Phosphorus

Spies, Saboteurs, & Scoundrels

How Russia, China, & Nefarious Actors Are Hacking xIoT Devices

Brian Contos

Board Advisor, Phosphorus Cybersecurity

https://www.linkedin.com/in/briancontos/

What is xIoT?

Printers

Phones

Cameras

Robotics

UPS systems

Wireless routers

Smart cities

Door controllers

Purpose-built firmware/HW

Network-connected

Can’t run Endpoint security

xIoT Volume, Velocity, & Variety

Cloud Security

10M 10 Million servers world-wide.

Endpoint Security

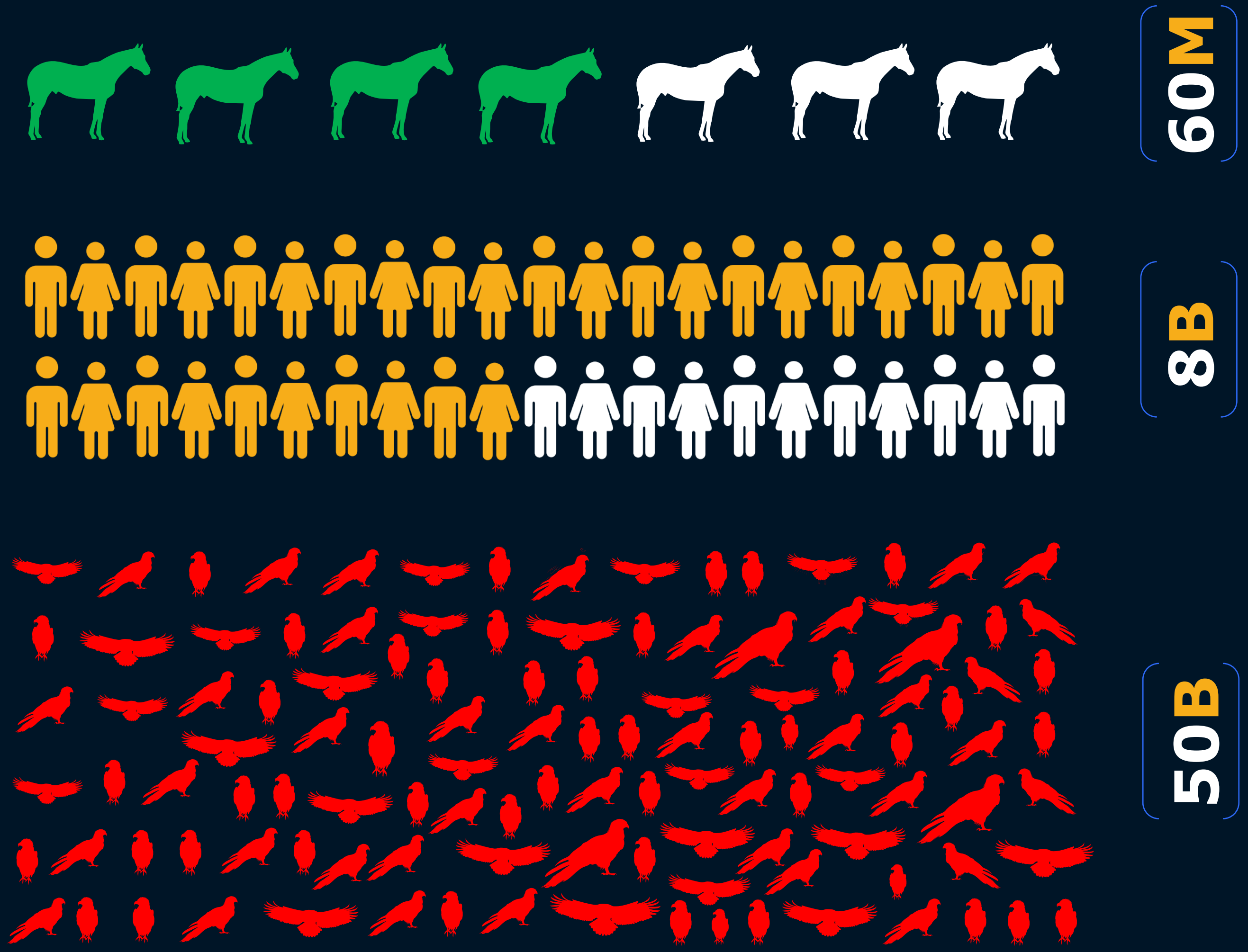
5B 5 Billion desktops world-wide.

