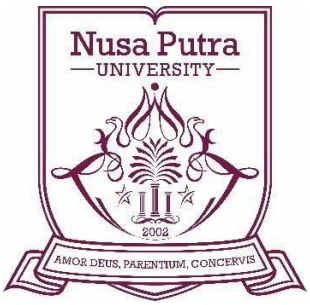
ANALISIS PRILAKU DAN DAMPAK *MALWARE RANSOMWARE LOCKY* METODE DINAMIS *FRAMEWORK FLAREVM*

SKRIPSI

SAHRUL ISMAIL USMAN
20200040045



PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK, KOMPUTER DAN DESAIN
UNIVERSITAS NUSA PUTRA
SUKABUMI
JUNI 2024

ANALISIS PRILAKU DAN DAMPAK *MALWARE RANSOMWARE LOCKY* METODE DINAMIS *FRAMEWORK FLAREVM*

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Dalam Menempuh Gelar Sarjana Srata Satu Teknik Informatika

SAHRUL ISMAIL USMAN

20200040045

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK, KOMPUTER DAN DESAIN

UNIVERSITAS NUSA PUTRA

SUKABUMI

JUNI 2024

PERNYATAAN PENULIS

JUDUL : ANALISIS PERILAKU DAN DAMPAK *MALWARE RANSOMWARE LOCKY* METODE DINAMIS *FRAMEWORK FLAREVM*

NAMA : SAHRUL ISMAIL USMAN

NIM : 20200040045

Sukabumi, ….Juni 2024

SAHRUL ISMAIL USMAN

PENGESAHAN SKRIPSI

JUDUL : ANALISIS PERILAKU DAN DAMPAK *MALWARE RANSOMWARE LOCKY* METODE DINAMIS *FRAMEWORK FLAREVM*

NAMA : SAHRUL ISMAIL USMAN

NIM : 20200040045

Skripsi ini telah diujikan dan dipertahankan di depan Dewan Penguji pada Sidang Skripsi tanggal 19 Juni 2024. Menurut pandangan kami, Skripsi ini memadai dari segi kualitas untuk tujuan penganugerahan gelar Sarjana Komputer (S.Kom)

Sukabumi, 19 Juni 2024

Pembimbing I

Ir. Somantri, S.T., M.Kom
NIDN. 0419128801

Pembimbing II

Anggun Fergina, M.Kom
NIDN. 0407029301

Ketua Penguji

Falentino Sembiring, M.Kom
NIDN. 0408029102

Ketua Program Studi Teknik Informatika

Ir. Somantri, S.T., M.Kom
NIDN. 0419128801

Plh. Dekan Faktultas Teknik, Komputer dan Desain

Ir. Paikun, S.T., M.T., IPM, ASEAN Eng
NIDN. 0402037401

HALAMAN PERUNTUKAN

السلام عليكم ورحمة الله وبركاتُه

Skripsi ini saya tujukan utamanya kepada kedua orang tua tercinta ayahanda dan Alm. Ibunda yang telah menjadi sosok pahlawan serta support terbaik hingga saat ini.

Serta kepada adik-adik tercintaku yang memberikan keceriaan dan kegembiraan dalam hidup, kepada seluruh keluarga yang telah memberi rasa kasih dan sayang yang begitu besar.

Terimakasih pula ku sampaikan pada Latifah Tasliyatundiyah semoga cepat S.Kom. yang akan menjadi teman hidup dimasa depan semoga tetap selalu memahami dan menemani didalam gelap dan terang jalan ini. serta ibu. Isah Aisyah dan keluarga merupakan sosok yang menjadi cermin dari cinta yang tulus dan ikhlas.

Serta seluruh elemen dan pihak yang telah membantu pada penelitian ini termasuk teman, Organisasi serta semua lingkungan yang tuhan berikan, saya sangat berterimakasih.

Sedikit saya sampaikan rasa yang takkan pernah hilang yaitu tentang rindu dan kasih sayang kepada kedua orang tua serta adik-adik tercinta, mengingat bisa sampai dititik ini merupakan perjuangan yang begitu keras.

