Special Message re: massive Log4j Vulnerability, mitigation tools & where to go for help.

This week, because of severity of this vulnerability and its' potential implications, I felt it best to share what/where I've found to be the best resources, tools and help. This vulnerability was discovered by cyber security researchers on 12/10, and it immediately became known globally to be a severely critical risk. Almost instantly it began being exploited by cyber-gangs, and state-backed hackers.

In the last 11 days, I've sat in on several meetings, presentations and phone calls coordinated and/or presented by various branches of US Cyber Security leadership (including the FBI, CISA, NSA, InfraGard, and others), as well as public/private cyber security specialist groups to which I belong.

I've found that some of the best resources, tools and information can be found at:

https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

https://www.cisa.gov/emergency-directive-22-02

In the private sector arena, CompTIA ISAO (Information Sharing and Analysis Organization) Cyber Forum is a private, members only threat intelligence forum designed to keep cyber-security pro's informed and up to date on all discovered threats as they emerge. This threat was deemed so critical that CompTIA opened its' doors to non-members (since I've been a member – I've not known them to do this):

 "As a courtesy to the industry and any impacted organizations, the CompTIA ISAO is providing complimentary access to our threat intelligence reports and Cyber Forum discussions related to the Log4j vulnerability. We all need to work together to help businesses better understand the threat landscape and prepare for attacks, current and future."

To access this forum: https://forum.comptiaisao.org/threads/log4j-vulnerability-information.1820/

We strive to protect our clients and their information. If you need further assistance, guidance or help, feel free to reach out. To keep updated on all known threats, as they emerge, visit: https://la-cyber.com/Cyber-Active-Threats.php

Bill

William T. Palisano, CISSP
President

Lincoln Archives, Inc. / LACyber

(716) 871-7040 / (585) 458-8980
Fax: 716-362-9760

Protecting your information for the past 25 years!