Business Reporter: Sekoia.io warns of rising threat from sophisticated Phishing-as-a-Service platforms

What controls must businesses put in place to fend off adversary-in-the-middle techniques?

LONDON, UNITED KINGDOM, September 12, 2025 /EINPresswire.com/ -- In an article published on Business Reporter, cybersecurity solutions provider Sekoia.io talks about how cybercriminals and nation states are weaponizing adversary-in-the-middle (AitM) techniques to intercept authentication sessions in real time in order to compromise corporate cloud accounts. Sekoia.io also makes suggestions regarding the controls that businesses must implement to minimise their exposure to this new attack vector.

Cyber-criminals are stepping up their attacks on businesses worldwide by exploiting a new wave of phishing techniques designed to bypass even multi-factor authentication (MFA). New global research from Sekoia.io's Threat Detection & Research team shows how AitM phishing – now available through Phishing-as-a-Service (PhaaS) platforms – has become a powerful tool for fraudsters.

The study, covering January to April 2025, identified eleven major phishing kits that are actively targeting corporate cloud accounts, particularly Microsoft 365 and Google. Once compromised, accounts are often used for business email compromise (BEC), financial fraud and ransomware attacks. Unlike traditional phishing, which steals passwords, AitM attacks intercept login sessions in real time. This allows criminals to hijack accounts without needing additional verification codes. Sekoia.io highlights Tycoon 2FA, EvilProxy and Evilginx among the most dangerous platforms, with Tycoon 2FA emerging as the most widespread. AitM packages typically costing $100 per month come with ready-to-use templates, campaign management tools and even customer support for attackers.

Sekoia.io suggests that to strengthen cyber defences against AitM attacks, security teams must prioritise monitoring authentication anomalies, implement advanced email security solutions capable of detecting malicious attachments and establish incident response procedures designed for these scenarios.

To learn more about how to increase your business's security against AitM attacks, read the article.

About Business Reporter

Business Reporter is an award-winning company producing supplements published in The Guardian and City AM, as well as content published on Business Reporter online hubs on Bloomberg.com, Independent.com, Business Insider Germany and Le Figaro, delivering news and analysis on issues affecting the international business community. It also hosts conferences, debates, breakfast meetings and exclusive summits.

www.business-reporter.co.uk

About Sekoia.io

Sekoia.io is the European cybersecurity technology company, leading provider of detection and response solutions boosted by AI and Cyber Threat Intelligence. By combining threat anticipation through knowledge of attackers with automation of detection and response, the Sekoia AI SOC platform provides security teams a unified view and total control over their information systems. Its open approach and interoperability with third-party solutions enable organizations to take full advantage of their existing technologies. Sekoia.io gives its customers the means to focus their human resources on high value-added missions, optimize their cyber-defense strategy and regain the advantage against advanced cyber threats.

https://www.sekoia.io/

Business Reporter
Press
+ +44 20 8349 6488
email us here