Semoga dengan menyelesaikan proses pendidikan strata satu saya kedepannya bisa membuat saya menjadi sosok yang lebih gigih dan giat untuk mencapai kesuksesan di masa depan serta dapat mengangkat derajat kedua orang tua saya serta keluarga semuanya.

وعليكم السلام ورحمة الله وبركاتُه

ABSTRACT

Locky ransomware malware is a very dangerous malware and malware has the potential to encrypt all important victim data in exchange for ransom in return, this will be very detrimental to victims who do not know anything. Malware that is easy to infiltrate and enter at any time makes the system vulnerable, so there needs to be in-depth research on malware, namely behavioral analysis and the impact of malware to determine the characteristics of malware, considering that the more the prevention system develops, the more malware developers develop their malware so that it cannot be detected by the prevention system. By conducting dynamic analysis, malware will be run on the Windows 10 operating system and allowed to infect with the support of the flarevm framework which has complete security standards and tools to analyze the behavior and impact of malware, with the results of the analysis obtained it can be concluded that the locky ransomware malware has a tendency to add key or value behavior and uses internet protocols to send and receive files, namely TCP (Transmission Control Protocol).

Keywords: Malware, Ransomware Locky, Dynamic Analysis

ABSTRAK

Malware ransomware locky merupakan *malware* yang sangat berbahaya dan *malware* berpotensi mengenkripsi semua data korban yang penting dengan imbalan tebusan sebagai gantinya, hal tersebut akan sangat merugikan korban yang tidak tahu apa-apa. *Malware* yang mudah menyusup dan masuk kapan saja membuat sistem menjadi rentan, maka perlu adanya penelitian yang mendalam tentang *malware* yaitu analisis perilaku dan dampak *malware* untuk mengetahui karakteristik dari *malware*, mengingat semakin berkembang sistem pencegahan maka semakin berkembang pengembang *malware* dalam mengembangkan *malware*nya agar tidak bisa terdeteksi oleh sistem pencegahan. Dengan melakukan analisis dinamis *malware* akan dijalankan disistem operasi windows 10 dan dibiarkan menginfeksi dengan didukung framework flarevm yang mempunyai standar keamanan dan tools lengkap untuk melakukan analisis perilaku dan dampak *malware*, dengan hasil analisis yang didapatkan bisa disimpulkan bahwa *malware ransomware locky* memilki kecenderungan perilaku menambahkan key atau value serta menggunakan protoko internet untuk mengirim da menerima file yaitu TCP (Transmission Control Protocol).

Keyword : *Malware*, *Ransomware Locky*, Analisis Dinamis

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT, karena atas rahmat dan hidayah-Nya, penulis dapat menyelesaikan skripsi dengan judul "Analisis Perilaku dan Dampak *Malware Ransomware Locky* Metode Dinamis *Framework Flarevm*" sebagai bagian dari pemenuhan syarat untuk meraih gelar Sarjana Teknik Informatika. Tujuan penelitian ini untuk memahami dan menyelidiki fenomena yang semakin mengkhawatirkan dalam dunia teknologi informasi, yaitu serangan *malware*. Keberadaan *malware* telah menjadi ancaman serius bagi keamanan sistem informasi, mengakibatkan kerugian besar dan mengancam privasi pengguna. Serta berusaha untuk mendalami secara komprehensif tentang perilaku *malware*, metode analisis yang dapat digunakan untuk mengidentifikasi dan memahami karakteristiknya. Penelitian ini diharapkan dapat memberikan kontribusi positif terhadap pengembangan keamanan sistem informasi dan membantu para profesional IT dalam melawan ancaman *malware* yang semakin canggih.

