

**Orange**  
Cyberdefense

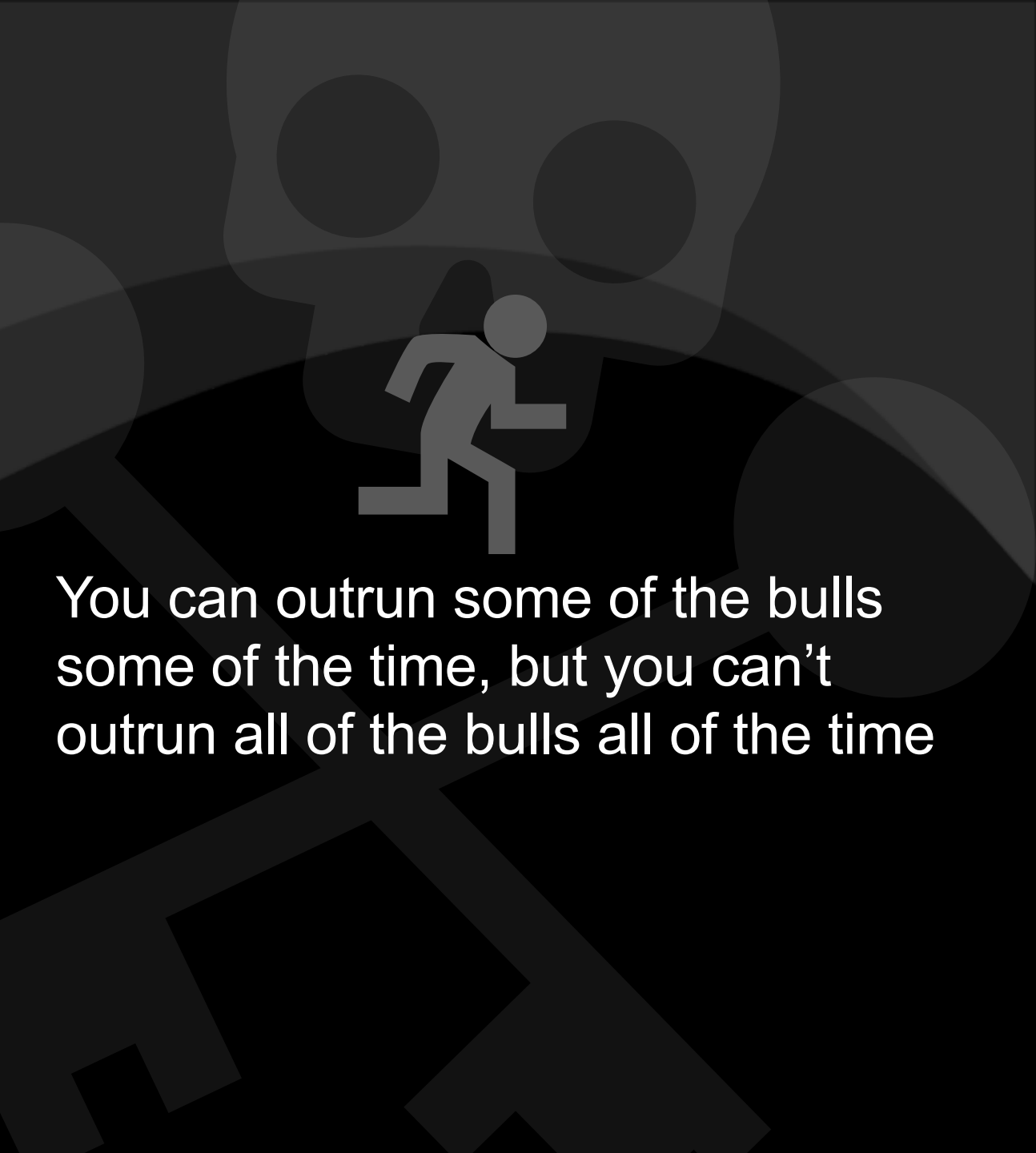
# Climate Change

Tracking the key themes in cybersecurity that are shaping the landscape.

Charl van der Walt, Head of Security Research

 orange™





You can outrun some of the bulls  
some of the time, but you can't  
outrun all of the bulls all of the time

# Hello!

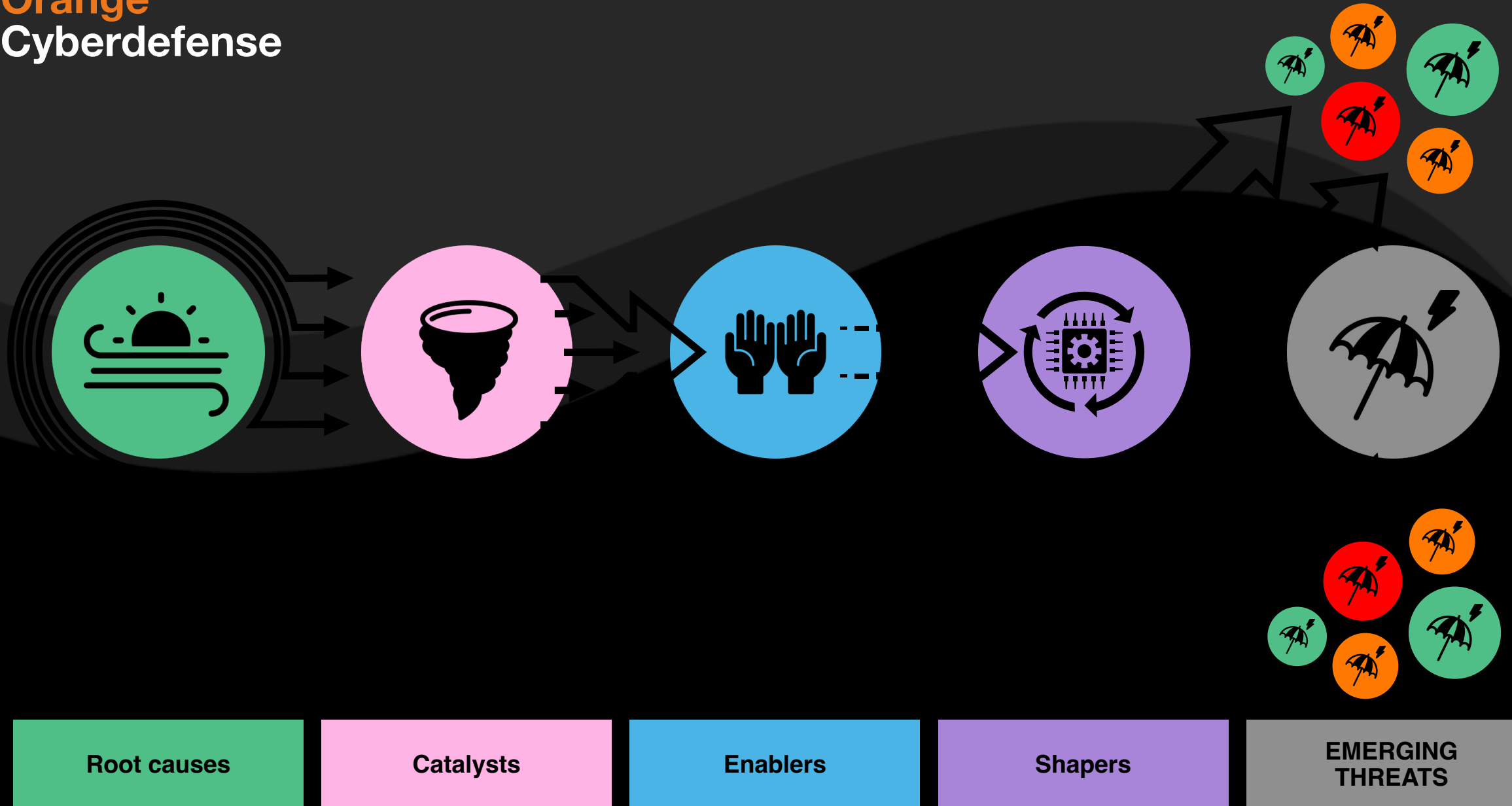
I am Charl.

Global Head of Security Research for Orange Cyberdefense

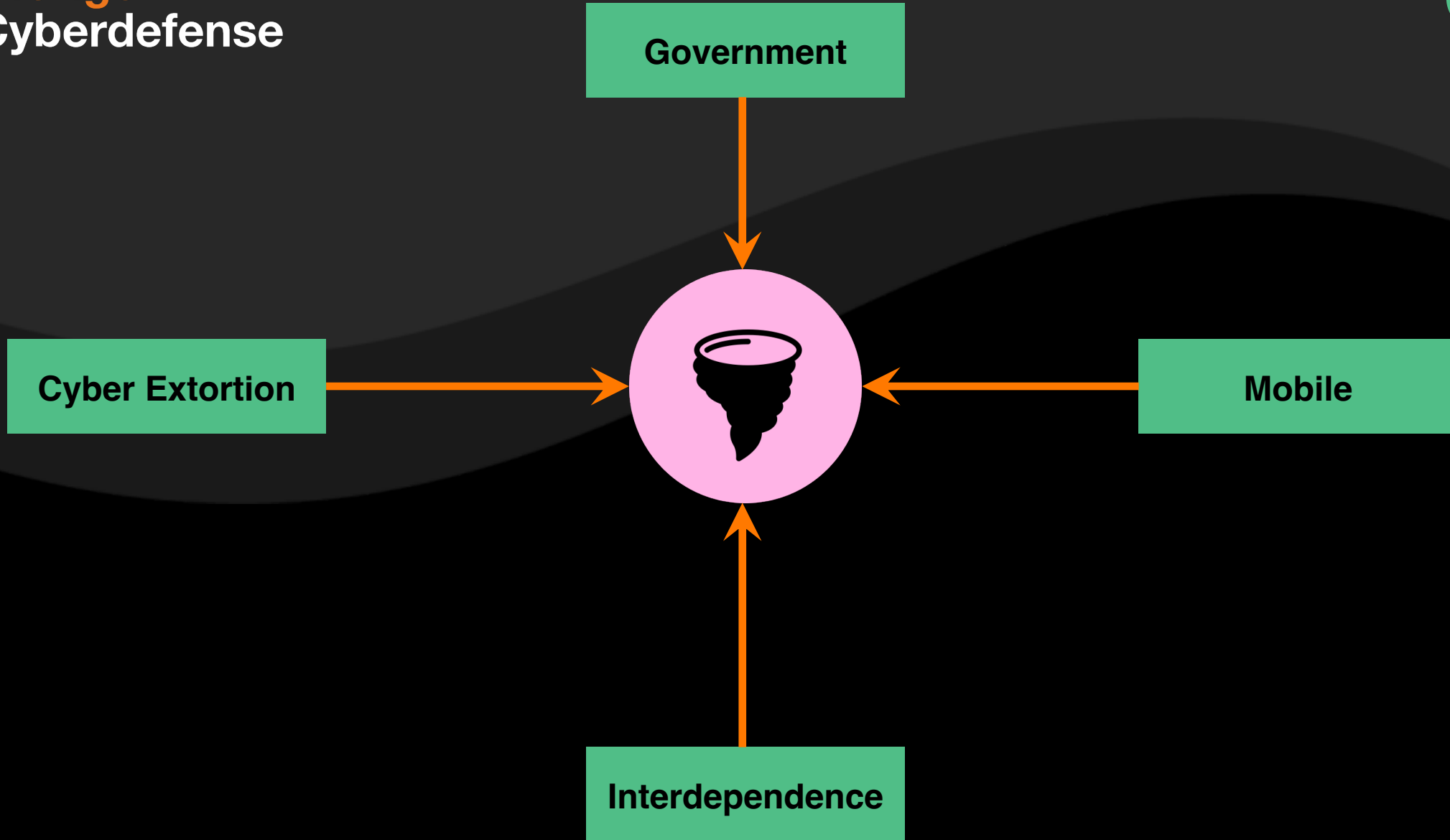
You can find me at [@charlvdwalt](https://twitter.com/charlvdwalt)



# Orange Cyberdefense



# Orange Cyberdefense





Government

**“Not a single military operation proceeds without a cyberdefence capacity implication.”**

- **Intelligence**
- **Psychologic operations**
- **Targeting**
- **Destruction**
- **Post-strike evaluation**

