CSCRL SPRING SYMPOSIUM
RETHINKING YOUR SUPPLY CHAIN – PREPARING FOR THE FUTURE
APRIL 11-12, 2024

ABSTRACT

xIoT Hacking Demonstrations to Disappoint Bad Actors

John Vecchi
Chief Marketing Officer
Phosphorus Cybersecurity

We've unleashed our dark allies from the nightmare dimension on an unholy crusade to demonstrate cyberattacks for your enlightenment. If you love seeing devices compromised as much as we do, join us for hacking demonstrations, detailed security research findings, and threat mitigation techniques that will disappoint cybercriminals. We'll demonstrate several hacks against xIoT, or Extended Internet of Things, devices. For those who would say, "But they're just security cameras monitoring the parking garage, wireless access points in the cafeteria, PLCs controlling robotic welding arms, or our OT devices aren't at risk like our IT devices are; what harm can they cause?" - this will illuminate that harm.

xIoT (IoT, OT and network assets) encompasses disparate but interrelated device groups with purpose-built hardware and firmware, are typically network-connected, run well-known operating systems and disallow the installation of traditional endpoint security controls. In addition, many xIoT devices have open ports, protocols, storage, memory, and processing capabilities. Even though most industrial environments have tens to hundreds of thousands of these devices in production, they go largely unmanaged and unmonitored and operate with weak credentials, old, vulnerable firmware, extraneous services, and problematic certificates.

Cybercriminals have shifted their focus to xIoT attacks. Why? Because they work. This massive, vulnerable attack surface is being successfully exploited by bad actors engaging in cyber espionage, data exfiltration, sabotage, and extortion, impacting xIoT assets. And this is especially true for operational technology as businesses gain powerful business benefits but increase their risk as OT and IT infrastructures converge.

Bad actors count on you being passive. They want you to fail so they can continue to evade detection and maintain persistence on your devices. Disappoint them! Take your devices back by understanding how to hack them, recognizing where they're most vulnerable, and employing strategies to successfully protect them at scale.

CSCRL
LEHIGH UNIVERSITY | College of Business