# “Laporan Hasil Analisis *Malware AsyncRAT* Berdasarkan Perilaku dalam Sistem Windows 11 Menggunakan Metode *Hybrid*”

**TUGAS AKHIR**

Oleh:

Satria Afif Ramdani – 4332111005

Disusun untuk Tugas Akhir Program Diploma IV


**PROGRAM STUDI REKAYASA KEAMANAN SIBER**
**JURUSAN TEKNIK INFORMATIKA**
**POLITEKNIK NEGERI BATAM**

**2026**

## 1. ANALYSIS ENVIRONMENT SPECIFICATION

Lingkungan analisis dirancang untuk menyediakan lingkungan yang terisolasi agar proses analisis malware dapat dilakukan denga aman tanpa mempengaruhi sistem host.

| Komponen | Spesifikasi |
|---|---|
| **Hypervisor** | Oracle VM VirtualBox |
| **Guest Operation System** | Windows 11 64-bit |
| **RAM** | 4096 MB |
| **Processor** | 2 vCPU |
| **Storage** | 80 GB Virtual Disk |
| **Network Config** | NAT adapter disconnected during malware execution |
| **Isolation Mechanism** | No shared folder, no USB passthrough |

## 2. MALWARE SAMPLE IDENTITY

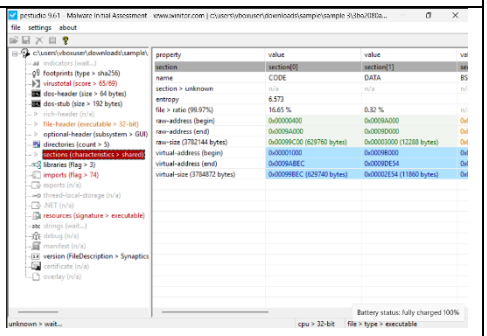
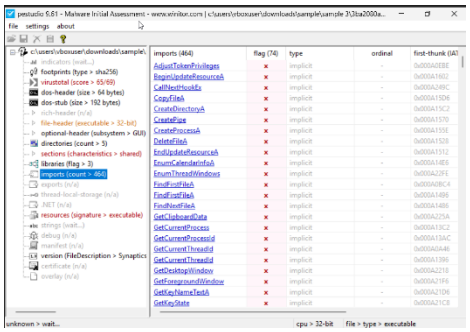
Sampel yang dikumpulkan berupa sampel malware AsyncRAT yang diperoleh dari platform MalwareBazaar. Rangkuman informasi mengenai sample tersebut adalah sebagai berikut:

| Komponen | Malware Sample 1 | Malware Sample 2 |
|---|---|---|
| **File Name** | 3ba2080a5a4791a7a8c5ea42ac40826bfca758f3abea4da90d3f22fbc50c2d60.exe | 3758bbe67d3bb290e49a4317881084eb64e1e4228af281382059d4ad0e5c11c1.exe |
| **SHA256** | 3ba2080a5a4791a7a8c5ea42ac40826bfca758f3abea4da90d3f22fbc50c2d60 | 3758bbe67d3bb290e49a4317881084eb64e1e4228af281382059d4ad0e5c11c1 |
| **File Size** | 209 KB | 783 KB |
| **Source** | MalwareBazaar | MalwareBazaar |

## 3. STATIC ANALYSIS

Analisis statis dilakukan di dalam lingkungan terisolasi virtual dengan tanpa menjalankan sampel malware. Indikator yang diamanti diantaranya yaitu Entropy, indikator persistence, indikator file system, process activity, dan memory/process manipulation. Kedua file executable (.exe) sampel dimasukkan ke dalam PEStudio dan diperoleh hasil sebagai berikut:

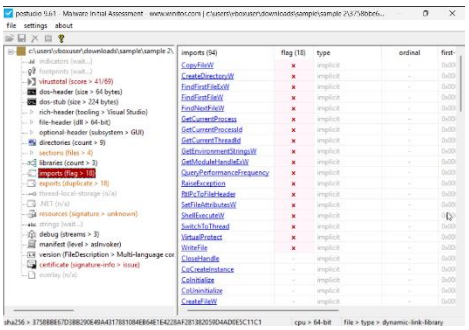
### 3.1 Sample 1 Static Analysis

| Indikator | Evidence | Screen Capture |
|---|---|---|
| **Entropy** | 6.573 |  |
| **Persistence Indicator** | Inkonklusif | - |
| **File System Indicator** | `CopyFileA`, `CreateDirectoryA`, `DeleteFileA` |  |
| **Process Activity** | `CreateProces`, `CreatePipe` | |
| **Memory/Process Manipulation** | `AdjustTokenPrivileges`, `CallNextHookE`, `GetKeyState`, `GetClipboardData` | |

| **Sample 1 Static Analysis Summary** |
|---|
| Hasil analisis statis menunjukkan bahwa Sampel 1 memiliki nilai entropy sebesar 6,573, yang menunjukkan tingkat keacakan (randomness) distribusi byte yang relatif tinggi. Nilai tersebut dapat mengindikasikan adanya penggunaan teknik packing, compression, atau encryption untuk menyamarkan kode berbahaya.<br><br>Pada analisis indikator persistensi, bagian Strings pada PEStudio tetap berada dalam status "waiting" dan tidak menampilkan hasil. Oleh karena itu, identifikasi mekanisme persistensi pada Sampel 1 menghasilkan temuan yang inkonklusif.<br><br>Pada indikator File System, ditemukan API `CopyFileA`, `CreateDirectoryA`, dan `DeleteFileA`, yang menunjukkan potensi kemampuan sampel untuk menyalin file, membuat direktori, dan menghapus file. |

Sementara itu, pada indikator Memory/Process Manipulation, ditemukan API `AdjustTokenPrivileges`, `CallNextHookEx`, `GetKeyState`, dan `GetClipboardData`. API tersebut menunjukkan potensi kemampuan yang berkaitan dengan pengaturan hak akses (privilege) proses, mekanisme hooking, pemantauan status tombol keyboard, serta akses terhadap data yang tersimpan pada clipboard.

### 3. 2 Sample 2 Static Analysis

| Indikator | Evidence | Screen Capture |
|---|---|---|
| **Entropy** | 6.417 | |
| **Persistence Indicator** | Inkonklusif | - |
| **File System Indicator** | `CopyFileW, CreateDirectoryW, FindFirstFileExW, FindNextFileW, WriteFile` |  |
| **Process Activity** | `ShellExecuteW` | |
| **Memory/Process Manipulation** | `VirtualProtect` | |

**Sample 2 Static Analysis Summary**

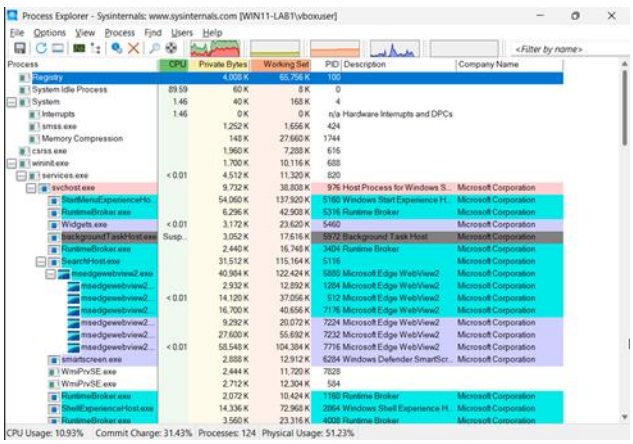
Hasil analisis statis menunjukkan bahwa Sampel 2 memiliki nilai entropy sebesar 6,417, yang menunjukkan tingkat keacakan (randomness) distribusi byte yang relatif tinggi. Nilai tersebut dapat mengindikasikan adanya penggunaan teknik packing, compression, atau encryption untuk menyamarkan kode berbahaya

