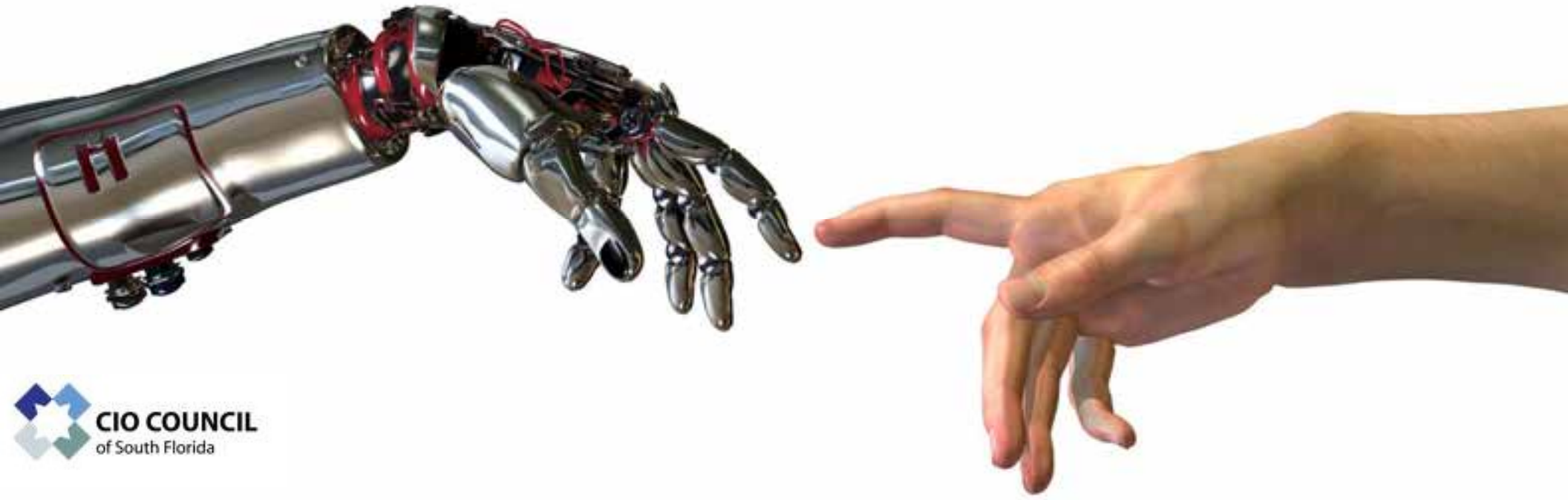
Artificial Intelligence & Internet of Insecure Things



CIO COUNCIL
of South Florida

Pete Nicoletti
Chief Data Officer, Cybraics, Inc.

Cybraics Confidential 2018

CYBRAICS

Challenges to IoT Security: Learning by examples review

1. IoT devices do not have full Operating Systems so traditional endpoint solutions can not be used.

2. Lack of Upgrades and vulnerabilities remain unaddressed

3. Air Gapped Networks do not work (ever)

4. Scale is Huge and log volume is epic, beyond human scale

5. Risk is real, players are serious, consequences real

Logging of IOT devices Challenges Review

Discuss Machine Learning Analysis Approach with Case Study

Show how to "hunt" for issues as well as reviewing some other information gathering tools, feeds and forensic analysis approaches

Finally we'll discuss some recommendations and future developments

Cybraics Confidential 2018

Logging challenges with IOT networks:

- Some IoT networks are huge, Creates massive amounts of logs
- Logs are “expensive” to transport over Cellular connections and sometimes not collected
- Logs are not able to be analyzed with traditional tools or humans….scale is billions of events per day…
- Humans can’t handle the volume of analysis that’s needed to maintain a secure network so machine learning and AI is key
- Signature based tools/SEIMs fail on zero-days from well sponsored nation-states

Why are IoT Devices Attacked?

Pending Copyright approval

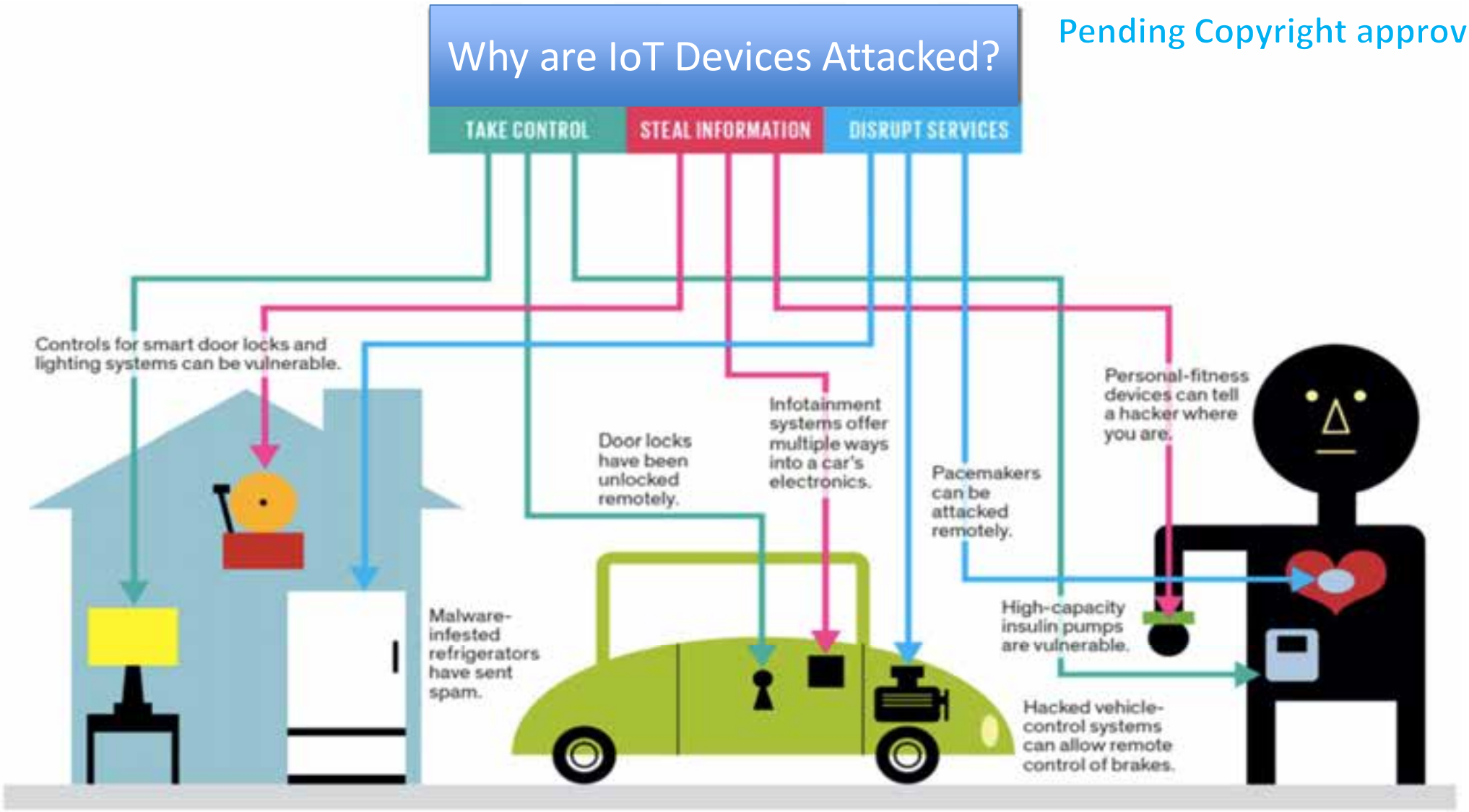
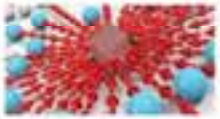


