ISSN : 1411-1624
e-ISSN: 2621-8089

# ANALISIS *TROJAN* DAN *SPYWARE* MENGGUNAKAN METODE *HYBRID ANALYSIS*

**Annisa Rizky Damanik [1], Henki Bayu Seta [2*] , Theresiawati [3]**
**Mahasiswa Universitas Pembangunan Nasional "Veteran" Jakarta [1]**
**Dosen Universitas Pembangunan Nasional "Veteran" Jakarta [2,3],**
**Jalan RS. Fatmawati Raya, Pd. Labu, Kec. Cilandak, Kota Depok, Jawa Barat 12450**
**Sur-el : annisard@upnvj.ac.id [1], henkiseta@upnvj.ac.id[2], theresiawati@upnvj.ac.id[3]**

***Abstract :*** *Malicious Software or malware is software created to damage a computer system. The increase in internet users is also in line with the increase in the use of software. However, there are still many users who still use pirated software because it is relatively free and easy to obtain. Pirated software is usually embedded with dangerous malware such as Trojans and spyware. All crimes of spreading this malware are always related to stealing credit card information, internet banking and other cybercrimes. To prove that the software installed and used on a computer is malicious software, digital forensics is required by analyzing the software. Hybrid analysis technique is a combination of static and dynamic analysis which is suitable for analyzing malware activity. Based on the results of the analysis that has been carried out, the ryuk.bin trojan has evolved and the malware forms new malware files when it is run and also changes and destroys the original files on the system.*

***Keywords:*** *Trojan, Spyware, Malware, Hybrid Analysis*

***Abstrak :*** *Malicious Software atau malware diciptakan untuk merusak sistem komputer. Peningkatan pengguna internet juga seiring dengan peningkatan penggunaan software. Namun, masih banyaknya pengguna yang masih menggunakan software bajakan karena relative gratis dan gampang didapatkan. Software bajakan biasanya sudah ditanamkan sebuah malware berbahaya seperti Trojan dan spyware. Semua tindak kejahatan penyebaran malware ini selalu berkaitan dengan mencuri informasi kartu kredit, internet banking dan tindak cybercrime lainnya. Untuk membuktikan bahwa software yang diinstal dan digunakan pada computer adalah software berbahaya, dibutuhkan tindak forensic digital dengan menganalisis software. Teknik analisis hybrid merupakan analisis statis dan dinamis dikombinasikan yang sesuai untuk menganalisis aktivitas malware. Berdasarkan hasil analisis yang telah dilakukan trojan ryuk.bin mengalami evolusi dan malware membentuk file malware yang baru jika dijalankan dan juga merubah dan merusak file original pada sistem.*

***Kata kunci****: Trojan, Spyware, Malware, Hybrid Analysis*

## 1. PENDAHULUAN

Malware adalah sejenis program komputer yang dimaksudkan untuk mencari kelemahan software sehingga pada perangkat akan terkena virus, malware dapat berisi kode berbahaya seperti *Virus, Worm, Trojan Horse* [1]. Malware telah dirancang secanggih mungkin untuk membuat celah pada sistem keamanan pada suatu komputer [2], bisa menjadi program untuk memonitoring dan mengontrol sistem dari jarak jauh [3]. *Malware* memiliki format yang berbeda-beda, seperti *executable, kode shell biner, skrip dan firmware*.

*Malware* dapat menyusup ke sistem operasi dan membuat sistem komputer menggunakan sumber daya tanpa sepengetahuan pemilik perangkat, bahkan mengumpulkan informasi pribadi untuk dibagikan ke pihak ketiga tanpa persetujuan pengguna [4]. Beberapa varian klasik *malware* yang dapat membahayakan pengguna antara lain *adware,*

ISSN : 1411-1624
e-ISSN: 2621-8089

*spyware, ransomware, virus (overwriting virus, prepending virus, appending virus, file infector virus, boot sector virus, multipartie virus, dan macro virus*), *Worms, dan Trojan Horse (remote access trojan, password sending trojan, keylogger, destructive trojan, FTP trojan, software detection killer, procy trojan* [5].