Penulis ingin menyampaikan apresiasi dan terima kasih yang tak terhingga kepada :

1. Rektor Universitas Nusa Putra Sukabumi Bpk. Dr. Kurniawan, S.T., M.Si., MM.
2. Wakil Rektor I Bidang Akademik Universitas Nusa Putra Sukabumi.
3. Kepala Program Studi Universitas Nusa Putra Sukabumi Bpk. Ir. Somantri, S.T., M.
4. Dosen Pembimbing I Universitas Nusa Putra Sukabumi Bpk. Ir. Somantri, S.T., M.
5. Dosen Pembimbing II Universitas Nusa Putra Sukabumi Ibu. Anggun Fergina, M.Kom
6. Dosen Penguji Bpk. Falentino Sembiring, M.Kom
7. Para Dosen Program Studi Teknik Informatika Universitas Nusa Putra Sukabumi
8. Kedua Orang Tua tercinta Ayahanda. Uus serta Ibunda. Alm.Isoh serta seluruh keluarga.
9. Rekan –rekan mahasiswa di Universitas Nusa Putra.
10. Seluruh pihak yang telah berkontribusi pada proses penelitian ini.

Semoga skripsi ini dapat memberikan manfaat dan wawasan baru bagi pembaca, serta menjadi landasan bagi penelitian lebih lanjut dalam memahami dan mengatasi tantangan keamanan yang dihadapi dalam dunia teknologi informasi.

Akhir kata, penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang bersifat membangun sangat penulis harapkan demi perbaikan di masa mendatang.

Sukabumi, 19 Juni 2024

Sahrul Ismail Usman

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika UNIVERSITAS NUSA PUTRA, saya yang bertanda tangan dibawah ini :

Nama : Sahrul Ismail Usman

NIM : 20200040045

Program Studi : Teknik Informatika

Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Nusa Putra **Hak Bebas Royalti Noneksklusif** ***(Non-exclusive Royalty- Free Right)*** atas karya ilmiah saya yang berjudul :

"Analisis Perilaku Dan Dampak *Malware Ransomware Locky* Metode Dinamis *Framework Flarevm*"

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Nusa Putra berhak menyimpan, mengalihmedia/format- kan, mengelola dalam bentuk pangkalan data (database), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Sukabumi
Pada tanggal : 19 Juni 2024

Yang menyatakan

(Sahrul Ismail Usman)

DAFTAR ISI

COVER ..... **i**
PERNYATAAN PENULIS ..... **ii**
PENGESAHAN SKRIPSI ..... **iii**
HALAMAN PERUNTUKAN ..... **iv**
ABSTRACT ..... **v**
ABSTRAK ..... **v**
KATA PENGANTAR ..... **vi**
DAFTAR ISI ..... **viii**
DAFTAR GAMBAR ..... **x**
DAFTAR TABEL ..... **xi**
BAB I **1**
PENDAHULUAN **1**
1.1. Latar Belakang 1
1.2. Rumusan Masalah 2
1.3. Batasan Masalah 2
1.4. Tujuan Penelitian 3
1.5. Manfaat Penelitian 3
1.6. Sistematika Penulisan 3
BAB II **5**
TINJAUAN PUSTAKA **5**
2.1 Penelitian Terkait 5
2.2 Landasan Teori 10
2.3 Kerangka Berpikir 14
BAB III **16**
METODOLOGI PENELITIAN **16**
3.1 Metode Penelitian 16
3.2 Tahapan Penelitian 16
3.3 Metode Pengumpulan Data 17
3.4 Metode Analisis 17
3.5 Analisis Kebutuhan 26
BAB IV **29**

HASIL DAN PEMBAHASAN 29
4.1 Implementasi 29
4.2 Konfigurasi *Flarevm* 29
4.3 Konfigurasi jaringan 30
4.4 Pengujian 31
4.5 Dampak 35
4.6 Hasil Rekomendasi Peningkatan Keamanan 37
BAB V 39
KESIMPULAN 39