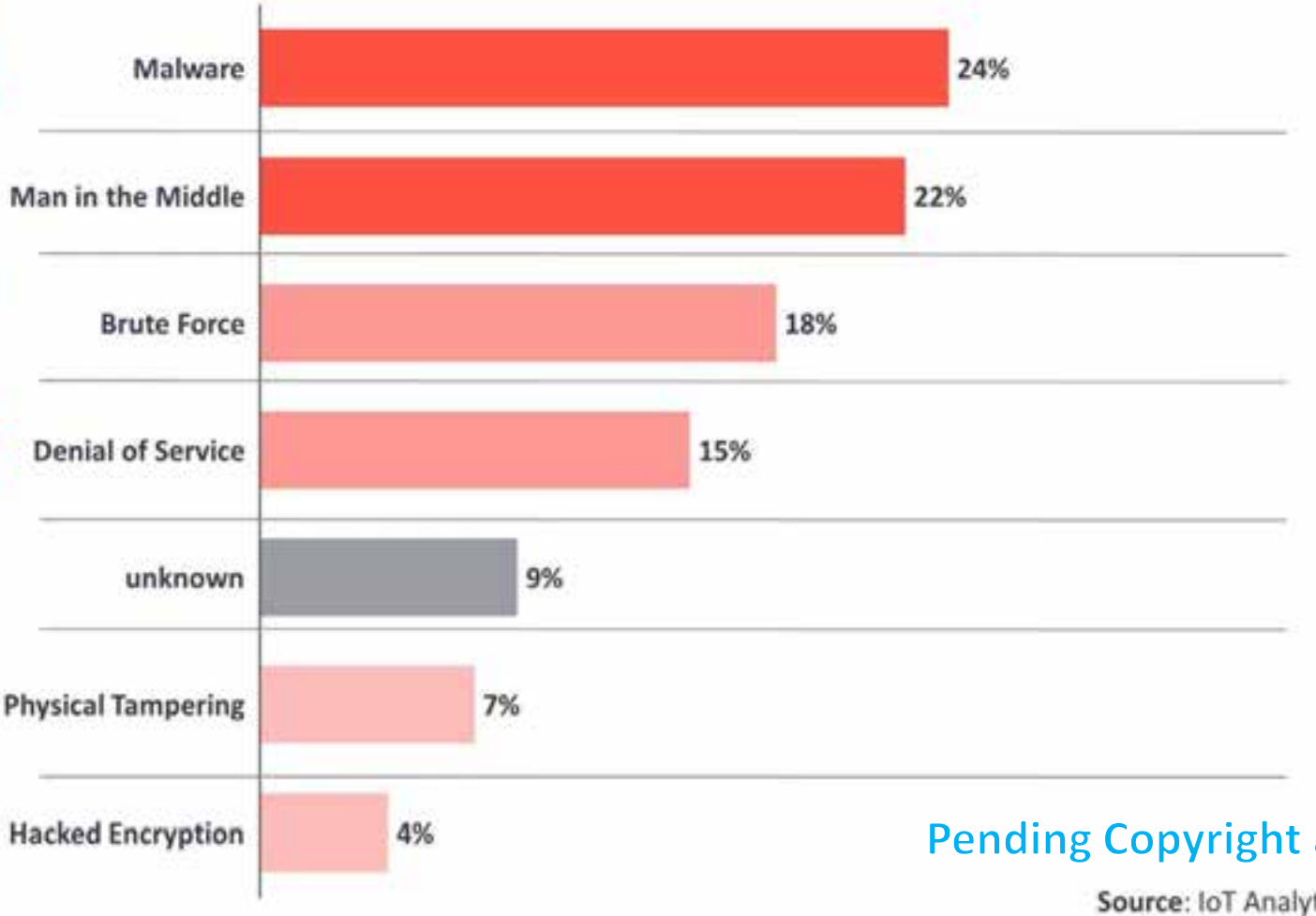
Illustration: J. D. King

How are IoT Devices Attacked?