*Malware* sangat membahayakan sistem keamanan data komputer dan menurunkan performa jaringan dengan menyerang masuk ke sistem komputer melalui port-port terbuka yang tidak digunakan dalam sistem jaringan [6]. *Trojan* dan *spyware* akan menginfeksi komputer melalui banyak cara seperti email, menyamar seolah software yang baik, berupa link atau file lainnya. Malware ini dapat melihat data dan file penting bahkan aktivitas pada perangkat pengguna

*Malware* pada *platform Android* menyusup lewat layanan distribusi aplikasi (*app store),* baik resmi (*Google Play Store*) maupun milik pihak ketiga, dengan menyamar menjadi aplikasi sah seperti pemutar video, permainan dan utilitas sistem [4]. Serangan *malware platform seluler Android* meningkat sebesar 105% dari tahun 2015 hingga 2016, dan jumlah varian baru malware seluler tumbuh sebesar 54% dari tahun 2016 hingga 2017 [7]. McAfee mobile threat report Q1, jumlah keluarga malware yang ditemukan di Google Play meningkat sebesar 30% pada tahun 2017.

Laporan Badan Siber dan Sandi Negara (BSSN) mencatat peningkatan serangan oleh peretas. Hal ini sejalan dengan pengguna internet di masa pandemic Covid-19. BSSN melaporkan tercatat jumlah kasus serangan siber di Indonesia mencapai 448 juta kasus, 88 juta serangan malware yang menyerang selama masa Januari – Agustus 2021 dan lebih banyak pada wujud malware, denial service ataupun kegiatan yang mengusik ketersediaan layanan sampai *Trojan activity* [8].

Dua pendekatan untuk mengumpulkan informasi tentang aktivitas malware yaitu analisis malware statis dan dinamis [9]. Dynamic analysis dilakukan dengan mengeksekusi contoh malware, mempelajari perilaku yang ditimbulkan oleh malware dalam lingkungan yang baik pada sebuah mesin fisik berupa virtual laboratorium (*VirtualBox* atau *VMware),* lalu dikumpulkan bukti atau jejak informasi mengenai dampak dari proses infeksi malware aktif terhadap sistem komputer [4]. Kelebihan analisis dinamis, mudah untuk mendeteksi *malware* yang sedang melakukan proses infeksi tentang cara kerja malware tersebut secara langsung [10].

Sedangkan *static analysis,* melakukan analisis malware dengan tidak menjalankan atau tidak mengeksekusi perangkat lunak yang terdapat malware didalamnya[11]. *Static analysis* membongkar *source code malware* kemudian mempelajari dan memahami kode tersebut [5][12]. Kelebihan analisis statis, data menjadi aman dan analisis juga cenderung cepat [10].

Penelitian ini menggunakan metode *hybrid Analysis* metode gabungan dari *Static d*an *Dynamic Analysis* [13] untuk mendeteksi infeksi malware secara akurat. Cara kerja hybrid Analysis, memeriksa source code yang diduga sebagai malware kemudian melihat perilaku dari malware setelah menginfeksi sistem [4].

ISSN : 1411-1624
e-ISSN: 2621-8089

Penelitian ini bertujuan, mengetahui dan mengimplementasikan proses analisis *Trojan* dan Spyware dengan menggunakan metode hybrid analysis. Penggunaan metode hybrid analysis memberikan informasi karakteristik dan indikator identik yang menunjukkan keberadaan malware dalam suatu sistem atau komputer dan hasil yang lebih lengkap untuk mengidentifikasi sistem atau komputer yang terinfeksi oleh malware pada sebuah *Indicator of Compromise* (IOC) yang tersimp*an pada suatu sistem* Cyber Threat Intelligence (CTI). CTI sebagai sumber informasi CTI dalam mendeteksi keberadaan dari malware di masa yang akan datang dengan menggunakan analisis gabungan analisis statis dan analisis dinamis.

Pada penelitian ini peneliti akan melakukan analisis malware yang berjenis *Trojan* dan *spyware*. Dimana *malware* ini, bersifat menyamar dan bersembunyi tanpa diketahui pengguna computer yang dapat membahayakan bocornya akun, file atau berkas yang bersifat penting.

