MAYO CLINIC

CYBER THREAT ALLIANCE

THREAT INTELLIGENCE PRACTITIONERS' SUMMIT

# FINDING IOC'S IN UNEXPECTED PLACES

## CTA THREAT INTELLIGENCE PRACTITIONERS' SUMMIT

John Alexander, CISSP & HCISPP
Senior Information Security Engineer, Mayo Clinic

Virus Bulletin 2022
29 September 2022, Prague, CZ

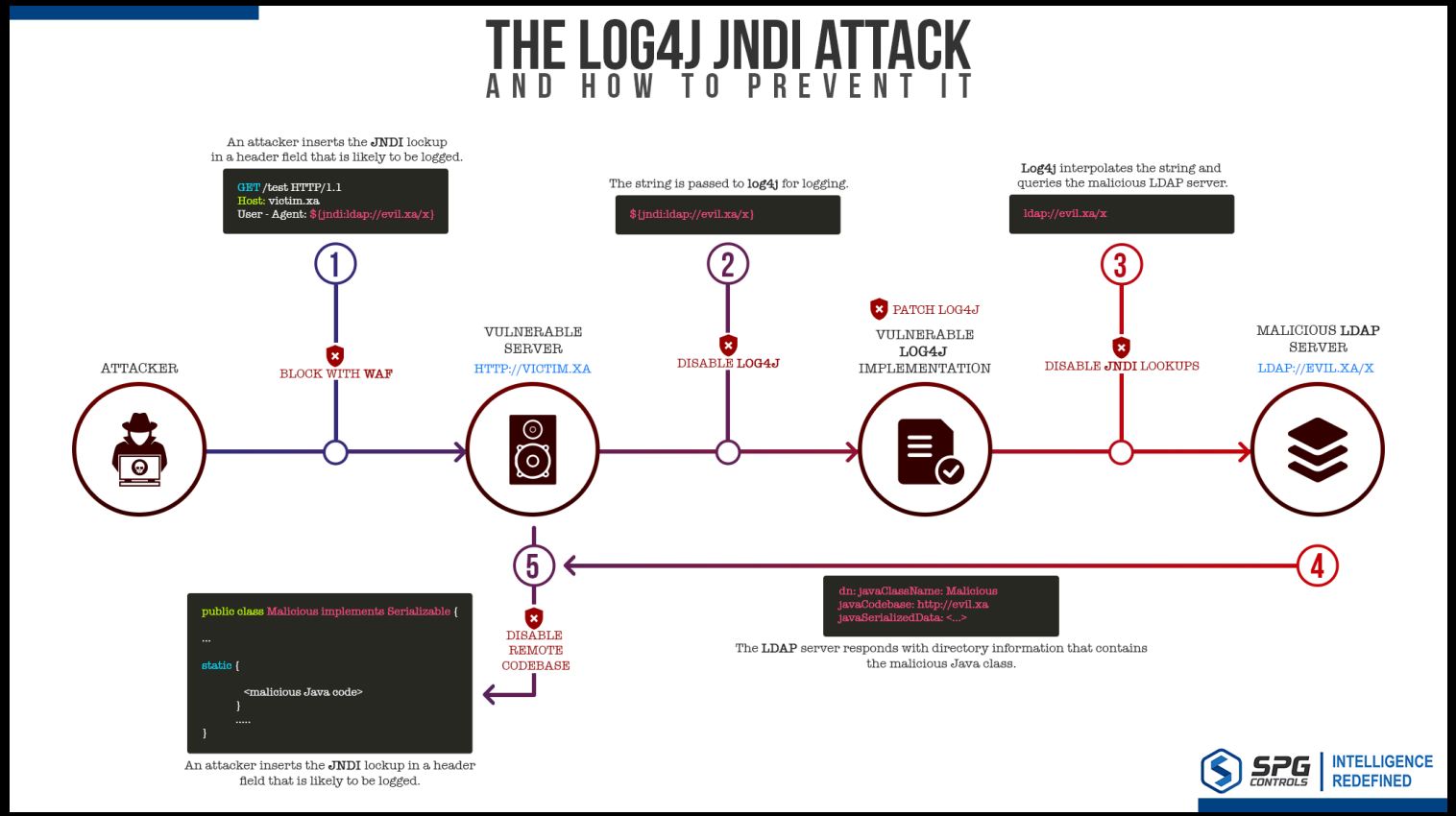
 

# LOG4J / LOG4SHELL

## CVE-2021-44228

CYBER THREAT ALLIANCE

THREAT INTELLIGENCE PRACTITIONERS' SUMMIT




https://spgcontrols.com/news/detect-and-mitigate-the-log4shell/

CYBER THREAT ALLIANCE

THREAT INTELLIGENCE PRACTITIONERS' SUMMIT

# LOG4J / LOG4SHELL

## OBSERVED

- Searching for “jndi” references in SIEM logs
  - Identified attacked hosts as subdomains of another domain in DNS
  - Example: server.mayo.edu.some.other.domain
  - Some noise reduction necessary (e.g. some SAAS offerings)
- “Other Domains”
  - Typically, free public DNS request logging services
  - Often new domains, various hosting
  - DNS requests could represent attacked assets in near real time
  - Can we mine these for blocking and/or alerting?

# LOG4J / LOG4SHELL
## CONJECTURE

- Insecure by Design?
  - Multi-Actor Coordination?
  - Perhaps Bot/Scanners to find vulnerable
  - Plausible Deniability / Burnable Initial Sources
  - DNS request logging services for collecting hostnames
  - Possible follow-up by others for more payloads

# LOG4J / LOG4SHELL

## SIEM SWIMMING

- Searched for our domains as subdomains of others
  - Intentionally Broad Search
  - Hosts, DNS, Processes, URLs, anything…
- Unexpected Finding: Email Logs
  - Hosts were not vulnerable
  - Hosts had error reporting enabled via email
  - Error condition encountered was in the Subject of the email

# LOG4J / LOG4SHELL
## CONCLUSIONS

- Inadvertent Honeypots
  - Non-vulnerable systems with error reporting enabled & configured
- IOCs
  - Blocking to detect & protect vulnerable assets
  - One domain identified, was not yet listed in our TI feeds (at that time)
- Theoretical Risk
  - Circumvention/Amplification - What if one of our email processing systems or email recipient clients had Log4J trigger off of an email?

CYBER THREAT ALLIANCE

THREAT INTELLIGENCE PRACTITIONERS' SUMMIT

# QUESTIONS & ANSWERS