
Financial
Cybersecurity
Predictions
for 2024
kaspersky

Increase in AI-powered cyberattacks

Expect a surge in cyberattacks leveraging artificial intelligence to mimic legitimate communication channels, leading to a proliferation of lower-quality campaigns


Cybercriminals will exploit the popularity of direct payment systems, leading to the emergence of clipboard malware and increased exploitation of mobile banking trojans
Fraudulent schemes targeting direct payment systems


Global adoption of Automated Transfer Systems (ATS)
The global adoption of mobile ATS will extend beyond Brazilian borders, allowing cybercriminals worldwide to exploit these systems for financial gain


Resurgence of Brazilian banking trojans
Brazilian banking trojans will fill the void left by desktop trojans, with families like Grandoreiro expanding abroad and targeting a growing number of banks


Ransomware groups will become more selective in their targets, focusing on financial institutions and organizations to maximize payment or demand higher ransoms
Ransomware target selection

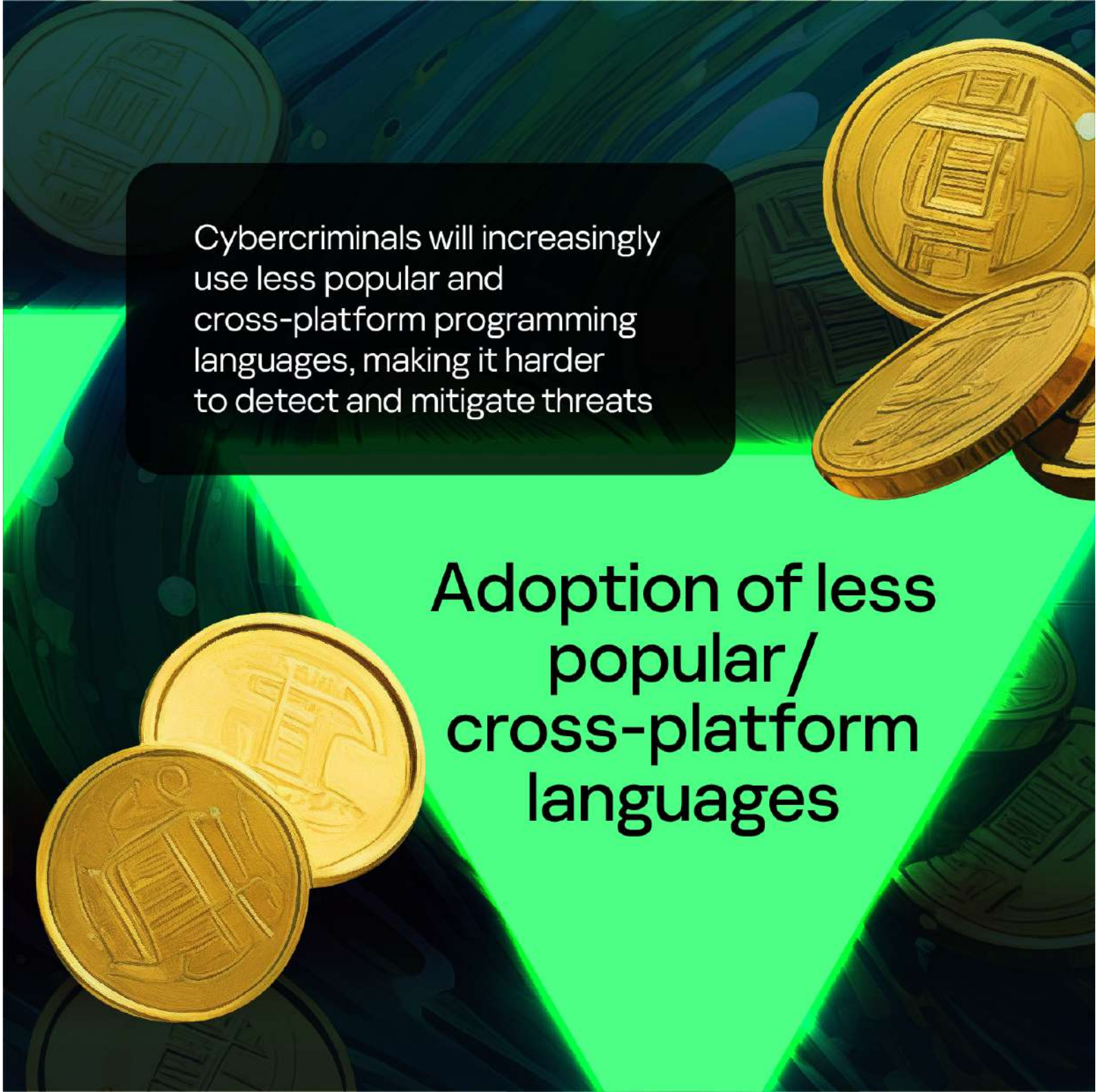

Open-source backdoored packages,
compromising widely-used software and potentially leading to data breaches
Decrease in 0-days, increase in 1-day exploits,
aiming for increased accessibility

Exploitation of misconfigured devices and services,

providing cybercriminals unauthorized access for launching attacks

Fluid composition of affiliate groups,

making it challenging for law enforcement to effectively combat cybercrime


Cybercriminals will increasingly use less popular and cross-platform programming languages, making it harder to detect and mitigate threats
Adoption of less popular/ cross-platform languages


Emergence of hacktivist groups
Socio-political conflicts will lead to the rise of hacktivist groups disrupting critical infrastructure, posing a significant threat to financial institutions