OpCode Security, Inc. 0x41414141

# Forward-thinking hospital. Vulnerabilities hidden-in-plain sight.

## "What happens when a cutting-edge medical center needs visibility into its device credentials?"

It's possible to be a forward-thinking leader —in this case medicine —and yet fall behind when it comes to device security. A mid-size regional hospital system faced a serious IT cyber security challenge. Investment in network security could still leave the organization at risk to easily exploitable vulnerabilities that were hard to find. A huge attack surface and low visibility into devices would allow an attacker to find default credentials on the network, gain access, and stay hidden for months. Critical systems, employees, patients, and the reputation of the hospital were at risk.

When scanning with IoT Crusher the organization found it had misconfigured its rules and had telnet exposed to the network, running on a core switch. IoT Crusher determined there was a default credential being used on the system that allowed Administrator access. After a bit of research through the product documentation it was determined that the default credential was most likely an undocumented vendor back door on the device.

> "Maintaining the security of medical devices is critical for maintaining patient safety and eliminating default credentials is an essential means of doing that."

–Chris F., Customer statement

### CHALLENGE

- Find default, embedded, and weak credentials across the network
- Closes gap left by other scanners when it comes to user names and passwords
- Discover non-centralized managed devices such as printers that may be vulnerable to credential issues
- Gain visibility and control over vulnerabilities on devices that are non-centrally managed

### SOLUTION

- Use IoT Crusher Advanced to conduct surgical credential tests
- Scan for vulnerable network services such as Telnet, FTP, and VNC
- More protocols in development

### RESULTS

- Found unexpected default privileged credential on core network switch
- Found devices that were left in default state and never configured
- Remediation of credential issues helped ensure compliance

# Problem

Several factors combined put this hospital especially at risk.

## Assurance: Moving to a Zero-Trust Network

As the hospital moved to an advanced zero-trust network they felt they had found and resolved most of the infrastructure vulnerabilities across the network. The decrease in shared infrastructure surface area would help ensure the reduction in cyber vulnerability exposure, thereby protecting the doctors, staff, and employees' core hospital mission: helping patients.

## Deployed Solutions Left Gaps

After running vulnerability scanners, doing remediation, segregating, VLANing, and re-configuring the network, IT felt they eliminated all of the low-hanging cyber security issues. They believed it was in a solid infrastructure position. But it wasn't.

### ZERO-TRUST WASN'T ENOUGH

- Existing market solutions left gaps
- Low-hanging vulnerabilities were hiding in plain sight
- Client is very forward thinking when it comes to security

# Solution

## Fixing the Problem

Customised IoT Crusher scans allowed IT to search and attack devices and services on the network. IT mimicked malware and attacked by specific device manufactures as well as known default combinations in the hospital's infrastructure. They easily mapped credentials for identified devices and even tested by specific malware and product combinations.

A critical default credential was discovered on a core switch, which, after analysis, appeared to be an undocumented product back door allowing anyone access into the core network using a specific user name without a password. This credential was previously missed by all of the latest updated vulnerability scanning solutions in the environment.

Additional default credentials were found on other infrastructure devices such as medical devices and printers.

### FROM FOUND TO FIXED

- Malware and manufacturer scan types yielded results
- Mapped credentials to devices for speed
- Critical switch vulnerability found in a day
- Default credentials found on medical devices and printers

# Results

## Default Credentials Scan

IoT Crusher was used to shore up the vulnerabilities and find threats that other products couldn't. Used in combination with other technologies it detected difficult to find low-hanging default credentials that other solutions missed.

## Business Benefits

IoT Crusher helps close the gap for credential scanning left open by other scanners. The features of IoT Crusher allowed for fast testing of their infrastructure with little to no account lock out. The price of IoT Crusher relative to other products on the market is very affordable. Running IoT Crusher helps ensure compliance with regulations on this timeless and critical security issue.

Beyond the immediate improvements in device security, the hospital experienced a significant extra benefit: higher efficiency operation. They have fewer manual checks, less human error and the network team can now quickly identify device and network vulnerabilities and threats for default, embedded and weak credentials.

Learn more about these solutions at

[opcode41.com/shop/](opcode41.com/shop/)

### TECH BENEFITS

- Fast testing
- No to little account lock out
- Closes gap left by other scanners

### BUSINESS BENEFITS

- Relatively inexpensive solution
- Reduce risk posture
- Compliance with regulations: HIPAA, PCI, SOX, and other regulations
- Uncover and fix fundamental security issues