RX-INT: Kernel and Hypervisor-Level Instrumentation for Stealthy Memory-Resident Payload Detection and Extraction

Arjun Juneja
School of Electronics and Computer Science
University of Southampton
Southampton, United Kingdom
aj2g24@soton.ac.uk

***Abstract*—RX-INT, a kernel-level driver for reliably detecting and dumping manually mapped or reflective DLLs and shellcode in protected Windows processes. The approach uses documented and undocumented kernel callbacks (thread tracking, VAD traversal), user-mode ETW telemetry, and an optional hypervisor-based trap to capture executable pages before they self-destruct or evade traditional detection. I implement and evaluate RX-INT in a Windows 11 environment, achieving relatively low overhead and high coverage against common anti-reverse-engineering techniques.**

***Index Terms*—Windows security, manual mapping, kernel driver, memory forensics, VAD, ETW, hypervisor, reverse engineering**

References