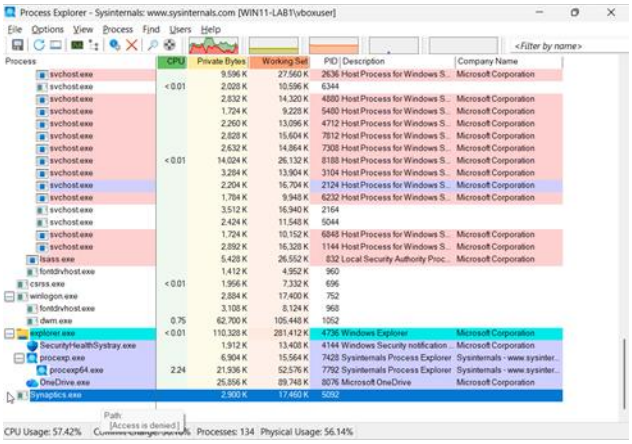
Pada indikator File System, ditemukan API `CopyFileW`, `CreateDirectoryW`, `FindFirstFileExW`, `FindNextFileW`, dan `WriteFile`. API tersebut menunjukkan potensi kemampuan sampel untuk menyalin file, membuat direktori, melakukan pencarian atau enumerasi file dan direktori, serta menulis data.

Pada indikator Memory/Process Manipulation, ditemukan API `VirtualProtect` yang memungkinkan program mengubah izin akses pada area memori. Dalam konteks malware, fungsi ini dapat mendukung aktivitas seperti eksekusi kode di memori atau code injection.

## 4. DYNAMIC ANALYSIS

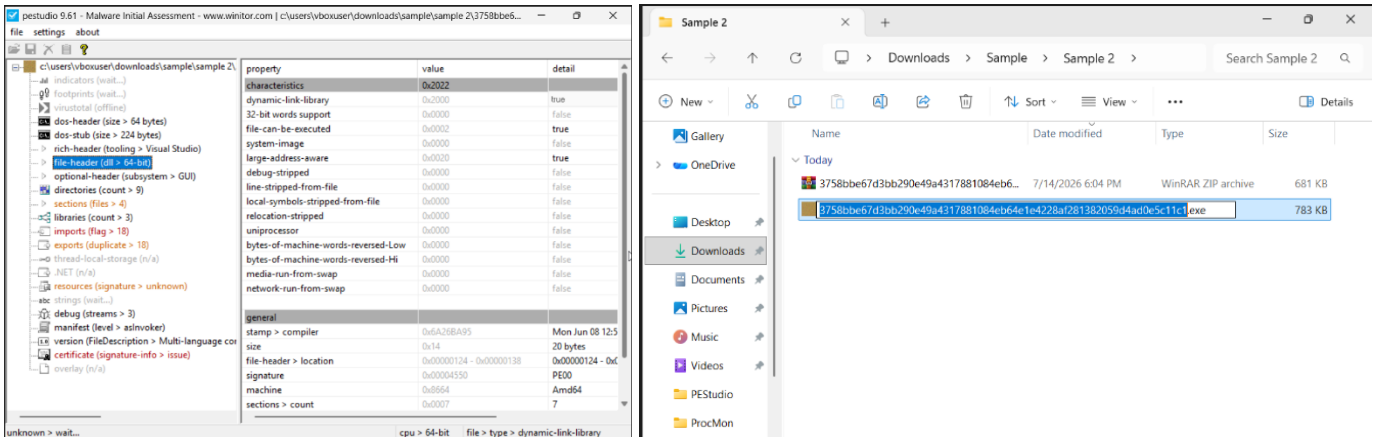
Pada sampel 1, saat dijalankan, User Account Control (UAC) menampilkan permintaan untuk memberikan hak administrator kepada Synaptics.exe, dengan publisher yang ditampilkan unknwon. Selanjutnya, melalui Process Explorer, Synaptics.exe teramati muncul dan berjalan dalam sistem. Sebelum sampel dijalankan. Synaptics.exe tidak terlihat di Process Explorer.





Hasil pemantauan menggunakan process monitor menunjukan sampel 1 melakukan beberapa operasi registri, seperti `RegOpenKey` dan `RegQueryValue`, serta mengakses berbagai berkas sistem Windows dan DLL. Namun, tidak terdapat modifikasi registri, pembuatan berkas, atau aktivitas terkait persistensi yang teramati selama pemantauan. Temuan dinamis ini selaras dengan temuan pada analisis statis yang mengidentifikasi API `AdjustTokenPrivileges`, yang berkaitan dengan pengaturan proses hak akses (privilege).

