CHECK POINT™

IP Cameras in Modern Warfare

Sergey Shykevich | Threat Intelligence Group Manager

cp<r>
CHECK POINT RESEARCH

Who Am I?

- Threat Intelligence Group Manager at Check Point Research
  - Nation state actors
  - Cybercrime
  - Hacktivists
  - Technological methods
- 8 year in private sector
- 9 years in government sector

IP Cameras – Why it Matters for Nation State Actors ?

Special Operations

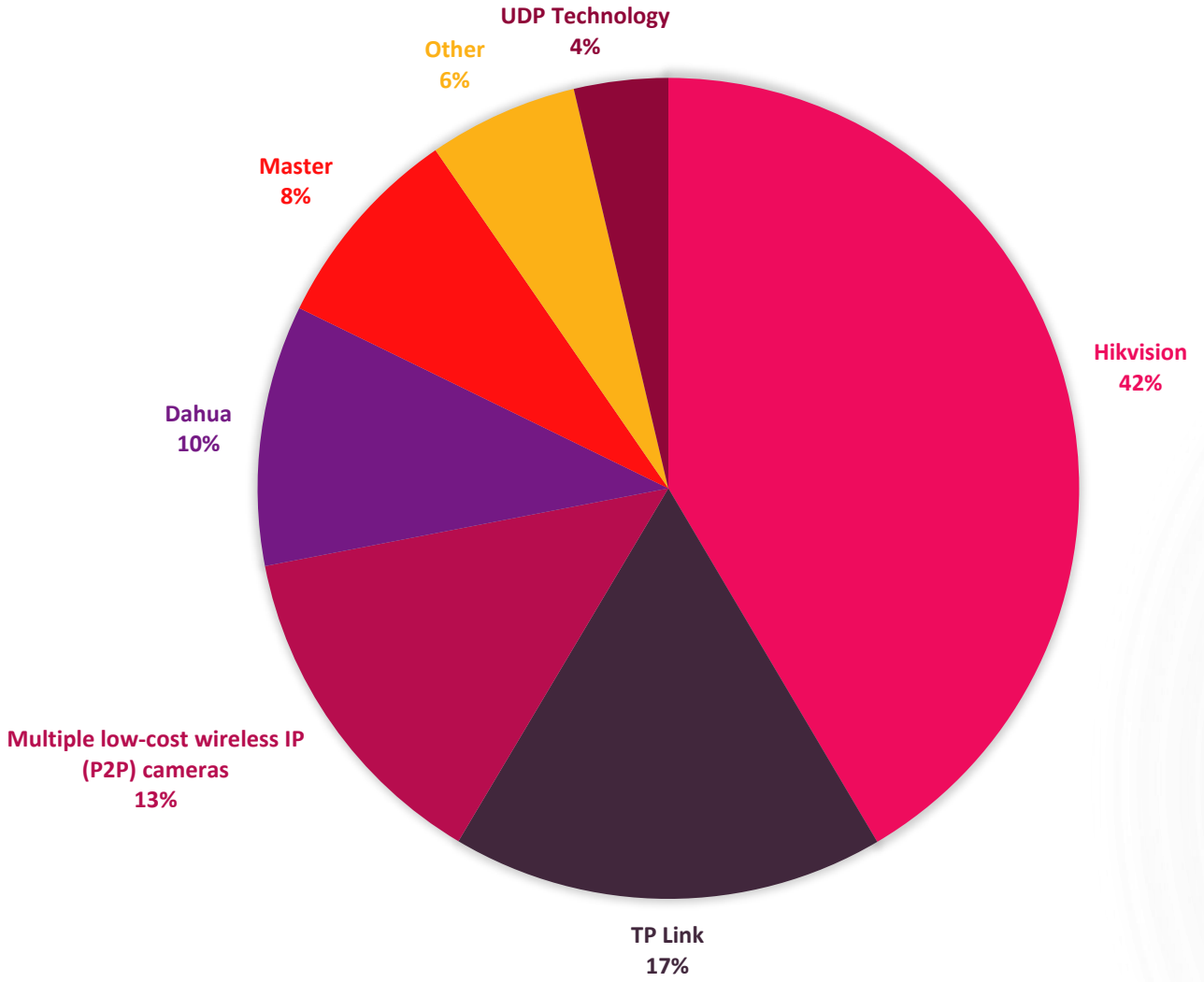
Pre Strike Intelligence

Post Strike Intelligence (BDA)

Continuous, cheap visual coverage

Civilian infrastructure becomes intelligence and operational asset

What IP Cameras are Exploited ?