**The resilience of the digital systems on which modern economies depend is critical**



**Laurent Celerier**  
**Orange Cyberdefense**

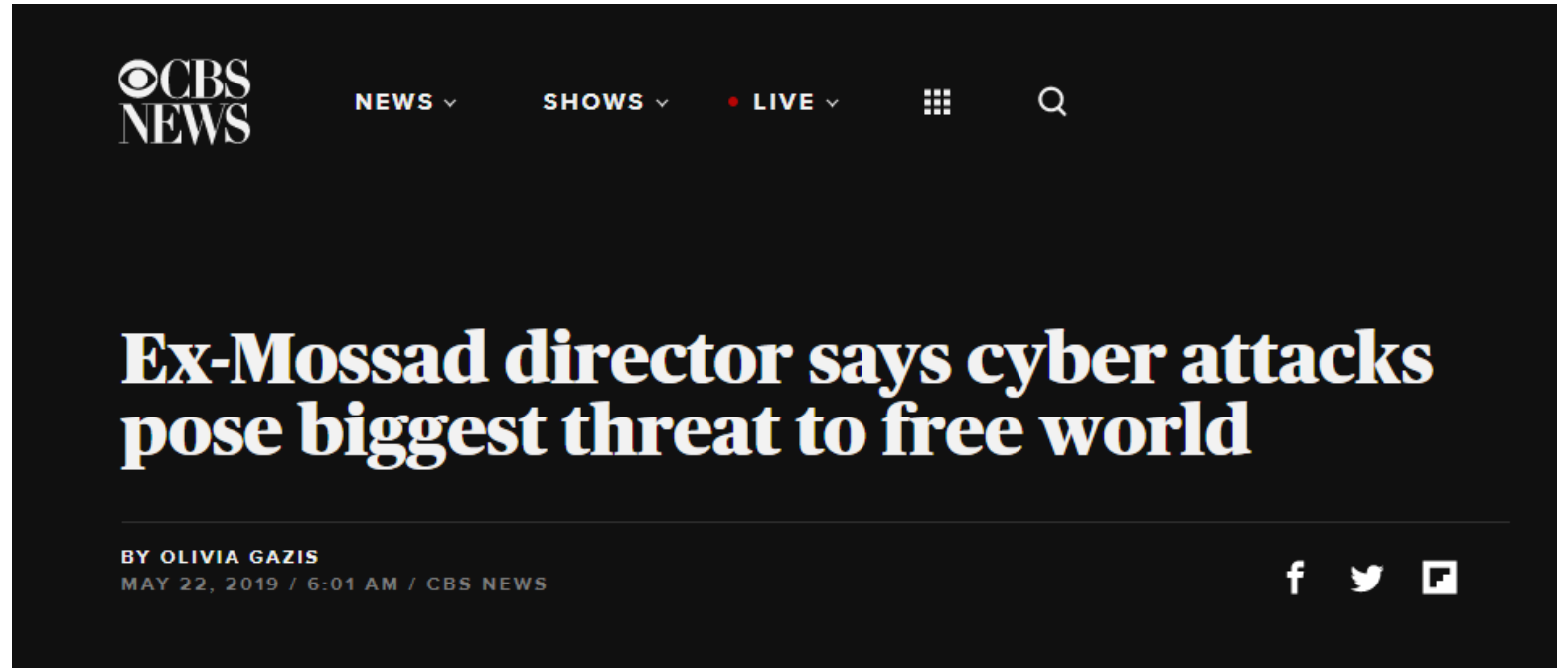


# Cyber attacks:

The biggest threat to the free world

A soft and silent nuclear weapon

With 1% of the cost of a fighter jet you can create a mess around the world

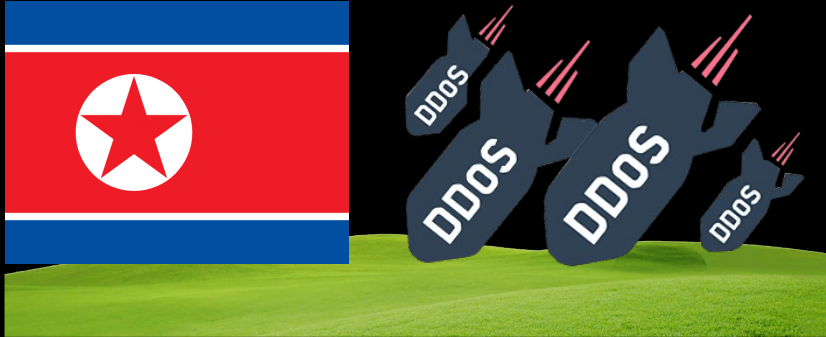


The former head of the Mossad, Israel's intelligence service, warned in a recent interview that the low cost and relative ease for states and non-state actors to conduct cyberattacks pose among the gravest security threats in the world.

Tamir Pardo, who spent more than three decades in the intelligence service before being tapped to lead it from 2011 to 2016, also told *Intelligence Matters* host and CBS News senior national security contributor Michael Morell that Washington may be ill-prepared to respond to a large-scale cyber attack on infrastructure or other critical targets.

# North-Korea: Attacks & Objectives

Ahead of the storm: Cyberwarfare



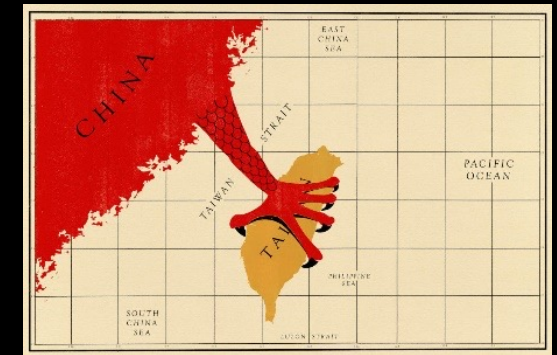
# Iran: Attacks & Objectives

Ahead of the storm: Cyberwarfare



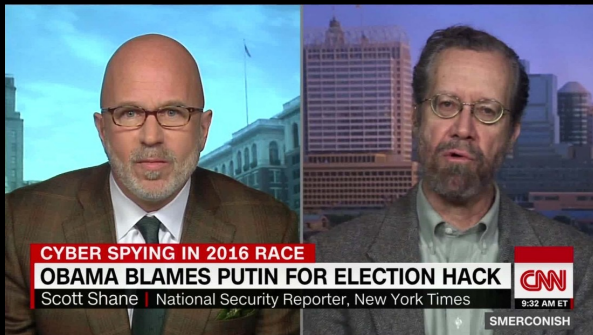
# China: Attacks & Objectives

Ahead of the storm: Cyberwarfare



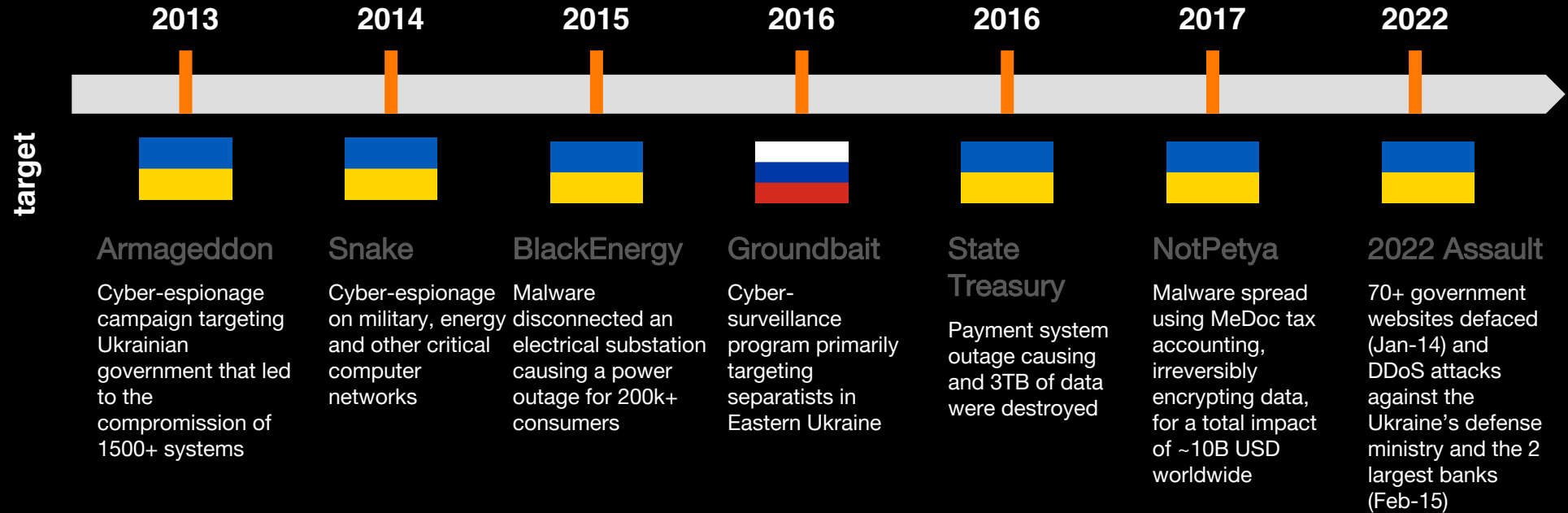
# Russia: Attacks & Objectives

Ahead of the storm: Cyberwarfare



# Cyber 'War'

High-Profile cyberattacks between Ukraine & Russia have been reported numerous times since 2013





< Back

## Updated - New insights on Killnet's recent hacktivist operations

Analysis

Appendices

Comments

### Update 1, 14/02/2023 - New insights on Killnet's recent hacktivist operations

Pro-Russian hacktivist group **Killnet** is still very active and has recently targeted the website of **NATO Sp** Belgium with a DDoS attack which lasted a couple of hours. Another DoS attack targeted the **Str** organisation which relies on NATO support in its task of providing military and humanitarian airlifts.

On January 30, the **US Department of Health and Human Services (HHS)** warned that Killnet h healthcare industry with DDoS attacks. This alert was completed by report released by **Radware**, wh entities had been targeted by the **Passion botnet** which was previously linked to Killnet. The report add are using **Telegram** to offer other cybercriminals access to their botnet service. The current merchant is S subscriptions for \$30 per week of service, or prepaid access for a year of service for \$1,440.

Furthermore, Killnet is still actively trying to **recruit** new hacktivists willing to attack the United State partnerships to do so. Indeed, cybersecurity company Radware detected the creation of a new forum and result of a collaboration between Killnet and Deanon Club. This new forum was registered on December 26 is protected by Cloudflare. Infinity is currently offering **a number of goods and services through its HA**

- a section for paid courses and tutorials
- a section for selling private data such as logs, dumps, and exploits
- a section for buying and selling DDoS, carding, and phishing services.

The leaders of hacktivists groups such as Killnet, KillMilk, Anonymous Russia have all **listed their crypto** asking their followers for **donations**.

As a reminder, malicious campaigns tied to Killnet have been also tracked in our separate advisory dedicated to the Ukraine war, available here. Over the last months, the hacktivist group targeted numerous organizations including:

- Japanese public institutions
- German government, airports, banking and hospital websites
- the European parliament
- US and Canadian airports
- Bulgarian government institutions

Nevertheless we maintain the risk-level attributed to this advisory to 1 as Killnet mostly leverage superficial DDoS attacks.

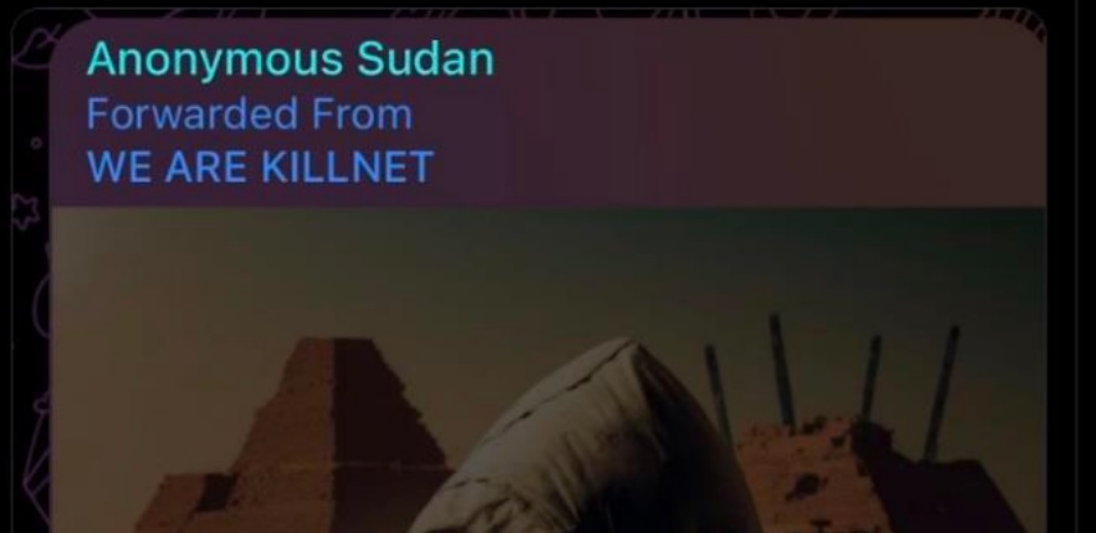
— Created at 02/14/2023, 11:38 AM

### Pro-Russian hacktivist group Killnet, a non-negligeable threat to Western organizations

#### 1.1 Executive summary

The pro-Russian hacktivist group **Killnet** has recently surfaced during the war in Ukraine and has conducted many attacks against Ukrainians as well

#Anonymous #OpRussia  
 Anonymous Sudan is not Anonymous and fuck you and fuck #Killnet you want to play then we will play  
 #SlavaUkraini  
 #Ukraine  
 Expect Us Sudan



- Appeared in January 2022 as a vendor of a bot service proposing to save data in a secured and centralized way via the blockchain Ethereum
- February 9<sup>th</sup> they launch a bot service dedicated to DDOS attacks
- The next day after the Russian invasion Killnet changes orientation from cybercrime to hacktivism –> attacks against Ukraine and countries that support Ukraine
- Some previously known attacks:
  - April 29<sup>th</sup>, DDOS attacks targeting Romania
  - Beginning of May, DDOS attacks against tens of Italian sites
  - May 14<sup>th</sup> : DDOS attack blocked against the Eurovision competition (after Russia was eliminated/disqualified)

