Rancang Bangun Framework Command and Control Berbasis PowerShell dan Injeksi USB Digispark untuk Uji Penetrasi = Development of a PowerShell-Based Command and Control Framework with Digispark USB Injection for Penetration Testing

Raden Bagus Senopati Kresna Ramdani Galih Rahayu, author

Abstrak

Penelitian ini merancang dan menguji framework serangan siber berbasis keystroke injection (Digispark) dan fileless PowerShell, sekaligus mengembangkan metode penangkalannya berbasis deteksi anomali perilaku. Diuji pada berbagai skenario Windows 10 dan 11, framework ini berhasil menjalankan seluruh tahapan serangan, mulai dari injeksi perintah otomatis hingga pemasangan backdoor persisten, bahkan saat Windows Defender aktif. Analisis kuantitatif menunjukkan performa waktu yang efisien pada Windows 10 (hingga 31,56% lebih cepat dari standar USENIX), namun memiliki jejak memori yang kontras: sangat tinggi saat instalasi (133 MB, 166% lebih berat dari acuan) yang rentan terdeteksi, tetapi sangat ringan saat per- sistensi (20 MB, 59% lebih efisien) sehingga sulit dilacak. Metode penangkal yang dirancang terbukti berhasil memblokir serangan pada semua skenario, mengonfir- masi bahwa mitigasi berbasis deteksi kecepatan input merupakan pertahanan yang efektif terhadap ancaman sejenis.
.....This research designs and tests a cyber attack framework based on keystroke in- jection (Digispark) and fileless PowerShell, while also developing a countermea- sure based on behavioral anomaly detection. Tested across various Windows 10 and 11 scenarios, the framework successfully executed all attack stages, from au- tomatic command injection to persistent backdoor installation, even with Windows Defender active. Quantitative analysis reveals efficient time performance on Win- dows 10 (up to 31.56% faster than the USENIX standard), but with a contrasting memory footprint: a high usage during installation (133 MB, 166% heavier than the benchmark) makes it vulnerable to detection, yet a very low usage during per- sistence (20 MB, 59% more efficient) makes it difficult to track. The designed countermeasure proved successful in blocking the attack in all scenarios, confirm- ing that mitigation based on input speed detection is an effective defense against similar threats.