## 2. METODOLOGI PENELITIAN

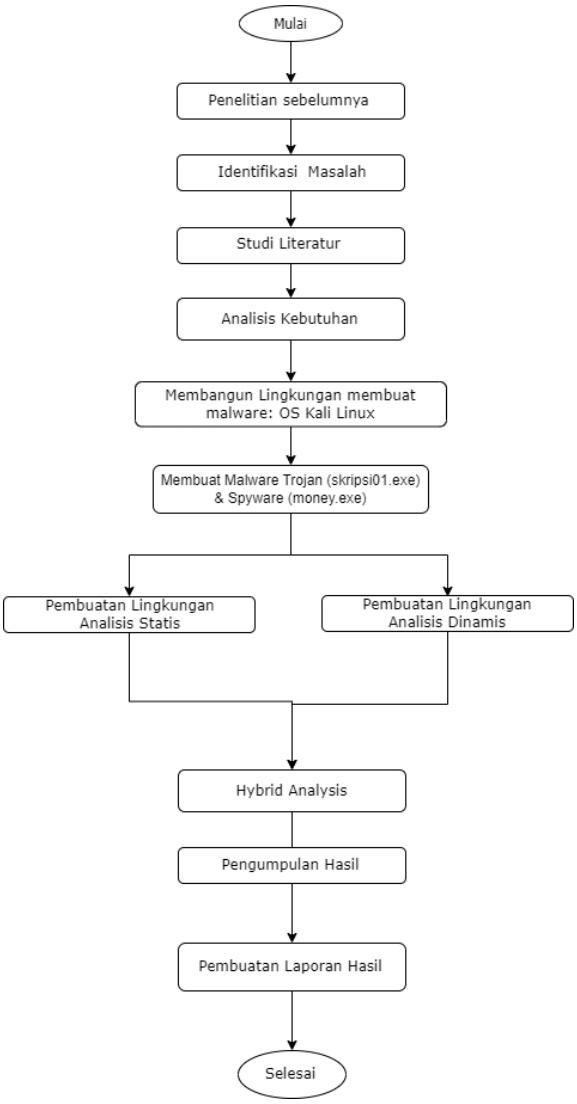
Penelitian ini difokuskan menggunakan metode gabungan atau metode *hybrid analysis* dengan menggabungkan metode *hybrid analysis* secara statis dan metode hybrid analysis secara dinamis [14]. Dalam penulisan ini, pertama peneliti membuat lingkungan yang aman seperti membuat virtual machine agar perangkat komputer yang utama aman dari *malware*. Selanjutnya dilakukan analisis *malware* dengan *metode hybrid*, kombinasi metode statis dan dinamis.

Dalam analisis statis dilakukan pengecekan pada file Trojan dan spyware tanpa menjalankan malware untuk melihat deskripsi dari file malware seperti library yang menggambarkan sifat kerja *Trojan* dan *spyware* saat dijalankan. Langkah selanjutnya adalah menganalisis dengan metode dinamis pada sampel malware dijalankan pada virtual machine yang terisolasi untuk melihat sifat dan perilaku malware yang dijalankan.

*Trojan* dan *spyware* akan di analisis menggunakan metode hybrid analysis, dengan metode ini dibutuhkan tools atau peralatan. yang diperlukan dalam penelitian analisis *trojan* dan *spyware* ini adalah PeStudio untuk analisis statis dan SpyStudio untuk analisis dinamis. Pemilihan ini dikarenakan kemudahan dalam pengoperasiannya dalam menjalankan analisa.

Dari latar belakang penelitian ini penulis ingin melakukan analisis terhadap malware jenis Trojan dan Spyware dengan metode hybrid analysis, menggabungkan teknik analisis statis dan dinamis. Alur dari metode penelitian dapat dilihat pada gambar 1.