Type of IoT-related Security breaches made public in last 2 years (n=67) in %

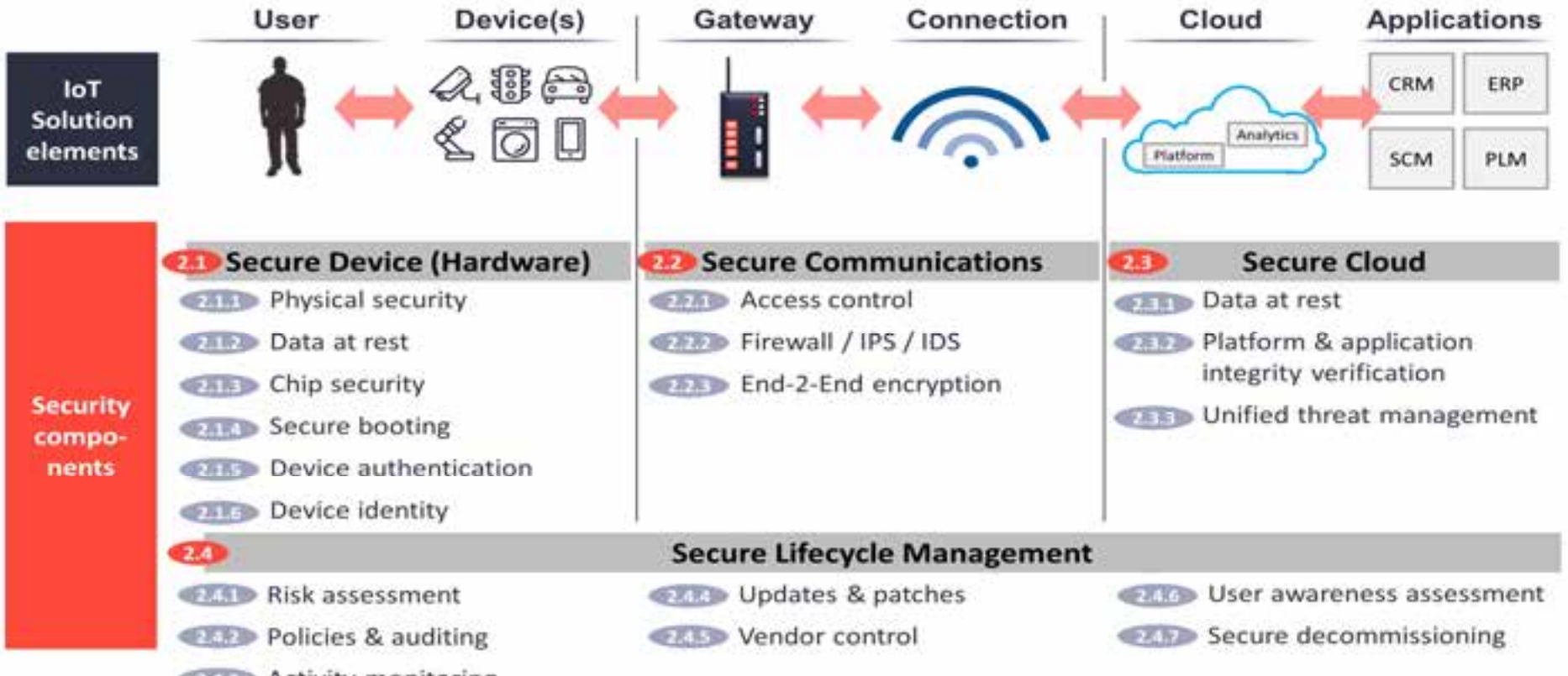


Pending Copyright approval

Source: IoT Analytics press research

Copyright © 2017 by www.iot-analytics.com All rights reserved

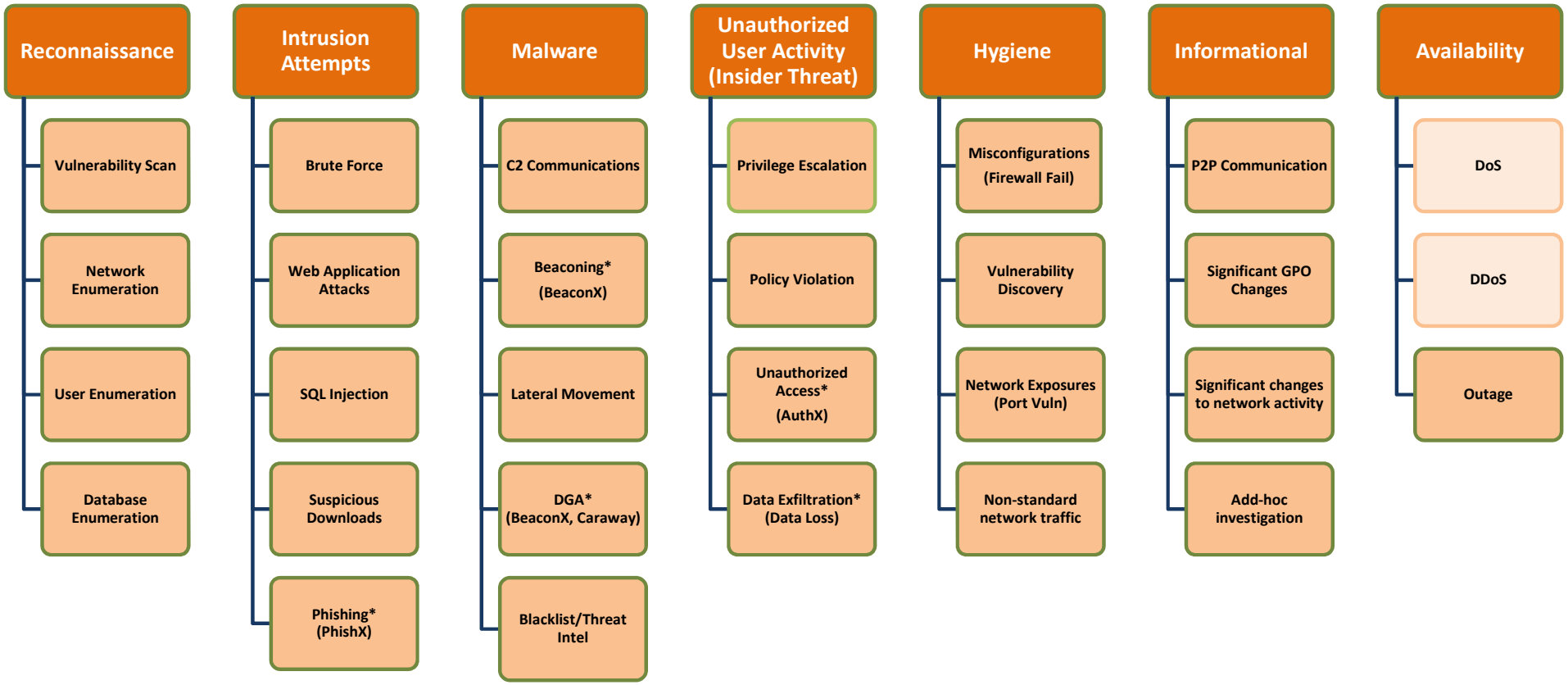
Where are IoT Devices Attacked?



Pending Copyright approval

Source: IoT Analytics

All Threat Matrix Categories need to countered by AI/ML



nLighten CYBRAICS

* Requires DNS data

Example #1: Hacking a Jeep

Security researchers Charlie Miller and Chris Valasek were able to identify a zero day exploit which allowed them to send instructions to the vehicle through Cellular connection to its entertainment system.

They could change Temp AND vehicle's steering and braking systems.

All it required was knowledge of the individual vehicle's IP address to take control.

Example #2: Stuxnet jumps Airgap

Iran Centrifuge's were destroyed by custom malware

IoT networks that are "air-gapped" are an attempt to prevent Internet based risks

Traditional update processes,
gateway tools and monitoring are not usable.

We know how well Air Gaps work

- They don't…..

nLighten CYBRAICS

Cybraics Confidential 2018

Example #3: IoT Cameras Hacked

A popular IoT security camera – NeoCoolCam

Can be attacked from outside the network they're on.

Compromised for unauthorized surveillance and as launch point

Researchers at Bitdefender have found that all it takes is for the easily accessible login screen to be manipulated in order to take control of any of the 100,000+ cameras currently in use.

Hacked Cameras Working together: Mirai Botnet:

Poor password management/Defaults are to blame

A piece of malware was unleashed which infects network devices running on Linux. Mirai instructs these devices to constantly search the internet for vulnerable IoT devices

Attack vector: leverage factory set default username and passwords that have never been changed.

Top 10 passwords

123456 = 1666 (0.38%)
password = 780 (0.18%)
welcome = 436 (0.1%)
ninja = 333 (0.08%)
abc123 = 250 (0.06%)
123456789 = 222 (0.05%)
12345678 = 208 (0.05%)
sunshine = 205 (0.05%)
princess = 202 (0.05%)
qwerty = 172 (0.04%)

Top 10 base words

password = 1373 (0.31%)
welcome = 534 (0.12%)
qwerty = 464 (0.1%)
monkey = 430 (0.1%)
jesus = 429 (0.1%)
love = 421 (0.1%)
money = 407 (0.09%)
freedom = 385 (0.09%)
ninja = 380 (0.09%)
writer = 367 (0.08%)

nLighten CYBRICS

Example #3: DDoS Attack on KrebsOnSecurity

Mirai Bot net of security cameras, DVR's and some routers grew to 600,000 IoT devices

24,000 devices were "rented" to attack this site with up to 620 Gbps of DDoS

The End User Costs born by unaware device owners cost $323,000 in excess power and bandwidth

It's cheap and easy to accomplish…and end users are basically oblivious…

- $13.50 each end user cost
- $200 to rent the bot net

Nobody cares and its not on your radar!