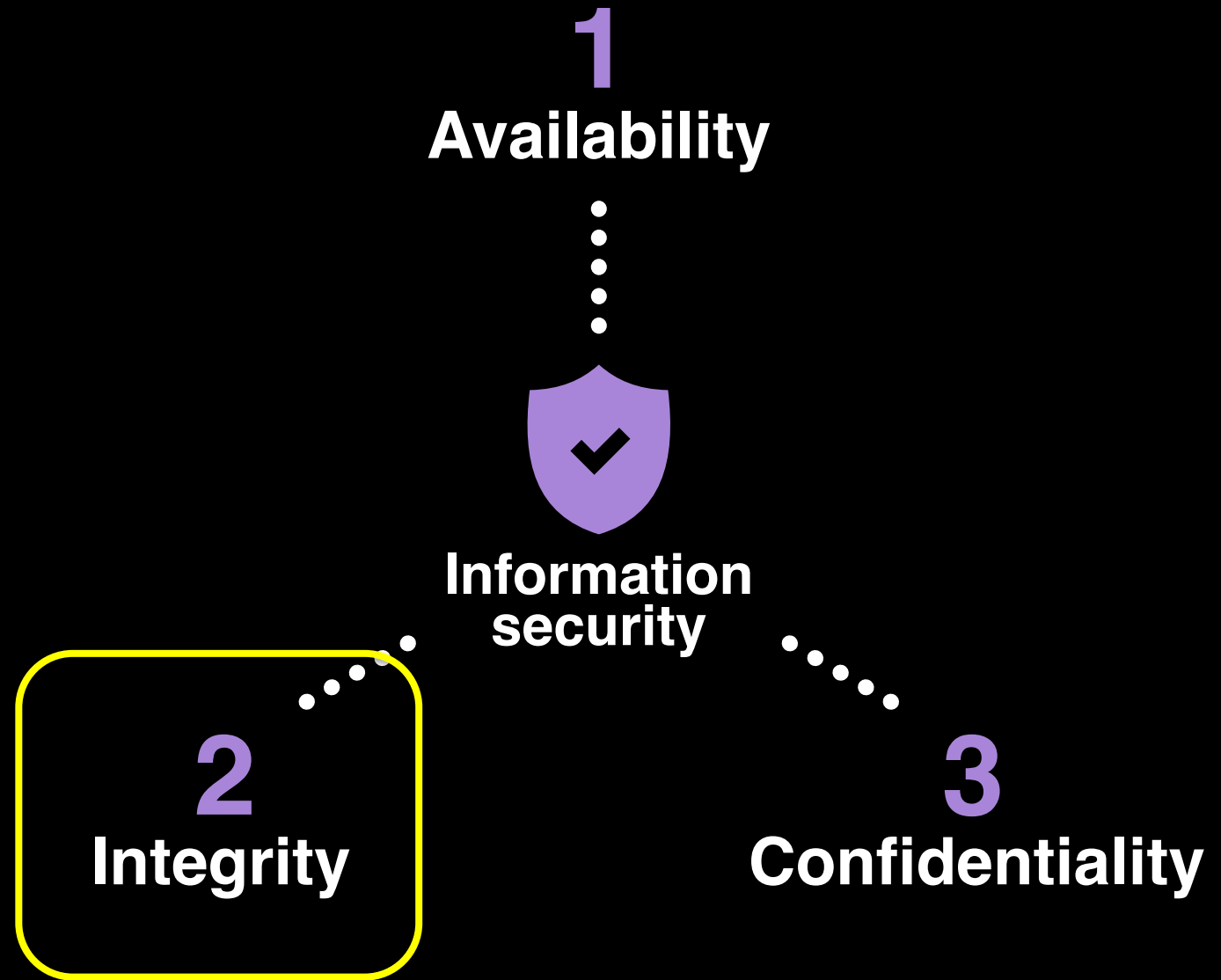


**F**ear **U**ncertainty **D**oubt



# Integrity:

Ensure data and information systems can be **trusted**





**Trust is infrastructure**

# USA: Attacks & Objectives

Ahead of the storm: Cyberwarfare



“

To protect New Zealand's most significant organisations from the types of threats which are typically beyond the capability of commercially available tools, and from threats which could potentially impact on the effective functioning of government administration or key economic sectors.



HOME

ABOUT US

NEWSROOM

INCIDENTS

RESOURCES

TICSA

## ABOUT THE NATIONAL CYBER SECURITY CENTRE

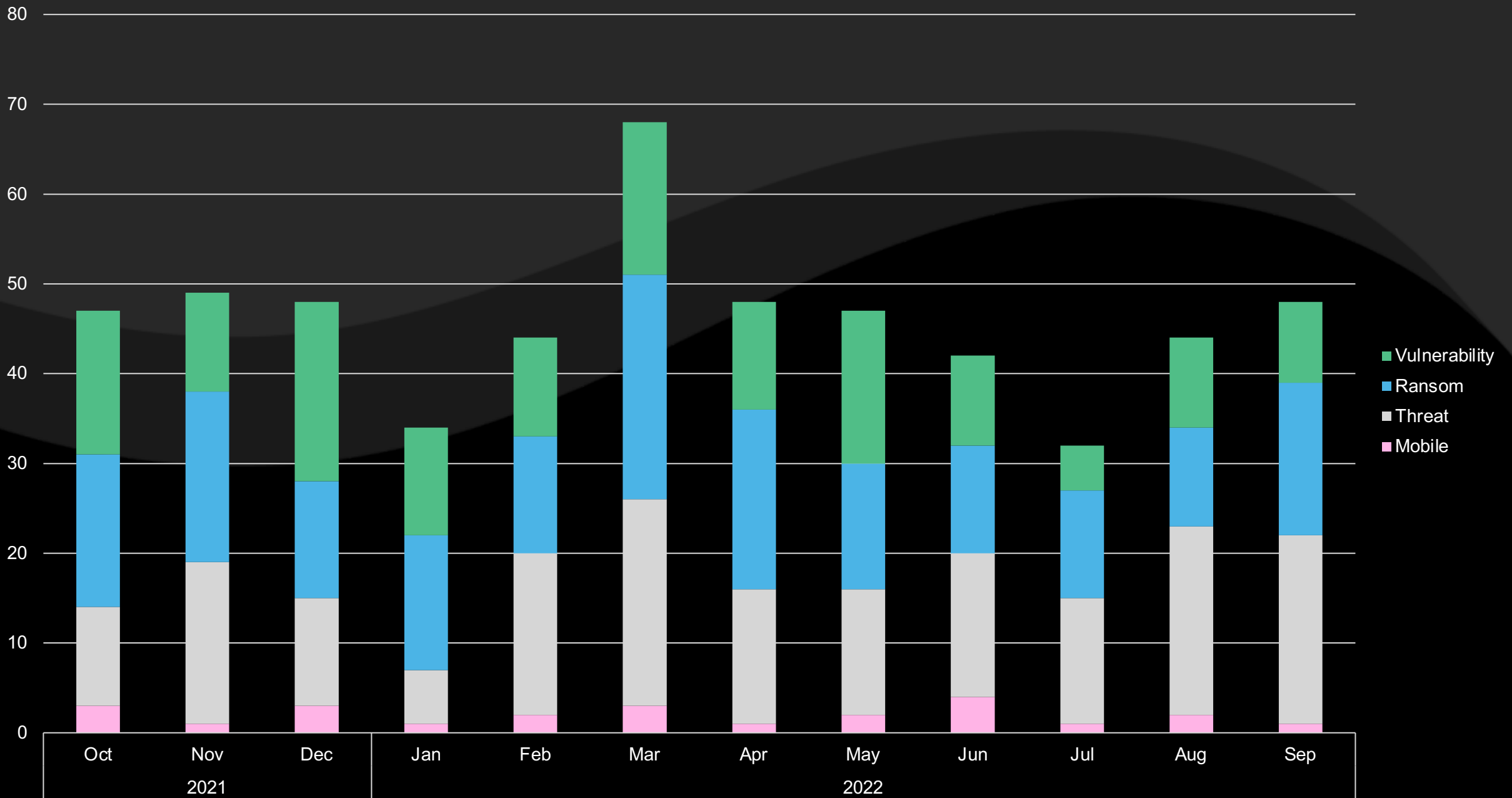
The New Zealand National Cyber Security Centre (NCSC) provides enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.

### Project Cortext:

“He can't say how Cortext will work or exactly which organisations will come under its protection. To do so would risk exposing vulnerabilities, he says. Nor will he say how much Cortext is costing.”



Mobile

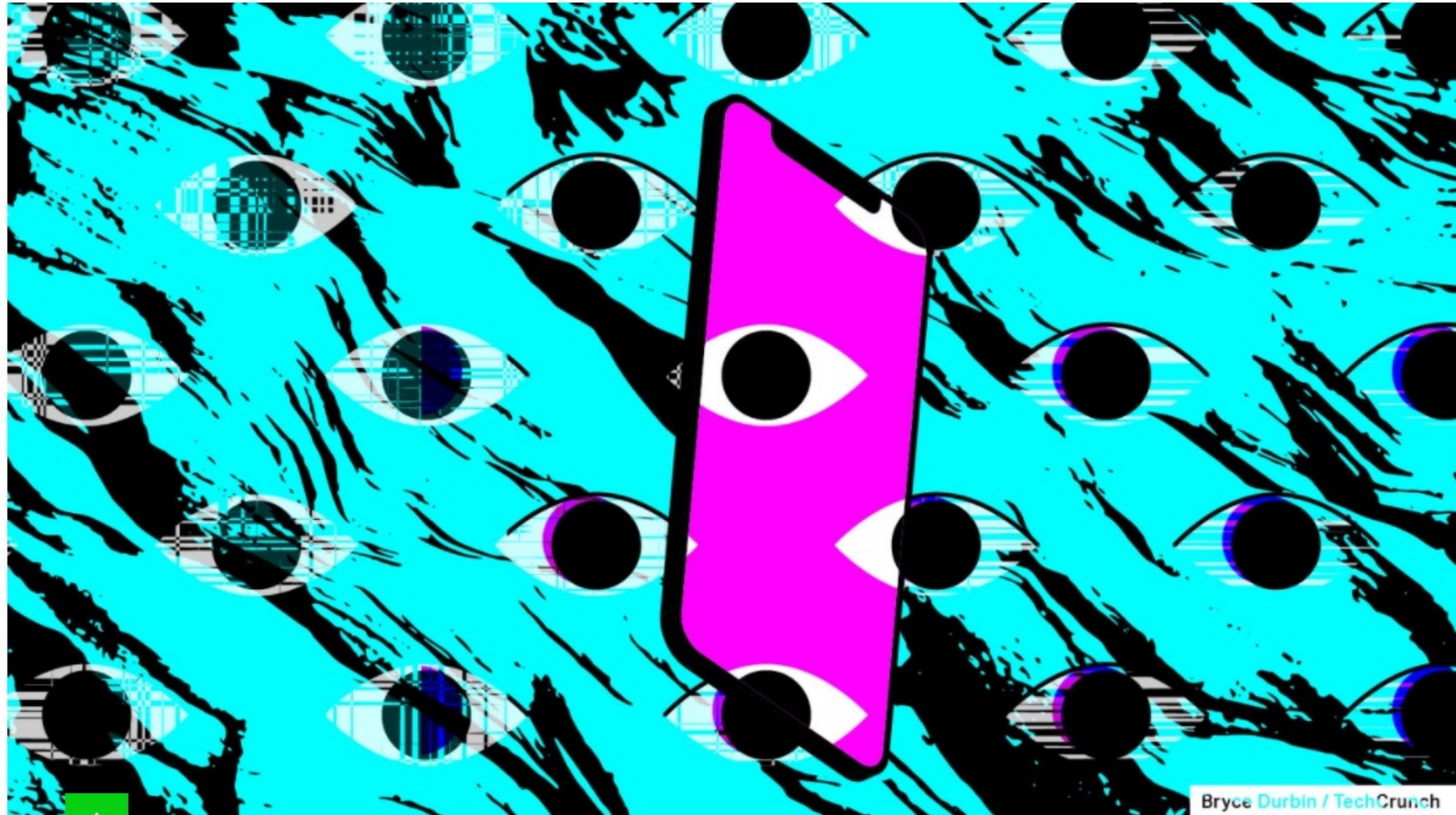


# Apple patches an NSO zero-day flaw affecting all devices

Citizen Lab says the ForcedEntry exploit affects all iPhones, iPads, Macs and Watches

Zack Whittaker @zackwhittaker / 9:15 PM GMT+2 • September 13, 2021

 Comment



Bryce Durbin / TechCrunch



יחידה 8200



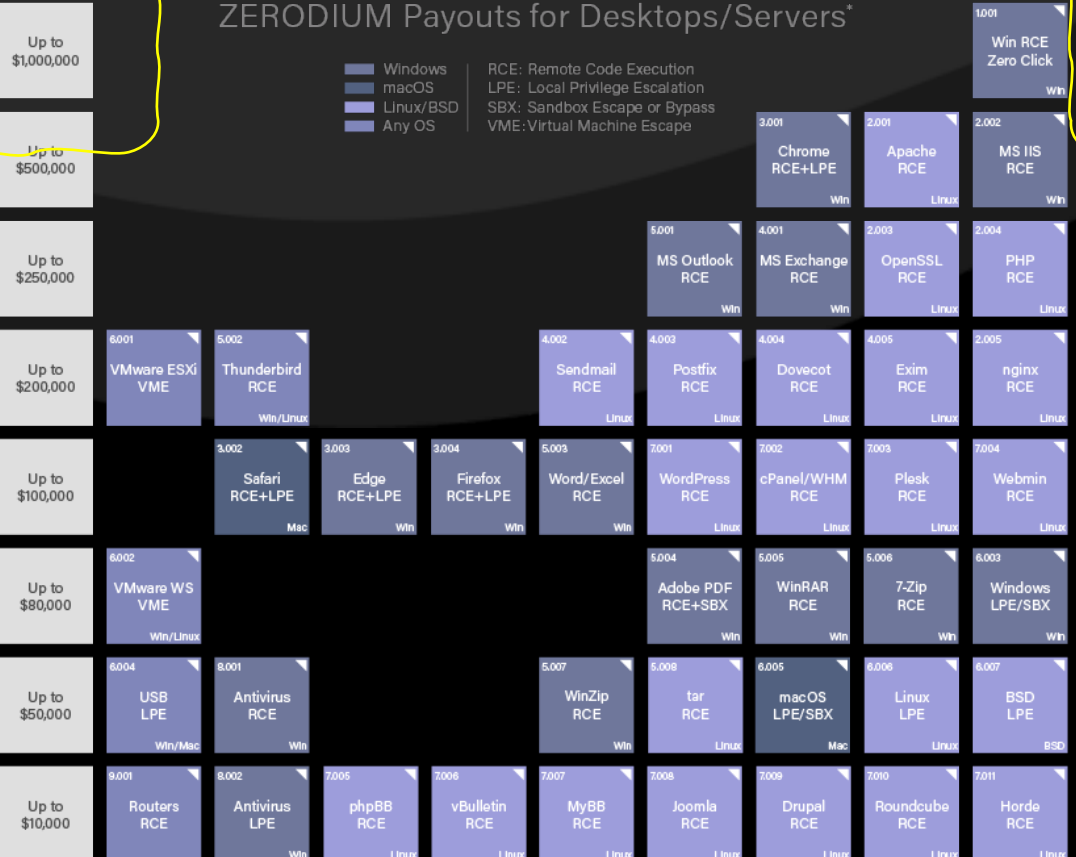
Governments can't possibly keep pace with demand, so a new breed of PMC emerges from the Military Industrial Complex, ready to offer its services.