ISSN : 1411-1624
e-ISSN: 2621-8089

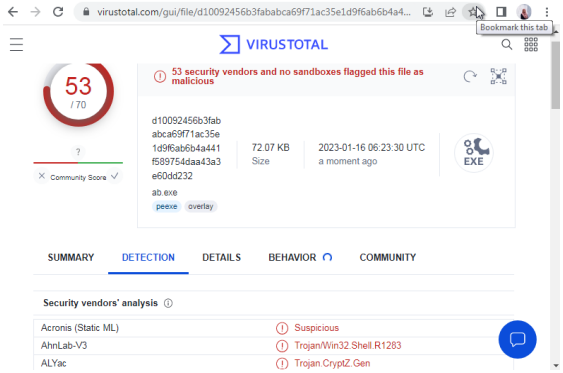



**Gambar 1. Tahapan Penelitian**

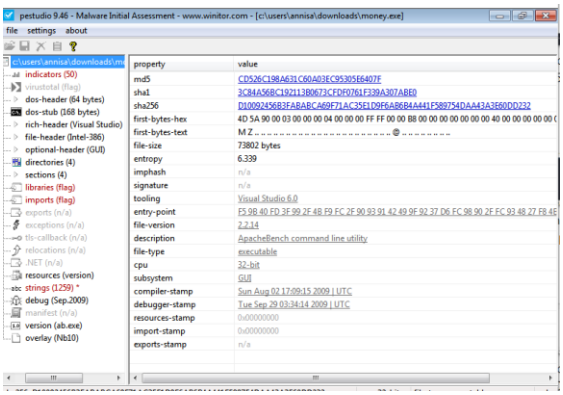
## 3. HASIL DAN PEMBAHASAN

### 2.1 Analisis Statis

Analisis statis adalah teknik untuk mengamati perilaku malware dengan menganalisa segmen code [15]. Sebelum menganalisis sampel *malware trojan* dan *spyware*, peneliti melakukan pengecekan terlebih dahulu pada sampel di VirusTotal untuk memastikan sampel malware yang akan dianalisis merupakan benar file berbahaya atau tidak. Berdasarkam pada gambar 2, sampel malware money.exe merupakan file yang berbahaya dari hasil 53 vendor keamanan mendeteksi bahwa sampel adalah software berbahaya.




**Gambar 2. Pengecekan sampel money.exe**



**Gambar 3. Struktur dari malware money.exe**

Gambar 3 menjelaskan hasil dari tool PeStudio menampilkan struktur dari file malware spyware money.exe seperti nilai hash (hasil MD5, SHA-1 atau SHA256), jenis file, compiler-stamp dan hasil lainnya. Data dikumpulkan dengan menggunakan dua tools, VirusTotal mengeluarkan hasil kemiripan perilaku spyware dengan database yang ada di pada laman virusTotal tersebut dan PeStudio merupakan software yang digunakan untuk menampilkan hasil analisis deskripsi dari file spyware seperti mendapatkan nilai hash dan kapan spyware di-compile.

Hasil analisis menggunakan tools PeStudio pada file spyware berupa lima string yang mencurigakan dan berbahaya dari tanda cros

ISSN : 1411-1624
e-ISSN: 2621-8089

merah pada bagian flag. Berdasarkan informasi yang didapat spyware money.exe ini bisa mengambil petunjuk pada keamanan sistem komputer (GetSecurityInfo dan GetNamedSecurityInfo), menulis dan mengirikan data dari satu atau lebih buffer yang terkoneksi pada jaringan komputer *(WSASend* dan *WSARecv)*, dan membaca file pada komputer *(ReadFile*). Hasil analisis malware spyware money.exe masih dengan tool PeStudio pada bagian library yang terlihat pada Tabel 1. Hasil tangkapan analisis library yang digunakan oleh money.exe, perilaku malware bisa dilihat dari library yang digunakan yaitu library WSOCK32.dll dan Library WS2_32.dll.

**Tabel 1. Library dari spyware money.exe**

| ***Library*** | ***Import*** | **Penjelasan** |
|---|---|---|
| WSOCK32.dll | 46 | File berisi windows sockets API yang digunakan oleh sebagian besar aplikasi internet dan jaringan untuk menangani koneksi jaringan. |
| WS2_32.dll | 15 | Library yang menghubungkan secara dinamis yang digunakan untuk menangani koneksi jaringan. |

