Title: Unveiling Zero-Click Attacks: Mapping MITRE ATT&CK Framework for Enhanced Cybersecurity

Authur names: Md Shohel Rana , Tonmoy Ghosh , Mohammad Nur Nobi , Anichur Rahman , Andrew H. Sung

Abastact : Zero-click attacks represent an advanced cybersecurity threat, capable of compromising devices without user interaction. High-profile examples such as Pegasus, Simjacker, Bluebugging, and Bluesnarfing exploit hidden vulnerabilities in software and communication protocols to silently gain access, exfiltrate data, and enable long-term surveillance. Their stealth and ability to evade traditional defenses make detection and mitigation highly challenging. This paper addresses these threats by systematically mapping the tactics and techniques of zero-click attacks using the MITRE ATT&CK framework, a widely adopted standard for modeling adversarial behavior. Through this mapping, we categorize real-world attack vectors and better understand how such attacks operate across the cyber-kill chain. To support threat detection efforts, we propose an Active Learning-based method to efficiently label the Pegasus spyware dataset in alignment with the MITRE ATT&CK framework. This approach reduces the effort of manually annotating data while improving the quality of the labeled data, which is essential to train robust cybersecurity models. In addition, our analysis highlights the structured execution paths of zero-click attacks and reveals gaps in current defense strategies. The findings emphasize the importance of forward-looking strategies such as continuous surveillance, dynamic threat profiling, and security education. By bridging zero-click attack analysis with the MITRE ATT&CK framework and leveraging machine learning for dataset annotation, this work provides a foundation for more accurate threat detection and the development of more resilient and structured cybersecurity frameworks.

Keywords: Bluebugging; bluesnarfing; cybersecurity; MITRE ATT&CK; pegasus; simjacker; zero-click attacks

10.32604/cmc.2025.069212

https://www.sciencedirect.com/org/science/article/pii/S1546221825010525