Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

**Jurnal Comasie**

ISSN (Online) 2715-6265

# ANALISIS DAN DETEKSI MALWARE PADA PROTOKOL JARINGAN MENGGUNAKAN METODE MALWARE ANALISIS DINAMIS DAN MALWARE ANALISIS STATIS

**Vicram Renondo Sianipar[1], Hotma Pangaribuan[2]**

[1]Mahasiswa Program Studi Teknik Informatika, Universitas Putera Batam
[2]Dosen Program Studi Teknik Informatika, Universitas Putera Batam
*email*: pb190210066@upbatam.ac.id

## ABSTRACT

*Network security is a crucial issue in the rapidly developing era of information technology. One of the main threats is malware, which is malicious software that harms systems and data. To solve this problem, analysis and detection of malware on network protocols need to be improved using effective methods. This research explores the application of two main methods, namely static and dynamic malware analysis. First, static malware analysis involves examining malware files without running them. This method includes analysis of signatures, heuristics, and malicious code to identify typical malware patterns in files on the network.Second, dynamic malware analysis executes malware in an isolated environment (sandbox) to monitor its behavior and impact on the system. This process allows detection of malicious changes and attempts by malware to propagate itself. By combining these two methods, a holistic and efficient approach in malware detection on network protocols can be achieved. It is hoped that the results of this research can improve network security, protect infrastructure from ever-evolving malware threats. The use of static and dynamic analysis methods will help deal with increasingly complex security challenges, enabling networks to operate more securely and reliably.*

***Keywords:*** *Malware; Analysis statis; Analysis Dynamis; Cuckoo Sandbox*

## PENDAHULUAN

Perkembangan teknologi telah berubah secara drastis. Peralatan pintar, seperti *smartphone*, telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari. *Internet of Things* (IoT) memungkinkan pengendalian perangkat melalui jaringan, sementara kecerdasan buatan (AI) mendorong kemajuan dibidang seperti otomatisasi, pengenalan suara, analisis data yang canggih. Teknologi baru seperti realitas virtual (VR) dan *augmented reality* (AR) memberikan pengalaman yang mendalam dan imersif. *Malware* merupakan perangkat lunak atau *software* yang diciptakan untuk meretas atau merusak sistem komputer. Banyak jenis dari *malware* yaitu *Virus, Trojan, Worm, Adware, Spyware, Ransomware, Rootkit, Keylogger, Botnet, Fileless Malware*. *Ransomware* dapat menyebar melalui metode yang sama seperti

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

*malware* lainnya, seperti melalui email phishing, situs *web* yang terinfeksi, atau eksploitasi kerentanan dalam sistem operasi atau perangkat lunak. Analisa *malware* secara umum dapat dilakukan dengan dua metode, yaitu *Dynamic Analysis*, dan *Static Analysis*. *Dynamic Analysis* dapat dilakukan menggunakan *tool* analisa otomatis yaitu *cuckoo sandbox*. *Malware Analysis Static* tidak sama seperti metode *Malware Analysis Dynamic*, dalam metode analisis statis ini file *malware* tidak akan diaktifkan secara langsung melainkan diteliti serta dianalisis terhadap kode sumber yang dituliskan didalam program *malware* dengan menggunakan tahapan pembedahan terhadap program *malware* tersebut. (Manoppo et al., 2020)

## KAJIAN TEORI

### 2.1 Jaringan Komputer

Jaringan komputer merupakan interaksi antara dua komputer *autonomous* atau lebih. (Harry Dwi Sabdho & Ulfa Maria, 2018)

### 2.2 Malware

*Malware* (*malicious software*) adalah perangkat lunak yang dirancang untuk merusak, menggangu, atau mengambil alih sistem komputer tanpa izin dari pengguna. Berikut adalah beberapa jenis *malware* yang umum ditemui (Ilhamdi & Kunang, 2021) :

1 Virus
Menempel pada file atau program dan menyebar saat file atau program tersebut dijalankan. Virus dapat merusak data bahkan menghancurkan seluruh sistem.

2. Worm
Menyebar melalui jaringan komputer dan menggandakan diri untuk menyerang perangkat lain.

3. Trojan Horse
Menyamar sebagai program yang berguna atau mengunduh tanpa izin pengguna, Trojan juga dapat membuka pintu belakang pada sistem untuk memungkinkan akses tanpa izin atau mencuri informasi.

4. Spyware
Mengumpulkan informasi tentang pengguna tanpa sepengetahuannya, Spyware sering kali digunakan untuk mencuri informasi pribadi, seperti kata sandi, data keuangan, atau riwayat penelusuran.