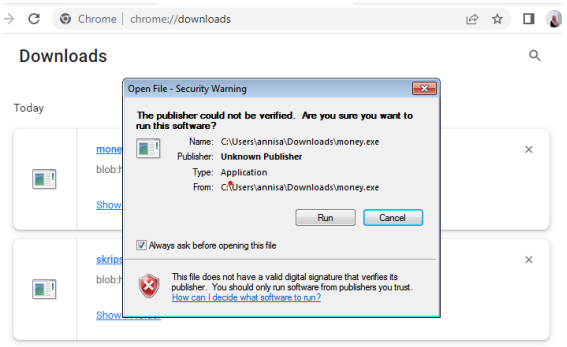
**Tabel 2. Import yang digunakan spyware money.exe**

| ***Import*** | **Grup** | ***Library*** |
|---|---|---|
| getsockopt | Network | WSOCK32.dll |
| connect | network | WSOCK32.dll |
| gethostbyname | network | WSOCK32.dll |
| closesocket | network | WSOCK32.dll |
| Inet_addr | network | WSOCK32.dll |
| WSARecv | network | WS2_32.dll |
| WSASend | network | WS2_32.dll |

Pada tabel 2 memperlihatkan hasil informasi fungsi yang di import oleh library. Dari hasil tabel 2 dibawah money.exe sebagai spyware malware ini menyerang jaringan komputer. Malware berusaha mengetahui segala sesuatunya tentang jaringan internet pada perangkat komputer pengguna.

## 2.2 Analisis Dinamis

Langkah awal yang harus dilakukan dalam penelitian ini adalah membuat lingkungan yang aman dalam meneliti malware. Lingkungan penelitian ini menggunakan sistem operasi windows 7 dalam virtual machine yang sudah di install. Setelah berhasil menginstall windows 7 dalam virtual machine, Menginstall tool yang akan digunakan dalam analisis malware. Peneliti menggunakan *tool Process Hacker* dan *SpyStudio*. Untuk melakukan analisis dinamis diperlukan sebelumnya menjalankan malware pada windows 7 seperti terlihat pada gambar 4.

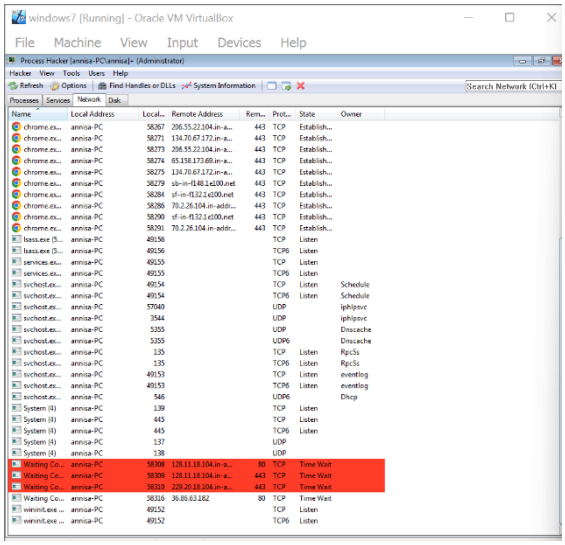



**Gambar 4. Menjalankan malware money.exe**

Pada monitor peretas yang menggunakan Metasploit pada kali linux menandakan malware sedang dijalankan oleh pengguna computer dengan OS windows 7. Setelah berjalan malware pada komputer pengguna maka dilakukannya analisis menggunakan alat *spystudio.* Berdasarkan hasil *tracker* dari sampel *malware*

ISSN : 1411-1624
e-ISSN: 2621-8089

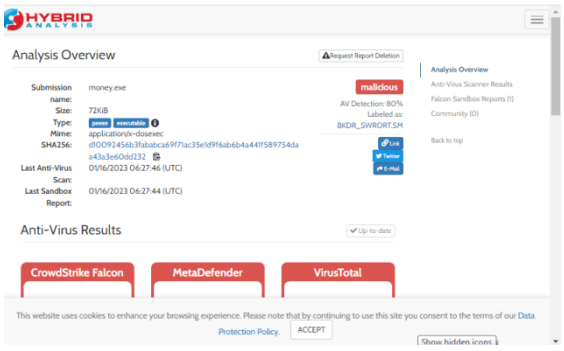
*money.exe*, *malware* mengganggil library ws2_32.dll dan library mswsock.dll dengan mengawali LoadLibrary kernelbase.dll. Pada library ws2_32.dll ini malware banyak menggunakan fungsi RegOpenKeyA yang merupakan fungsi membuka kunci registry yang ditentukan. Ada juga fungsi RegQueryVelueA yang merupakan fungsi mengambil data yang terkait dengan nilai default atau tanpa nama dari kunci registry yang ditentukan dan fungsi CreateFile yang merupakan fungsi untuk membuat sebuah file. Pada tangkapan layar gambar 5 diatas merupakan sebuah proses jalannya malware spyware money.exe, terlihat malware tersebut pada network berusaha memasuki jaringan dengan memasuki Remote Address dengan jenis TCP.