nLighten CYBRAICS

Cybraics Confidential 2016

#3 Krebs: DDoS External Players and Costs

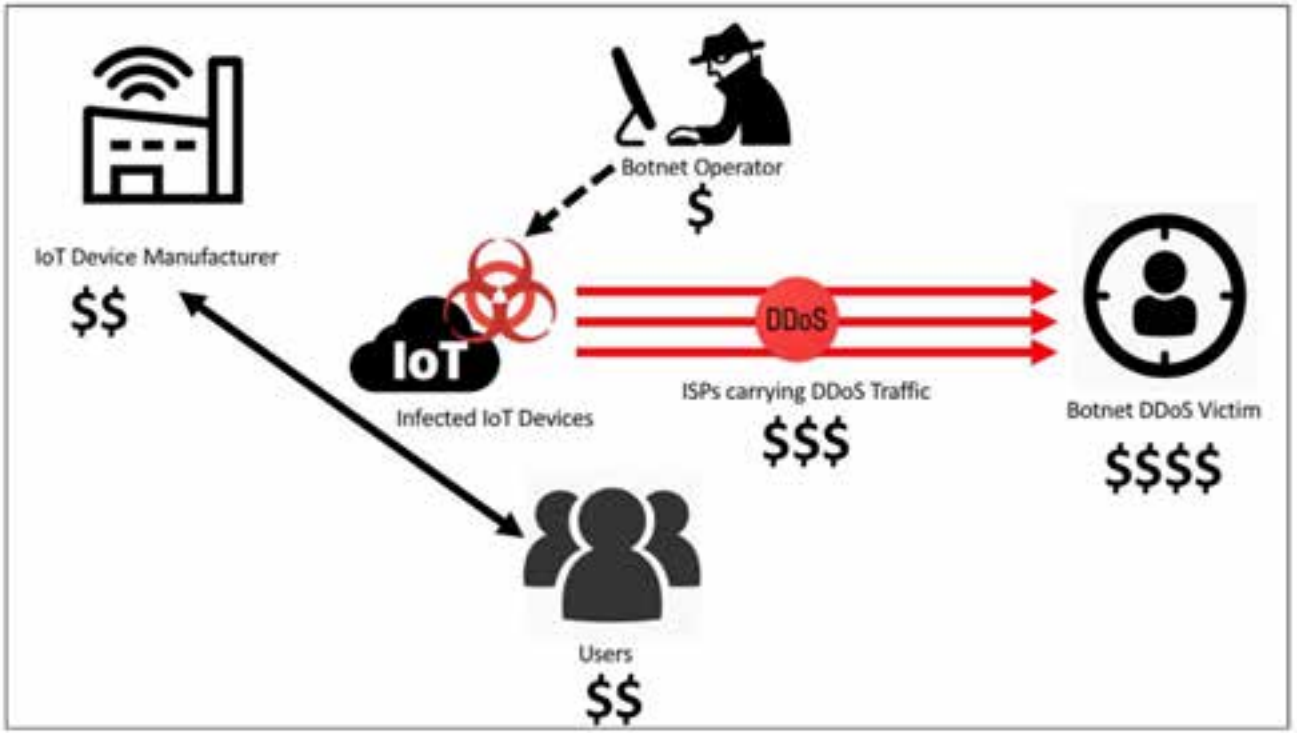


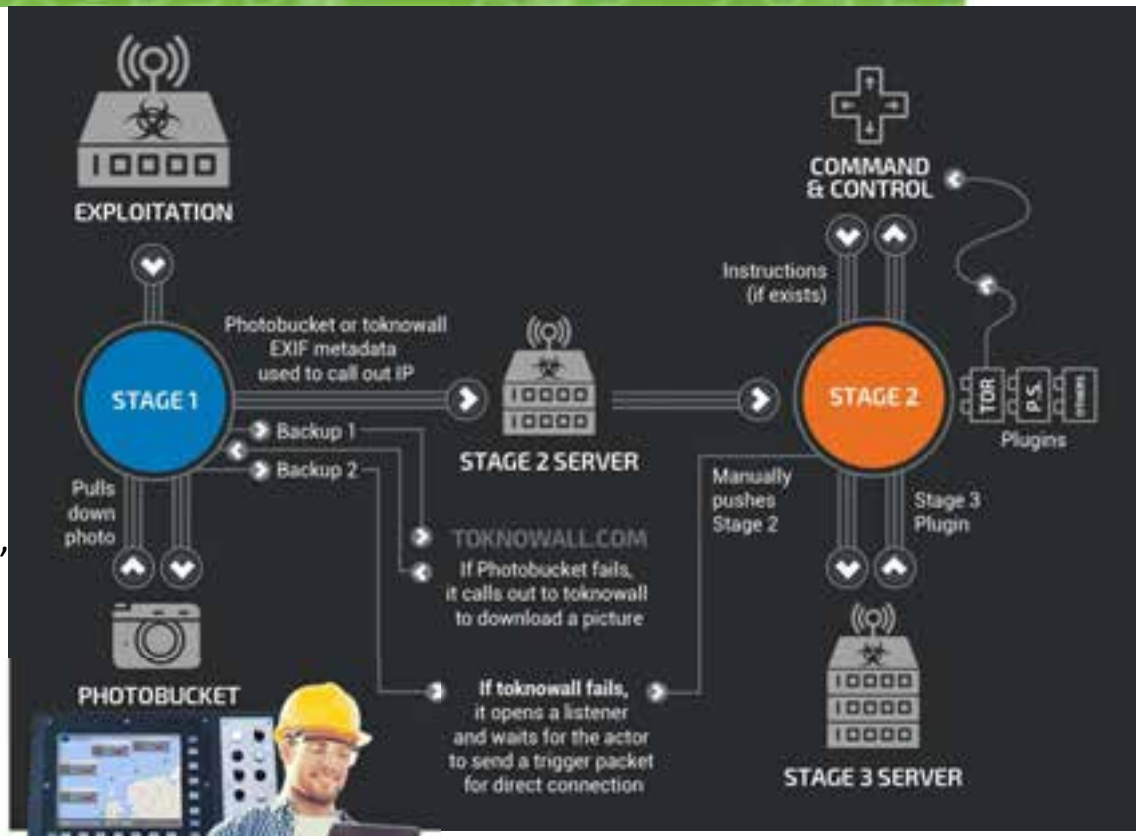
Figure 1: DDoS Stakeholder Externalities

#4: VPNFilter: FBI asks 500,000 to reboot!

The stage 1 malware persists through a reboot, utilizes multiple redundant command and control (C2) mechanisms to discover the IP address of the current stage 2 deployment server, making this malware extremely robust and capable of dealing with unpredictable C2 infrastructure changes.

The stage 2 malware: file collection, command execution, data exfiltration and device management. And elf-destruct capability that overwrites a critical portion of the device's firmware and reboots the device, rendering it unusable

Stage 3 modules : a packet sniffer for collecting traffic that passes through the device, including theft of website credentials and monitoring of Modbus SCADA protocols, and a communications module that allows stage 2 to communicate over Tor



Example #5: Supermicro Chip Hack?

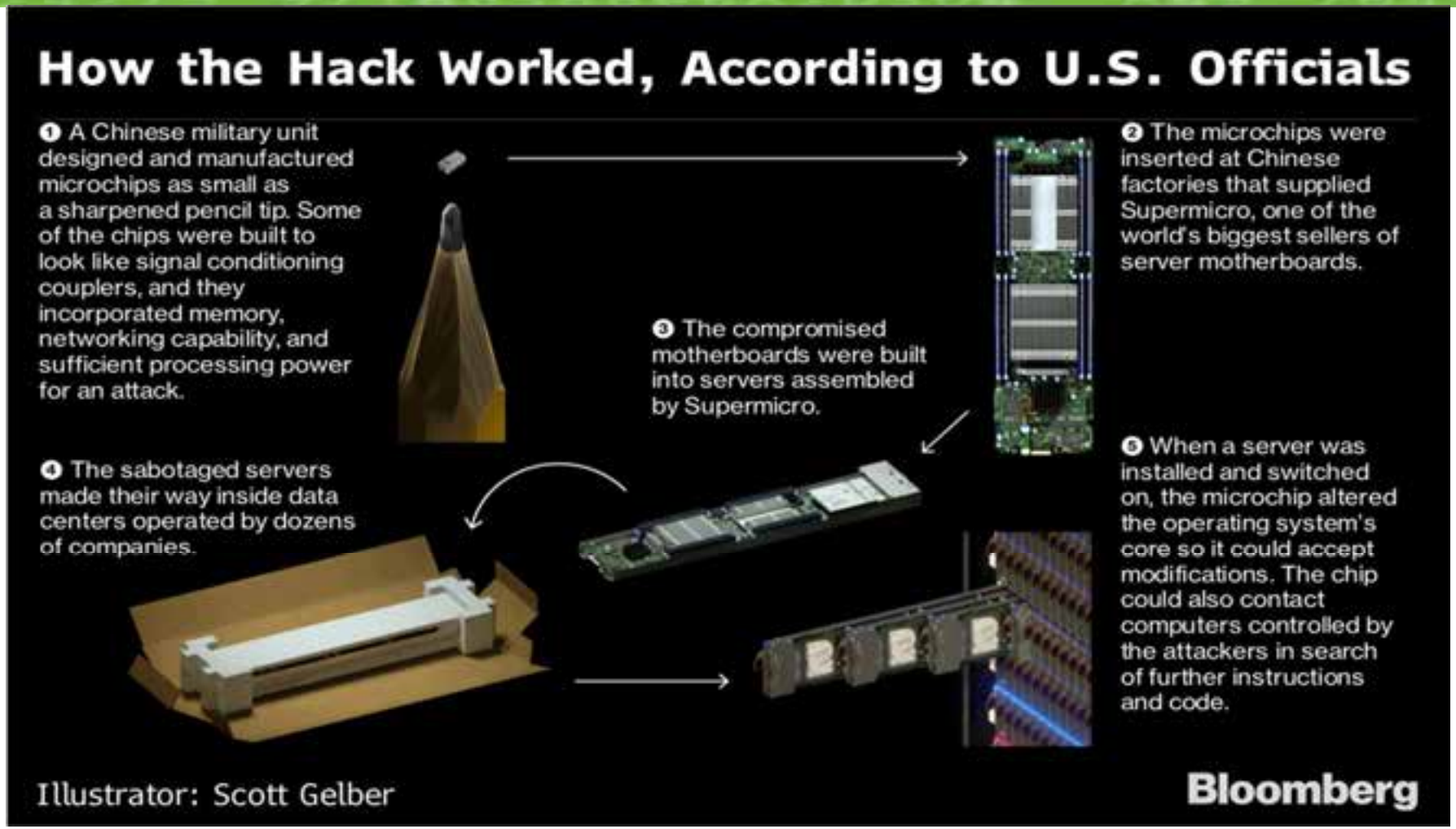
A major US telecommunications company discovered a foreign implant in a server back in August, according to a new report by *Bloomberg*. It's the first time a source has decided to go on the record to corroborate the claims made in a report by the publication last week, alleging that Chinese spies were able to compromise servers belonging to 30 of the US's top tech companies through the use of hardware manipulations.

