AutomaTech™ CBPacific™ NOZOMI NETWORKS

Presenters

Jack Nedelman
Business Development Manager
AutomaTech

Tom Jensen
Senior Solution Architect
AutomaTech

Alex Dumitrescu
Technical Sales Engineer
Nozomi Networks

Alexey Kleymenov
Senior Cyber Threat Analyst
Nozomi Networks

AutomaTech™ CBPacific NOZOMI NETWORKS

Agenda

- AutomaTech - Who we are
- What is Apache Log4j vulnerability
- What is the threat and what it affects
- What OT systems are affected including SCADA, Historian or other plant floor systems
- Suggested actions to reduce your vulnerability
- Prevent & anticipate vulnerabilities in the future
- Solutions that can help including Moxa and Nozomi

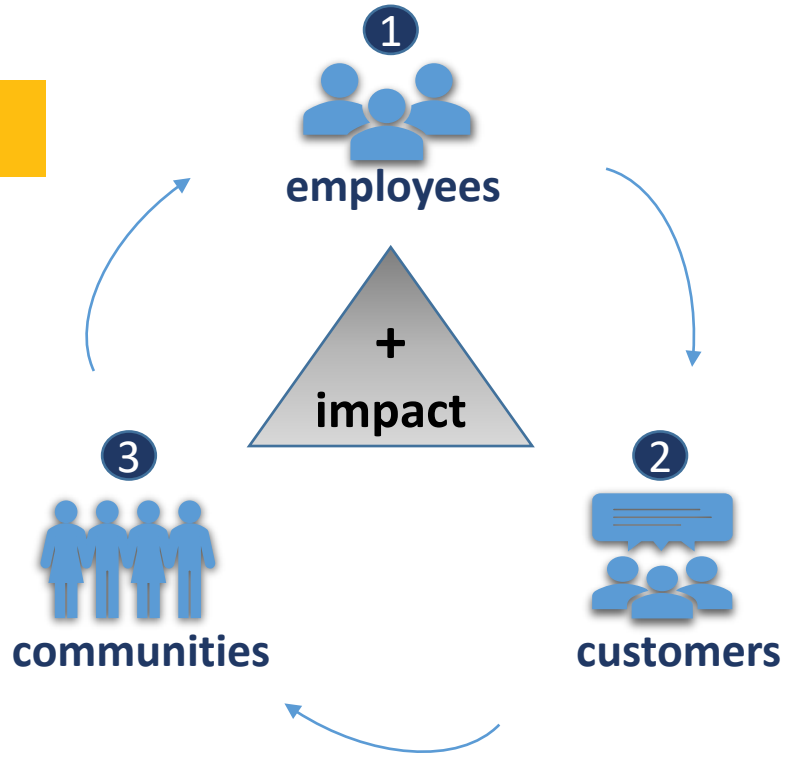
Poll Question #1

What are you hoping to get out of this webinar?

1. Educate myself and my team on Log4Shell
2. Learn about tools to help remediate impact
3. Start my Cyber journey
4. Expand on my Cyber Journey

Our purpose

Why?



Our mission

We build long-term relationships with industrial customers by:

- Solving tough problems
- Being your trusted advisor
- Providing exceptional lifecycle support & service

Have a positive impact…every time, all the time!

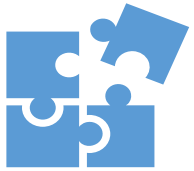
AutomaTech's Promise

Great service: Every time, all the time!

WHAT:

Great service
Great support Customer first mindset

Build enduring relationships measured in decades *(not quarters)*



Solve tough business problems

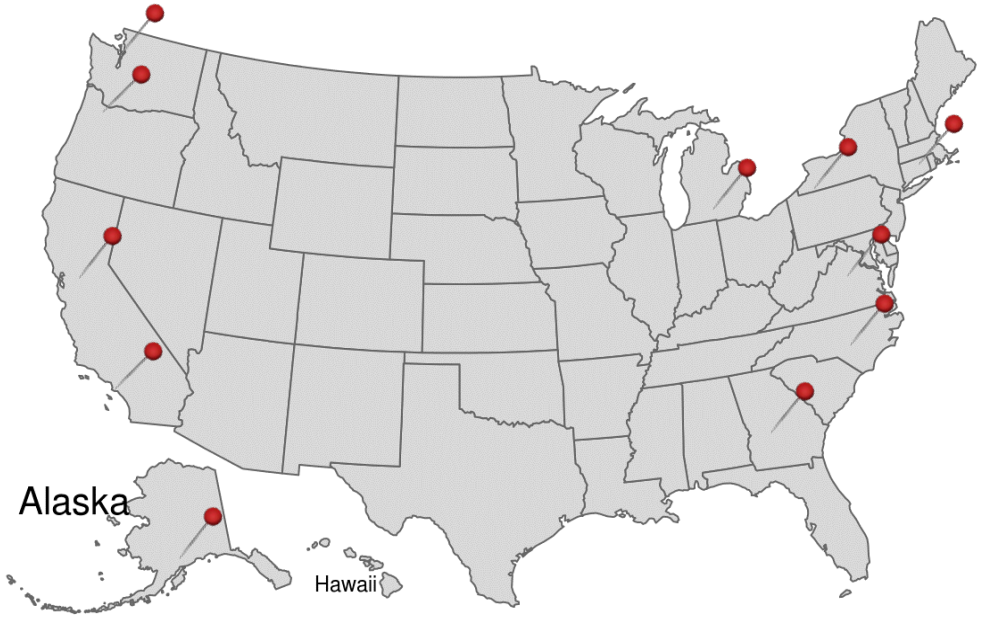
HOW:

Deep technical and application knowledge

Great supplier relationships

Provide 7x24 hour support

Supporting Customers



- AutomaTech & CB Pacific are part of Flow Control Group Automation spanning North America
- Part of KKR – 3rd largest private equity group – 665B of enterprise value
- Comprehensive support services with experienced Solution Architects and Engineering support team
- Well-established network of Solution Providers to deliver a complete solution including design, installation and commissioning
- Certified training services, seminars & webinars, user conferences & workshops, value-added services

AutomaTech Solutions

Controls & SCADA Automation

- PLCs
- HMI/SCADA
- Mobility & Remote Connectivity
- Automated Data Collection & Reporting
- Alarm Notification
- Enterprise SCADA Consulting

Manufacturing & Information Systems

- Manufacturing Execution Systems (MES) & Consulting
- Enterprise Data Collection, Reporting & Visualization
- Advanced Analytics & AI

Industrial Internet (IoT) & Cloud Solutions

- IoT EDGE Connectivity
- Remote Monitoring & Diagnostics
- Equipment Optimization
- Asset Performance Management (APM)

Systems & Network Infrastructure

- High Availability & Fault Tolerant Servers,
- Virtualization, & Disaster Recovery
- Thin Client Infrastructure
- Industrial Networking

OT Cyber Security

- Cyber Security Assessments
- Intelligent Security Appliances
- Identify Defined Networking
- Industrial Firewalls & VPNs
- Bridging OT/IT Networks

Securely we help… connect | control | visualize | analyze | optimize

AutomaTech™ CBPacific NOZOMI NETWORKS

Nozomi Networks at a Glance

CUSTOMERS
+1,000 Global Installations

DEVICES
+300,000 Monitored

DEPLOYMENTS
In 5 Continents

GLOBAL REACH
Local Support

- UTILITIES
- CHEMICALS
- PHARMACEUTICALS
- TRANSPORTATION
- MINING
- OIL & GAS
- WATER
- MANUFACTURING

enel | VERMONT ELECTRIC CO-OP | gsk | ...and more.

Nozomi Networks Breakdown

Achieve Complete Visibility into Your OT Network

Rapidly Detect Vulnerabilities, Threats & Incidents

Reduce Troubleshooting & Remediation Efforts

Successfully Deploy at Scale in the Largest Distributed Environments

Agile Development & Integrations with Rapid New Protocol Support

Centrally Monitor & Control Distributed Networks

Poll Question #2

Is Log4Shell hype or real?

1. It's very real and something I deal with frequently
2. It's very real and something people in my company deal with frequently
3. It's just hype – another flavor of the week
4. I'm not sure

What is Log4j and what is the vulnerability?