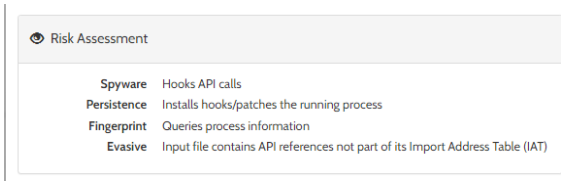
**Gambar 5. Process hacker menjalankan money.exe**

## 2.3. Hybrid Analysis

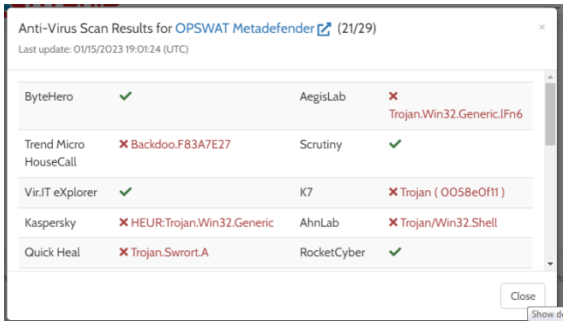
Langkah selanjutnya peneliti melakukan analisis hybrid analysis terhadap sampel *malware* Trojan (Ryuk.bin) dan sampel malware spyware (regasm.bin). Peneliti menggunakan laman tool *hybrid-analysis.com* untuk melakukan hybrid analysis. Pada gambar 6 terlihat data informasi mengenai sampel malware. Terlihat type file malware dengan type: peexe, dan executable. Dan waktu terakhir malware di scan oleh antivirus tanggal 16 januari 2023. Terdeteksi 19 antivirus yang mendeteksi perilaku malware pada file database. Dan juga pada hybrid analysis ini menampilkan hasil jenis perilaku pada file malware dapat dilihat pada gambar 7.




**Gambar 6. hybrid analisis pada money.exe**




**Gambar 7. tipe perilaku pada malware**




**Gambar 8. hasil scan anti virus pada malware**

Berdasarkan gambar 8 memperlihatkan data informasi mengenai sampel malware. Terlihat type file malware dengan type peexe, dan executable. Dan waktu terakhir malware di scan oleh anti virus tanggal 15 januari 2023.

ISSN : 1411-1624
e-ISSN: 2621-8089

Terdeteksi 21 antivirus yang mendeteksi perilaku malware pada file database.

Berdasarkan hasil analisis dari tiga metode yang telah dilakukan bahwa diketahui komponen-komponen struktur dari malware trojan dan spyware adalah metode mengenkripsi file pada komputer dan metode dalam penyerangan dalam sistem komputer pengguna. Berikut merupakan perbandingan dari jumlah yang ditemukan dari banyaknya string, library dan import yang digunakan oleh sampel malware trojan dan spyware. Pada tabel 3 penjelasan informasi yang didapatkan dari analisis menggunakan tool PeStudio dengan penjelasan flag mengartikan string atau import dinyatakan berbahaya. Sedangkan group adalah jumlah pengelompokan dari tipe file akan dijalankan.

**Tabel 4. Jumlah String, Library dan Import pada sampel**

| *Nama file Sampel* | *String yang digunakan* | | *Library yang digunakan* | *Import yang digunakan* | |
|---|---|---|---|---|---|
| | **flag** | **group** | | *flag* | *group* |
| *Spyware*: money.exe | 16 | 10 | 2 | 20 | 8 |
| Trojan: skripsi01.exe | 17 | 11 | 5 | 25 | 11 |

Malware menggunakan metode yang berbeda-beda dalam melakukan penyerangan sistem pada komputer pengguna dan mencegah proses pengoprasian komputer oleh penggunanya hingga korban dipaksa untuk bernegosiasi dengan si penyerang atau si pembuat malware. Pada tabel 5 merupakan hasil dari analisis dinamis dalam menyerang.

