AI in the Trenches:

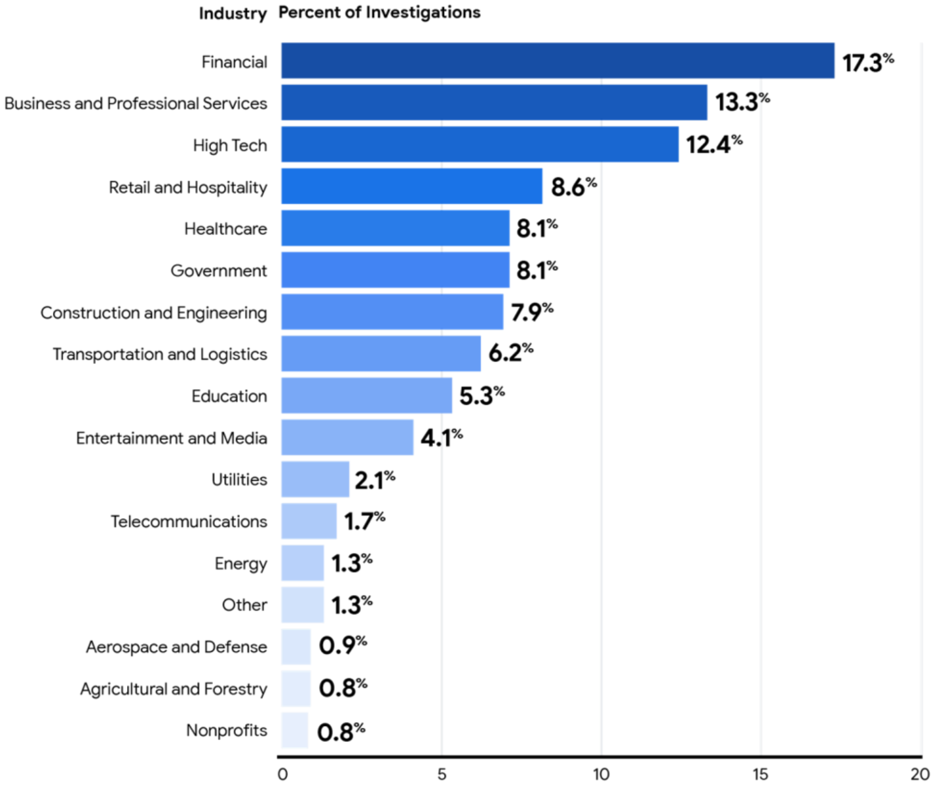
Enhancing Cyber Security with Artificial Intelligence

James Reynolds-Brown

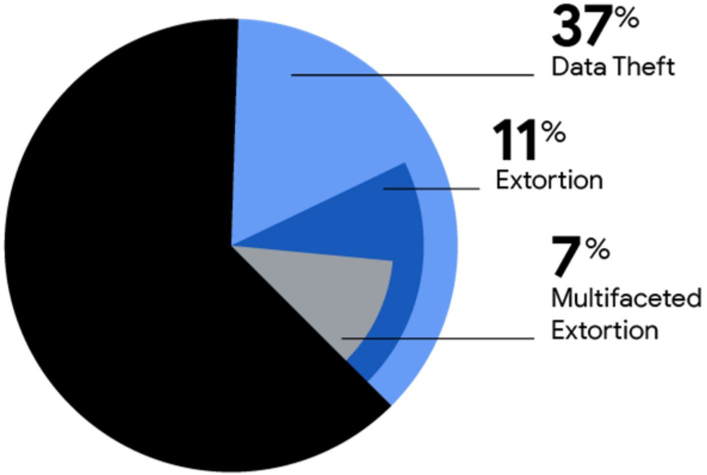
Principal consultant, EMEA Government
Mandiant Consulting, Google Cloud

Cyber Threats: bigger and badder

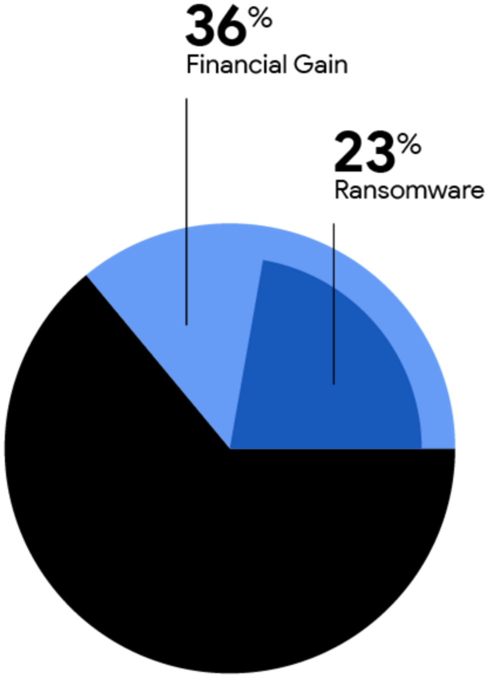
- The top four most targeted industries in this reporting period are financial services, business services, high tech, and retail and hospitality
- 626 new malware families tracked.
- Median dwell time increased to 22 days in 2023 throughout EMEA.
- 22% of intrusions related to ransomware — a significant increase compared to only 7% in 2022.x