DAFTAR GAMBAR

Gambar 2.1. *System Operasi Windows 10* 11
Gambar 2.2. *Virtual machine* 11
Gambar 2.3. *Flarevm* 13
Gambar 2.4. *Regshot* 13
Gambar 2.5. *Procmon* 13
Gambar 2.6. *Fakenet* 14
Gambar 2.7. *Procdot* 14
Gambar 2.8. Kerangka Berpikir 15
Gambar 3.1. Tahapan Penelitian 16
Gambar 3.2. Desain Topologi 18
Gambar 3.3. Tahapan Analisis 19
Gambar 3.4. *General Basic* 19
Gambar 3.5. *General Advanced* 20
Gambar 3.6. *System Motherboard* 20
Gambar 3.7. *System Processor* 20
Gambar 3.8. Bagian *Storage* 21
Gambar 3.9. Bagian *Network* 21
Gambar 3.10. Penonaktifan *Windows Defender* 22
Gambar 3.11. Penonaktifan *Windows Update* 22
Gambar 3.12. Tampilan *Powershell 5* 23
Gambar 3.13 . Spesifikasi *Windows* 23
Gambar 3.14. Pengambilan *Shot* Pertama 24
Gambar 3.15. Pengambilan *Shot* Kedua 24
Gambar 3.16. Proses Perbandingan 25
Gambar 3.17 . Tampilan Utama *Procmon* 25
Gambar 4.1. Tampilan Utama *Flarevm* 39
Gambar 4.2. Memastikan Internet Terputus 30
Gambar 4.3. Konfigurasi *Fakenet* 30
Gambar 4.4. *Fakenet* Berhasil 30
Gambar 4.5. Proses *Malware* Menginfeksi Sistem 32
Gambar 4.6. Hasil *Regshot* 34

Gambar 4.7. Hasil *Fakenet* 1..... 35
Gambar 4.8. Hasil *Fakenet* 2..... 35
Gambar 4.9. Hasil *Fakenet* 3..... 35
Gambar 4.10. Hasil *Fakenet* 4..... 35
Gambar 4.11. Jumlah *Byte* Pertama 36
Gambar 4.12. Jumlah *Byte* Kedua..... 36
Gambar 4.11. Dampak Notifikasi 36
Gambar 4.12. Dampak *Wallpaper* 37
Gambar 4.13. Dampak Pada *File* 37
Gambar 4.14. Contoh *Email Phising* 38

DAFTAR TABEL

Tabel 2.1. Studi Pustaka 5
Tabel 3.1. Informasi Sistem Operasi *Windows 10* 26
Tabel 3.2. Informasi *Malware Ransomware Locky* 26
Table 3.3. Informasi *host* utama 27
Tabel 3.4. Informasi Spesifikasi *Virtualbox* 27
Tabel 3.5. Informasi *Tools* Perekam 27
Table 4.1. Hasil *Procmon* 31
Tabel 4.2. Hasil Perilaku *Malware* 31
Tabel 4.3. Pengambilan *Shot* Pertama 33

BAB I
PENDAHULUAN

1.1. Latar Belakang

Malware atau *malicious software* merupakan perangkat lunak yang didesain untuk melakukan aktivitas berbahaya atau perusak perangkat lunak[1], salah satu jenisnya adalah *ransomware* dengan tingkat bahaya *malware* yang sangat tinggi dan dapat merusak sistem[2] serta secara karakteristik dan perilakunya dapat dibedakan menjadi 2 yaitu *crypto* dan *locker*, varian *crypto* yang diluncurkan sebagai bagian dari langkah pemerasan dimana data penting dalam komputer di enkripsi untuk meminta korban membayar[3]yang selanjutnya disebut locky. locky adalah varian ransomware(mhmmd), locky ditemukan sekitar tahun 2016[4] malware biasanya menyebar melaluli *email*, *message* dan *pop-ups* [5].

Ransomware as a service (RaaS)-RaaS adalah model distribusi Ransomware dimana penyerang menyewakan serangan Ransomware kepada penjahat dunia maya lainnya, layanan ini mencakup kompilasi, penyesuaian serta instruksi Ransomware, hal ini memungkinkan para penjahat yang tidak memiliki keterampilan terhadap pengembangan malware bisa meluncurkan serangan dengan cepat dan mudah[6], Menurut chainanalysis jumlah tebusan yang dihasilkan dari kejahatan ransomware pada tahun 2019 mencapai $220M, 2020 = $905M, 2021 = $983M, 2022 = $567M dan 2023 = $1.1B jumlah tertinggi yang berhasil dianalisis yaitu pada tahun 2023 walaupun pada tahun 2022 mengalami penurunan tetapi secara grafik serangan ransomware terus menerus meningkat. IEEE juga menyebutkan mereka meninjau penelitian yang ada selama beberapa tahun sehubungan dengan teknik deteksi, pencegahan, mitigasi, dan prediksi. Analisis ekstensif kami, berdasarkan lebih dari 150 referensi, telah mengungkapkan hal yang signifikan penelitian, khususnya 72,8%, berfokus pada pendeteksian Ransomware, namun terdapat kurangnya penekanan ditempatkan pada prediksi malware. hal tersebut menunjukan betapa pesatn serta pentingnya penelitian tentang memahami karakteristik malware[7] untuk dapat memahami dan mencegah malware menyerang.

