

AI-Driven Identity Attacks: From Phishing to Session Hijacking

Toni Nakovski

Faculty of ICT-Bitola

University St. Kliment Ohridski Bitola

Bitola, R. of N.Macedonia

toni.nakovski@uklo.edu.mk

Natasha Blazheska-Tabakovska

Faculty of ICT-Bitola

University St. Kliment Ohridski Bitola

Bitola, R. of N.Macedonia

natasa.tabakovska@uklo.edu.mk

Abstract—Identity-based attacks have become the primary vector for cyber intrusions, fundamentally shifting the cybersecurity landscape from the exploitation of software vulnerabilities to the compromise of valid user accounts. This paper presents an empirical analysis of a 15-month dataset collected from a managed Security Operations Center (SOC) comprising 10,046 incidents across 31 organisations spanning multiple sectors, including hospitality, shipping, real estate, nongovernmental organisations (NGOs) and financial services. The results indicate that identity-related incidents account for 35.9% of total SOC activity, with a notable increase in both the volume and the sophistication of phishing attacks observed in early 2026. These findings are examined in the context of the evolving threat landscape, highlighting the role of generative artificial intelligence in enabling highly convincing, multi-stage phishing campaigns capable of bypassing Secure Email Gateways (SEGs). The paper further analyses post-compromise techniques, including the creation of malicious inbox rules and Business Email Compromise (BEC). Finally, the paper outlines key defensive measures, emphasising phishing-resistant Multi-Factor Authentication (MFA) and Identity Threat Detection and Response (ITDR) as essential components of modern cybersecurity.

Keywords—identity-based attacks; account takeover; phishing; generative AI; secure email gateway evasion; Business Email Compromise; SOC telemetry; ITDR; phishing-resistant MFA