5. Adware
Menampilkan iklan yang tidak diinginkan kepada pengguna, Adware biasanya terpasang bersama dengan perangkat lunak gratis atau didistribusikan melalui unduhan tidak sah.

6. Keylogger
Merekam setiap ketukan tombol yang dilakukan pengguna pada perangkat termasuk kata sandi dan informasi sensitif lainnya.

7. Ransomware
Memblokir akses pengguna ke sistem atau file dengan mengenkripsi data dan meminta tebusan agar data tersebut dikembalikan

### 2.3 Tools Analisis statis

Tools yang digunakan untuk menganalisis statis. (Pan et al., 2020)

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

1. HXD Editor

Alat perangkat lunak yang digunakan untuk menganalisis dan memodifikasi berkas biner dengan format heksadesimal. (Pan et al., 2020)

2. PE Studio

Alat perangkat lunak yang dapat digunakan untuk menganalisis berkas eksekusi windows..

3. CFF Explorer

Alat perangkat lunak yang digunakan untuk memeriksa dan menganalisis berkas biner, terutama berkas eksekusi windows.

4. EXE Info

Sebuah perangkat lunak yang digunakan untuk melakukan analisis statis pada file *executable*.

5. Virustotal

Merupakan layanan online yang menyediakan pemindaian dan analisis berkas untuk mendeteksi *malware* dan ancaman keamanan lainnya.

### 2.4 Tools Analisis Dinamis

Tools yang digunakan untuk menganalisis dinamis. (Manoppo et al., 2020)

1. Virtualbox

Virtualbox merupakan perangkat lunak virtualisasi yang popular yang dikembangkan oleh *oracle,* yang memungkinkan pengguna untuk menjalankan beberapa sistem operasi di dalam satu mesin fisik tanpa memerlukan penginstalan ganda atau partisi yang rumit.

2. Linux Ubuntu

Linux ubuntu merupakan salah satu distribusi Linux yang popular dan berbasis debian, yang dirancang untuk keperluan umum dan dapat digunakan diberbagai perangkat, termasuk komputer desktop, laptop, server, dan perangkat *Internet of Things* (IoT).

3. Windows 7

Yang merupakan sistem operasi yang dikembangkan oleh Microsoft. Fitur-fitur terkenal termasuk Start Menu yang ditingkatkan, taskbar yang dioptimalkan, dan kemampuan multitasking yang baik.

4. Cuckoo Sandbox

Cuckoo Sandbox merupakan platform analisis *malware* yang berbasis pada teknologi machine learning. Platform ini dirancang untuk mendeteksi, menganalisis, dan memahami perilaku *malware* secara otomatis. Dengan menggunakan teknik pembelajaran terawasi, Cuckoo Sandbox memanfaatkan data set yang telah dilabeli dengan baik untuk melatih model dalam mengenali pola dan karakteristik yang mencurigakan dari *malware*.

5. Volatility Framework

Merupakan sebuah framework forensic memori sumber terbuka yang digunakan untuk menganilisis memori volatile (RAM) pada sistem komputer.

## METODE PENELITIAN

### 3.1 Desain Penelitian

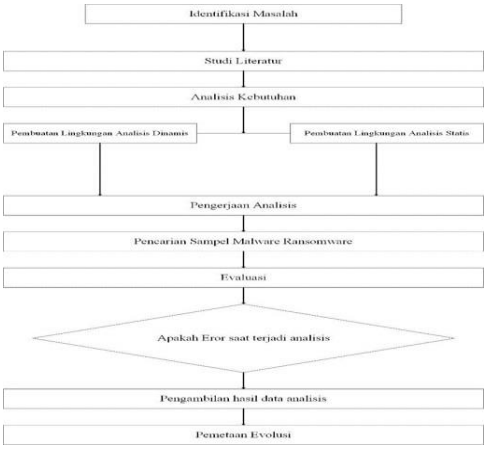
Dalam peneitian ini penulis merangcang sebuah desain sistematis analisis *malware ransomware* dengan membandingkan hasil dari kedua metode yang disimpulkan dalam perbandingan

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

tabel dengan analisis kualitatif. (Fadli, 2021)



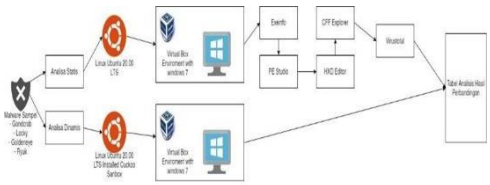

**Gambar 3.1** Desain penelitian
(Sumber: Data Penelitian, 2023)

1. Pada tahapan kedua peneliti melakukan studi literatur dari berbagai sumber dan jurnal untuk mendapatkan metode yang diterapkan.