Total computers with keyboards.

xIoT Security

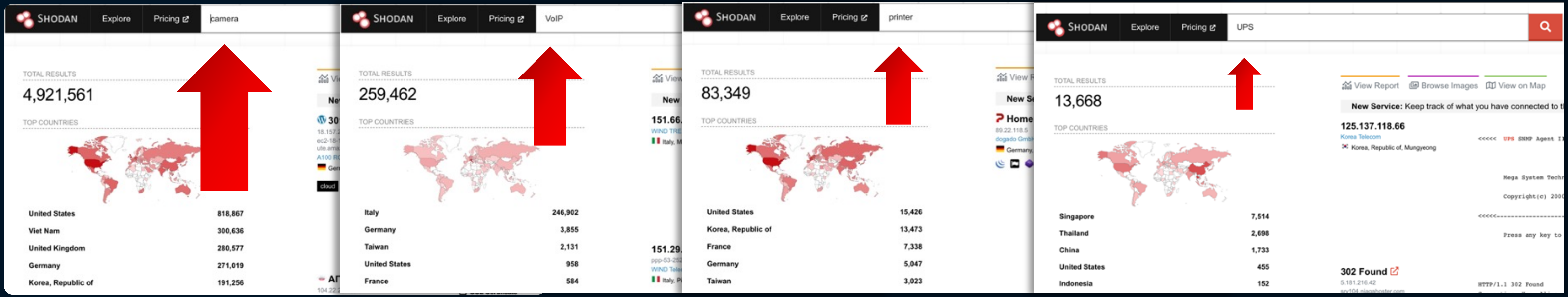
50B 50 Billion xIoT devices world-wide.

Spanning IoT, OT, and Network Devices.



Internet-accessible xIoT

Phosphorus



camera

TOTAL RESULTS
4,921,561

TOP COUNTRIES

United States	818,867
Viet Nam	300,636
United Kingdom	280,577
Germany	271,019
Korea, Republic of	191,256

VoIP

TOTAL RESULTS
259,462

TOP COUNTRIES

Italy	246,902
Germany	3,855
Taiwan	2,131
United States	958
France	584

printer

TOTAL RESULTS
83,349

TOP COUNTRIES

United States	15,426
Korea, Republic of	13,473
France	7,338
Germany	5,047
Taiwan	3,023

UPS

TOTAL RESULTS
13,668

TOP COUNTRIES

Singapore	7,514
Thailand	2,698
China	1,733
United States	455
Indonesia	152

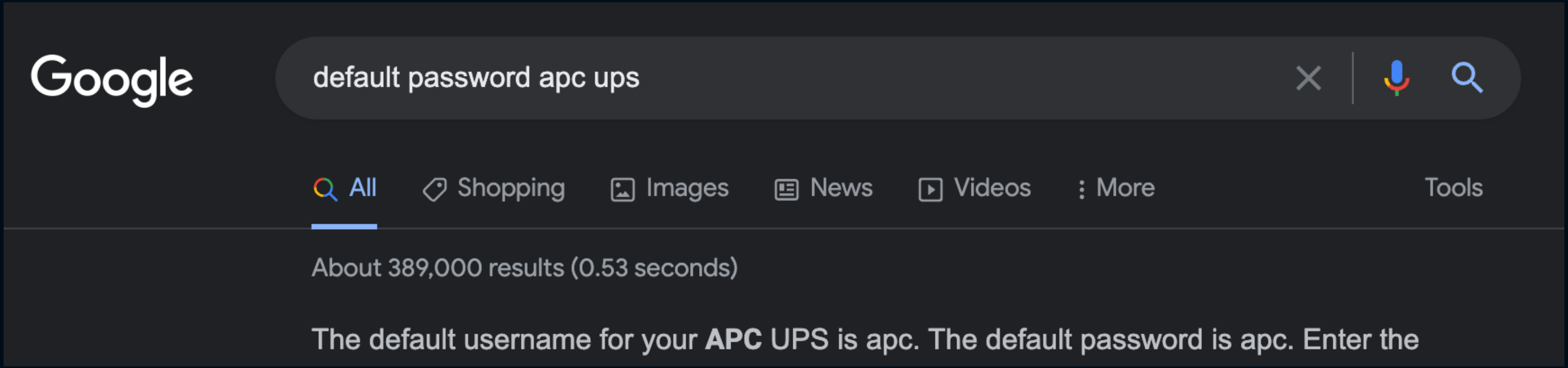
New Service: Keep track of what you have connected to t