Pentingnya mengetahui informasi ringkasan karakteristik malware dan perilaku malware untuk meminimalisir penyerangan yang berdampak pada kerugian pada

salah satu pihak[8], dengan melakukan analisis perilaku malware salah satu cara untuk melakukan prediksi dan mengetahui sifat dari malware itu sendiri[9] dengan didukung dengan metode analisis dinamis merupakan metode mengamati perilaku malware dengan menjalankan malware iti sendiri pada lingkungan yang diawasi selama proses eksekusi dan infeksi malware[10], untuk mengetahui aktivitas registri[11], alamat yang dipanggil serta dampak pada sistem yang terinfeksi.

Dengan menganalisis perilaku dan dampak dari malware ransomware locky menggunakan pendekatan dinamis melalui framework flarevm, diharapkan penelitian ini dapat memberikan pemahaman yang lebih mendalam tentang strategi dan teknik yang digunakan oleh jenis malware ini. Hasil dari penelitian ini diharapkan dapat memberikan wawasan yang berharga dalam upaya peningkatan keamanan sistem informasi dan perlindungan terhadap serangan malware ransomware yang semakin kompleks dan merugikan.

1.2. Rumusan Masalah

Pada penelitian yang berjudul "Analisis perilaku dan dampak *malware Ransomware Locky* metode analisis dinamis *framework Flarevm*" adapun rumusan masalah pada penelitian ini adalah :

1. Bagaimana karakteristik *malware ransomware locky* ketika dianalisis menggunakan metode dinamis *framework flarevm* ?
2. Bagaimana *malware ransomware locky* ini menyebar dan masuk ke sistem operasi *windows 10* ?
3. Bagaimana aktivitas registry dan dampak pada sistem *virtual machine windows 10* yang terinfeksi *malware ransomware locky* ?

1.3. Batasan Masalah

Adapun batasan dari masalah pada penelitian ini adalah :

1. *Malware* yang digunakan pada penelitian ini adalah *malware Ransomware Locky* SHA 1 Hash : 97bae63417df5bde4a05cd44c6c523db50f6ab76
2. Peneliti menganalisis aktivitas registry dan dampak pada sistem yang terinfeksi *malware ransomware locky* pada *virtual machine windows 10*.

3. Metode yang digunakan pada penelitian ini adalah metode dinamis dengan menjalankan *malware* secara langsung pada sistem operasi *windows 10* sebagai objek.
4. Lingkup penelitian memiliki batasan sistem yaitu pada *virtual machine windows 10* sebagai objek yang digunakan saat dilakukan pengujian.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Melakukan analisis *malware Ransomware Locky* SHA 1 Hash : 97bae63417df5bde4a05cd44c6c523db50f6ab76 dengan menggunakan metode dinamis *framework flarevm*
2. Mengetahui aktivitas *registry* dan dampak pada sistem *virtual machine windows 10*.
3. Mengetahui karakteristik *malware ransomware locky*.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini adalah :

1. Pemahaman perilaku *malware* ini meliputi tentang bagaimana *malware ransomware locky* beroperasi, mencakup bagaimana *malware* itu menyebar dan menginfeksi pada sistem
2. Mengidentifikasi titik lemah mengetahui bagaimana *malware* tersebut menyerang dan mengeksploitasi perangkat atau jaringan dapat membantu meningkatkan keamanan dengan memperbaiki kerentanannya.
3. Peningkatan Keamanan Jaringan hasil penelitian dapat digunakan untuk meningkatkan keamanan jaringan secara keseluruhan. Ini mencakup implementasi langkah-langkah keamanan tambahan untuk melindungi perangkat dan jaringan dari ancaman *malware ransomware locky*.

