A Random walk through (a few) 1,000,000 Things
A Story of Millions Interrogated Devices

Chris Rouland
Founder and CEO, Phosphorus Cybersecurity
What is xIoT?

- Purpose-built firmware/HW
- Network-connected
- Can’t run Endpoint security
Endpoint Security

.57 desktops per person
World-wide desktops or laptops per person.

5 Billion desktops WW
Total computers with keyboards world-wide.
50 Billion xIoT devices world-wide

Spanning IoT, OT, and Network Devices.
State of xIoT Security

The need to Find, Fix, and Monitor xIoT devices automatically.

- **78%** of Enterprise IoT devices have a CVE of 8+
- **26%** of Enterprise IoT devices are end-of-life by their manufacturer
- **50%** of enterprise IoT/OT devices use default credentials
- **3-5** IoT devices per enterprise employee

7 years Average firmware age of an embedded device
Phosphorus Research Stats

50% Default Passwords
50% Passwords Changed at Least Once

Rotation frequency
Complexity
Length

Default Passwords
Passwords Changed at Least Once
**Phosphorus Research Stats**

**EoL Firmware**

- 26% EoL
- 74% Supported, but 6-year average age
xIoT Security Today = IT Security In 1995
U.S. House of Representatives passed H.R.5515 - prohibits federal agencies from using IoT devices from certain China-based firms including Huawei, ZTE, Hikvision, Dahua & Hytera.
“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
Russian State Hackers Target xIoT

Internet-accessible xIoT

Two default passwords
One unpatched vulnerability

Internal Enterprise Environment

Sniff traffic with tcpdump
Scan & expand
Enumerate administrative groups

Strontium APT28 - aka Fancy Bear aka SoFancy - Linked to Russian Intelligence GRU

Discovered by the Microsoft Threat Intelligence Center
Russian State Hackers Target Routers

Compromised through extraneous services like remote management that were running with default passwords

VPNFilter Malware

- Traffic capture
- Firmware wiping – destroying router
- Post reboot malware persistence

500,000 infected business & home routers: Linksys, MikroTik, Netgear, QNAP, & TP-Link

Discovered by Cisco
Russian State Hackers Target Net. Devices

A separate attack

- Remote login with default username & password
- Initial boot credentials
- Undocumented user account with privilege level 15
- Full access to all commands & changes

Russian Dragonfly Cyber Unit targets millions of Cisco network devices with port TCP 4786 (Smart Install) open

Exfiltrate configurations over TFTP, execute commands, replace the IOS images, and set up accounts

Patch the firmware, turn of extraneous services & manage credentials correctly... & eat your vegetables
Mirai Botnet

Actual brand not pictured

Default & eight common passwords

PayPal, Twitter, Reddit, Sony, Netflix, GitHub

© 2022 Phosphorus Cybersecurity Inc. – confidential & proprietary
Russian xIoT Botnet Takedown

RSOCKS Botnet

Industrial Control Systems (OT), Network Gear, Enterprise xIoT...

$ Millions of compromised devices operated by Russian cybercriminals & leased ~$30/day

Law enforcement from the US, UK, Germany & Netherlands participated in the takedown
APTs Achieving Persistence with xIoT: QuietExit

Compromise & C2 Tunnel

Dropbear SSH client-server software

API calls on-prem & in the cloud

Data exfiltration

Data retrieval

UNC3524 was published by Mandiant on May 2nd, 2022 & labeled “QuietExit”

Associated with Russian Espionage Threat Actors: APT 28 Fancy Bear & APT 29 Cozy Bear

It exfiltrates executive, corporate development, M&A, and security staff data – 18 month+ dwell time

© 2022 Phosphorus Cybersecurity Inc. – confidential & proprietary
General PLC Exploits

- Real Time OS (RTOS)
- VxWorks & OS-9
- C++ & Python
- (1) Runtime on embedded device
- (2) Editor – laptop for writing programs
- (3) SCADA GUI – monitor

Interruption
blast messages, it’s simple so you can easily DoS a PLC (flood w/ 1,000 msg./sec.)

Interception
read the message, there is no encryption across the network

Modification
change the message, like a bump in the wire, modify the content and resend

Injection
make your own message (Modbus/TCP frame), all messages are welcome

- Critical
- Hyper-connected
- Modern & legacy protocols
- Poor user documentation
- Proprietary encryption
- Depreciation over decades
- Unmaintained
- Mostly no authentication
- No integrity (tamper away)
- No confidentiality (plain text)
KVM Switches

Running Ubuntu Linux v10 from ~October 2010 (current release is v21.1 as of October 2021)

Totally unpatched with hundreds of vulnerabilities
Lights Out Management Controls

Three common types of lights out management controllers including HP, Dell, & Supermicro

They are IoT devices running their own OS and applications (Linux or VxWorks)
Server Cabinets & Racks

- UPS backup, cooling, cable management & tamper sensors
- Passwords are usually default; old firmware with critical CVEs
During a POV we could lock and unlock 6,400 doors at a FS company

Nortek Security & Control systems had several CVSS scores of 9.8/10 & 10/10

Allowing remote, unauthenticated, and low-skill exploitation for full control
Black Hat 2019: critical level vulnerabilities were discovered in 10,000 printer brands/types/versions

Promiscuous & multi-vector access with everything on by default and default credentials

Some of the most targeted assets by state sponsored attackers
VoIP Phones & Video Conf. Systems

Some run Android OS and have undocumented SSH with default credentials.

A beacon of hope: one customer had 31,000 phones and “only” 700 had critical CVEs.
Knew about six of them

No CVEs
WHICH xIoT DEVICE TYPE IS THE #1 BIGGEST OFFENDER?
The #1 worst offender; running Linux such as BusyBox; some ship with malware preloaded

Everyone has them; nobody knows who’s responsible: IT, IT Sec., Facilities, Corp. Sec., Network Ops...
Beyond Enterprise xIoT

- Internet of Battlefield Things (IoBT)
- Industrial Internet of Things (IIoT)
- Internet of Healthcare Things (IoHT)
- Smart Ships
- Smart Buildings & Cities
- Network Gear

© 2022 Phosphorus Cybersecurity Inc. – confidential & proprietary
Organizations don’t know what things they have. So, they don’t know what things to fix. They don’t have the ability to fix things at scale. They aren’t monitoring things to keep them fixed. This is leaving xIoT and IT/cloud assets at risk. It’s resulting in data theft, destruction, spying, ransomware...
Thank you!

Chris Rouland  
Founder and CEO, Phosphorus Cybersecurity  

chrishphosphorus.io  
https://www.linkedin.com/chrisrouland/