**Tabel 5. Hasil data yang didapat dari metode dinamis**

| *Nama Sampel* | *Metode yang ditemukan* |
|---|---|
| Money.exe | Melakukan pengambilan informasi lokasi IP, data dan *file* pada jaringan internet sistem komputer pengguna |

Pada analisis dengan metode statis hasil yang akan dikeluarkan berupa string yang perlu diteliti atau diperhatikan untuk melihat perilaku atau cara kerja pada malware untuk menyerang komputer terlihat pada tabel 6.

**Tabel 6. Hasil data yang didapat dari metode analysis**

| *Nama Sampel* | *Metode yang ditemukan* | |
|---|---|---|
| | *String* | *Penjelasannya* |
| Money.exe | *Registry modify, File scanning, detect monitor Detect inet_addr* | Mengubah *registry*, melakukan pencarian informasi data atau *file* melalui jaringan komputer dan mendeteksi monitor *computer* pengguna. |

**Tabel 7. Hasil data yang didapat dari metode hybrid analysis**

| *Nama sampel* | *Metode yang ditemukan* |
|---|---|
| Money.exe | Menulis atau menangkap data *computer* dengan proses jarak jauh atau melaui jaringan komputer, melakukan interaksi pada *registry* windows dan membaca kunci *registry*. Malware mencari dan menggunakan akun untuk masuk ke perangkat menggunakan RDP. Dan juga malware dapat mengambil tangkapan layar dari desktop untuk mengumpulkan informasi selama perangkat beroperasi. |

Berdasarkan hasil analisis diatas pada tabel 7 didapatkan metode hybrid analysis pada setiap sampel malware memiliki cara kerja infeksi computer tersendiri. Perilaku spyware lebih kearah mengambil informasi pada computer dan di kirimkan ke pembuat malware sedangan trojan melakukan cara merubah atau memodifikasi file dan mendapatkan segala informasi penting data pada komputer.

ISSN : 1411-1624
e-ISSN: 2621-8089

## 4. KESIMPULAN

Berdasarkan analisis yang telah dilakukan terhadap malware terlihat cara kerja trojan (skripsi01.exe) menginfeksi langsung pada sistem komputer dan malware akan merusak dan mengubah sebagian besar dari file-file original yang ada menjadi file yang aneh dan tidak bisa dibuka pada sistem komputer.

Dan untuk malware spyware (money.exe) memiliki cara kerja seperti: ketika file malware berjalan ke dalam sistem komputer, maka proses kerja malware ini berproses tanpa di ketehaui pengguna komputer. Malware ini juga berkerja mengambil semua data pada jaringan internet. Malware ini berjalan proses berjalannya malware ini akan menggunakan daya CPU yang tinggi yang mengakibatkan sistem komputer semakin lama semakin lambat.

Dengan analisis hybrid analysis dapat diketahui lebih lengkap dan mendetail mengenai informasi tentang karakteristik, sifat dan perilaku malware terkhusus berjenis trojan dan spyware. Dimana analisis hybrid penggabungan dari dua analisis statis dan dinamis dimana metode tersebut berbeda dalam pengerjaannya. Dengan menggabungkan kedua analisis tersebut memberikan hasil yang menutupi satu sama lainya. Dari analisis yang telah dilakukan trojan ryuk.bin mengalami evolusi, malware ini membentuk file malware yang baru jika dijalankan dan juga merubah dan merusak file original pada sistem.

Penelitian ini terdapat banyak kekurangan karena proses yang dilakukan dalam analisis ini masih dikategorikan analisis dasar dalam melakukan analisis malware trojan dan spyware. Untuk penelitian berikutnya diharapkan dapat dilakukan penelitian analisis lebih mendalam pada sampel malware trojan dan spyware.