125.137.118.66
Korea Telecom
Korea, Republic of, Mungyeong

```
<<<<<  UPS SNMP Agent I

       Mega System Tech

       Copyright(c) 200

<<<<<-----------------

       Press any key to
```

302 Found
5.181.216.42

```
HTTP/1.1 302 Found
```



default password apc ups

About 389,000 results (0.53 seconds)

The default username for your **APC** UPS is apc. The default password is apc. Enter the

2022 xIoT Threat & Trend Report

Phosphorus

15 30.974 P Phosphorus

Labs

xIoT Security Research

xIoT Threat & Trend Report

2022

Phosphorus

www.Phosphorus.io

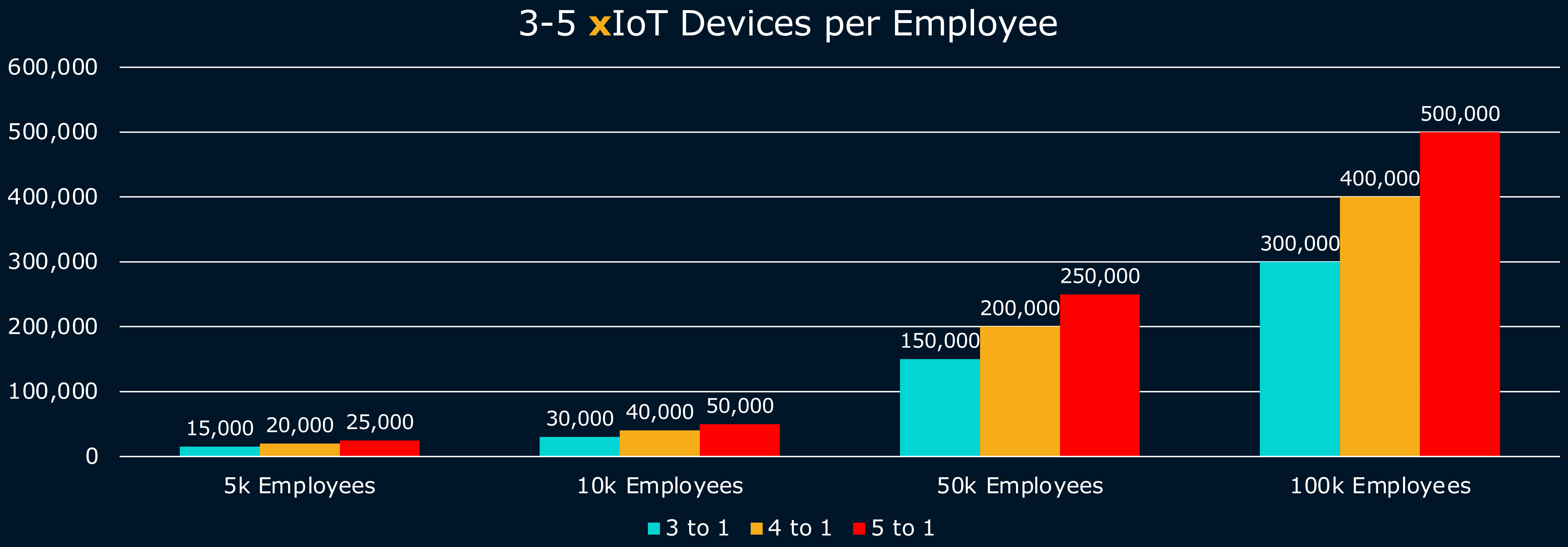
2022 Edition

⬇Download

https://phosphorus.io/xiot-threat-and-trend-report-2022/

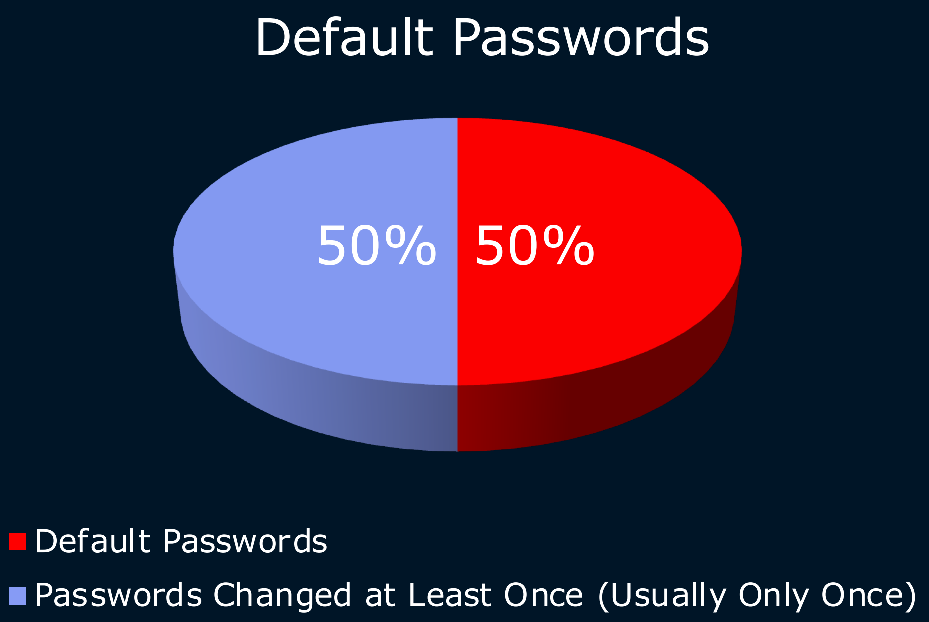
Phosphorus Research Stats

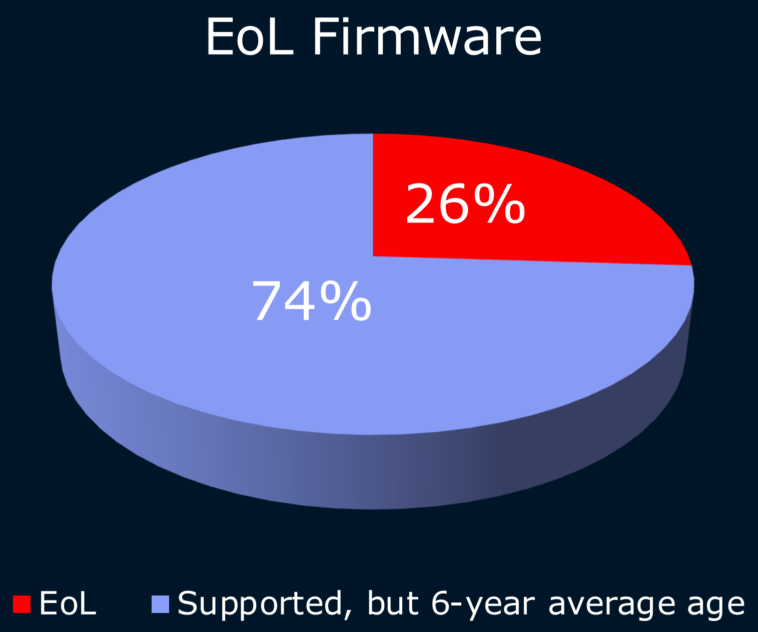
Phosphorus

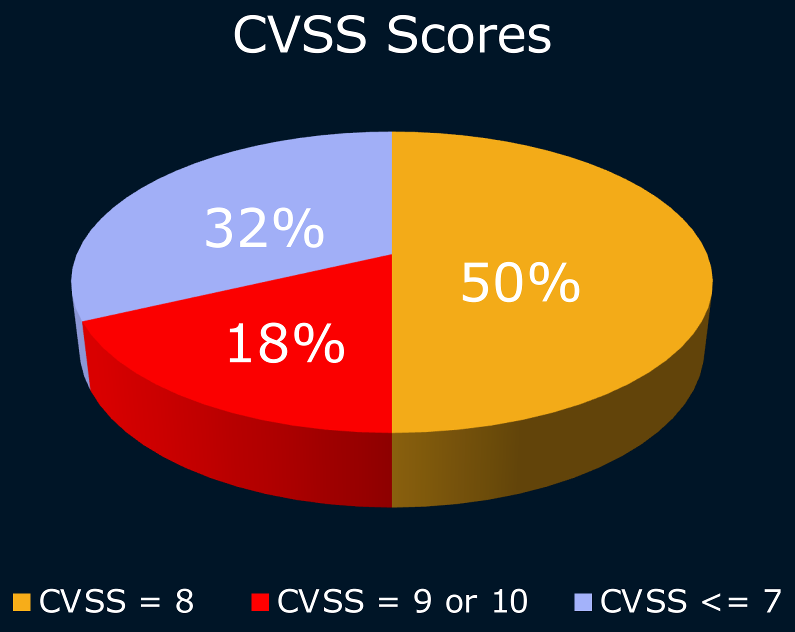


Customer estimations of their **xIoT** inventories are consistently off by **40-60%**

Phosphorus Research Stats







Common xIoT Attack Types

Legacy attacks: Attacks on **x**IoT assets for the sake of the **x**IoT assets & opportunistic attacks like botnets monetized by cybercriminals *(RSOCKS)*