Pada analisis dinamis untuk sampel 2, proses eksekusi tidak dapat dilakukan secara normal karena file memiliki ekstensi .exe teridentifikasi oleh PEStudio saat aanalisis statis sebagai Dynamic Link Library (DLL). Ketidaksesuaian tersebut menyebabkan sampel 2 tidak dapat dijalankan seperti file executable pada umumnya. Kondisi menunjukan extensi file tidak selalu merepresentasikan file sebenarnya dan termasuk dalam teknik file masquerading yang digunakan penyerang untuk menyamarkan file berbahaya.



Meskipun analisis dinamis tidak dapat dilakukan pada Sampel 2, analisis statis tetap memberikan informasi mengenai karakteristik dan potensi kemampuan sampel, termasuk indikator yang berkaitan dengan manipulasi file system dan memory. Temuan ini menunjukkan pentingnya analisis statis sebagai tahap awal dalam pendekatan hybrid, khususnya dalam mengidentifikasi karakteristik internal file sebelum melakukan analisis perilaku. Dalam kasus Sampel 2, analisis statis membantu mengungkap bahwa file yang tampak sebagai executable berdasarkan ekstensi `.exe` sebenarnya memiliki karakteristik sebagai DLL 64-bit.

## 5. HYBRID ANALYSIS

Hasil analisis *hybrid* pada sampel 1 menunjukan adanya korelasi antara beberapa temuan analisis statis dan dinamis. Pada analisis statis, ditemukan API `AdjustTokenPrivileges` yang berkaitan dengan pengaturan proses hak akses (*privilege*). Temuan ini didukung oleh hasil analisis dinamis, di mana saat sampel 1 dijalankan, sistem menampilkan permintaan UAC untuk memberikan hak administrator kepada `Synaptics.exe`. Selain itu, analisis statis mengidentifikasi beberapa API yang berkaitan dengan *file system*, seperti `CopyFileA`, `CreateDirectoryA`, dan `DeleteFileA`, sedangkan analisis dinamis menggunakan *Process Monitor* menunjukkan adanya interaksi dengan *file system* melalui operasi `CreateFile` dan `ReadFile`. Hal ini menunjukkan adanya kesesuaian antara kemampuan yang teridentifikasi secara statis dan aktivitas yang diamati selama eksekusi saat analisis dinamis.

Analisis dinamis juga menunjukkan adanya aktivitas terhadap registri melalui operasi seperti `RegOpenKey` dan `RegQueryValue`, serta akses terhadap *file system* Windows dan DLL. Namun, tidak ditemukan aktivitas modifikasi registri, pembuatan *file*, atau aktivitas terkait persistensi. Sementara itu, beberapa API yang teridentifikasi pada analisis statis, seperti `GetClipboardData`, `GetKeyState`, dan `CallNextHookEx`, belum terlihat saat analisis dinamis. Secara keseluruhan, hasil analisis *hybrid* menunjukkan bahwa sebagian kemampuan yang teridentifikasi melalui analisis statis memiliki korelasi dengan perilaku yang diamati secara dinamis, sementara beberapa kemampuan lainnya belum teramati selama sampel dieksekusi.

Pada Sampel 2, hasil analisis *hybrid* menunjukkan bahwa analisis statis memberikan informasi yang tidak dapat diperoleh melalui analisis dinamis. Analisis statis mengidentifikasi beberapa API yang berkaitan dengan interaksi dan manipulasi *file system*, seperti `CopyFileW`, `CreateDirectoryW`, `FindFirstFileExW`, `FindNextFileW`, dan `WriteFile`,

serta API `VirtualProtect` yang berkaitan dengan manipulasi proteksi memori. Namun, ketika dilakukan analisis dinamis, Sampel 2 tidak dapat dijalankan secara normal karena *file* yang menggunakan ekstensi `.exe` teridentifikasi sebagai *Dynamic Link Library* (DLL). Oleh karena itu, perilaku *runtime* dari API yang teridentifikasi secara statis tidak dapat diamati.

Secara keseluruhan, hasil analisis *hybrid* menunjukkan bahwa analisis statis dan dinamis memiliki peran yang saling melengkapi dalam mengidentifikasi karakteristik dan perilaku *malware*.