1.6. Sistematika Penulisan

Memberikan gambaran secara garis besar, dalam hal ini dijelaskan isi dari masing masing bab dari tugas akhir ini. Sistematika penulisan dalam pembuatan laporan ini sebagai berikut :

BAB I : PENDAHULUAN

Berisi tentang latar belakang mengapa penulis mengambil judul "Analisis perilaku dan tingkat bahaya *malware ransomware locky* metode dinamis" meliputi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini berisi tentang dasar teori dan penjelasan komponen komponen yang akan digunakan.

BAB III : METODOLOGI PENELITIAN

Pada bab ini berisi tentang metode penelitian, tahapan penelitian, teknik pengumpulan data serta metode analisis yang digunakan untuk melakukan analisis *malware ransomware locky*.

BAB IV : HASIL DAN PEMBAHASAN

Berisi tentang hasil pengujian secara keseluruhan dari penelitian dan pembahasan dari setiap kategori pengujian yang dilakukan dalam analisis *malware* secara dinamis.

BAB : V KESIMPULAN

Bagian akhir yang menjelaskan hasil penelitian secara keseluruhan dari mulai mengambil subtema sampai hasil dari penelitian itu sendiri, dan saran-saran yang harus dilakukan pada penelitian selanjutnya.

BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terkait

Penelitian dengan judul "analisis perilaku dan dampak *malware ransomware locky* metode dinamis *framework flarevm*" tentunya terinspirasi dari pada penelitian-penelitian terdahulu yang berkaitan dengan penelitian ini. Berikut penelitian sebelumnya yang berkaitan dengan penelitian skripsi ini yaitu :

Tabel 2.1. Studi Pustaka

1	Judul	Analisis Perilaku *Malware Malware* Menggunakan Metode Analisis Dinamis
	Nama, Tahun	Khalif Ibrahim dan kawan-kawan (2023)
	Gambaran umum penelitian	Penelitian yang melakukan pengujian dan melakukan perbandingan terhadap *malware-malware* dengan melakukan analisis secara dinamis dalam ruang lingkup yang diawasi seperti *virtual machine*. Dengan hasil bahwa *malware* : Trojan.AgentWDCR.PZW merupakan *malware* paling berbahaya dalam melakukan pengaruh aktivitas pada sistem dan *malware* : Variant.Strictor.171520 merupakan paling berbahaya karena memiliki kemampuan untuk melakukan intersepsi dan transmisi data pada 1993 protocol, terbanyak diantara *malware* lainnya[10].
	Kesamaan	Penelitian diatas memiliki keterkaitan tentang analisis perilaku *malware* menjelaskan tahapan secara garis besar pada perilaku *malware*
	Keterbaruan	Keterbaruan dari penelitian terkait adalah *framework Falrevm* dimana penelitian diatas menganlisis perilaku *malware* tanpa *framework*
2	Judul	ANALISIS *MALWARE* PADA SISTEM OPERASI WINDOWS MENGGUNAKAN TEKNIK FORENSIK
	Nama, Tahun	Yuriansyah Ilhamdi , Yesi Novaria Kunang (2021)