RSOCKS

Common xIoT Attack Types

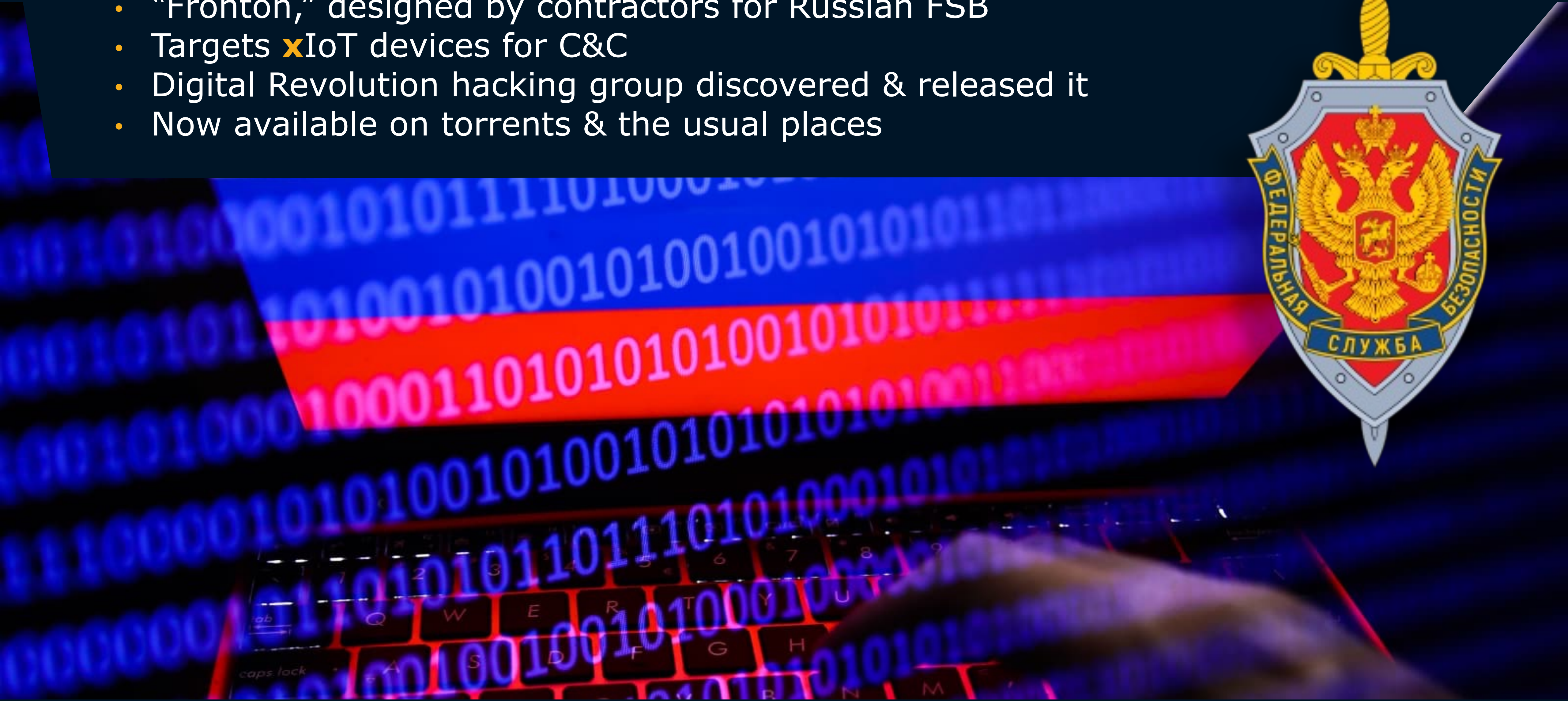
Phosphorus

Legacy attacks: Attacks on **x**IoT assets for the sake of the **x**IoT assets & opportunistic attacks like botnets monetized by cybercriminals *(RSOCKS)*

Physical attacks: Spying, attacks on power, unlocking doors, & devices that control physics - often associated with nation-states *(FRONTON)*

Fronton

- "Fronton," designed by contractors for Russian FSB
- Targets xIoT devices for C&C