The implant was reportedly built into a server's Ethernet port, giving hackers a back door into the telecommunications company's computer networks

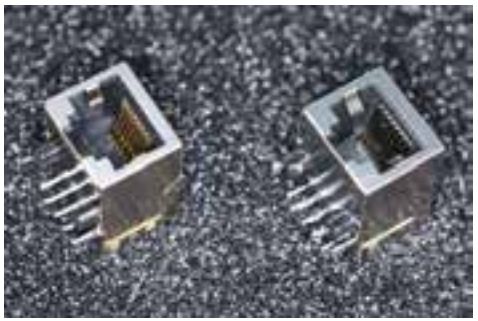
1st Chip hack: Owned the Baseboard Management Controller (BMC), essentially a second small computer built into the server. The BMC implements the Intelligent Platform Management Interface, a tool enabling a remote administrator to reset the computer, reinstall the operating system, and perform other tasks without needing physical access. It is effectively "god," able to take over the computer entirely.

nLighten CYBRAICS

Example #5: Supermicro Chip Hack?



Example #5: Supermicro Chip Hack?



This incident once again illustrates the "Coventry problem," referring to Winston Churchill's apocryphal decision not to prevent the bombing of Coventry in order to keep secret that British intelligence had decrypted the Enigma machine. Robertson and Riley describe a U.S. intelligence apparatus that knew of these ongoing attacks, but could not effectively notify the affected companies nor provide useful recommendations. If the intelligence community had warned these companies, it would probably have revealed to the Chinese that the U.S. was aware of these activities, as well as potentially compromise an ongoing FBI investigation described in the article.

Cryptographically signed firmware updates for Supermicro motherboards are still not publicly available. That means that, for the past five years, it is trivial for people with physical access to the boards to flash them with custom firmware that has the same capabilities as the hardware implants reported by Bloomberg.

Time to call www.trapezoid.com for some integrity management!

Deep Dive Case:
LPG Transport
Camera System/ICS Compromise

nLighten CYBRAICS

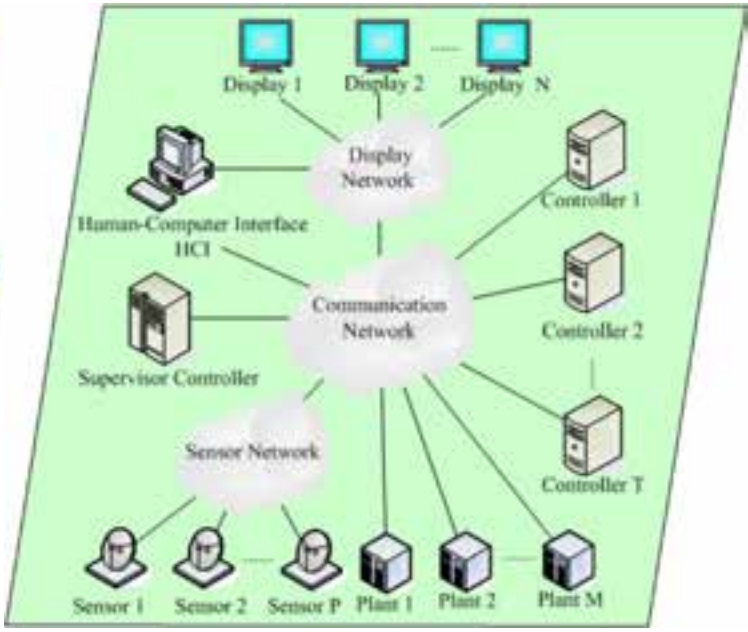
Deep Dive Case: Shipboard IoT Compromise

Liquid Natural Gas (LNG) Transport Vessel

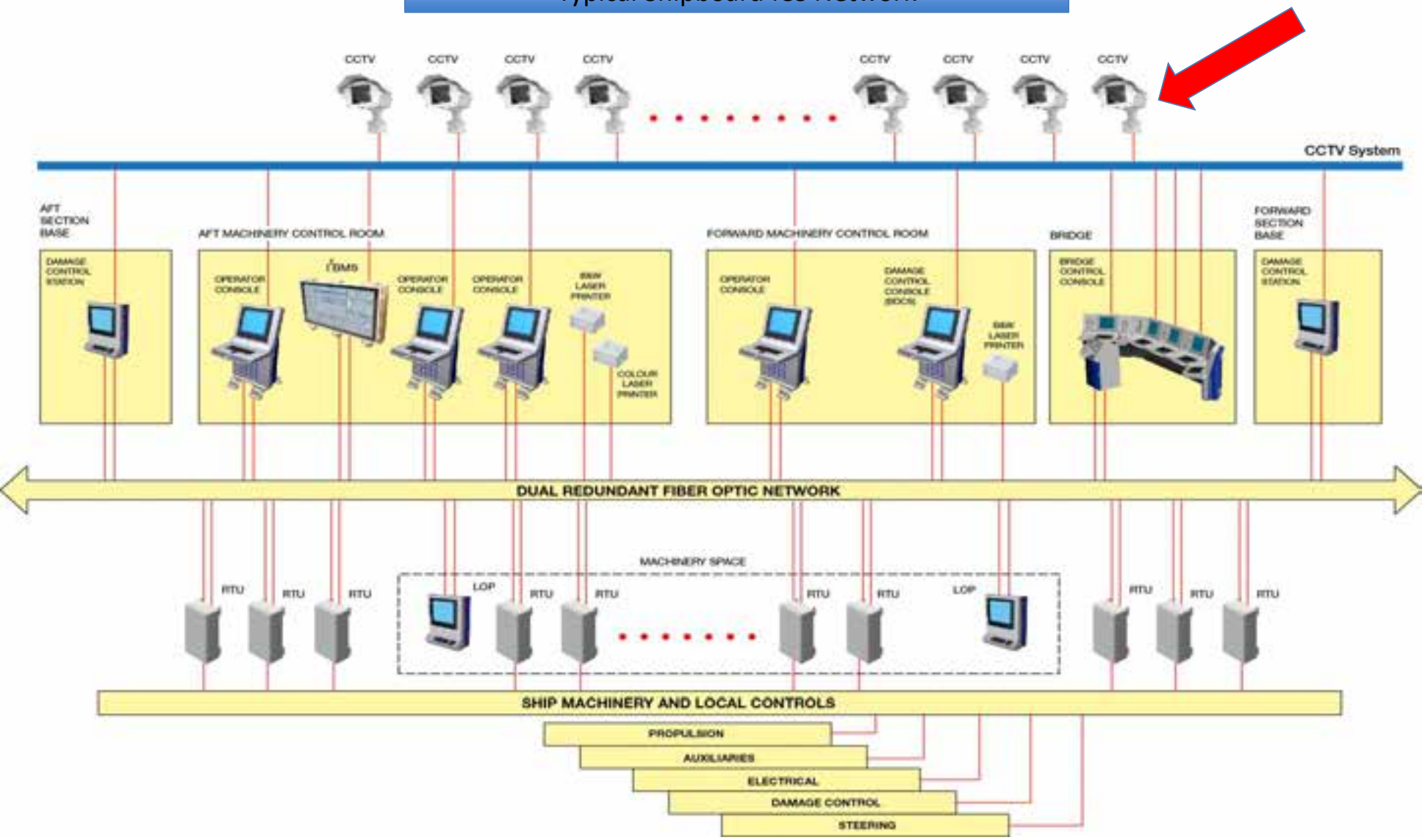
- Industrial Control System (ICS) – cameras and all connected servers were compromised
- Part of Extensive ICS system commonly called “Integrated Control and Monitoring Systems”
- Outcome of “Herald of Free Enterprise” ferry capsizing in 1987 – 188 people died
- Currently imposed through the International Safety Management Code (“ISM Code”)
- Ship unable to travel without this system
- All Control systems are linked together: engine management, fuel management, cargo management, valve remote control, tank level gauging, etc.
- None of the customer’s security tools (dozens of them) found this, including their MSSP

