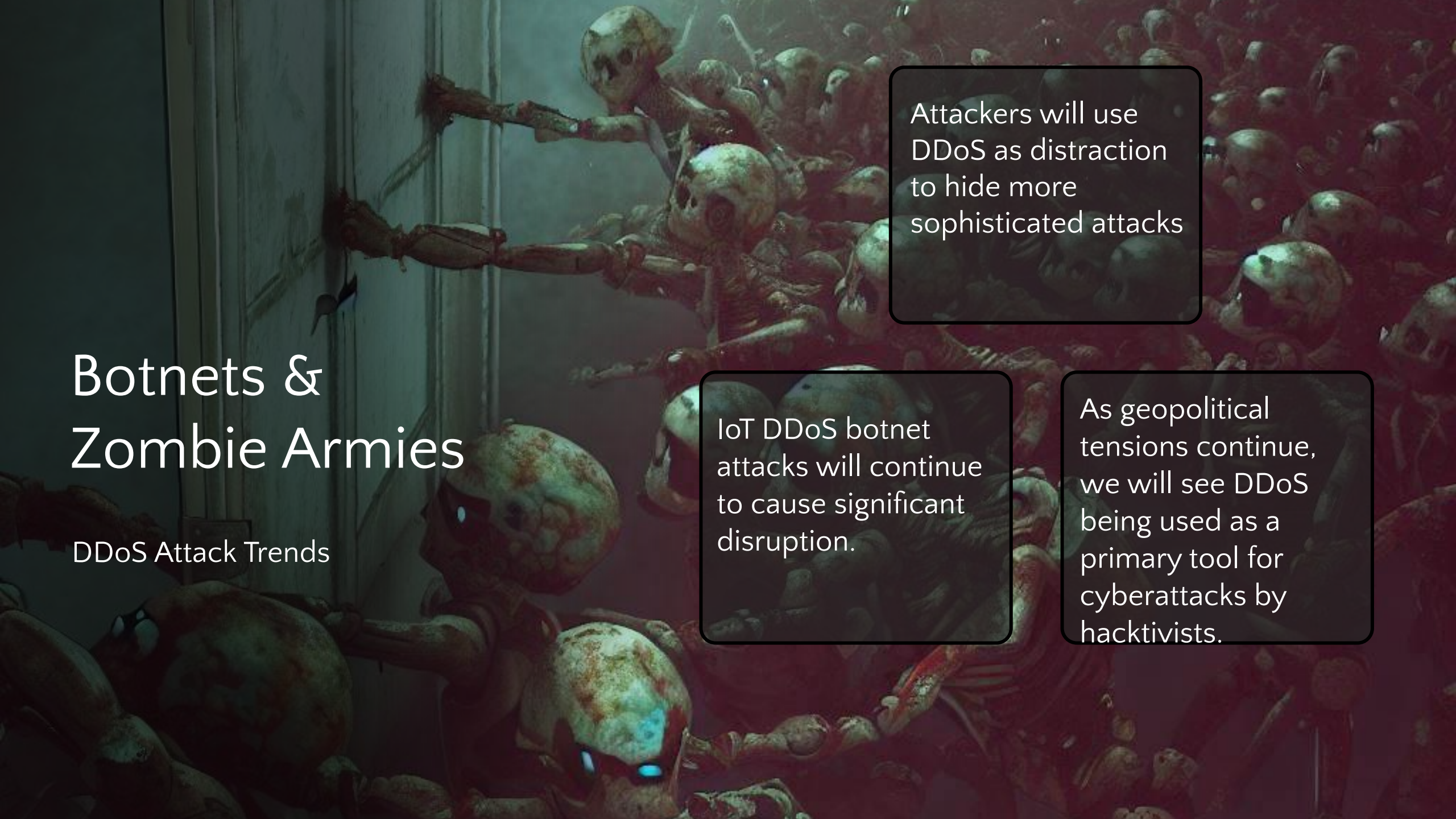
Safety controllers in petrochemical facility compromised with purpose-built back door in TRITON attack.

Threats against IoT and OT are global



Top countries originating IoT malware during 2022

Percentages of observed outbound malware infection attempts. Country of origin (location identification) does not infer nation-state sponsored activity (actor attribution). Microsoft threat analysis of 2022 data.