Most Exploited CVEs

CVE-2017-7921	An improper authentication vulnerability in **Hikvision** IP camera firmware
CVE-2021-36260	A command injection vulnerability in the **Hikvision** web server component
CVE-2023-6895	An OS command injection vulnerability in **Hikvision** Intercom Broadcasting System
CVE-2025-34067	An unauthenticated remote code execution vulnerability in **Hikvision** Integrated Security Management Platform
CVE-2021-33044	An authentication bypass vulnerability in multiple **Dahua** products
CVE-2017-6343	An authentication bypass vulnerability in multiple **Dahua** products
CVE-2017-8225	Authentication bypass in Wireless IP Camera (P2P) **WIFICAM** devices

Have public POCs

- Straightforward to exploit

Case Studies

Chinese Nexus Actors

Russian Nexus Actors

Iran Nexus Actors

Chinese Nexus Actor - Ink Dragon Case Study

- Focus on South-East Asia and Latin America, with recent activity moving to Europe and Africa

- Creates relay network - one of the tools deployed in the victim's environment is used in other attacks by this threat actor

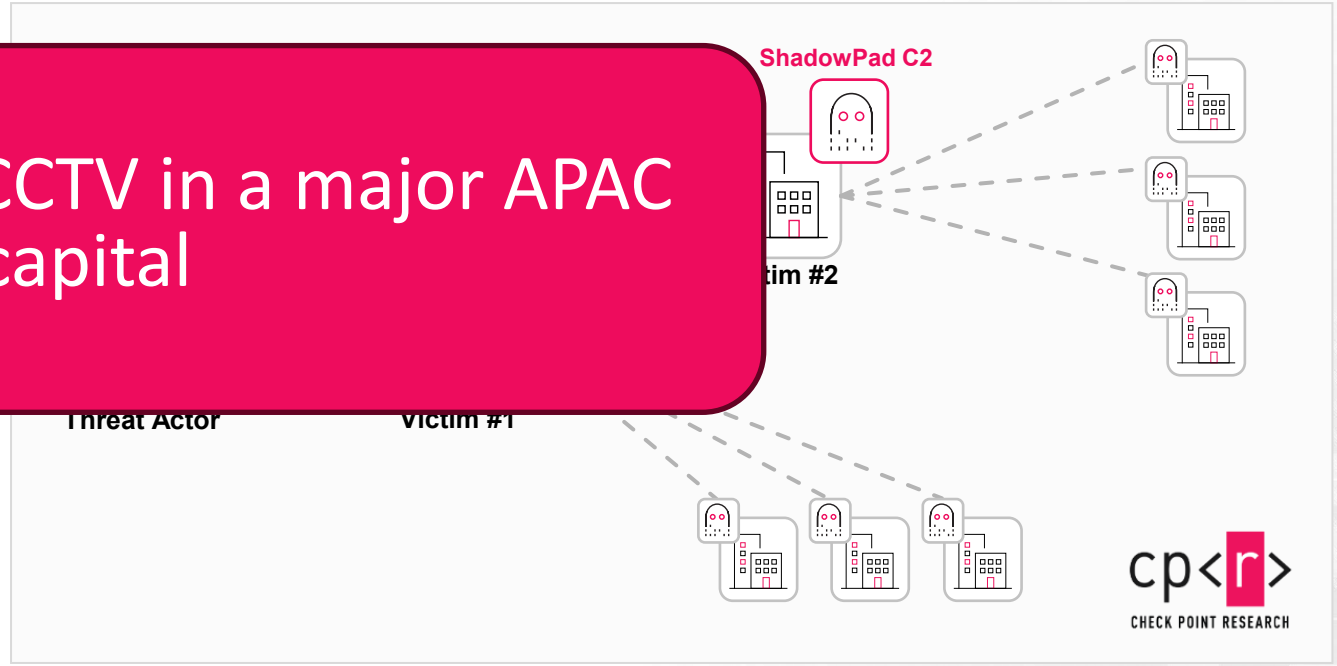
FinalD

Custom b
exfiltratio

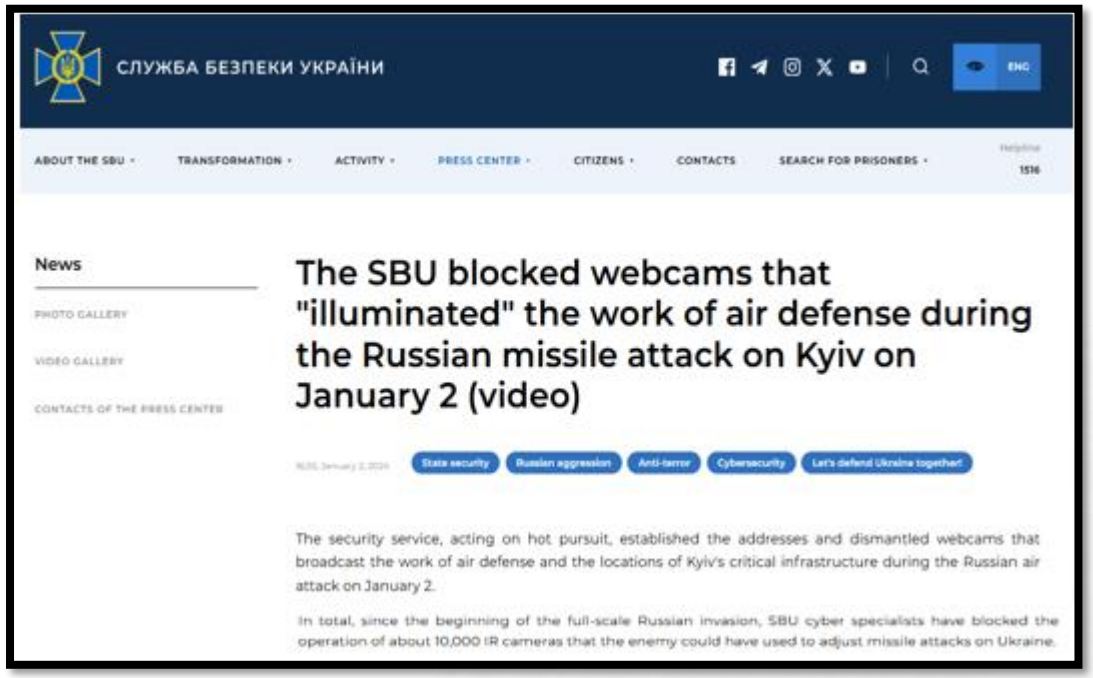
Shadow

Shared malware framework among Chinese actors

Compromised CCTV in a major APAC capital

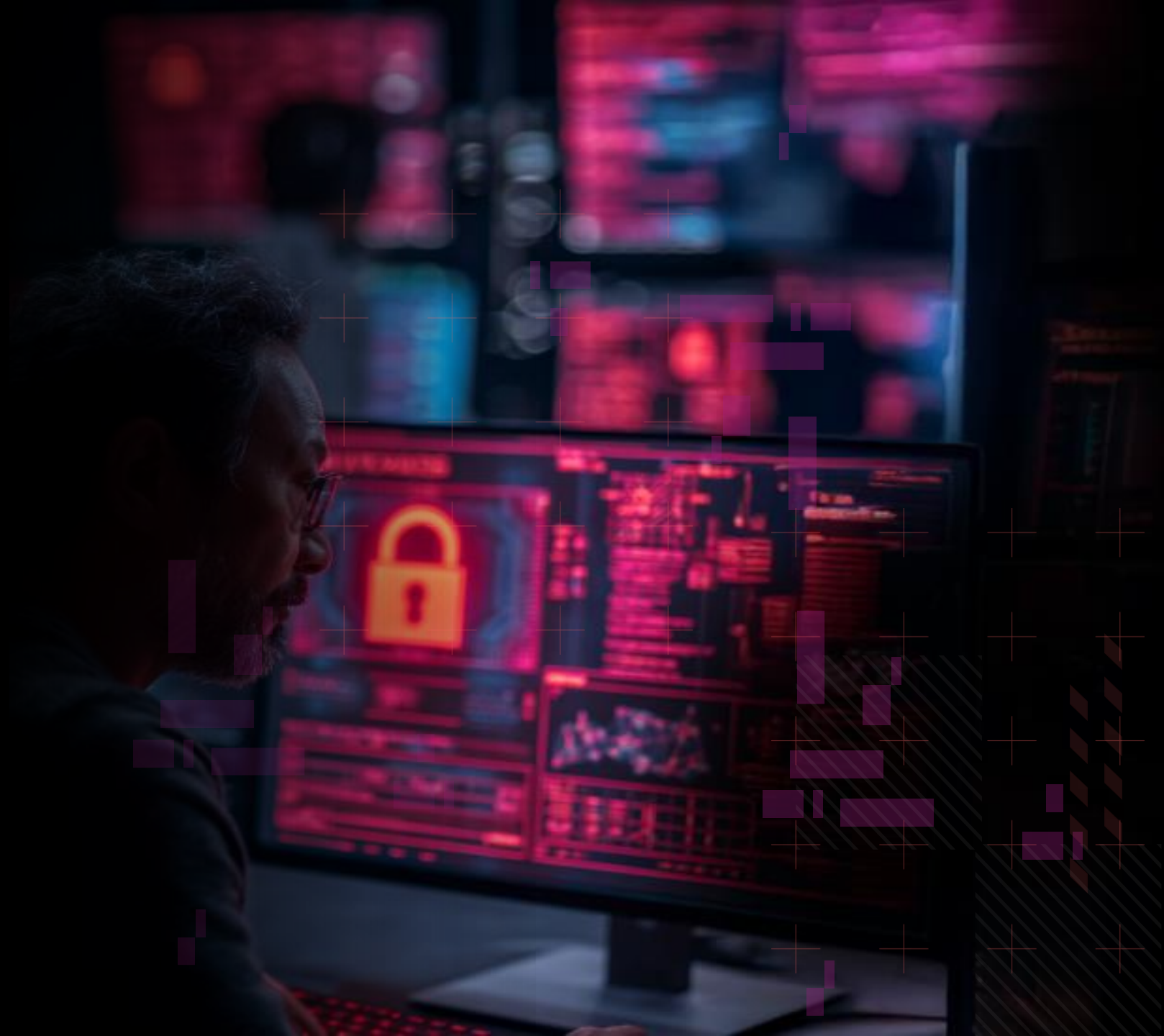


Russian Nexus Actors



https://www.theguardian.com/world/2025/may/21/russia-accused-trying-disrupt-aid-ukraine-hacking-border-crossings

INTERPLAY BETWEEN IRANIAN TARGETING OF IP CAMERAS AND PHYSICAL WARFARE IN THE MIDDLE EAST



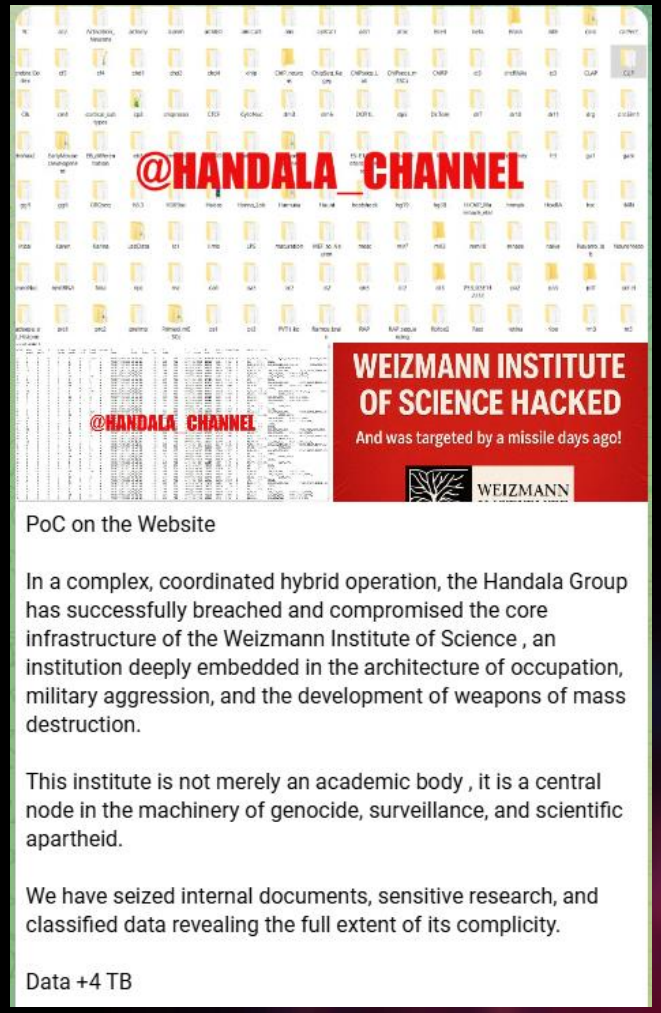
Why We Started the Research?

