INTISARI

ANALISIS KERENTANAN SISTEM OPERASI *WINDOWS* 10 DAN 11 MENGGUNAKAN *USB RUBBER DUCKY*

Prama Yugas Nurhakim

21/474280/SV/18892

Pada era digital saat ini, sistem operasi Windows, khususnya Windows 10 dan Windows 11, menjadi platform utama bagi pengguna komputer desktop. Namun, seiring berakhirnya dukungan Windows 10 pada Oktober 2025, serta tetap adanya kerentanan pada Windows 11, ancaman keamanan terhadap kedua sistem operasi ini semakin nyata. Penelitian ini mengkaji efektivitas serangan Rubber Ducky berbasis mikrokontroler ATtiny85 dibandingkan dengan USB Flashdrive konvensional.

Pengujian dilakukan pada 50 PC di laboratorium Universitas Gadjah Mada dengan sistem operasi Windows 10 Pro dan Windows 11 Pro. Hasil menunjukkan bahwa Rubber Ducky mampu melakukan injeksi keystroke secara otomatis tanpa deteksi oleh sistem, khususnya pada OS versi 22H2 ke atas, sementara kegagalan terjadi pada versi lama seperti 1703. Keberhasilan Rubber Ducky disebabkan oleh pengenalannya sebagai perangkat Human Interface Device (HID), sehingga lolos dari deteksi keamanan standar seperti antivirus bawaan sistem yaitu Windows Defender. Sebagai solusi preventif, disarankan implementasi interupsi input, pembatasan port USB, serta penguatan proteksi antivirus untuk mencegah potensi serangan serupa di masa depan.

Kata Kunci: *Rubber Ducky, Windows* 10*, Windows* 11*,* Keamanan Siber*, Human Interface Device (HID), Keystroke Injection*

ABSTARCT

VULNERABILITY ANALYSIS OF WINDOWS 10 AND 11 OPERATING SYSTEMS USING USB RUBBER DUCKY

Prama Yugas Nurhakim

21/474280/SV/18892

In the digital era, Windows operating systems, particularly Windows 10 and Windows 11, have become the primary platforms for desktop computer users. However, with the end of Windows 10 support scheduled for October 2025 and the ongoing vulnerabilities present in Windows 11, security threats to both operating systems are becoming increasingly evident. This study examines the effectiveness of Rubber Ducky attacks based on the ATtiny85 microcontroller compared to conventional USB flash drives.

Testing was conducted on 50 PCs at the Universitas Gadjah Mada laboratory, all running Windows 10 Pro and Windows 11 Pro. The results show that Rubber Ducky was able to perform automatic keystroke injection without system detection, particularly on OS versions 22H2 and newer, while failures occurred on older versions such as 1703. The success of Rubber Ducky is attributed to its recognition as a Human Interface Device (HID), allowing it to bypass standard security detection such as the built-in antivirus, Windows Defender. As preventive solutions, the implementation of input interruption, USB port restrictions, and strengthening antivirus protection are recommended to mitigate the potential for similar attacks in the future.

Keywords : *Rubber Ducky, Windows 10, Windows 11, Cybersecurity, Human Interface Device (HID), Keystroke Injection*