2. Pada tahapan keempat peneliti mendapati dua metode analisis *malware ransomware* yaitu metode statis dan dinamis. Kedua metode ini diterapkan pada jenis sistem operasi yang berbeda, serta tools yang akan digunakan untuk mendukung proses kedua analisis tersebut.

3. Pada tahap kelima peneliti mengambil beberapa sampel *ransomware* yang akan digunakan untuk pengujian dari berbagai sumber.

4. Setelah mendapatkan beberapa sampel jenis *malware* pada tahap keenam peneliti mengevaluasi terlebih dahulu sampel yang akan digunakan dalam *sandbox* buatan dan terpisah dari jaringan PT NPCB untuk mengurangi resiko tersebarnya *malware ransomware* jika terjadi kesalahan.



5. Pada tahap ketujuh peneliti mengambil hasil dari beberapa tahapan dan toolsyang digunakan.

6. Pada proses tahap kedelapan meneliti, mengamati apakah ada kendala dari kedua analisis tersebut baik secara tools atau sampel yang digunakan.

7. Pada tahapan kesembilan peneliti melakukan peta evolusi perkembangan *malware* jenis *ransomware* dari tahun ke tahun.

### 3.2 Analisis Keamanan Jaringan yang berjalan

PT NPCB menggunakan komputer sebanyak 26 client dan satu server sebagai alat bantu operasional dan perangkat 4 printer sharing serta 2 mesin fotocopy untuk penunjang operasional. Implementasi jaringan menggunakan *full wired* (*ethernet wire*) sebagai media transmisi jaringan. Kapasitas *bandwidth* yang digunakan layanan dedicated 50Mbps dengan layanan *provider* jasa Batam Bintan Telekomunikasi (BBT).

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

### 3.3 Kebutuhan Sistem Analisis Ransomware

Pada rancangan analisis keamanan jaringan baru di PT NPCB team IT dan peneliti bekerja sama untuk mempelajari jenis-jenis *ransomware* khususnya jenis *Grandcrab* dan *Petya*. Dengan membuat *environment* terpisah dengan bantuan linux dan virtualbox agar selama proses analisa sampel *malware* yang akan diperiksa tidak menyebar ke lingkungan jaringan PT NPCB. Berikut topologi dari rancangan analisis keamanan yang akan diterapkan oleh peneliti:

**Gambar 3.2** Rancangan Kebutuhan Sistem Analisa *Malware Ransomware*
(Sumber Penelitian : 2023)

## HASIL DAN PEMBAHASAN

### 4.1 Hasil Penelitian Analisis Malware Statis

#### 4.1.1 Petya

Rangkuman analisa *malware ransomware* jenis petya menggunakan kode hash yang sama dan *compiler* dilakukan ditahun 2016 sesuai pada tabel diatas dan merupakan file *executable* yang berjalan di program berbasis 32 bit dan bukan merupakan paket dengan skor potensi bahaya 65/71 dari virustotal.

**Tabel 4.1** Rangkuman Analisa Petya Metode Statis

| Tool | Variabel | Value |
|---|---|---|
| PE Studio | Nama | Petya |
| | MD5 | A92F13F3A1B3B39833D3CC336301B713 |
| | SHA-1 | D1C62AC62E68875085B62FA651FB17D4D7313887 |
| | SHA-256 | 4C1DC737915D76B7CE579ABDDABA74EAD6FDB5B519A1EA45308B8C49B950655C |
| | Compiler-Stamp | Sat Jan 30 02:56:43 2016 |
| | Section | 5 |
| | Processor 32 bit | *TRUE* |
| | Executable | *TRUE* |
| EXEinfo PE | Paket | *Not Package* |
| Virustotal | Skor | 65/71 |

(Sumber Penelitian : 2023)

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

### 4.1.2 Grandcab

Pada hasil menggunakan tools maka ditemukan kesimpulan kode hash yang digunakan *malware* sama dengan beberapa tools lain. *Compiler stamp* juga menunjukkan *malware* ini dibuat ditahun 2016, bukan merupakan paket. Kemudian berjalan di 32 bit sistem dan berformat *executable* atau *windows only*. Selanjutnya pada virustotal memberikan skor 63/71, dengan potensi serangan yang besar dan berbahaya.

## 4.2 Hasil penelitian Analisis Malware Dinamis

### 4.2.1 Petya

Pada gambar 4.1 menunjukkan *process tree* dari *malware* petya ini memiliki satu proses dengan menginfeksi 9 bagian file dengan penyerangan dimulai dengan proses registy, file, services, dan synchronisatiton yang berarti proses infeksi *malware* ini dilakukan pada tahap registy dan mengkripsi file tanpa mengunduh file yang bisa dilihat pada bagian droped file hanya mengkripsi file yang berada pada local harddisk tersebut.

