

2022 THREAT TRENDS

As recent events illustrate, threat actors are more numerous, persistent, and sophisticated than ever. However, new cybersecurity approaches offer a stronger defense. To keep your business protected, stay informed on these emerging threat trends:

THREAT VULNERABILITIES INCREASE WITHIN THE SUPPLY CHAIN

2/3 of supply chain attacks relied on exploiting the customer's trust in their service provider.¹



2000 organizations affected by the Kaseya supply-chain attack by REvil in July 2021.²



1. <https://www.cpomagazine.com/cyber-security/enisa-predicts-fourfold-increase-in-software-supply-chain-attacks-in-2021-warning-that-strong-cyber-defenses-were-no-longer-effective/>

2. <https://www.csoonline.com/article/3626703/the-kaseya-ransomware-attack-a-timeline.html>

MOST COMMONLY USED EXOTIC PROGRAMMING LANGUAGES

4 LANGUAGES (GO, NIM, DLANG, AND RUST)

are behind the increase in malware families used in many of the latest cyberattacks.³

3. <https://blogs.blackberry.com/en/2021/07/old-dogs-new-tricks-attackers-adopt-exotic-programming-languages>

RANSOMWARE EXTORTION ESCALATING

935%

more double extortion attacks, with data from 2,300+ companies posted onto ransomware extortion sites.⁴



93%

surge in triple extortion ransomware attacks in 2021.⁵

4. <https://www.infosecurity-magazine.com/news/double-extortion-ransomware-soar/>
5. <https://cybernews.com/news/ransomware-surge-93-in-last-6-months-fueled-by-triple-extortion/>

\$5.3M

average ransom demand for attacks, which grew 518% from 2020 due to quadruple extortion tactics being used.⁶



6. <https://threatpost.com/ransomware-payments-quadruple-extortion/168622/>



ATTACKS DOMINATE CRITICAL INFRASTRUCTURE

14 OF 16

U.S. critical infrastructure sectors, considered vital to national security, public health, or safety, were victims of ransomware attacks in 2021.

COVID-19-THEMED ATTACKS PERSIST

400%

rise in cyberattacks primarily due to people working from home.⁷



18M

phishing emails and malware related to COVID-19 are blocked daily by Google.⁷



7. <https://techjury.net/blog/covid-19-cyber-attacks>

CLOUD TECHNOLOGIES INCREASINGLY USED FOR ATTACKS



\$20B

in damages in 2021 from malware run on cloud architecture, a 57X increase over 2015.⁸

8. <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>

MAJORITY OF MOBILE APPLICATIONS REMAIN VULNERABLE TO ATTACKS

76%

of tested mobile applications store data insecurely, according to recent studies.⁹



9. <https://www.stealthlabs.com/blog/how-to-make-sure-your-app-is-secure-penetration-testing/>

As the threat landscape rapidly evolves, it is essential that you get the latest information and cyber prevention strategies to keep your organization protected.

Get the latest Threat Report @ BlackBerry.com/TR22