Shipboard IOT Sensors and network

- Temperature Sensor
- Pressure Sensor
- Displacement Sensor
- Speed & Position Sensor
- Vibration & Motion Sensor
- Shock & Acceleration Sensor
- Flow Sensor
- Tilt Switches
- Strain Sensor
- Mass Air Flow Sensor
- Piezo Sensor
- Ultrasonic Transducer
- Voltage Sensor
- Current Sensor
- Force Sensor



Typical Shipboard ICS Network



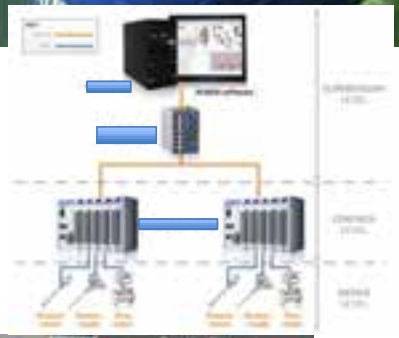
Control Room Example: All Systems OK!

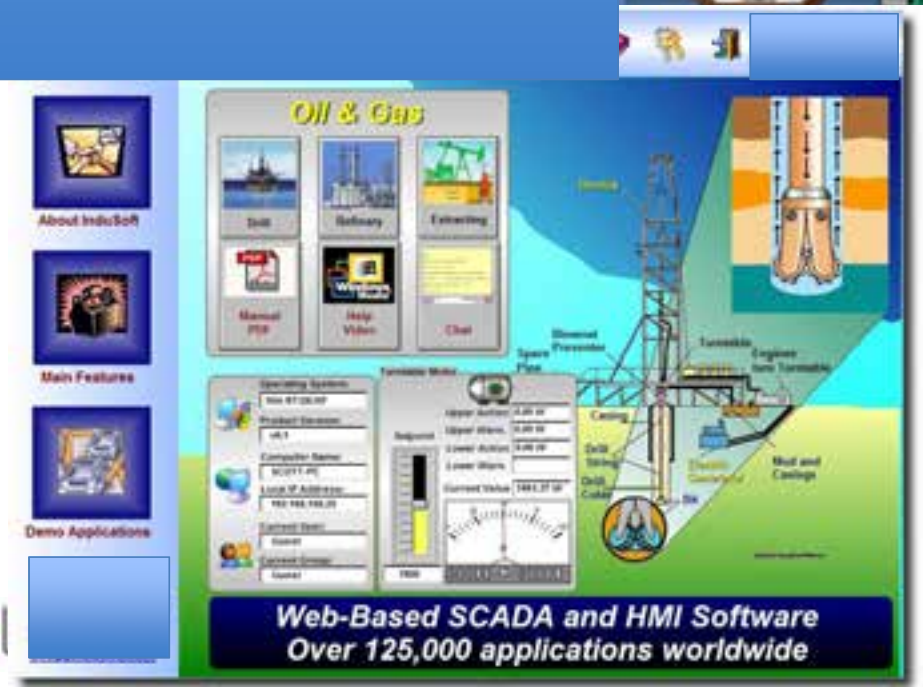
Shipboard ICS Management

Dashboards

Sensors

Alarm panels





Shipboard Log Counts are at inhuman Scale

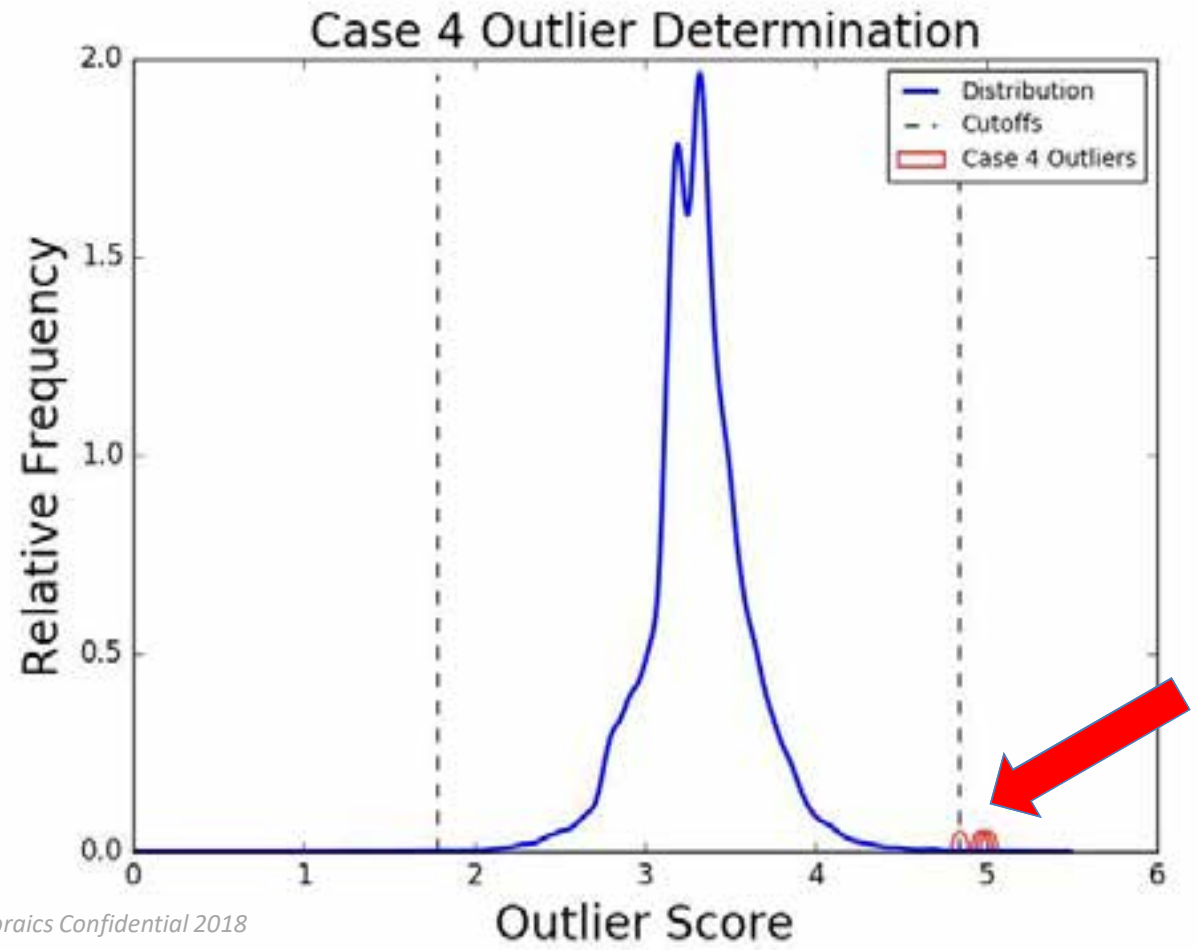
Everything Running Securely and Smoothly?