June 2025 war between Iran and Israel

1200% increase in targeting of Hikvision cameras in Israel

Weizmann Institute – Triple Attack – June 2025

https://apnews.com/article/israel-iran-scientists-weizmann-strike-047e6115726fcc417af46036f25d5c37



PoC on the Website

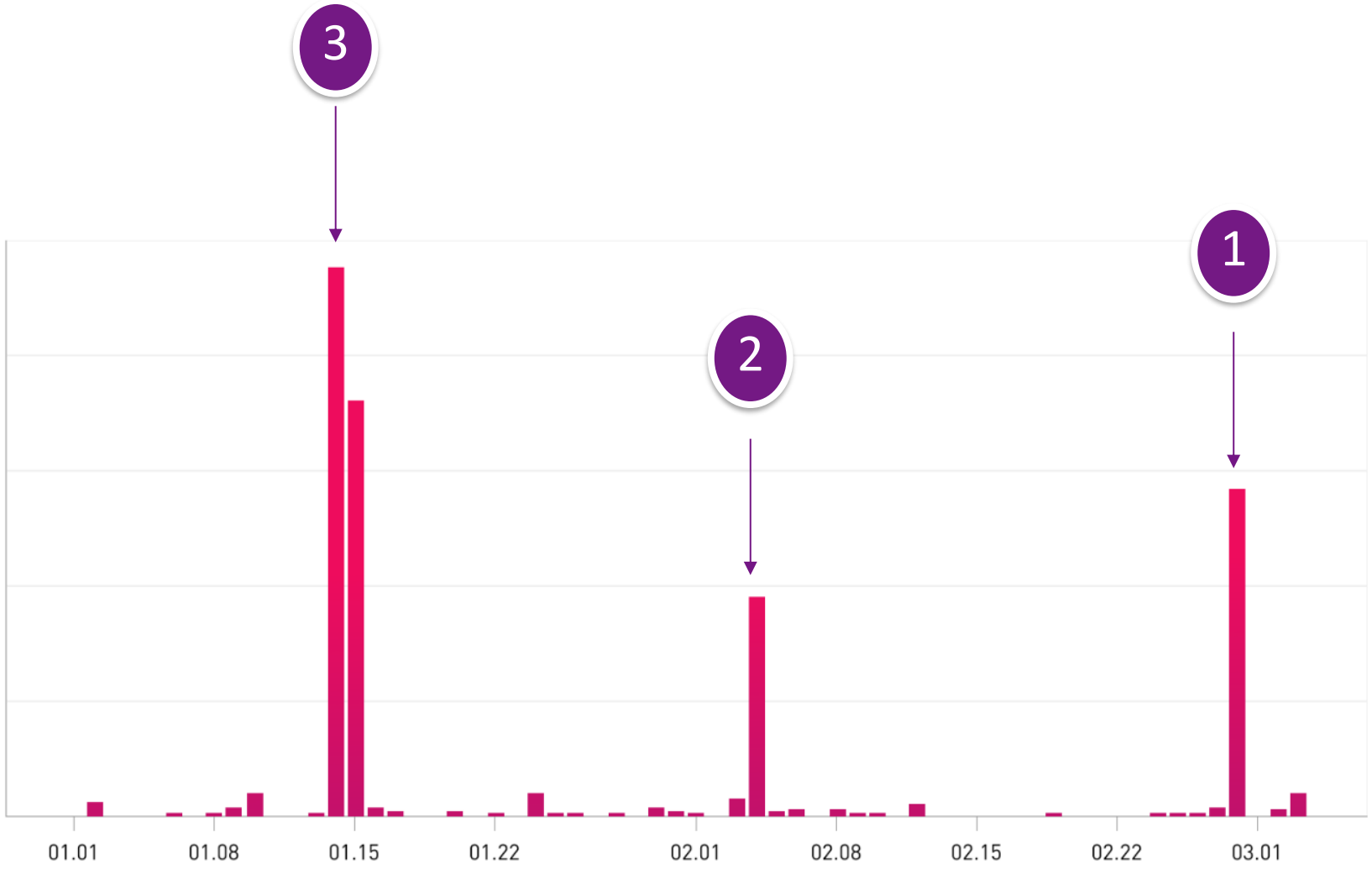
In a complex, coordinated hybrid operation, the Handala Group has successfully breached and compromised the core infrastructure of the Weizmann Institute of Science , an institution deeply embedded in the architecture of occupation, military aggression, and the development of weapons of mass destruction.

