Your Weekly Security Awareness Newsletter #198

#WeeklyCybersecurityTip: Don't click on suspicious links provided in emails!

To receive these direct to your inbox, sign up **here**

20 December 2021

1 Critical Apache HTTPD Server Bugs Could Lead to RCE, DoS

Don't duck at the latest mention of Apache: Two critical bugs in its HTTP web server – HTTPD – need to be patched pronto, lest they lead to attackers triggering denial of service (DoS) or bypassing your security policies. Apache, the open-source software foundation behind the Log4J logging library t...

Read more

2 Java Code Repository Riddled with Hidden Log4j Bugs; Here's Where to Look

There's an enormous amount of software vulnerable to the Log4j bug through Java software supply chains — and administrators and security pros likely don't even know where to look for it. About 17,000 Java packages in the Maven Central repository, the most significant collection of Java packages avai...

Read more

3 GUEST ESSAY: Introducing 'killware' — malware designed to contaminate, disrupt critical services

Within the past year, we have seen a glut of ransomware attacks that made global news as they stymied the operations of many. In May, the infamous Colonial Pipeline ransomware attack disrupted nationwide fuel supply to most of the U.S. East Coast for six days. Related: Using mobile apps to radicaliz...

Read more

4 Telegram Abused to Steal Crypto-Wallet Credentials

Attackers are targeting crypto-wallets of Telegram users with the Echelon infostealer, in an effort aimed at defrauding new or unsuspecting users of a cryptocurrency discussion channel on the messaging platform, researchers have found. Researchers at the SafeGuard Cyber's Division Seven threat analy...

Read more