nLighten CYBRAICS

NO! Outlier Detection Details

Summary

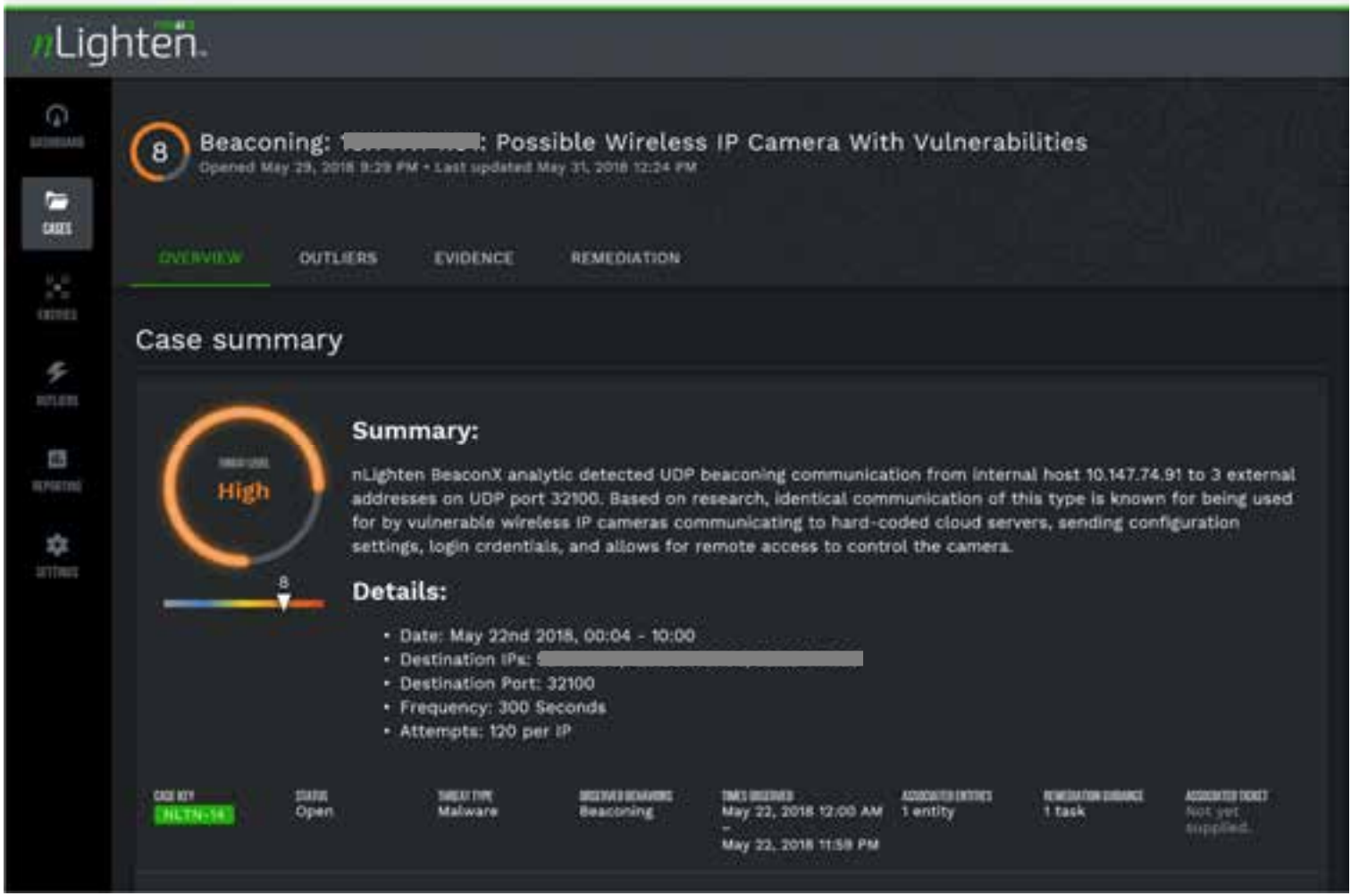
Illustration of outlier distribution to look for the statistically significant deviations that represent only the most interesting IPs/users. Cybraics uses outlier detection algorithms to isolate significant anomalies on the “tails” of the curve – drives false positives down/out.