- Digital Revolution hacking group discovered & released it
- Now available on torrents & the usual places



Common xIoT Attack Types

- **Legacy attacks**: Attacks on **x**IoT assets for the sake of the **x**IoT assets & opportunistic attacks like botnets monetized by cybercriminals *(RSOCKS)*

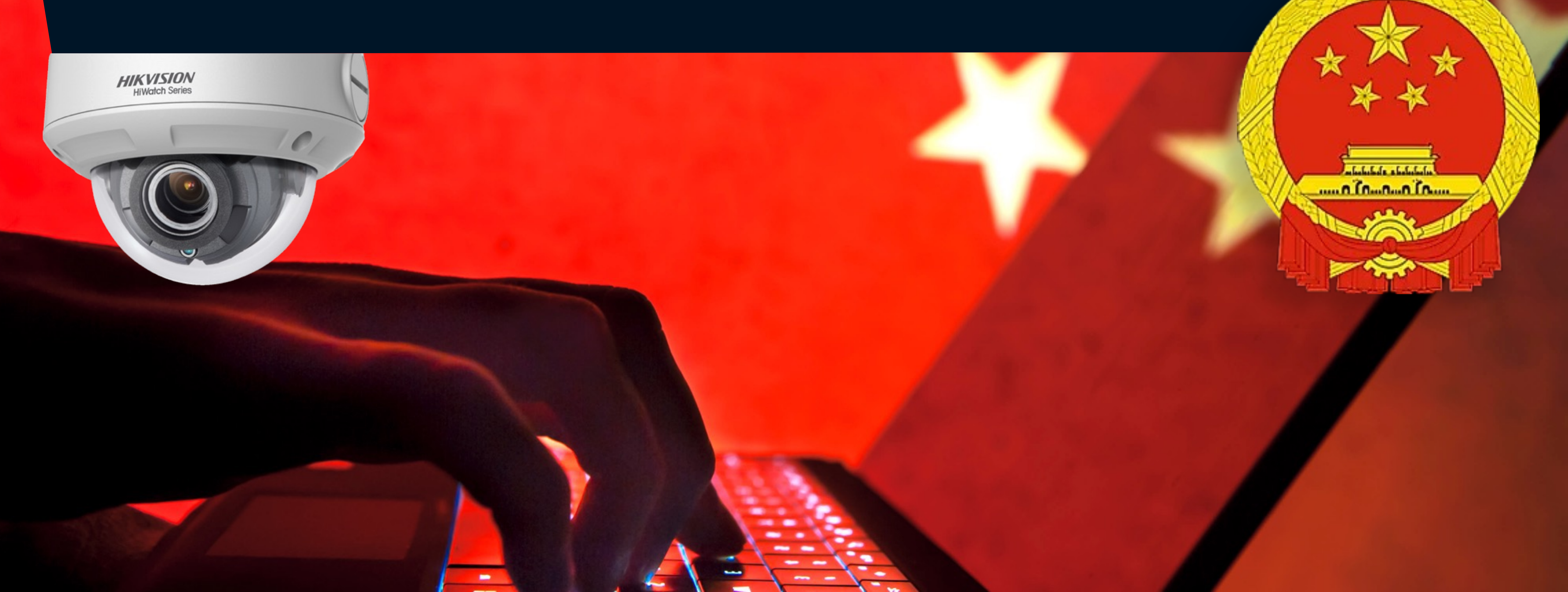
- **Physical attacks**: Spying, attacks on power, unlocking doors, & devices that control physics - often associated with nation-states *(FRONTON)*