- Apache Log4j is an open-source logging utility developed by the Apache Software Foundation.
- It is used to log events and incidents for applications. This software helps to track bugs and program crashes; the information later is used in software improvements.
- Many Java based applications use Log4j for this purpose.
- Log4Shell vulnerability in the Log4j library allows attackers to remotely control and execute code on vulnerable machines making it easy to load malware.

AutomaTech™ CBPacific NOZOMI NETWORKS

Why did the Log4j vulnerability receive so much coverage in news?

Poll Question #3

How frequently does your organization add new innovations on the OT Side? Example IoT

1. Innovating frequently and seamlessly
2. Innovating and free do so, but slow to adopt technology
3. Can't innovate without IT approval
4. Not Sure

How quickly did this become abused by malicious actors?

Notable examples?

A Month after Disclosure – What's Up?

- Mostly minor hacks so far
  - Stealing processing power for crypto-mining
  - Minecraft Chat

- Why nothing major yet?
  - Waiting for the attention on the vulnerability to die down, focus on the next one
  - New enough that many infections may not have been discovered yet
  - Standard – Land and Expand methodology – wait to see if still active in a month to ensure not detected before starting mischief
  - Some companies with mature cyber practices acted quickly

Is there any way to know if you have been comprised?

In particular for Operation Technology equipment like SCADA, PLCs, etc?

For OT systems, how do you know you've been comprised?

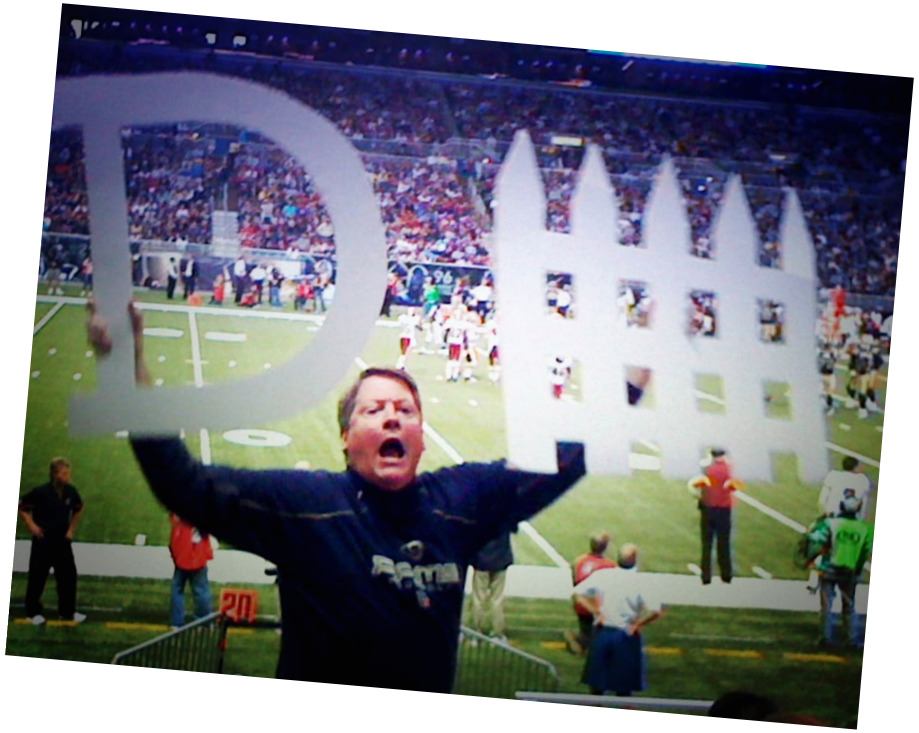
- Look for Log4j binary files – several examples and tools hosted on the CISA site: (https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
- Review web server logs for occurrences of jndi:ldap, jndi:ldaps and other similar patterns
- Look for software trying to connect to sites and not using port 443 https:// or port 80 http://
- PLCs are not a likely target and don't call or use the Log4J libraries
- Most SCADAs can host various web pages including some that may rely on Log4J libraries
- Visibility in OT environment

Poll Question #4

What do you already have in place to prevent/identify/remediate?

1. Network visibility tools
2. Threat Detection
3. Vulnerability Scanning
4. At least 2 or more
5. None

What type of defense can someone use to avoid being impacted by Log4Shell?