Zerodium pays **BIG bounties** to security researchers to acquire their original and previously unreported zero-day research. While the majority of existing bug bounty programs accept almost any type of vulnerabilities and PoCs but pay very little, at **Zerodium we focus on high-risk vulnerabilities with fully functional exploits** and we pay the highest rewards in the market (**up to \$2,500,000 per submission**).

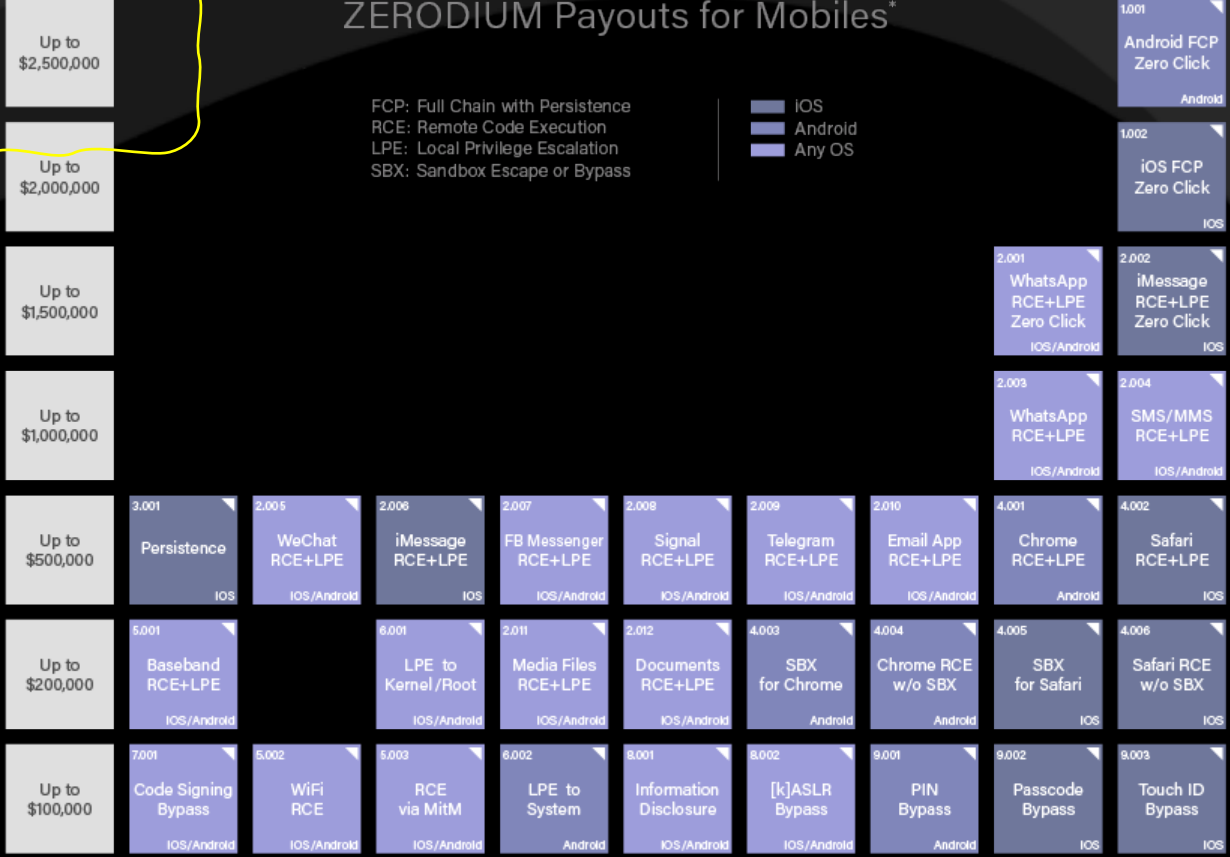
### ZERODIUM Payouts for Desktops/Servers\*

- Windows
  - macOS
  - Linux/BSD
  - Any OS
- RCE: Remote Code Execution  
 LPE: Local Privilege Escalation  
 SBX: Sandbox Escape or Bypass  
 VME: Virtual Machine Escape



### ZERODIUM Payouts for Mobiles\*

- IOS
  - Android
  - Any OS
- FCP: Full Chain with Persistence  
 RCE: Remote Code Execution  
 LPE: Local Privilege Escalation  
 SBX: Sandbox Escape or Bypass



\* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

\* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

**1. Cyber “War”,  
Espionage &  
Police Powers**

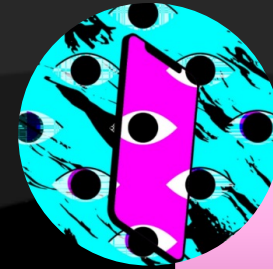
**4. Industrialization**

**2. Professionalization**

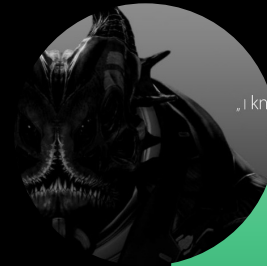
**3. Exploit  
Commoditization**

THIS IS A TRUE STORY

# An historical pattern to watch for



Unprecedented new threats, attacks & compromises.



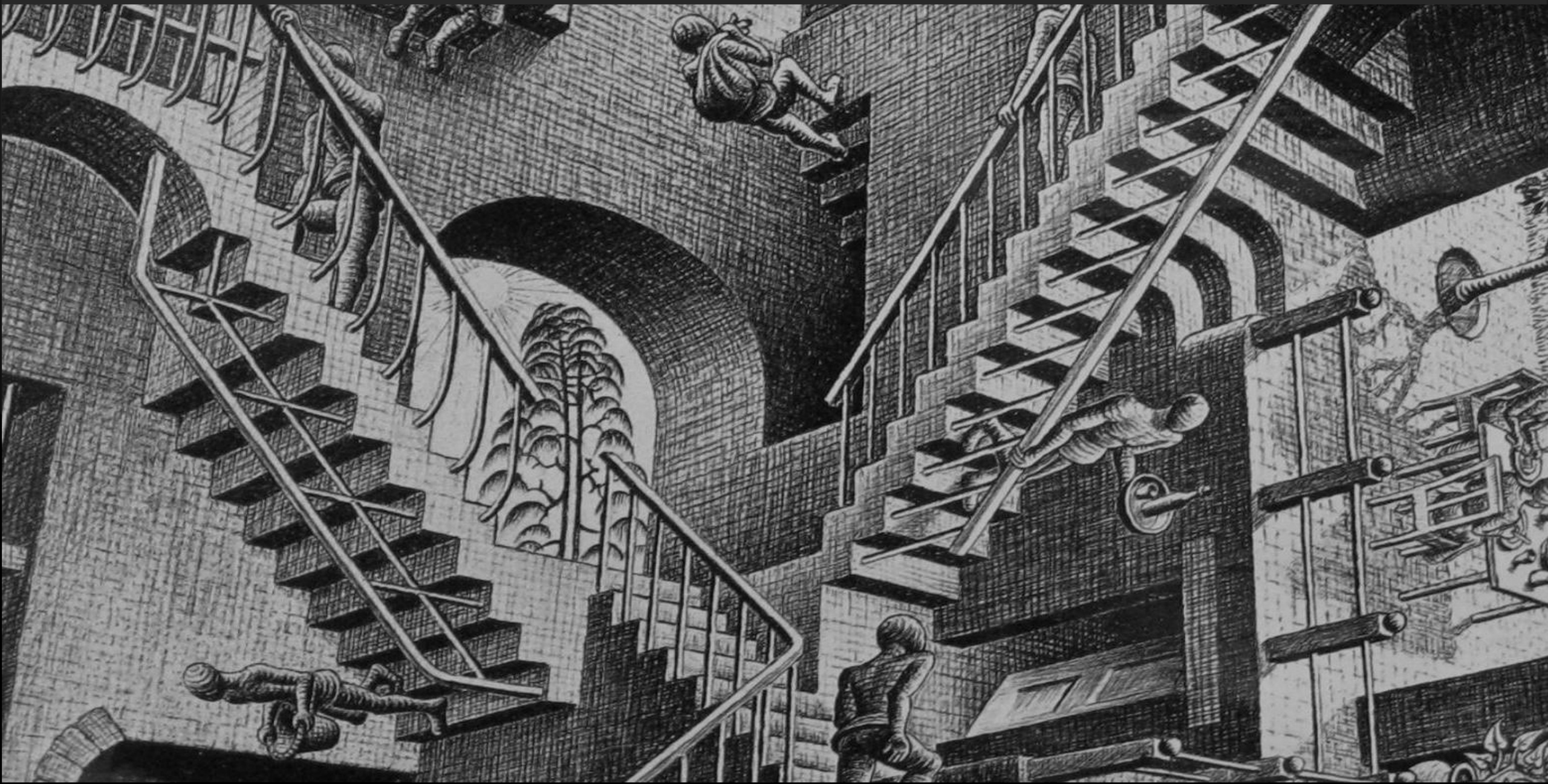
Government hacking investment leak into the civilian space



New types and levels of cybercrime are enabled by cryptocurrencies



A Cybercrime ecosystem hungry for new revenues





- Social Engineering
- Phishing
- Person in the Middle
- Golden SAML

Ldp

Active Directory

Cloud

Secure Remote Access

Go passwordless|



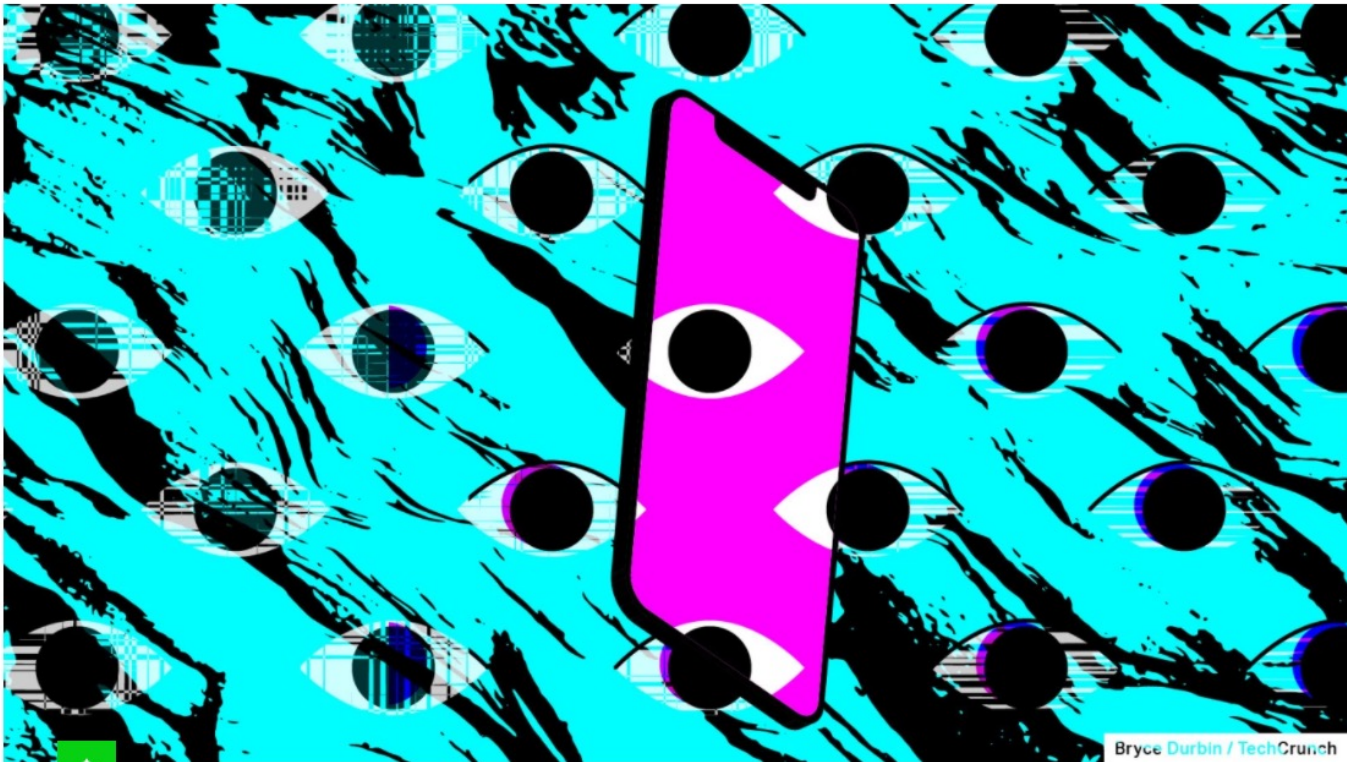
With your Microsoft account

# Apple patches an NSO zero-day flaw affecting all devices

Citizen Lab says the ForcedEntry exploit affects all iPhones, iPads, Macs and Watches