	Gambaran umum penelitian	*Malware* merupakan perangkat lunak atau software yang diciptakan untuk menyusup atau merusak sistem komputer. *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. Penyebaran *malware* saat ini begitu mudah baik melalui usb flashdisk, iklan-iklan tertentu pada website, dan media lainnya. Windows merupakan salah satu sistem operasi yang paling banyak di gunakan, dengan jumlah pengguna dan penyedia aplikasi di internet yang banyak, memungkinkan penyebaran *malware* pada windows mudah untuk dilakukan. Metodologi yang di gunakan dalam penelitian ini adalah *malware* dynamic analysis. Penelitian ini nantinya akan menghasilkan informasi mengenai aktivitas dan pola serangan *malware,* yang di harapkan dapat membantu pengguna sistem operasi windows untuk mengantisipasi ancaman dan serangan *malware*[12].
	Kesamaan	Keterkaitan penelitian ini yaitu menyangkut tentang analisis *malware* pada *windows.*
	Keterbaruan	*Malware* diatas menggunakan Trojan sedang didalam penelitian ini menggunakan *ransomware*.
3	Judul	Analisis *Ransomware* Wannacry Menggunakan Aplikasi Cuckoo Sandbox
	Nama, Tahun	Gratiyo Wahyu Wahidin, Syaifuddin, Zamah Sari (2022)
	Gambaran umum penelitian	Penelitian *ransomware* merupakan bagian dari *malware* yang melakukan enkripsi data pada targetnya. *Malware* tersebut kebanyakan menyerang instansi pemerintah dengan cara menyebar melalui jaringan lokal yang diawali dengan menyusup melalui email atau data yang tidak terpercaya. Untuk mengetahui hal apa saja yang dilakukan *malware*

		ketika sedang melakukan penyerangan perlunya untuk melakukan analisis baik menggunakan teknik statis maupun dinamis. Pada Cuckoo Sandbox terdapat teknik analisis dinamis dan statis, didalam analisis dinamis Cuckoo Sandbox menjalankan *malware* dalam lingkungan virtual sehingga dapat meminimalisir adanya penyebaran *malware*. Analisis statis dilakukan dengan cara melakukan dekompilasi *malware* tanpa melakukan uji coba secara langsung, sedangkan analisis dinamis melakukan uji *malware* dengan cara eksekusi cara langsung. Dengan perangkat lunak Cuckoo Sandbox informasi data yang didapat diharapkan dapat digunakan untuk mengetahui tentang aktivitas dan kebiasaan dari *Ransomware*. Beberapa dari *ransomware* mempunyai kebiasaan yang berbeda-beda, dalam analisis yang dilakukan oleh Cuckoo Sandbox terdapat pula hasil dari analisis kebiasaan dari *malware*[13].
	Ketekaitan Penelitian	Pada penelitian diatas keterkaitan dengan penelitian ini yaitu peneliti menganalisis *ransomware*
	Keterbaruan	Penelitian diatas membahas tentang malware wannacry sedangkan dalam penelitian ini membahas tentang *ransomware locky*
4	Judul	ANALISIS STATIS DETEKSI *MALWARE* ANDROID MENGGUNAKAN ALGORITMA SUPERVISED MACHINE LEARNING
	Nama, Tahun	Raden Budiarto Hadiprakoso, Wahyu Rendra Aditya, Febriora Nevia Pramitha 2022
	Gambaran umum penelitian	Mengidentifikasi *malware* ini sangat penting untuk menjaga keamanan dan privasi pengguna. Karena proses identifikasi *malware* yang semakin rumit, maka perlu digunakan

		machine learning untuk klasifikasi *malware*. Penelitian ini mengumpulkan fitur analisis statis dari aplikasi aman dan berbahaya. (*malware*). Dataset yang digunakan pada penelitian adalah dataset *malware* DREBIN yang merupakan dataset *malware* yang tersedia secara publik. Dataset tersebut terdiri dari fitur API CALL, system command, manifest permission, dan Intent. Data tersebut kemudian diproses menggunakan berbagai algoritma supervised machine learning di antaranya *Support Vector Machine* (SVM*), Naive Bayes, Decision Tree* dan *KNearest Neighbors*. Kami juga berkonsentrasi pada memaksimalkan pencapaian dengan mengevaluasi berbagai algoritma dan menyesuaikan beberapa konfigurasi untuk mendapatkan kombinasi terbaik dari hyper-parameter. Hasil eksperimen menunjukkan bahwa klasifikasi model SVM mendapatkan hasil terbaik dengan mencapai akurasi 96,94% dan nilai AUC (Area Under Curve) 95%[14].
	Kesamaan	Keterkaitan pada penelitian ini adalah adalah tentang analisis malware menggunakan metode
	Keterbaruan	Penelitian diatas melakukan analisis *malware* dengan metode statis sedangkan penelitian ini menggunakan metode dinamis.
5	Judul	ANALISIS *MALWARE* DENGAN METODE DINAMIK MENGGUNAKAN *FRAMEWORK CUCKOO SANDBOX*
	Nama, Tahun	Hairil Novansyah (2023)
	Gambaran umum penelitian	Adapun penelitian membahas tentang analisis *malware* dengan tujuan dari penelitian ini adalah untuk menganalisis karakteristik *malware* yang ditemukan pada jaringan Institut Teknologi Pagar Alam. Adapun metode yang digunakan