nLighten CYBRAICS

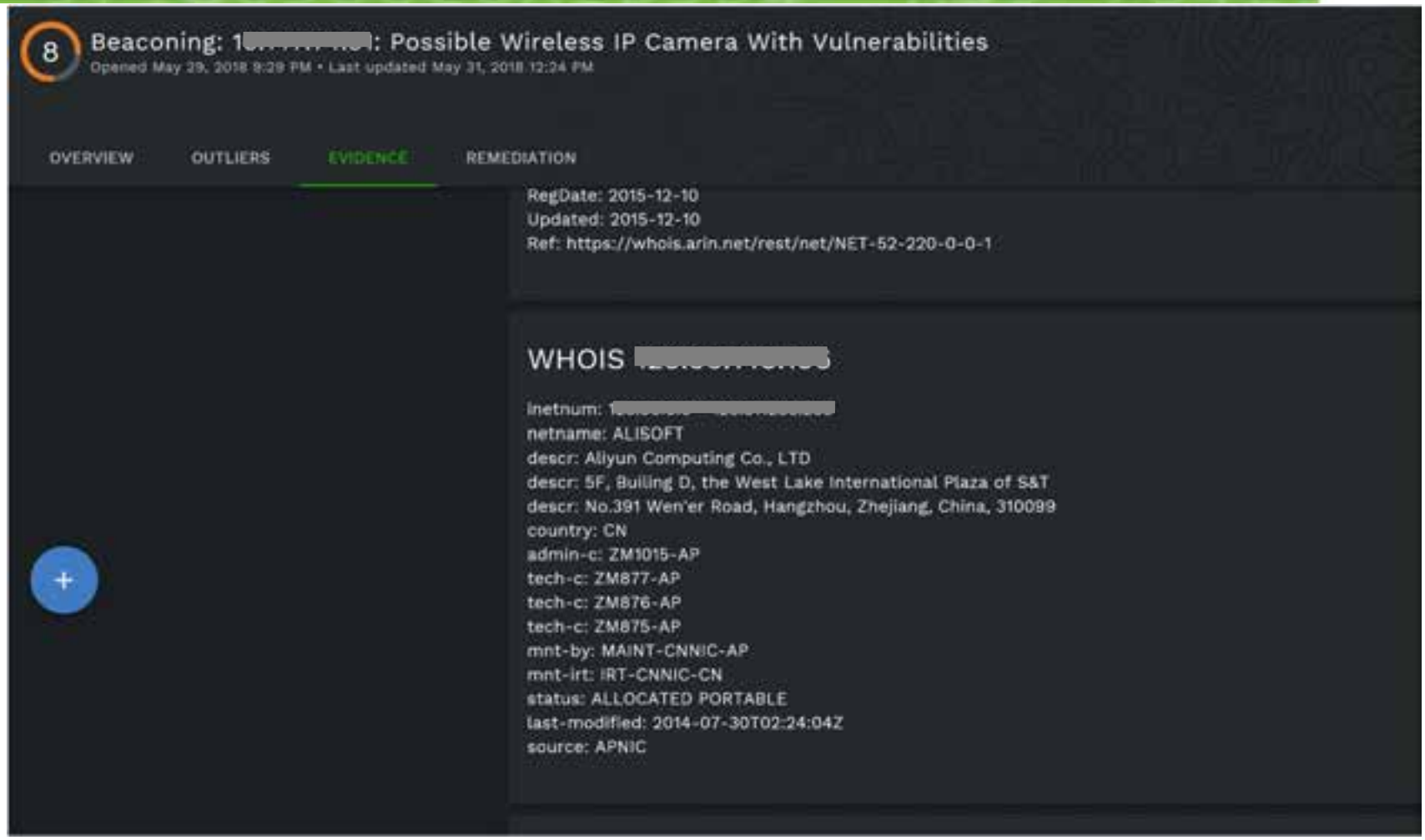
Cybraics Confidential 2018

Analytics spot Beaconing and creates a case!



nLighten CYBRICS

Evidence Gathering and Context



nLighten CYBRICS

Evidence/Conclusion/Remediation

Vulnerabilities Summary

The Wireless IP Camera (P2) WIFICAM is a camera overall badly designed with a lot of vulnerabilities. This camera is very similar to a lot of other Chinese cameras.

It seems that a generic camera is being sold by a Chinese company in bulk (OEM) and the buyer companies resell them with custom software development and specific branding. Wireless IP Camera (P2) WIFICAM is one of the branded cameras.

So, cameras are sold under different names, brands and functions. The HTTP interface is different for each vendor but shares the same vulnerabilities. The OEM vendors used a custom version of GoAhead and added vulnerable code inside.

GoAhead stated that GoAhead itself is not affected by the vulnerabilities but the OEM vendor who did the custom and specific development around GoAhead is responsible for the cause of vulnerabilities.

Because of code reusing, the vulnerabilities are present in a huge list of cameras (especially the InfoLeak and the RCE), **which allow to execute root commands against 1250+ camera models with a pre-auth vulnerability**.

The summary of the vulnerabilities is:

1. CVE-2017-8224 - Backdoor account
2. CVE-2017-8222 - RSA key and certificates
3. CVE-2017-8225 - Pre-Auth Info Leak (credentials) within the custom http server
4. Authenticated RCE as root
5. Pre-Auth RCE as root
6. CVE-2017-8223 - Misc - Streaming without authentication
7. CVE-2017-8221 - Misc - "Cloud" (Aka Botnet)

nLighten CYBERICS

If we can keep figuring this out….
Things run smoothly and safely…

nLighten CYBAUCS

Outcome of this case

- LNG Transport Ship was taken out of service
- Cameras were all replaced
- Servers were all wiped and restored from clean sources
- Upgrade processes were put in place
- Additional log sources were added for additional fidelity

- Prevented LNG transport disaster and millions in costs and lives

nLighten CYBAUCS


This is what failure looks like…

Cybraics: Other Recent IoT Cases

- Hacked Medical devices:
  - Identified malware that was active on a bone density machine that had evaded the AV platform – found it the minute our platform was turned on (had been there for months). The adversary could have easily adjusted the controls on the device and radiated patients and anyone within 100 ft of that room.
  - Found a misconfigured server open to man-in-the-middle attacks – happened to be the bedside monitoring server for the entire hospital system!
  - Identified patient devices that did not accept a firmware upgrade from the manufacturer. Manufacturer let the domain for the devices lapse (assuming the old URL was not necessary anymore). An attacker purchased the domain and started communicating with those devices (and ALL devices for that manufacturer that did not accept the upgrade). We stopped a PHI issue for the health system at the manufacturer.
  - Identified devices across the network communicating with blacklists not blocked by the AV system – potential ransomware attack.

Recommendations:

- **Relegate IoT devices to a "separate, firewalled, monitored network,"** just as you would in guest networks. "This allows you to restrict incoming traffic, prevent crossover to your core network, and profile traffic to identify anomalies."
- **Turn off stuff that's not being used.** That may seem obvious, but the checklist also recommends the "physical blocking/covering of ports, cameras, and microphones."
- **Ensure that people can't physically access these IoT devices** to reset the passwords, etc.
- **Enable encryption whenever possible**, and consider allowing only devices that support encryption to connect to your networks. If that's not possible, "consider using a VPN or other means to limit data exposure."
- **Keep firmware and software updated** (via automatic updates or monthly checks). Avoid products that cannot be updated, follow the lifecycle of all devices, and remove them from service when they are no longer updatable or secure.
- **LOG activities** from devices, Firewalls, Netflow, and server activities
- **Analyze logs** with tools that can spot anomalous behavior

nLighten CYBRICS Checklist from the Internet Society: https://www.internetsociety.org/

Cybrgics Confidential 2018

The Future:

Scale of IoT devices and Networks are increasing

Dependence on and Integration into our lives continues

We need to insist on more device security from our manufacturers

Log Volume growth will continue to be exponential

Attacks will continue to increase and become more sophisticated and damaging

Development of Machine Learning to spot issues must continue

If we fail, people will die and we will have significant unplanned expenses for recovery and remediation

nLighten CYBAUCS

The cost of prevention is FAR cheaper than consequences


YOU! Don’t let this happen!

THANK YOU!

Pete Nicoletti pete@Cybraics.com

Pete has 31 years of impressive success and responsibility in the deployment, marketing, sales, product development, engineering design, project implementation and operation of information technology, IaaS/SaaS/PaaS, cloud, data center operations, the entire spectrum of security technologies, compliance frameworks, Global Security Deployments and operations and Managed Security Service Provider services and operations.

Skills

IR, Product Management, Cyber Security, MSSP, Operations

Education/Certifications/Presentations

BS University of Tennessee

CCSK, CISA,CISSP,SANS GIAC, FCNSP, CCSE

"Opensource Security Concerns" Security Mag. 11/17
"How to Sell Cybersecurity to your Team" CSO Mag.
"Not Obscured by Clouds, Forensics and Cloud Visibility," Netscout Global Conference, April, 2017
"Cloud Forensics, A practitioners View," CS World 2016
"Cloud Security, Latest Developments," ISSA Conf 2016
"Auditing the Cloud Challenges," ISACA Conference, 2017
"Best Practices and the Latest Advances in Cloud Security,"

nLighten CYBRAICS

Prior Experience

- CISO for Hertz Global, Virtustream/RSA/EMC/DELL, VP Security Engineering Terremark
- Gartner's "most secure cloud design" #1 and #2
- Whitehouse.gov, FBI.Gov, DOT.gov, VA, Library of Congress and more Federal Projects
- Managed two clouds through FEDRAMP and eventually to EAL 5
- Book Author/Contributor: "An Intel Reference Design for Secure Cloud"
- 20 years Security, Red Team leader, Incident Response leader
- CDO at Cybraics focused on Security Operations, NIST 800-53 certification and product development
- Miami Electronic Crime Task Force (SS), FBI Infragard Contributor
- Awarded Top 100 Global CISO in 2017