Zack Whittaker @zackwhittaker / 9:15 PM GMT+2 • September 13, 2021

Comment



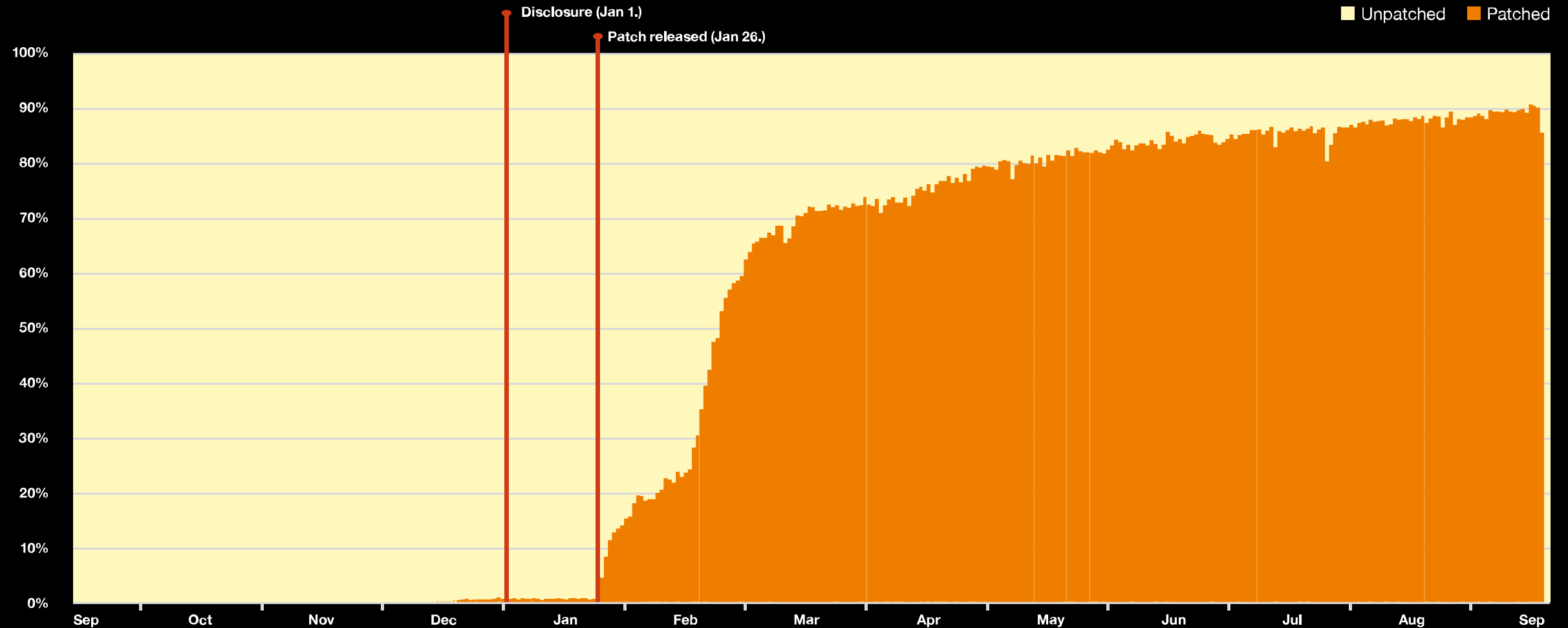
Bryce Durbin / TechCrunch



# Patch application (iOS)

- Patching status for iOS vulnerability CVE-2022-22587 over time

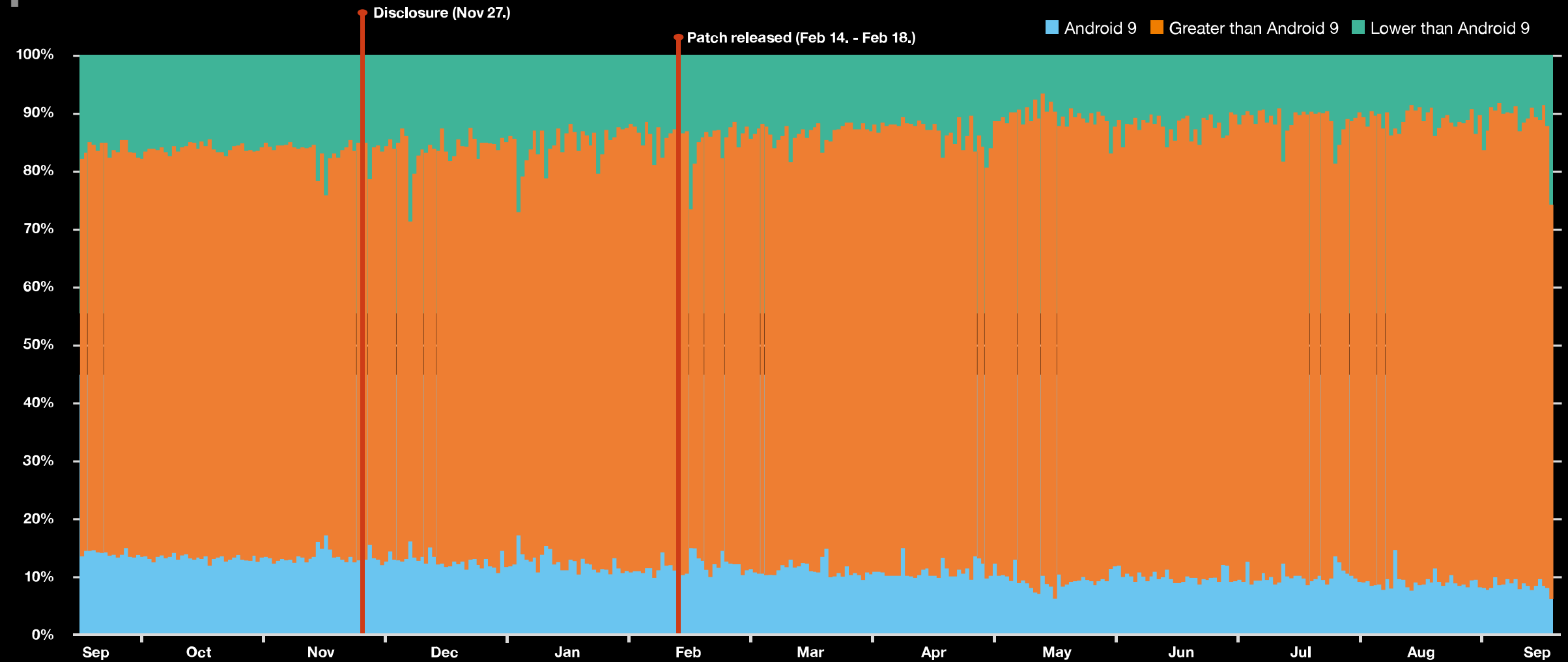
▪





# Version status (Android)

## ■ Distribution of Android vulnerable and not vulnerable to CVE-2022-22292

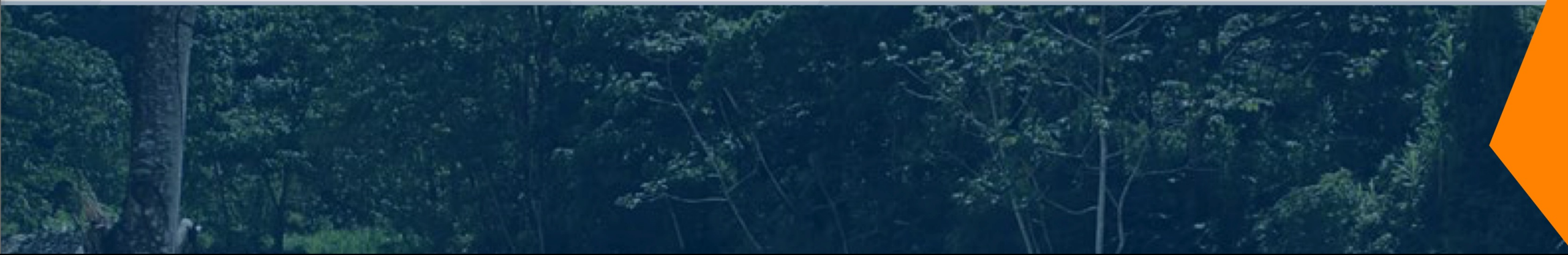


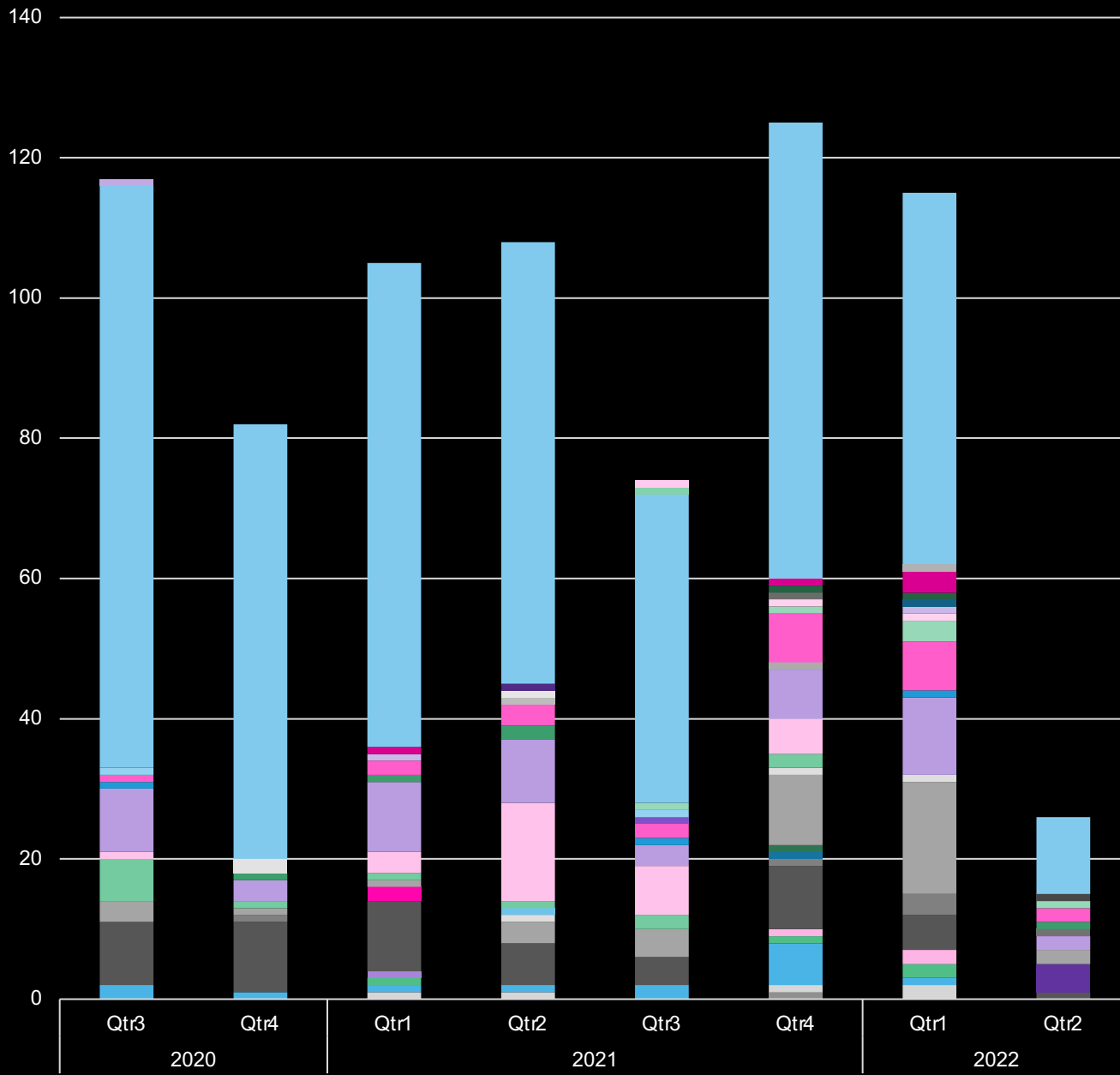


**Cyber Extortion**



# Comisión Nacional de Prevención de Riesgos y Atención de Emergencias





- AR ■ AT ■ AU ■ BE ■ BR ■ BS ■ CA ■ CH ■ CL ■ CN ■ CO ■ CR ■ DE ■ DK ■ DO ■ ES ■ FR ■ GB ■ GR ■ HK ■ ID
- IN ■ IT ■ JP ■ KR ■ LU ■ MX ■ NL ■ NO ■ NZ ■ PE ■ PK ■ RS ■ SA ■ SE ■ SG ■ TN ■ TW ■ US ■ VN ■ ZA ■ ZZ

# CONTI NEWS

[Web mirror](#)
[Tor mirror](#)

**"ALIMENTOS Y FRUTOS S.A."**

<https://www.minutoverde.cl>

Camino Lo Echevers 250 SANTIAGO, Santiago, 8730594 Chile See +56-223678000

It is meeting the needs of consumers looking for Practical, Rich and Functionally Nutritious food through the production, sale and distribution of frozen fruits and vegetables, both in Chile and in the rest of the world.

We will continuously seek innovation and will work with the highest standards of quality, respecting the environment and providing our employees a pleasant working environment and professional development opportunities.

Achieving the above we will keep our leadership and thus maximize the return on investment of our shareholders.

PUBLISHED 30%

23/05/2022 👁️ 15138 [READ MORE >>](#)

**"AGILE SOURCING PARTNERS"**

<https://www.agilesourcingpartners.com>

2385 Railroad St, Corona, California, 92880, United States (951) 279-4154

Based in Corona, CA, Agile is a national supply chain management organization committed to providing integrated solutions that best meet each customer's unique.

PUBLISHED 30%

23/05/2022 👁️ 14155 [READ MORE >>](#)

**"EUROFRED"**

<https://www.eurofred.com>

MarquA.L s de Sentmenat 97, Barcelona, Catalonia, 08029, Spain +34 934 19 97 97

Founded in 1966, Eurofred is a noted leader in the distribution of air conditioning, industrial heating, commercial refrigeration & catering equipment.