Adversary mission objectives

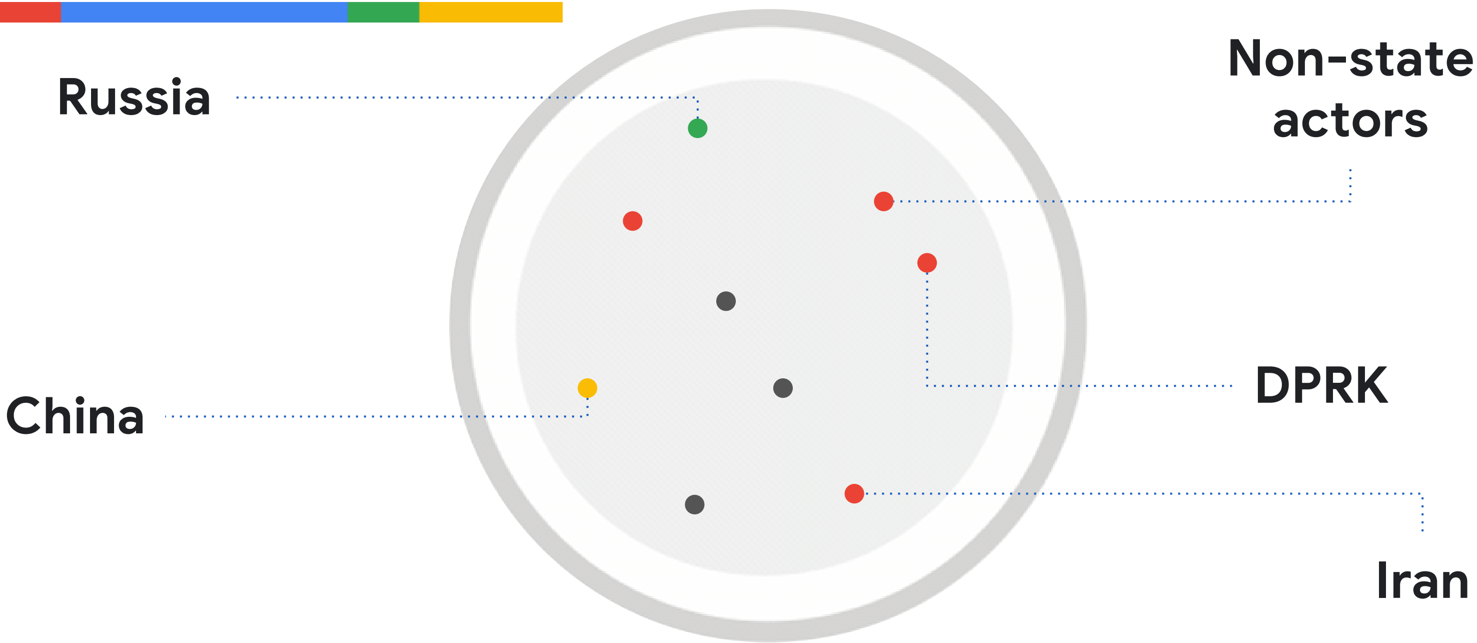


Data theft



Financial gain

Threat Picture



…cyber espionage poses an almost continuous and serious threat to NATO member states…

Google Cloud

Adversarial use of AI

Deception and Fraud

- Attackers are using AI to help bypass Know Your Customer (KYC) requirements
- Deepfake audio and video
- Tricking biometric verification tools

Augmenting attacks

- Accelerating code development
- Identifying vulnerabilities
- Target selection
- Information operations

Threat to AI models

- Increasing number of compromises against cloud-based identities configured with MFA
- Attackers are overcoming MFA with techniques (web proxy or adversary-in-the-middle (AiTM) phishing pages) that can render MFA

Defender
Attackers

The Defender's Dilemma or a Golden Opportunity?

Google Cloud

What is Google doing?

Secure AI Framework

Enabling a safer ecosystem

Educational Programmes

Expanding our $15 million Cybersecurity Seminars Program

Open source tools

Including Magika, a new AI-powered tool to aid defenders

Frontier Models Forum

Advancing frontier AI safety with industry partners

Mandiant

Thank you

Google Cloud