This institute is not merely an academic body , it is a central node in the machinery of genocide, surveillance, and scientific apartheid.

We have seized internal documents, sensitive research, and classified data revealing the full extent of its complicity.

Data +4 TB

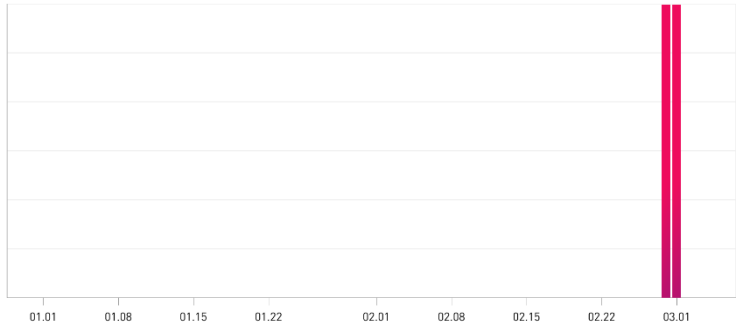
2026 War - Exploitation Attempts per Day / Israel



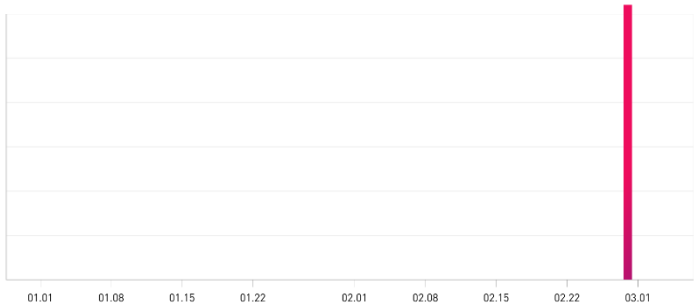
The Whole Region was Targeted

EXPLOITATION ATTEMPTS PER DAY 2026 QATAR

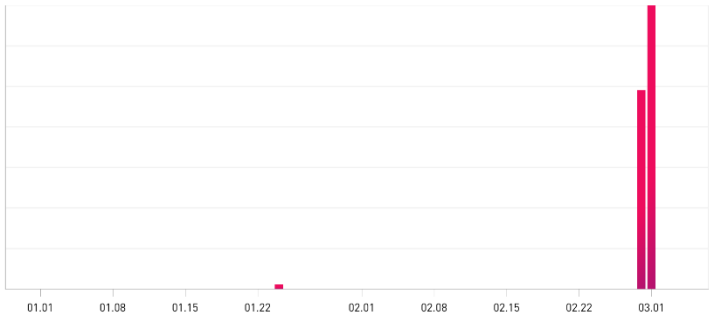
EXPLOITATION ATTEMPTS PER DAY 2026 BAHRAIN