PUBLISHED 30%

23/05/2022 👁️ 13945 [READ MORE >>](#)

**"CONCEPTS IN MILLWORK"**

<https://www.conceptsinmillwork.com>

1490 Tuskegee Pl, Colorado Springs, Colorado, 80915, United States (719) 570-7353

Concepts in Millwork is a family-owned business that was founded in 1980 and built on hard work, dedication and a commitment to excellence. We are continually improving our quality, methods, equipment, and service to ensure we continue to serve satisfied customers. Concepts is considered a small business, we are AWI premium-grade certified and work on many LEED projects.

As a stable and secure commercial millwork company, we are responsible and timely in paying our suppliers. This ensures long-term, trusted partnerships with a positive impact on completing great projects.

Our exceptional people are always ready to help you every step of the way in planning, engineering, and designing your CONCEPTS into reality.

PUBLISHED 30%

**"FOR COSTA RICA"**

<https://www.hacienda.go.cr/>

<https://www.mtss.go.cr>

<https://fodesaf.go.cr>

<https://siva.ac.cr>

On Monday we will upload the rest of the data and delete your key, we can't wait for you anymore

PUBLISHED 97%

**"CJK GROUP, INC."**

<https://www.cjkgroup.com>

3323 Oak St Brainerd, MN, 56401-3807 (800) 328-0450

Headquartered in Brainerd, MN, CJK Group, Inc. is an international portfolio of print and publishing service companies.

PUBLISHED 1%

# Cy-X as a crime requires a relationship

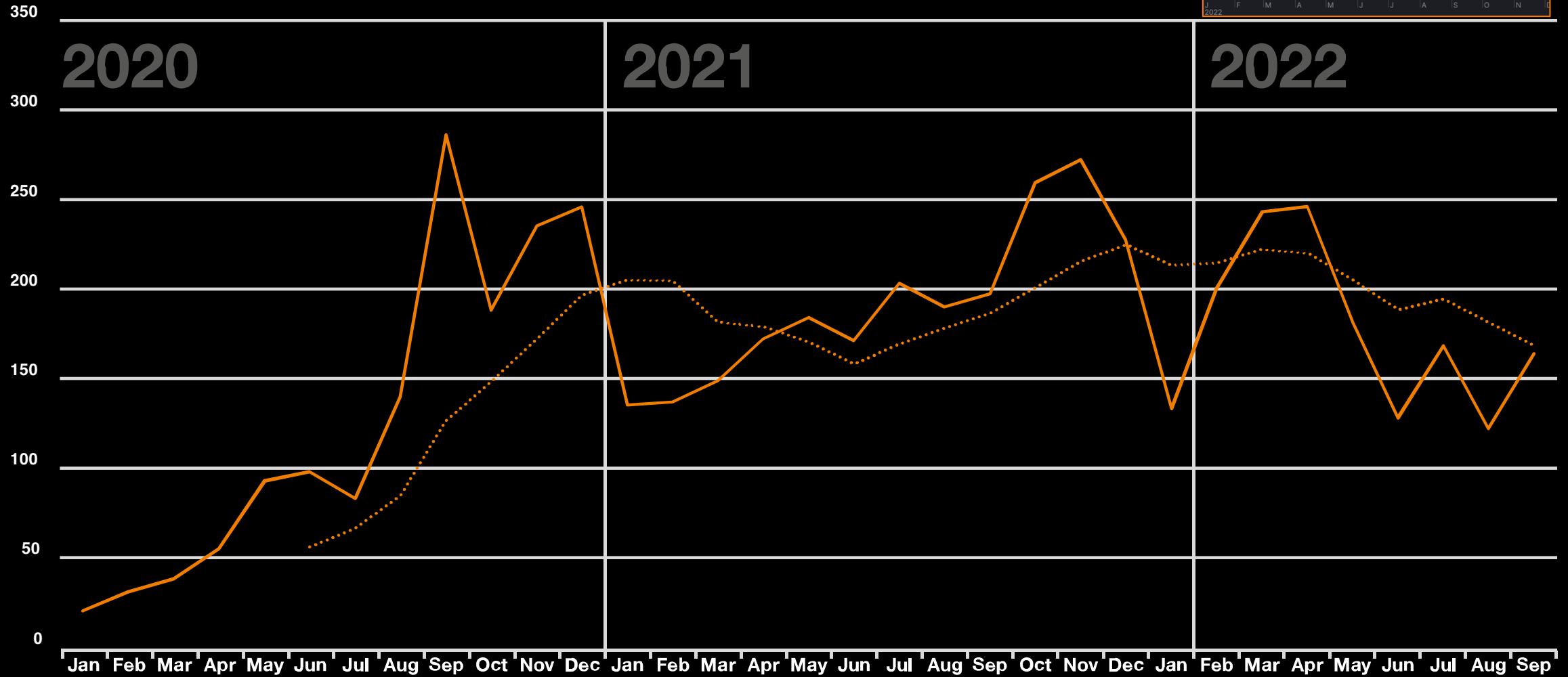
Language, culture and an understanding of the business environment are the only barriers to entry  
Government pressure the only real impediment

mango	skippy	there is a case
mango	skippy	important)
skippy	mango	I listen
mango	skippy	P-----c.com
mango	skippy	need a report on them
mango	skippy	what can be put on
mango	skippy	hung chat something with them
skippy	mango	plan report?
mango	skippy	what can be extorted from them
mango	skippy	it's like some kind of city chtoli I didn't really understand
mango	skippy	they say that the poor offer 20k)))



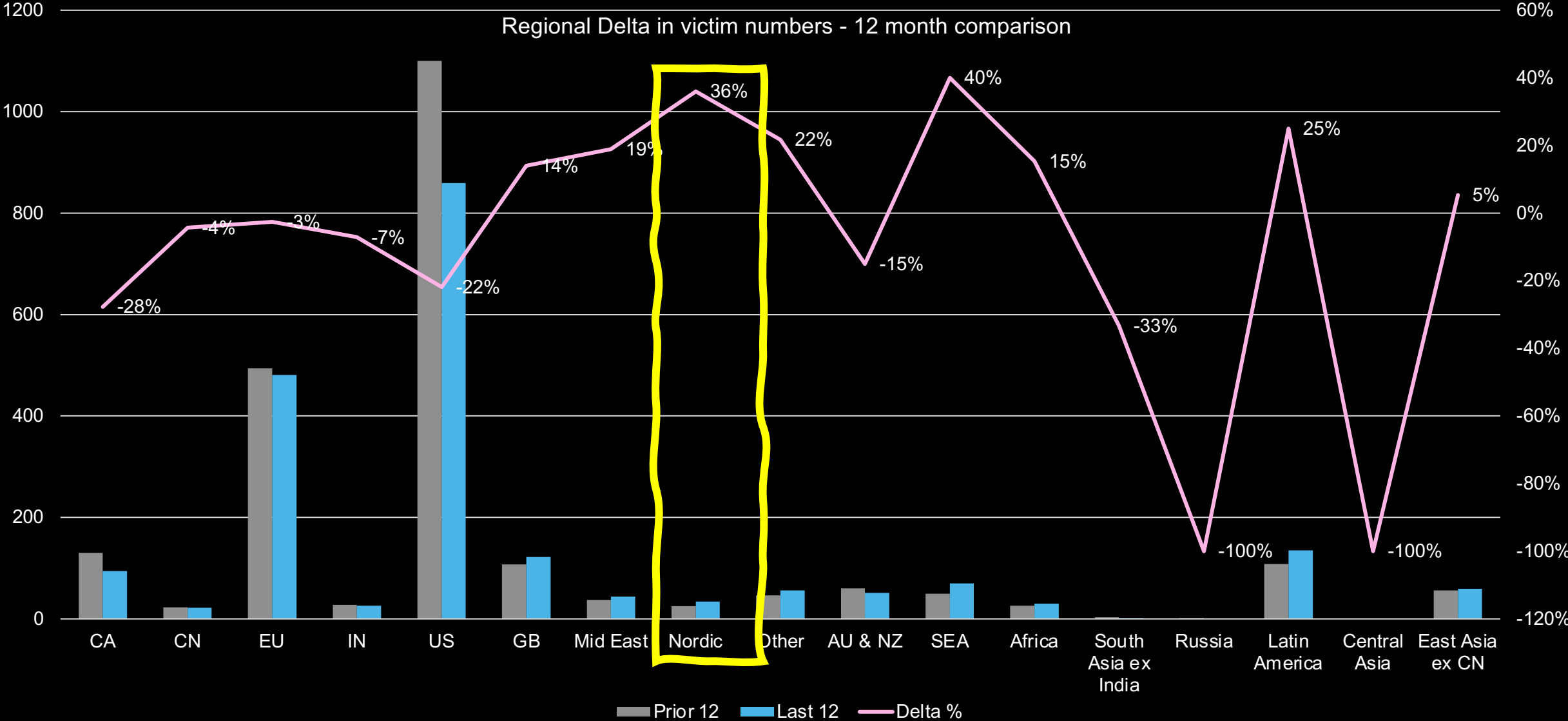
# Cyber extortion victims: over time

- Observable victims on leak sites

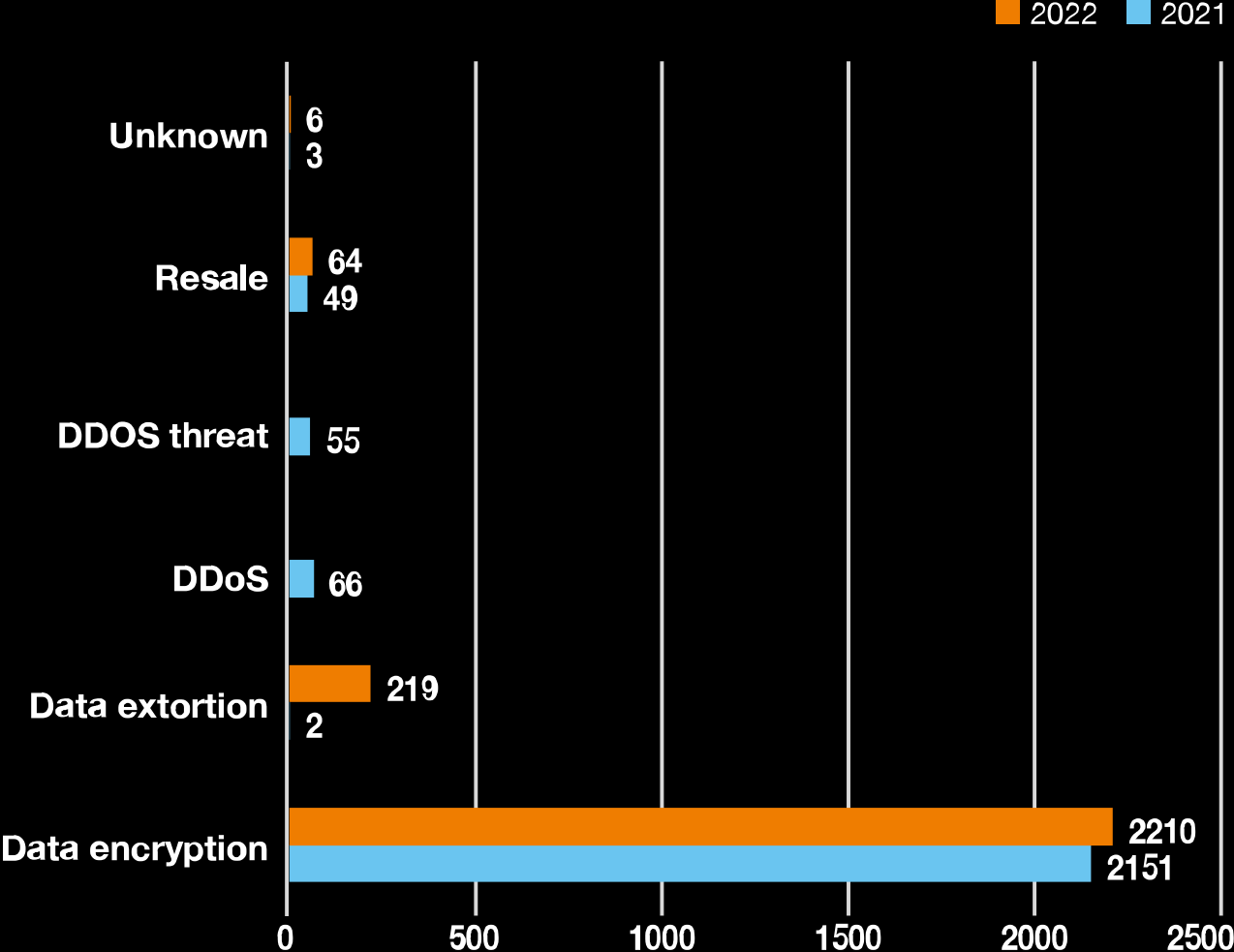


# Cy-X victims: geographic shift

Regional Delta in victim numbers (12 month comparison ending 01 Feb 2023)