- **OEM attacks**: Malicious **x**IoT assets out of the box *(Huawei, ZTE, Hikvision, Dahua & Hytera)*

Illegal xIoT Devices

Phosphorus

- China-based firms including Huawei, ZTE, Hikvision, Dahua & Hytera
- NOW illegal to import or sell in the USA as of November 2022



Common xIoT Attack Types

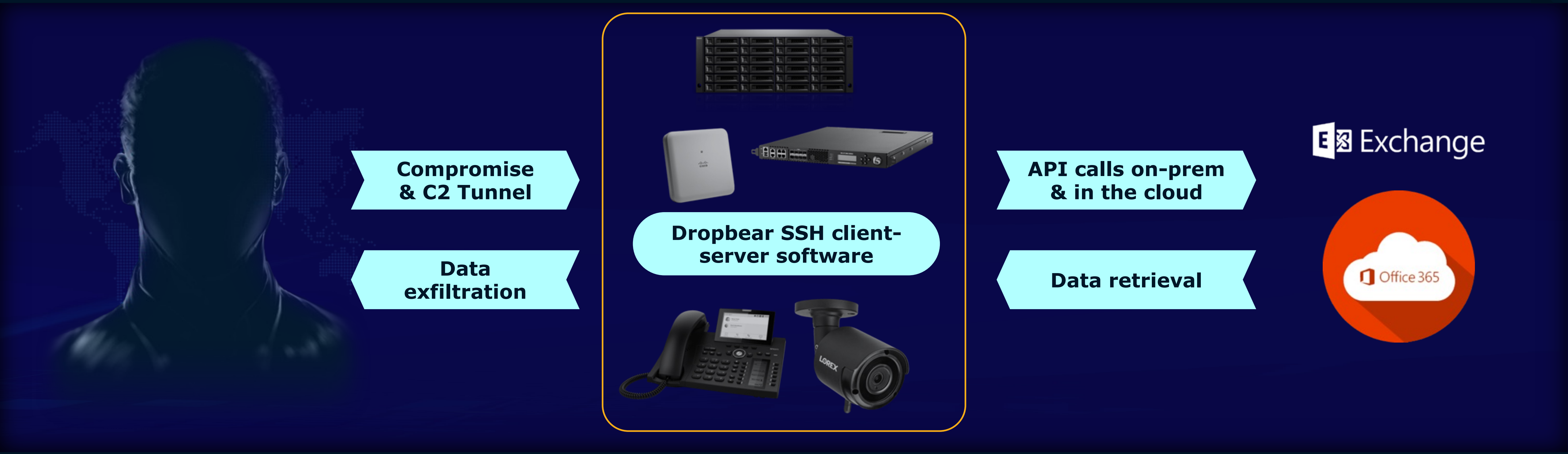
Legacy attacks: Attacks on **x**IoT assets for the sake of the **x**IoT assets & opportunistic attacks like botnets monetized by cybercriminals *(RSOCKS)*

