VOLATILE MEMORY FORENSICS

Kelompok:

2540123403 – Bertrand Redondo Mulyono

2502064303 – Betrand Gabrialdi Leonard

2540125024 – Felysia Meytri

2540123100 – Victor Benaya

INTRODUCTION

- Volatile memory: jenis memori yang kehilangan data yang disimpan di dalamnya saat daya dimatikan atau sistem dimatikan.
- "volatile" :data yang tidak dapat dipertahankan secara permanen. Contoh: Random access memory (RAM)
- Jurnal ini membahas pentingnya analisis volatile memory khususnya RAM, dalam mengidentifikasi ancaman siber.
- Data yang tersimpan dalam RAM dapat memberikan wawasan forensik yang berharga, termasuk fragmen konten berkas terenkripsi, daftar proses yang berjalan, dan daftar koneksi jaringan.
- Hal ini sulit diekstrak dari sistem berkas karena penggunaan enkripsi disk penuh dan tindakan perlindungan lainnya. Namun, melalui analisis memori volatil, informasi yang tersembunyi ini dapat diekstrak dalam format yang tidak terenkripsi.

Literature Review

- **Memory Acquistion**
- **Volatility Memory Analysis**

Memory Acquistion

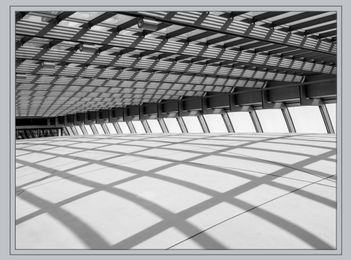
Discuss about tools to determine the correctness of memory acquistion method and surveys about analysis method in Windows.

Memory Analysis

Discuss about types of fileless malware and their problem with the methods to analyze the malware memory address

Memory Acquisition

Dalam Penelitan ini, *Memory Acqusition* merujuk pada proses pengumpulan data dari *Volatile Memory* seperti RAM dalam sebuah sistem komputer. Didalam paper, membahas bagaimana cara *Memory Acquisition* dilakukan dengan menggunakan metode Taxonomy yang terbagi menjadi beberapa level.

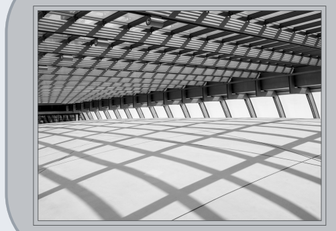


1. User Level
2. Kernel Level
3. Hypervisor Level
4. SMM (System Management Mode)
5. Asynchronous Device Level

Memory Analysis

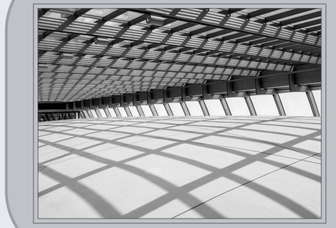
Setelah proses Memory Acqusition, langkah selanjutnya ialah Memory Analysis. Untuk mengidentifikasi informasi yang relevan. Ada beberapa cara untuk melakukan Memory Analysis :

Tools



- Didalam paper tersebut menjelaskan penggunaan tools seperti *Volatility* dan *Rekall,* Kedua tools tersebut bisa menganalisa *memory dumps* dari Windows, Linux atau bahkan Macintosh Machines.

Traditional Methods

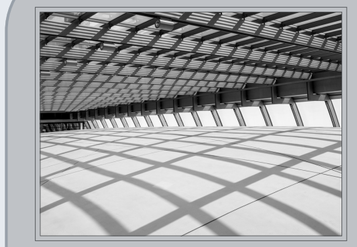


- Didalam paper tersebut menjelaskan penggunaan *Traditional Methods* untuk mengindetifikasi malware, ada dua cara yang di sebutkan yaitu *Scanning Methods* dan *Dynamic Analysis in Sandbox.*

Memory Analysis

Cara selanjutnya yang sering dilakukan adalah dengan cara:

Machine Learning



- Penggunaan Machine Learning untuk mendeteksi malware telah dilakukan dari tahun ke tahun, yang dimana memberikan tingkat kesuksesan yang tinggi sehingga sudah menguasai problem dengan lingkup yang luas.
- Machine Learning dilakukan dimana malware dijalankan dalam sistem sandbox yang dimana fitur diambil dari Memory Dump Menggunakan tools seperti Volatility atau Rekall yang dilanjutkan dengan Classification Algorithm
- Lalu didalam Paper disebutkan ada pendekatan menggunakan Computer vission, yang dimana data memory diubah menjadi graph atau gambar, lalu dilanjutkan dengan Classification Algorithm

Kesimpulan

- *Volatile Memory Acquisition* telah menjadi salah satu metode forensic yang sangat berharga.
- Terdapat tiga klasifikasi dalam *Memory Forensics*
  - *Dynamic Analysis*
  - *Scanning Method*
  - *Machine learning approach*
- Masing-masing metode tersebut memiliki keunggulan tersendiri, dengan penggunaan yang sesuai

Thank You