EXPLOITATION ATTEMPTS PER DAY 2026 KUWAIT



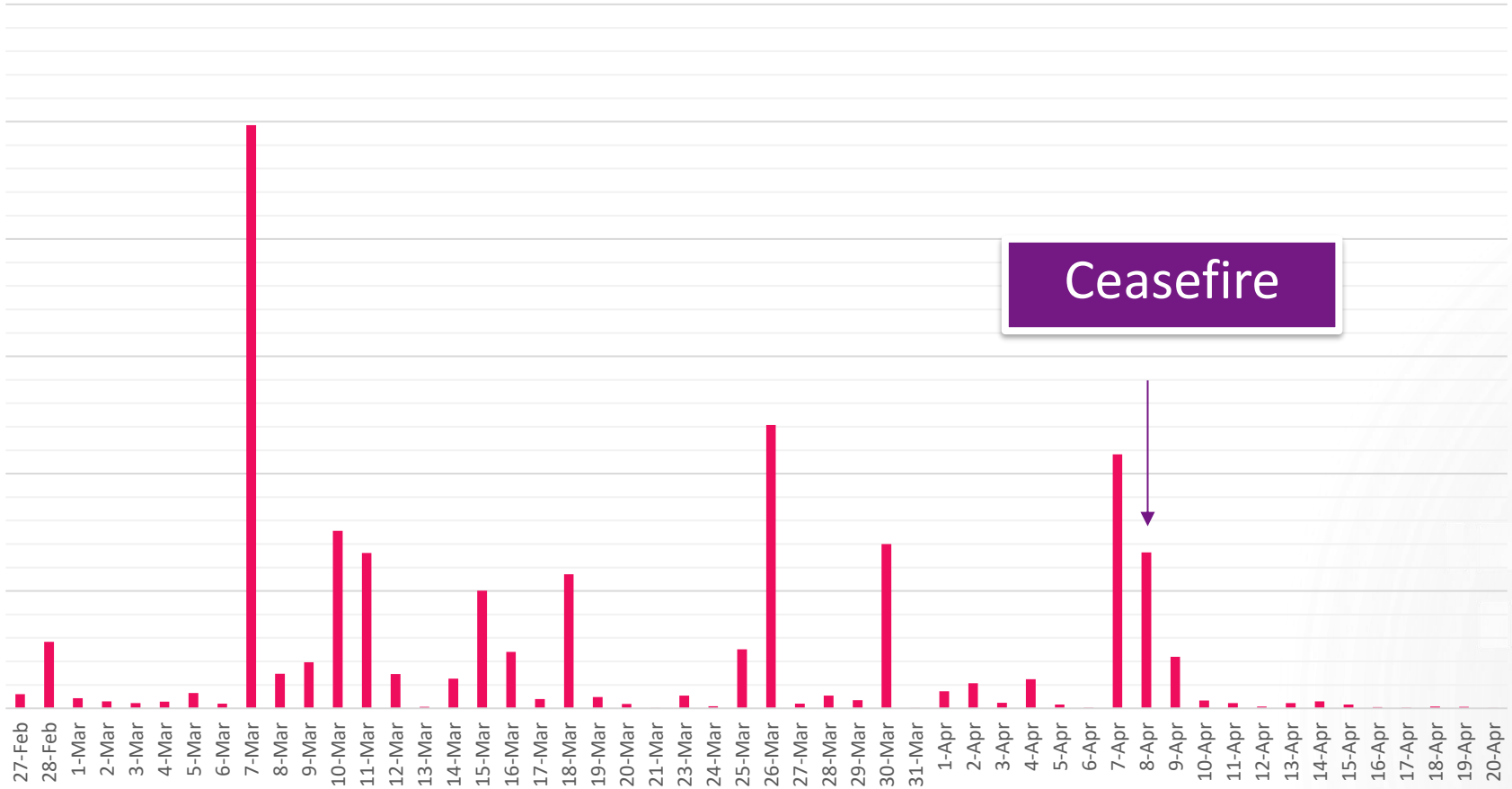
EXPLOITATION ATTEMPTS PER DAY 2026 UAE



EXPLOITATION ATTEMPTS PER DAY 2026 LEBANON

EXPLOITATION ATTEMPTS PER DAY 2026 CYPRUS

Total Cameras Targeting During the War



Recommendations

- **Eliminate public exposure -** place cameras behind VPN or a zero-trust access gateway
- **Enforce strong credentials -** change default passwords, enforce unique credentials
- **Patch management -** keep cameras/NVR firmware and management software updated
- **Network segmentation -** isolate cameras on a dedicated VLAN with no lateral access to corporate/OT networks
- **Monitoring & detection -** repeated login failures, unexpected remote logins
- **Mapping -** identify the cameras of your physical supply chain

Takeaways

- All cameras are targeted
- Cameras are now an integrated part of military warfare
- Cameras is a cheap and easy mean for real time visual coverage

CHECK POINT™

Questions?

sergeyshy@checkpoint.com

cp<r>
CHECK POINT RESEARCH