# Extortion Types



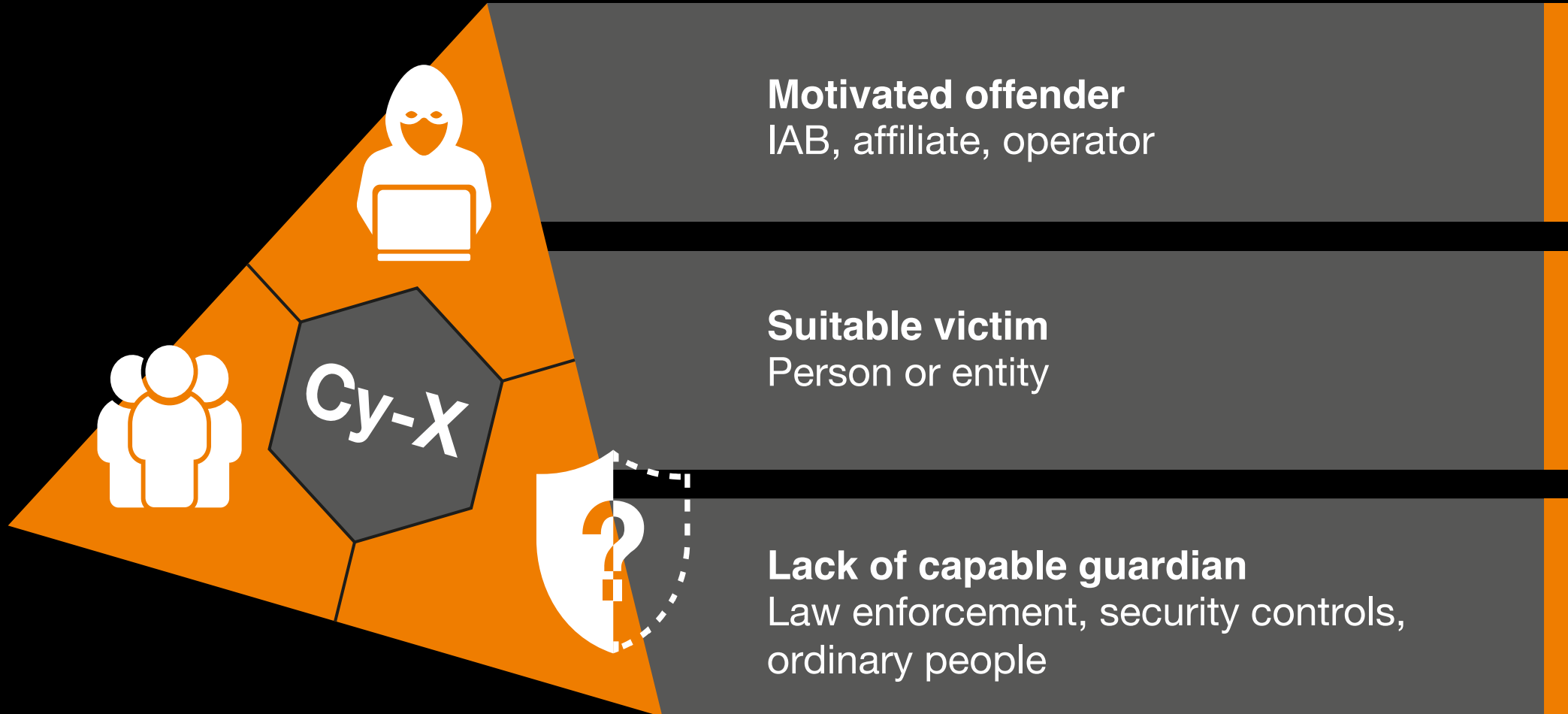




You can't stop the mafia with better locks  
on your door.

# Routine Activity Theory (RAT) applied to cyber extortion

A standard model of criminology applied to a digital crime

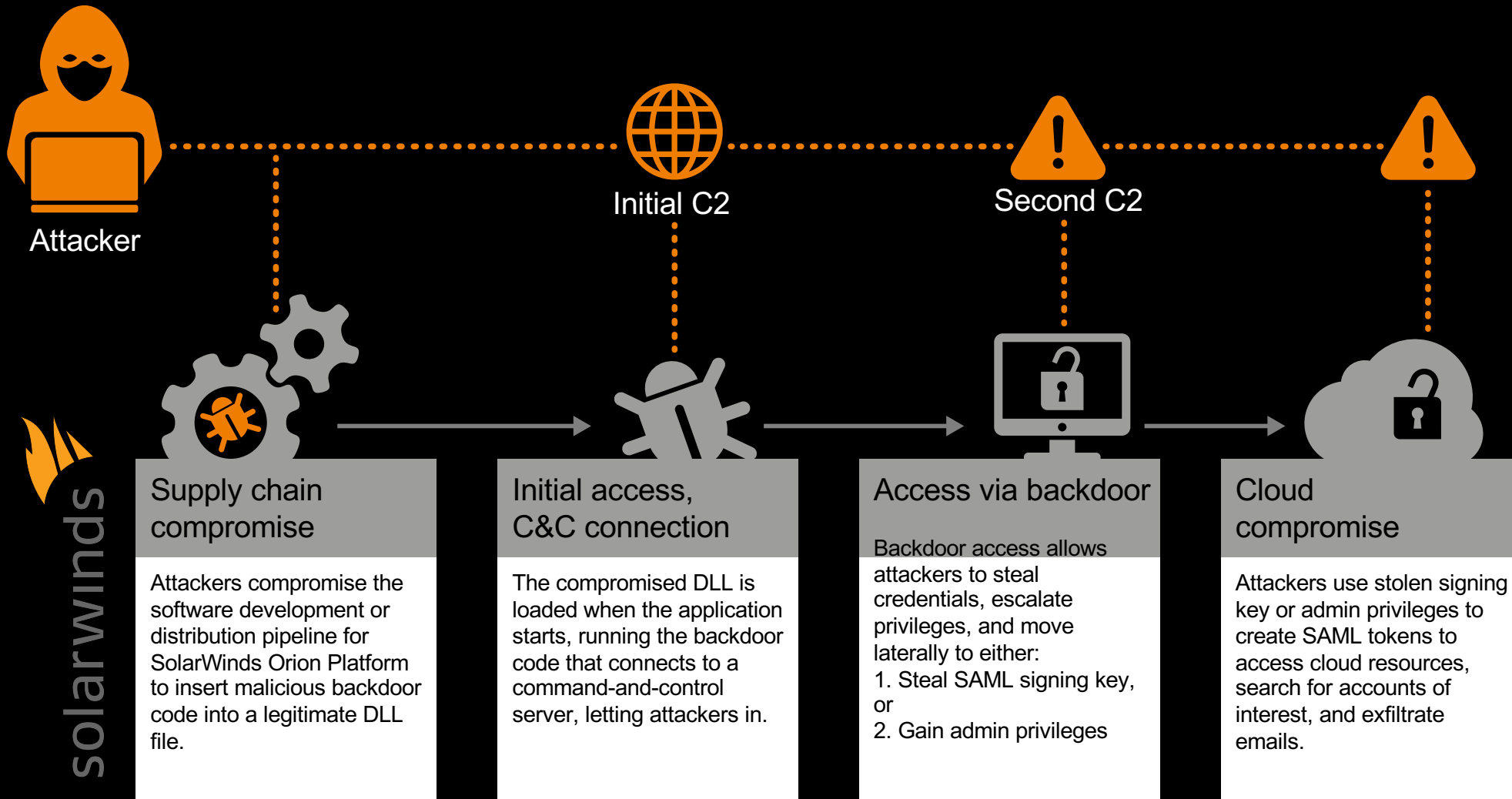




Interdependence

# Solorigate attack summary

## High-level end-to-end sophisticated supply-chain compromise

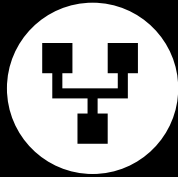


# Systemic issues driving Solorigate



## Government cyber operations

Involves work or investment by governments, state-sponsored or supported hackers, state-developed tools or capabilities, or their associated contractors.



## Cyber interdependence

A threat, vulnerability or incident emerging from the inter-dependence businesses have on each other. Example: attacks against MSSPs & attacks against shared (e.g. Open Source) code bases or systems (e.g. DNS or domain registrars). Incidents involving risk, attacks or compromises being spread from one organization to another (e.g. Maersk and notPetya or the Marriott breach would also fall into this category).



## Security debt

Security debt accumulates deep in the architectures, legacy code, 3rd party libraries and dependencies and even the fundamental economic principles that some business models are based on.

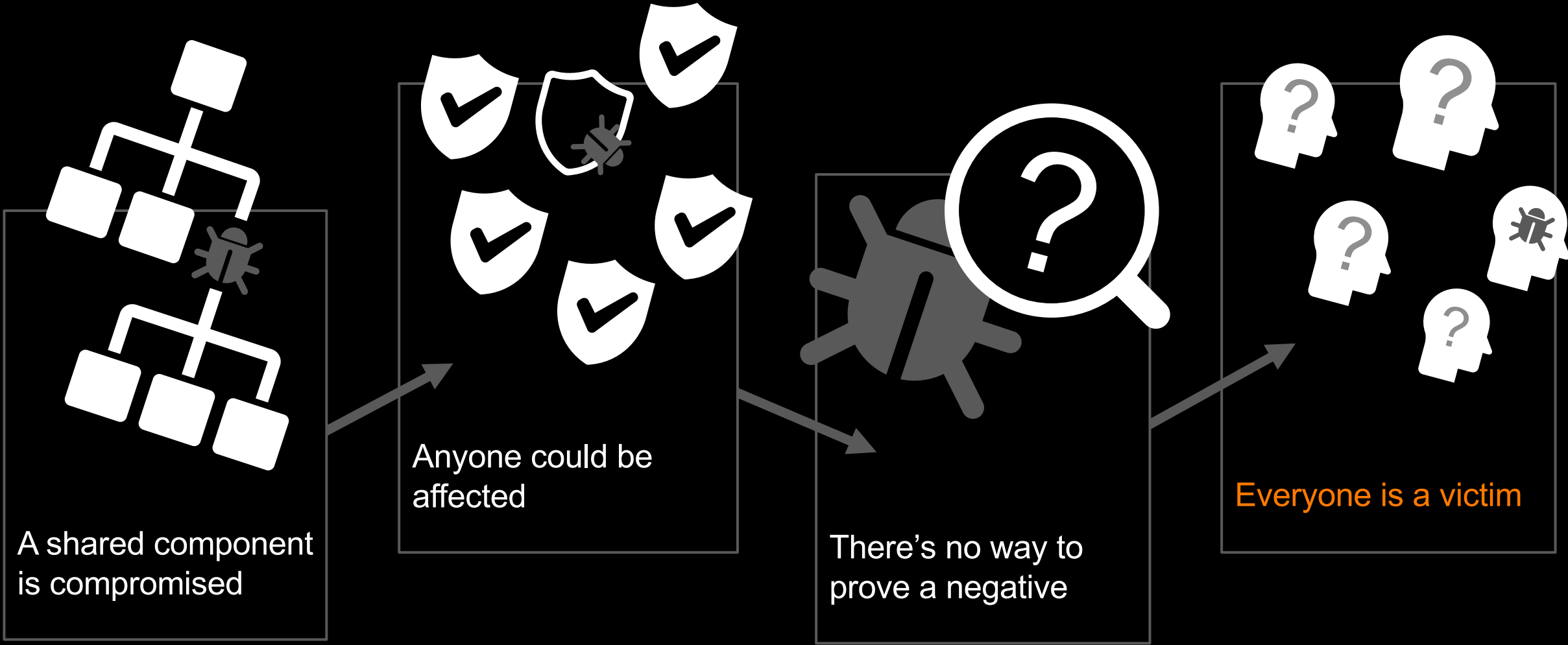


## Supply Chain Attacks

The notion that the 'supply chain' is a growing new threat vector. 'Supply chain' would include software supply chain (including full applications, Open Source tools or common modules, service providers, contractors and other suppliers).

It makes sense for hackers to target the supply chain because it's often the 'weak' link in security, but also because a single carefully-selected supply chain compromise (e.g. a commonly used package or system) could allow for a high number of downstream compromises.

# Compromising integrity & trust, causing “contagious” effect



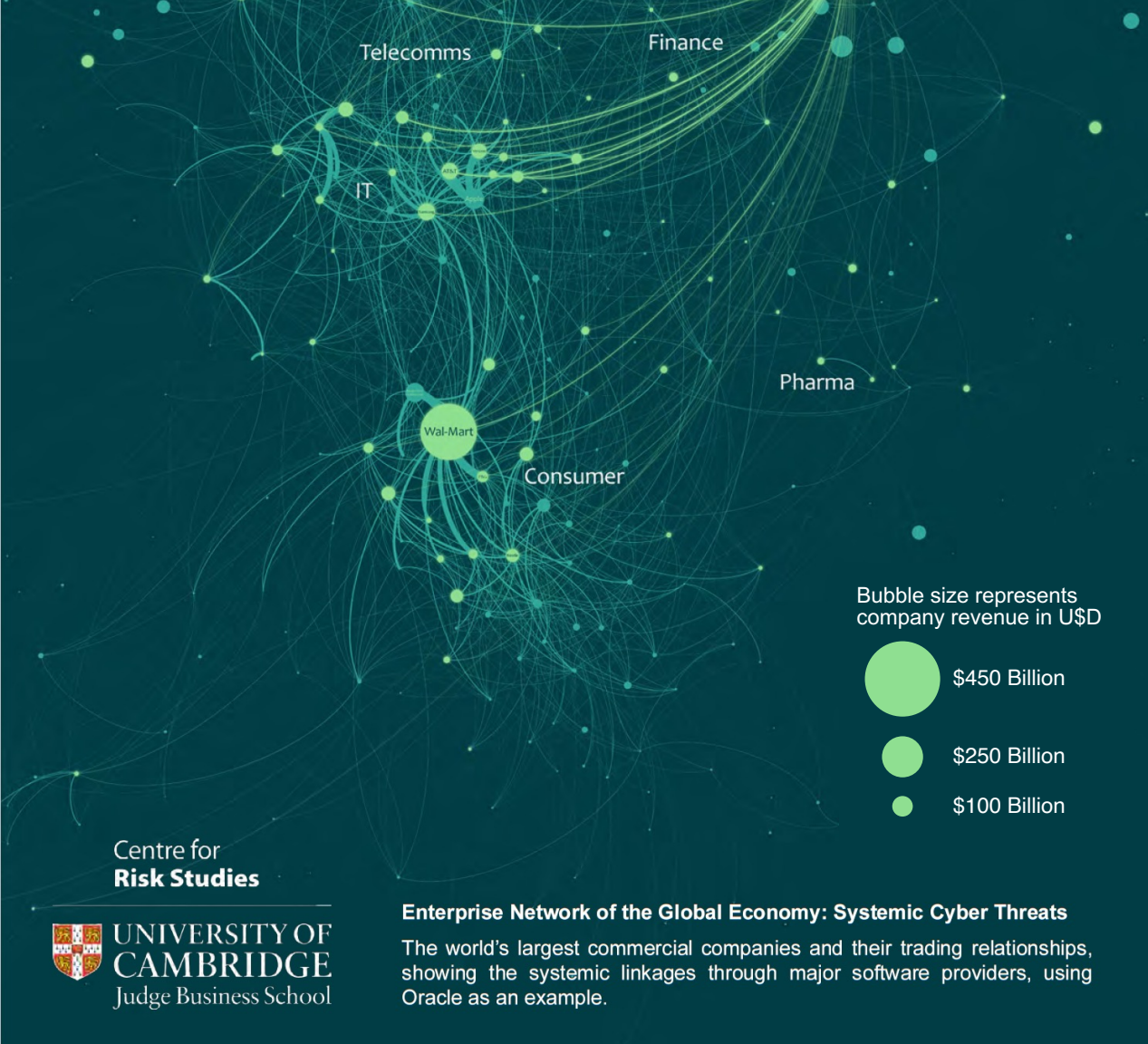
# Global Financial Crisis (2007–2012)

A contagion event caused  
by **unmanaged debt**

Approximately  
**\$20 trillion cost**  
to the world economy



“I thought we were just  
buying a house!”