Physical attacks: Spying, attacks on power, unlocking doors, & devices that control physics - often associated with nation-states *(FRONTON)*

OEM attacks: Malicious **x**IoT assets out of the box *(Huawei, ZTE, Hikvision, Dahua & Hytera)*

Pivot attacks: Gain access through an IT asset, hide on multiple **x**IoT assets, attack IT assets, & exfiltrate data through the **x**IoT assets *(QUIETEXIT)*

"QUIETEXIT"



Compromise & C2 Tunnel

Data exfiltration

Dropbear SSH client-server software

API calls on-prem & in the cloud

Data retrieval

Phosphorus

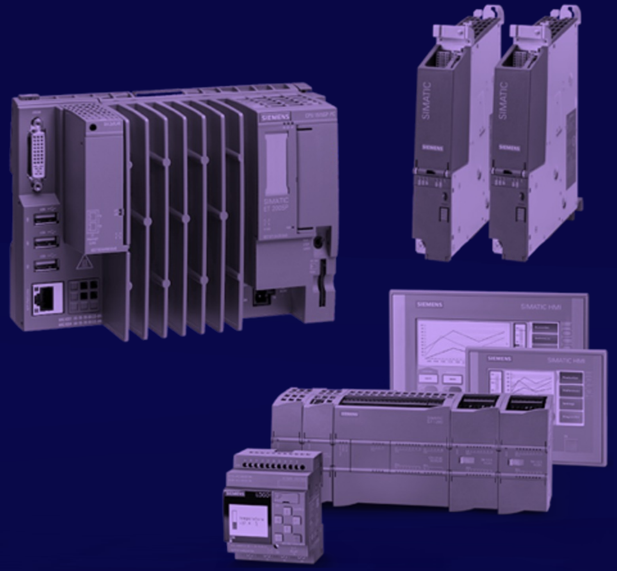
HACKING

Security Cameras Demo

“S7+:Crash”

Phosphorus

Send packets over TCP/102
Remote, unauthenticated DoS



Siemens security suggestions

- Update firmware
- Enable access control
- Set a password
- Disable unneeded protocols

Phosphorus

HACKING

Industrial Robots Demo

Phosphorus

"Some people want to see you fail. Disappoint them!"

Joker

Arthur Fleck

Disappoint Bad Actors

Discovering

Issues with “old school” discovery – sniffing, scanning, & IT asset managers

VS

xIoT

Enterprise xIoT Security Platforms

Disappoint Bad Actors

Managing Credentials & Validating Certificates

Passwords can’t be managed at scale & PAMs don’t speak **x**IoT

VS

xIoT

Enterprise xIoT Security Platforms

Disappoint Bad Actors

Upgrading Firmware & Hardening

VLANs ☺ ☹

VS

xIoT

Enterprise xIoT Security Platforms

Disappoint Bad Actors

Phosphorus

Monitoring for Environmental Drift & Reporting

xIoT state changes aren’t monitored & lack alerts & most security reports don’t consider xIoT assets or xIoT risks

VS

xIoT

Enterprise xIoT Security Platforms

Disappoint Bad Actors

Isolating Malicious / Illegal Devices

There are a multitude of known, malicious & illegal **x**IoT devices that can't be secured or patched – they ship with nefarious design from the manufacturers

VS

xIoT

Enterprise xIoT Security Platforms

Summary

Phosphorus

xIoT Attack Surface Management & Preventative Risk Mitigation

xIoT security is IT & cloud security too.

Know what you have.
(Attack Surface Management)

Be Proactive.
(Preventative Risk Mitigation)

Fix assets; if they are malicious, isolate them.

Fix assets at scale.

Keep assets fixed.

Phosphorus

Thank You!

Brian Contos

Board Advisor, Phosphorus Cybersecurity

https://www.linkedin.com/in/briancontos/