Strategies for Remedying Log4j Exploit

- Make sure the up-to-date detections are in place as soon as possible but don't rely on it only as there are multiple ways how they can be evaded
- Identify all the vulnerable software that uses Log4j
- Make sure you update any software that uses Log4j to the most recent version
- Keep checking what the most recent version is as it is still subject to change relatively quickly

How to Defend Against Log4j

ICS Security Management System

- Accurate asset inventory of ICS network devices
- Visualized network topology and device status
- Real-time alerts and event logging
- Troubleshooting tools to aid in network recovery

Poll Question #5

Do you have a good handle on Log4j vulnerabilities and impact within your OT environment?

1. Yes, we have worked with the IT team to track this down
2. Yes, we've done a lot of the work on the OT side
3. Somewhat – things are still siloed
4. No – because I don't know where to start

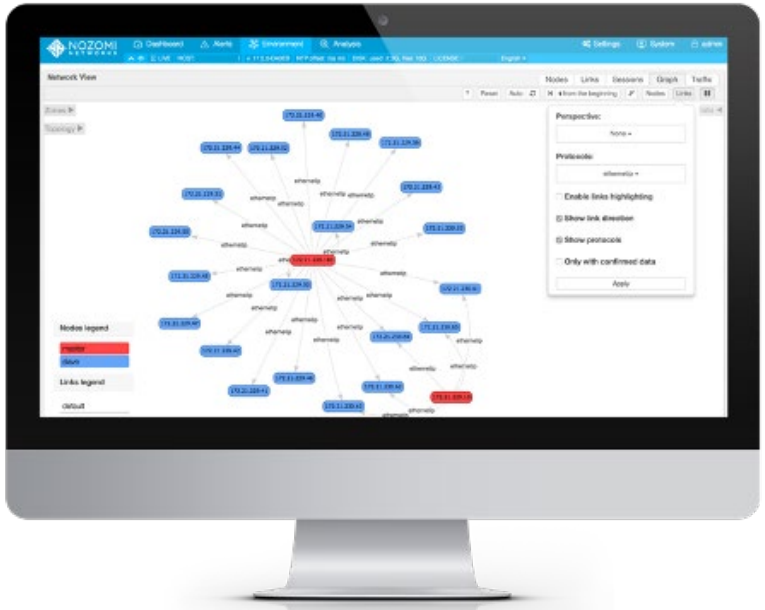
How does Nozomi help with this threat?

How does Nozomi help with this threat?

Passive and active monitoring of IT, IoT and OT sectors

24/7 Network Visibility into control and process networks

Anomaly Detection based on Network Behavior profiles



Continuously updated Threat Intelligence checks for vulnerabilities at a large scale and potential traces of malicious activity

How can AutomaTech help with Log4J/Log4Shell?

What other ways can AutomaTech help with Log4Shell?

- Industrial and OT Firewalls
- Intrusion Protection System & Intrusion Detection System (IPS/IDS)
- Secure Remote Access
- Network Segmentation
- Disaster Recovery (Planning, High Availability, Fault Tolerance)

Poll Question #6

Do you have a good handle on Log4Shell and next steps?

1. Yes – I'm interested in a follow up from Nozomi and AutomaTech
2. Yes – I need to create an internal plan before following up
3. No – I need more clarity

What additional resources are here to help with finding the latest updates for software that may be affected on someone's system?

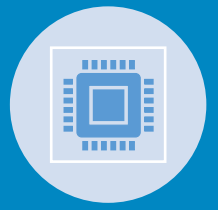
Resources

- Guidelines and a list of affected software by CISA
- A tool for scanning potentially vulnerable assets by CERT
- Log4Shell-related technical blog post by Nozomi Networks
- Try Nozomi Networks Community Edition
- AutomaTech Technical Support Wiki
- AutomaTech - Log4J-Log4Shell - Wiki CVE-2021-44228

Contact AutomaTech

138 Industrial Park Road, Plymouth, MA 02360

Phone: (508) 830-0088



Fax: (508) 830-0111

Sales
sales@automatech.com

Technical Support
support@automatech.com

www.automatech.com