**Tabel 4.2** Rangkuman Analisa Grandcab Metode Statis

| Tool | Variabel | Value |
|---|---|---|
| PE Studio | Nama | Grandcab |
| | MD5 | 97A449FED7D800A8A635592605FF8A67 |
| | SHA-1 | 2F339D8B2EDB7C07126D9A3C37EFFE14966817C5 |
| | SHA-256 | 233437B647F9482A8A3BA51D0AF69039BB58FB48609704A39 DB1F709A0E6ACA6 |
| | Compiler-Stamp | Sat Jan 30 02:56:43 2016 |
| | Section | 5 |
| | Processor 32 bit | TRUE |
| | Executable | TRUE |
| EXEinfoPE | Paket | Not Packed |
| Virustotal | Skor | 63/71 |

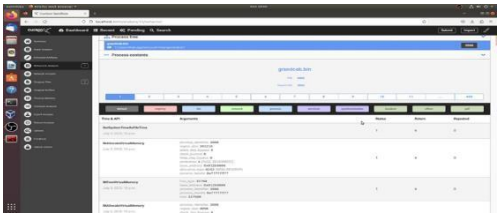
(Sumber Peneitian :2023)

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

**Jurnal Comasie**

ISSN (Online) 2715-6265

**Gambar 4.1** Process Tree Petya Metode Dinamis
(Sumber Penelitian : 2023)



### 4.2.2 Grandcab

**Gambar 4.2** Process Tree Grandcab Metode Dinamis
(Sumber Penelitian 2023)

Pada gambar 4.2 didapatkan *process tree* pada *malware* Grandcab ini hanya satu proses kemudian menginfeksi 9 tahapan, serangan dilakukan melalui registy, file, process, dan *synchronization* yang artinya serangan ini melakukan manipulasi pada registy *windows* dan mengenkripsi file tersebut.

### 4.3 Perbedaan Kedua Analisis

Perbedaan diantara kedua analisa ini adalah dimana pada analisa statis peneliti berusaha menyimpulkan satu per satu *process tree* dan komponen dari kedua sampel *malware* tersebut. Sedangkan pada analisa *malware* dinamis melakukan virtualisasi dari serangan tersebut sehingga proses debug dan *signatures* dapat dianalisa. Dari kedua analisa tersebut proses dinamis lebih efektif dibanding dengan statis dimana saat melakukan analisa statis peneliti harus memiliki teknik khusus dalam membaca alur serangan dan ancaman *malware* tersebut.

## SIMPULAN

Analisa *malware* dengan menggunakan statis lebih membutuhkan keterampilan yang sangat kompleks dan analisis yang mendetail tentang struktur dari jenis serangan tersebut.

Analisa *malware* dengan menggunakan metode dinamis dilakukan dengan melakukan simulasi di lingkungan tertutup dengan memperhatikan dampak dari jenis *malware ransomware* tersebut.

Dari kedua metode yang dilakukan bahwasanya teknik analisa dinamis lebih efisien digunakan dibandingkan dengan metode statis.

## DAFTAR PUSTAKA

Fadli, M. R. (2021). Memahami desain metode penelitian kualitatif. *Humanika*, *21*(1), 33–54. https://doi.org/10.21831/hum.v21i1.38075

Harry Dwi Sabdho, & Ulfa Maria. (2018). Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

**Jurnal Comasie**

ISSN (Online) 2715-6265

PT. Mora Telematika Indonesia Regional Palembang. *Semhavok*, *1*(1), 15–24.

Ilhamdi, Y., & Kunang, Y. N. (2021). Analisis Malware Pada Sistem Operasi Windows Menggunakan Teknik Forensik. *Bina Darma Conference on Computer Science*, *3*, 256–264. https://conference.binadarma.ac.id/index.php/BDCCS/article/view/2124

Manoppo, V. A., Lumenta, A. S. ., & Karouw, S. D. . (2020). Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi. *Jurnal Teknik Elektro Dan Komputer*, *9*(3), 181–188.

Pan, Y., Ge, X., Fang, C., & Fan, Y. (2020). A Systematic Literature Review of Android Malware Detection Using Static Analysis. *IEEE Access*, *8*, 116363–116379. https://doi.org/10.1109/ACCESS.2020.3002842


| | |
|---|---|
|  | Penulis pertama, Vicram Renondo Sianipar, merupakan mahasiswa Prodi Teknik Informatika Universitas Putera Batam |
|  | Penulis kedua, Hotma Pangaribuan, merupakan Dosen Prodi Teknik Informatika Universitas Putera Batam. |