

ABSTRAK

Keamanan dalam komunikasi data menjadi perhatian global yang semakin besar, terutama di era perangkat nirkabel yang terkoneksi secara luas. Salah satu teknologi yang banyak digunakan adalah Bluetooth. Meskipun Bluetooth memudahkan transfer data antar perangkat, teknologi ini juga menyimpan beberapa potensi kerentanan yang serius. Beberapa kelemahan pada protokol Bluetooth, terutama yang memungkinkan serangan dengan melakukan *pairing* atau “zero-click” menjadi perhatian utama dalam keamanan siber. Penelitian ini mengevaluasi kerentanan pada protokol Bluetooth dengan memanfaatkan teknik serangan *Keystroke Injection* menggunakan *tools* bernama *Blue Ducky*. Fokus utama penelitian ini adalah mempelajari serangan yang memanfaatkan kelemahan dalam proses *pairing* Bluetooth untuk mendapatkan kendali atas perangkat target. Melalui pengujian berbagai skenario serangan, penelitian ini mengevaluasi seberapa efektif *Blue Ducky* dalam menyisipkan perintah pengetikan secara langsung, menunjukkan bagaimana *zero-click* dapat digunakan untuk mengambil alih perangkat yang rentan.

Hasil penelitian menunjukkan bahwa serangan *Keystroke Injection zero-click BlueDucky* berhasil pada perangkat Xiaomi Redmi Note 9 Pro, Samsung A9, dan Xiaomi Redmi 8, dengan rata-rata waktu respons 29.5 detik. Namun, perangkat Samsung SM-A715F dan Samsung A25 secara konsisten menolak serangan karena mekanisme keamanan bawaan yang aktif memblokir koneksi mencurigakan. Temuan ini menyimpulkan bahwa kerentanan *zero-click* sangat dipengaruhi oleh implementasi keamanan vendor dan versi sistem operasi Android.

Kata kunci : Bluetooth, *Blue Ducky*, *Keystroke Injection*, *Penetration Testing*, *Zero-click*.

ABSTRACT

Security in data communications is a growing global concern, especially in the era of widespread wireless connectivity. One widely used technology is Bluetooth. While Bluetooth facilitates data transfer between devices, it also harbors several potentially serious vulnerabilities. Several weaknesses in the Bluetooth protocol, particularly those that allow pairing or “zero-click” attacks, are a major concern in cybersecurity. This research evaluates vulnerabilities in the Bluetooth protocol by utilizing the Keystroke Injection attack technique using a tool called Blue Ducky. The primary focus of this research is to study attacks that exploit weaknesses in the Bluetooth pairing process to gain control of a target device. By testing various attack scenarios, this research evaluates Blue Ducky’s effectiveness in inserting direct typing commands, demonstrating how zero-click attacks can be used to take over vulnerable devices.

The results show that the BlueDucky zero-click Keystroke Injection attack was successful on Xiaomi Redmi Note 9 Pro, Samsung A9, and Xiaomi Redmi 8 devices, with an average response time of 29.5 seconds. However, the Samsung SM-A715F and Samsung A25 devices consistently resisted the attack due to built-in security mechanisms actively blocking suspicious connections. These findings conclude that zero-click vulnerabilities are heavily influenced by vendor security implementations and Android operating system versions.

Kata kunci : Bluetooth, *Blue Ducky*, *Keystroke Injection*, *Penetration Testing*, *Zero-click*.