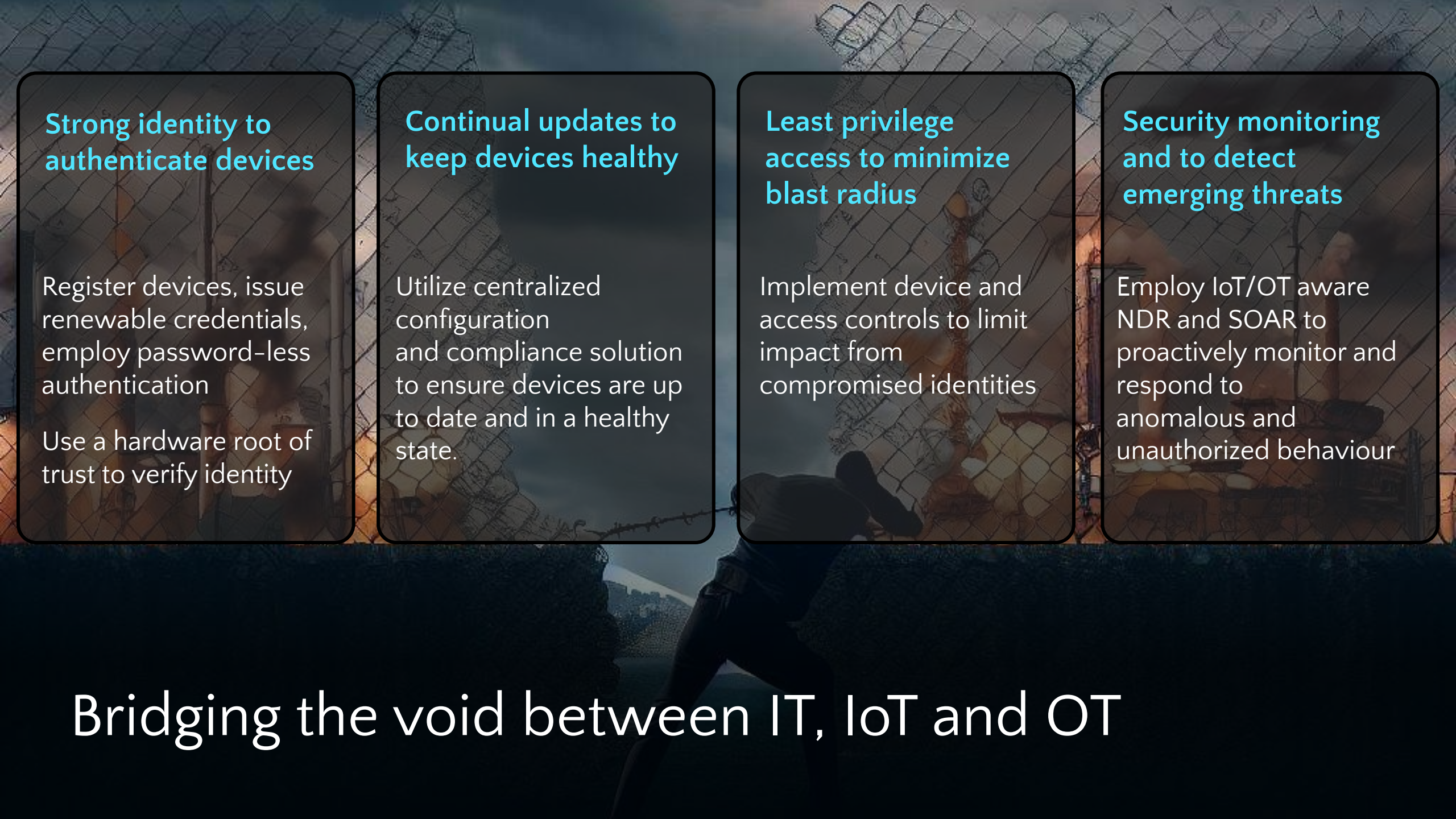
Botnets & Zombie Armies

DDoS Attack Trends

Attackers will use DDoS as distraction to hide more sophisticated attacks

IoT DDoS botnet attacks will continue to cause significant disruption.

As geopolitical tensions continue, we will see DDoS being used as a primary tool for cyberattacks by hacktivists.



Strong identity to authenticate devices

Register devices, issue renewable credentials, employ password-less authentication

Use a hardware root of trust to verify identity

Continual updates to keep devices healthy

Utilize centralized configuration and compliance solution to ensure devices are up to date and in a healthy state.

Least privilege access to minimize blast radius

Implement device and access controls to limit impact from compromised identities

Security monitoring and to detect emerging threats

Employ IoT/OT aware NDR and SOAR to proactively monitor and respond to anomalous and unauthorized behaviour

Bridging the void between IT, IoT and OT

Beware the insider


Most people are
just trying to do
the best they can

How much trust is too much trust?

The Battle for AI: Friend or Foe


Addressing the elephant in the board room…

Poll 1: What are your biggest concerns going forward…