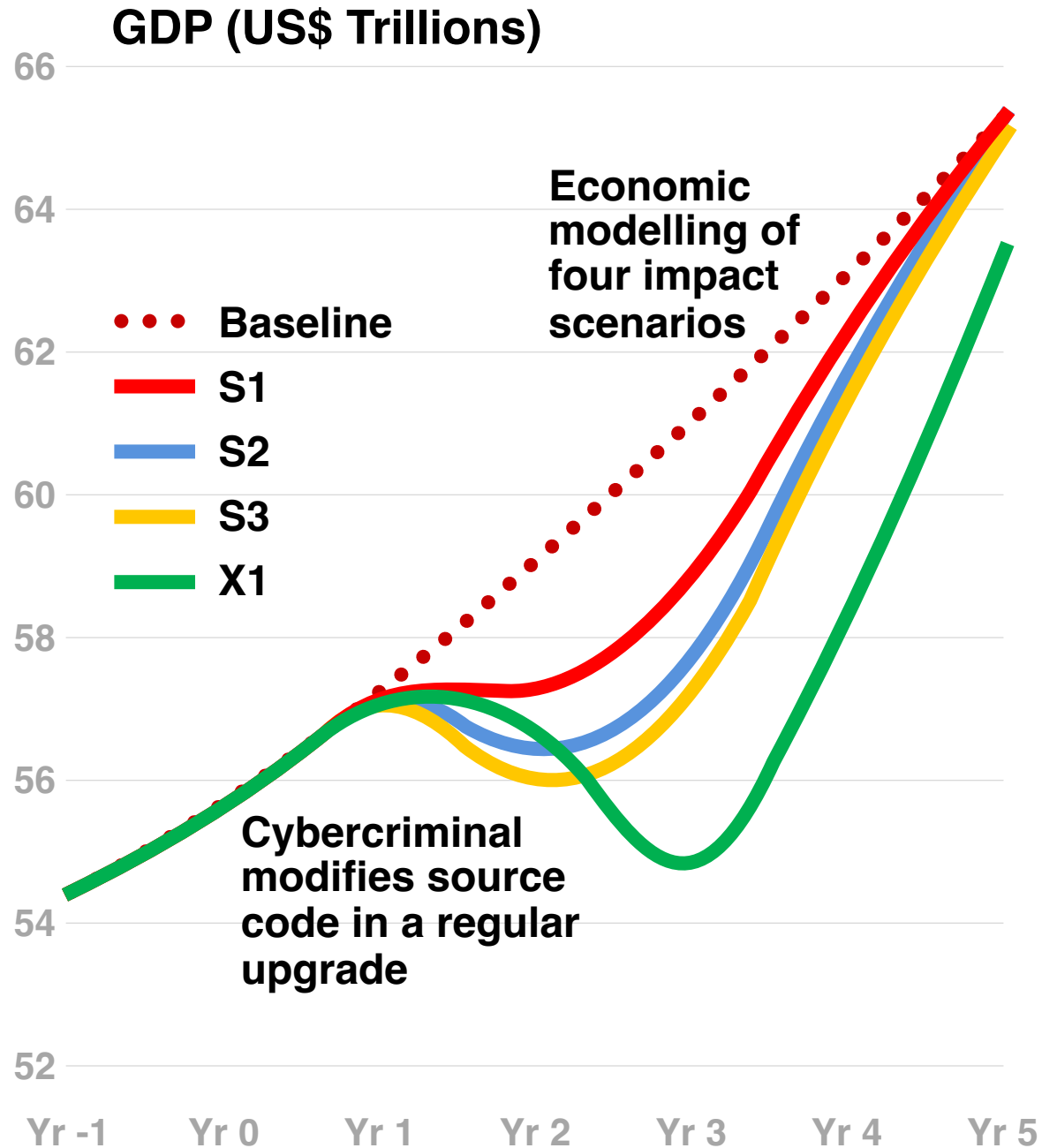
# The “Internet of Enterprises” era of business ecosystems

- Threats from **systemic linkages** between enterprise software systems
- **Loss of trust** in IT by business leaders, investors and consumers
- Risk of an **“information malaise”**
  - Lack of data flows
  - Leads to panic
  - Similar to a ‘fire sale’

**The world’s largest commercial companies and their trading relationships**



**Sybil:**  
a “hypothetical”  
database  
application  
that is widely  
around the world



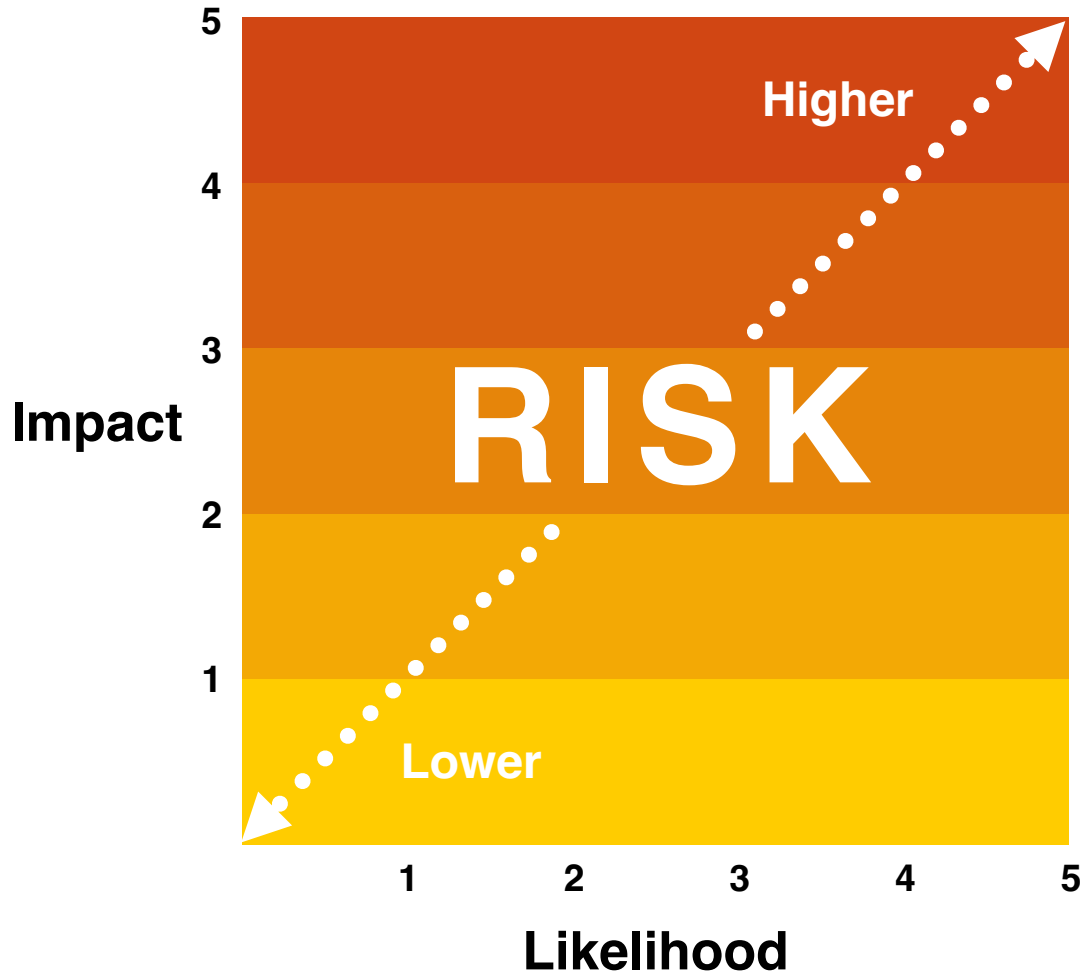
**A global cyber  
crisis**

**<\$15**  
trillion cost to GDP

**Global  
financial crisis**

**<\$20**  
trillion cost to GDP

# Risk: a function of both likelihood and impact



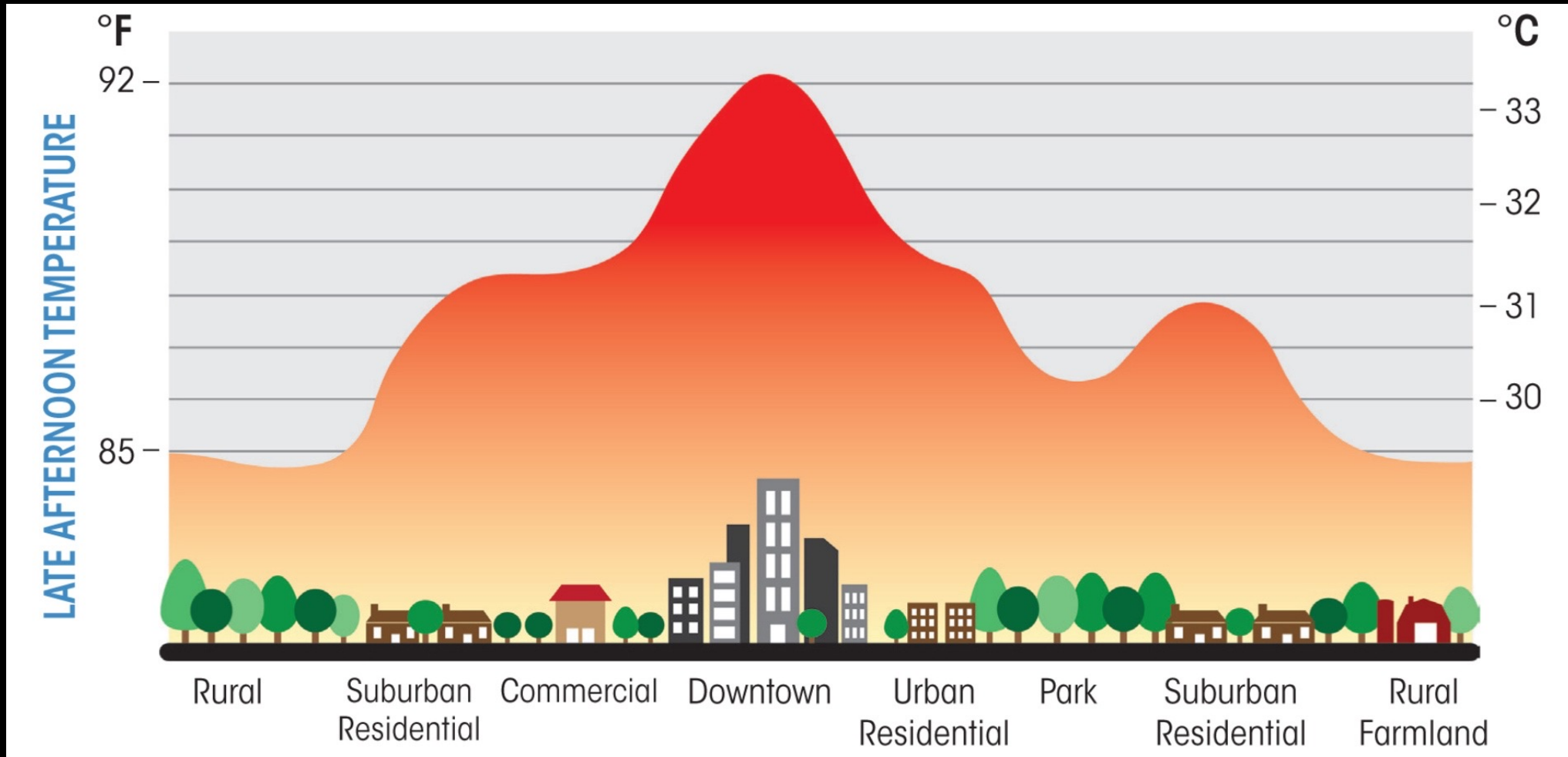
- Threats with severe consequences cannot be tolerated, even if they are unlikely
- We need to recognise our interdependence and counter such threats as a community

**“Everybody  
complains about  
the weather, but  
nobody does  
anything about it.”**

**Charles Dudley Warner (1829 – 1900)**



# Architecture Influences Weather



# Orange Cyberdefense

Building a safer digital society

## Thank you

<https://cyberdefense.orange.com>