## DAFTAR PUSTAKA

[1] Y. Ilhamdi and Y. N. Kunang, "Analisis Malware Pada Sistem Operasi Windows Menggunakan Teknik Forensik," *Bina Darma Conf. Comput. Sci.*, vol. 3, pp. 256–264, 2021, [Online]. Available: https://conference.binadarma.ac.id/index.php/BDCCS/article/view/2124

[2] P. Setiaji, L. Mayrezka Pradipta, A. Budhi Utomo, and A. Rahmad Rahim Correspondence, "Web-Based Village Information System in Dalegan Village-Panceng District-Gresik Regency Author," *KONTRIBUSIA*, vol. 2, no. 2, p. 39, 2019, [Online]. Available: https://github.com/OpenSID/opensid/wiki/Penga

[3] M. Hazri, "Analisis Malware PlasmaRAT dengan Metode Reverse Engineering," *J. Rekayasa Teknol. Inf.*, vol. 4, no. 2, p. 192, 2020, doi: 10.30872/jurti.v4i2.4131.

[4] A. S. Rusdi, N. Widiyasono, and H. Sulastri, "Analisis Infeksi Malware Pada Perangkat Android Dengan Metode Hybrid Analysis," *J. Ilm. Inform.*, vol. 7, no. 2, pp. 99–107, 2019.

[5] V. A. Manoppo, A. S. . Lumenta, and S. D. . Karouw, "Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi," *J. Tek. Elektro Dan Komput.*, vol. 9, no. 3, pp. 181–188, 2020.

[6] D. Pratiwi, "Penerapan Metode Filtering Video Streaming dan Malware Pada Jaringan Local Area Network," *Sistemasi*, vol. 7, no. 3, p. 230, 2018, doi: 10.32520/stmsi.v7i3.354.

[7] S. Alam, S. Yildirim, M. Hassan, and I. Sogukpinar, "Mininng Dominance Tree of API Calls for Detecting Android Malware," *ISMSIT 2018 - 2nd Int. Symp. Multidiscip. Stud. Innov. Technol. Proc.*, pp. 1–4, 2018, doi: 10.1109/ISMSIT.2018.8567264.

[8] Ronal Hadi, Y. Yuliana, and H. A.

ISSN : 1411-1624
e-ISSN: 2621-8089

Mooduto, "Deteksi Ancaman Keamanan Pada Server dan Jaringan Menggunakan OSSEC," *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 3, no. 1, pp. 8–15, 2022, doi: 10.30630/jitsi.3.1.58.

[9] Ferdiansyah, "Analisis Aktivitas Dan Pola Jaringan Terhadap Eternal Blue Dan Wannacry Ransomware," *JUSIFO (Jurnal Sist. Informasi)*, vol. 2, no. 1, pp. 44–59, 2018, [Online]. Available: http://eprints.binadarma.ac.id/3873/1/Ferdiansyah-Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue dan Wannacry Ransomware.pdf

[10] G. W. Wahidin, S. Syaifuddin, and Z. Sari, "Analisis Ransomware Wannacry Menggunakan Aplikasi Cuckoo Sandbox," *J. Repos.*, vol. 4, no. 1, pp. 83–94, 2022, doi: 10.22219/repositor.v4i1.1373.

[11] D. Ucci, L. Aniello, and R. Baldoni, "Survey of machine learning techniques for malware analysis," *Comput. Secur.*, vol. 81, pp. 123–147, 2019, doi: 10.1016/j.cose.2018.11.001.

[12] J. Dwi Nugraha, A. Budiono, and A. Almaarif, "Analisis Malware Berdasarkan Api Call Memory Dengan Metode Deteksi Signature-Based Malware Alaysis Based on Call Memory Api With Signature-Based Detection Method," vol. 6, no. 2, pp. 7820–7827, 2019.

[13] E. Tansen and D. W. Nurdiarto, "Analisis dan Deteksi Malware dengan Metode Hybrid Analysis Menggunakan Framework MOBSF," *J. Teknol. Inf.*, vol. 4, no. 2, pp. 191–201, 2020, doi: 10.36294/jurti.v4i2.1338.

[14] M. A. Qbeitah and M. Aldwairi, "Dynamic malware analysis of phishing emails," *2018 9th Int. Conf. Inf. Commun. Syst. ICICS 2018*, vol. 2018-Janua, no. April, pp. 18–24, 2018, doi: 10.1109/IACS.2018.8355435.

[15] A. Febrianto, A. F., Budiyono, A., & Almaarif, "Analisis Malware Pada Sistem Operasi Android Menggunakan Permission-Based Malware Analysis in Android Operation System Using Permission-Based," vol. 6, no. 2, pp. 7845–7851, 2019.