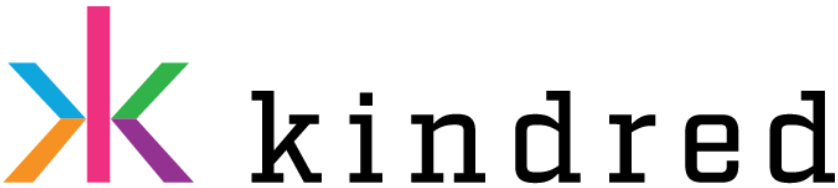


Security Newsletter

20 Dec 2021

Subscribe to this newsletter

The Next Wave of Log4J Attacks Will Be Brutal

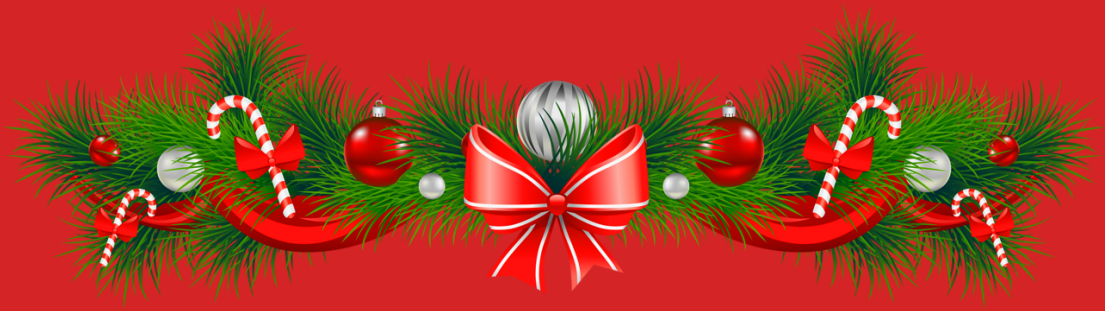
A week ago, the internet experienced a seismic event. Thanks to a vulnerability in Log4j, a popular open source library, multitudes of servers around the world were suddenly exposed to relatively simple attacks. The first wave of hacking is well underway. But it's what comes next that should worry you.

So far, the vanguard of Log4j hacking has primarily comprised cryptominers, malware that leeches resources off of an affected system to mine cryptocurrency. (These were extremely popular a few years ago, before everyone realized that the real money's in ransomware.) Some nation-state spies have dabbled as well, according to recent reports from Microsoft and others.

What's seemingly missing is the extortion, the ransomware, the disruptive attacks that have defined so much of the past two years or so. This won't be the case for long.

Read More on Wired

This is the last Kindred Security Newsletter for 2020



It's time for the Kindred Group Security team to take some holiday. The newsletter will be off for a few weeks during Christmas and New Year's Eve. But don't worry, we'll be back. See you soon for some awesome infosec news!

More #News

- Egyptian Politician Hacked by 2 Government Hacking Groups, Researchers Say
- Patch fixing critical Log4J 0-day has its own vulnerability that's under exploit
- NY Man Pleads Guilty in $20 Million SIM Swap Theft
- Inside Ireland's Public Healthcare Ransomware Scare
- Facebook disrupts operations of seven surveillance-for-hire firms
- Google Calendar now lets you block invitation phishing attempts

#Breach Log

- Credit card info of 1.8 million people stolen from sports gear sites
- McMenamins breweries hit by a Conti ransomware attack
- Experts Discover Backdoor Deployed on the U.S. Federal Agency's Network
- Over 500,000 Android Users Downloaded a New Joker Malware App from Play Store

#Patch Time!

- Microsoft Patch Tuesday, December 2021 Edition
- Serious Security: OpenSSL fixes "error conflation" bugs – how mixing up mistakes can lead to trouble
- Apple security updates are out – and not a Log4Shell mention in sight
- Western Digital warns customers to update their My Cloud devices
- Upgraded to log4j 2.16? Surprise, there's a 2.17 fixing DoS
- CISA urges VMware admins to patch critical flaw in Workspace ONE UEM
- Google pushes emergency Chrome update to fix zero-day used in attacks
- Lenovo ThinkPads vulnerable to privilege escalation exploit

#Tech and #Tools

- FPGAs: Security Through Obscurity?
- Inside a PBX - Discovering a Firmware Backdoor
- A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution
- log4j-tools: tools for finding log4shell in jars and source

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us