THE EVOLUTION OF VOLATILE MEMORY FORENSICS

ANGGOTA KELOMPOK

2501963822 Josua Abraham
2502009412 Ramadhana Khalaf Sandhyakala
2502001441 Ayubi Sholahudin
2502018480 Carlson King
2501991536 Vaustin

TUJUAN PAPER

Memberikan survei komprehensif tentang alat dan teknik mutakhir untuk akuisisi memori volatil dan analisis untuk identifikasi malware.

VOLATILE MEMORY

Memori volatil adalah Random Access Memory (RAM) dari sistem komputer, yang berisi informasi berharga tentang keadaan, proses, dan aktivitas sistem.

VOLATILE MEMORY

DI SISI LAIN

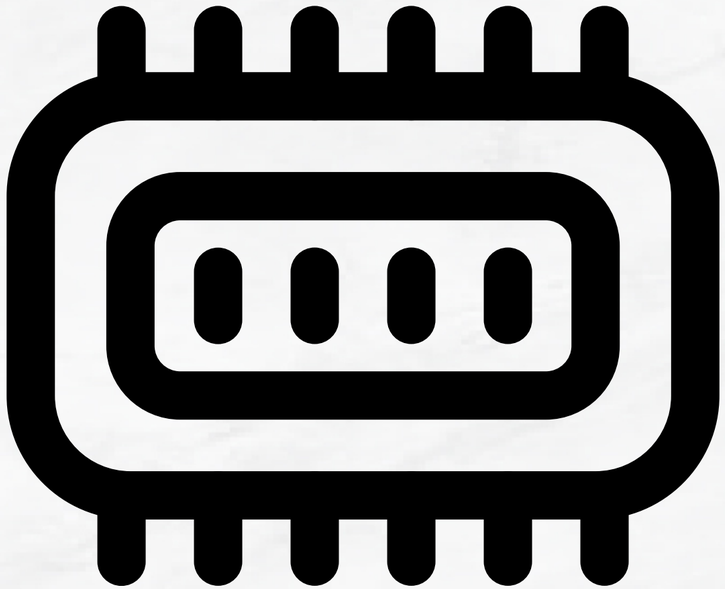
Memori volatil juga bersifat sementara, yang berarti bahwa memori ini akan hilang ketika sistem dimatikan atau di-boot ulang.

FORENSIK MEMORI VOLATIL

MAKA DIBUTUHKAN

Proses menangkap dan menganalisis konten memori volatil untuk mendeteksi dan menyelidiki ancaman siber, seperti malware tanpa file, yang tidak meninggalkan jejak apa pun dalam sistem file.

Dua Metode Volatile Memory Forensics



MEMORY ACQUISITION METHODS

Pada paper dijelaskan tentang berbagai cara untuk mendapatkan snapshot memori volatil, seperti metode berbasis perangkat keras, berbasis perangkat lunak, dan berbasis hypervisor. Paper ini juga mengevaluasi pertukaran di antara metode-metode ini dalam hal kualitas snapshot, overhead kinerja, dan keamanan.

MEMORY ANALYSIS METHODS

Pada paper ini juga dijelaskan tentang berbagai teknik untuk menganalisis snapshot memori untuk mengidentifikasi malware dan aktivitas berbahaya lainnya, seperti metode berbasis tanda tangan, metode dinamis yang dilakukan di lingkungan sandbox, dan metode berbasis pembelajaran mesin. Paper ini juga merangkum alat yang saat ini tersedia untuk analisis memori, dan membandingkan fitur dan keterbatasannya.

Tantangan dan Kesempatan

Mengidentifikasi kesenjangan penelitian utama dan masalah terbuka dalam forensik memori yang mudah menguap, seperti berurusan dengan enkripsi, kompresi, dan fragmentasi memori, meningkatkan akurasi dan efisiensi analisis memori, dan mengembangkan aplikasi baru dan kasus penggunaan untuk forensik memori yang mudah menguap.

THANK YOU!!