		dalam penelitian ini adalah *Dynamic Analysis* dan menggunakan *tool Flarevm*, sehingga tidak ada resiko untuk terinfeksi *malware*. Berdasarkan Analisis yang dilakukan tentang karakteristik dari *malware*, dapat disimpulkan bahwa terdapat signature, string, dan perubahan pada value registry[1].
	Kesamaan	Keterkaitan pada penelitian ini ada melakukan analisis menggunakan framework
	Keterbaruan	Keterbaruan dari penelitian diatas adalah framework dimana framework yang digunakan dari penelitian diatas yaitu cuckoo sandbox dan framework yang digunakan pada penelitian kali ini yaitu flarevm
	Kesimpulan	Kesimpulan yang dapat diambil dari beberapa penelitian terkait diatas adalah tentang alat serta objek yang digunakan, dimana subjek atau malware, objek atau window serta alat atau framework yang digunakan pada penelitian kali ini menggunakan update terakhir yang diambil sebagai bahan penelitian. Mengedepankan keterbaruan dalam melakukan analisis keamanan adalah point yang sangat penting mengingat ancaman serta kerentanan pada sistem terus berkembang.

Keterbaruan : Dalam penelitian ini memiliki unsur keterbaruan yaitu *malware* yang yang berjenis *ransomware locky* pada Mei 2024 merupakan malware yang sangat berbahaya dan rentan terhadap keamanan sistem, serta sistem yang digunakan pada penelitian ini menggunakan sistem operasi *windows 10* merupakan dengan *update* terbaru pada Maret 2024 sehingga memungkinkan peneliti menemukan temuan penting untuk meningkatkan sistem keamanan yang berkelanjutan.

2.2 Landasan Teori

2.2.1 Malware

Malware yang diartikan dengan bahasa Indonesia adalah perangkat lunak atau program berbahaya[15], yang dirancang dan diciptakan untuk menyusup bahkan merusak sistem untuk melakukan kejahatan.

2.2.2 *Ransomware*

Ransomware merupakan salah satu keluarga dari *malware* atau perangkat lunak berbahaya. Penyebaran *ransomware* dapat melalui berbagai metode seperti *phising*, *malicious attachments*, pesan email palsu, dan sebagainya. Jenis *malware* ini memungkinkan object targetnya menjadi tidak bisa diakses atau terenkripsi[16], selanjutnya apabila serangan berhasil korban akan diminta menebus untuk mendapatkan key agar sistem dapat dibuka kembali.

2.2.3 *Locky*

Locky adalah salah satu jenis *malware Ransomware* yang ditemukan di awal tahun 2016 dan masih terus berlanjut berhasil dengan memanfaatkan permukaan serangan yang besar, sembunyi-sembunyi, dan cara pemerasan uang yang mahal. Locky Ransomware menyematkan makro di dalamnya dokumen Word dan email spam locky berjenis *crypto* yang biasanya melalui email phising atau lampiran yang berbahaya sehingga sangat rentan terjadi penyerangan.

2.2.4 Jenis-Jenis Metode Analisis *Malware*

1. Analisis Metode Statis

   Analisis metode statis adalah melakukan analisis *malware* dengan tidak menjalankan atau tidak mengeksekusi perangkat lunak yang terdapat *malware* didalamnya[17].

2. Analisis Metode Dinamis

   Analisis *malware* dinamis merupakan sebuah proses untuk mempelajari perilaku *malware* dengan menjalankannya pada lingkungan yang diawasi[18], dengan menjalankan kinerja dari *malware* itu sendiri kita dapat memahami secara kompleks aktivitas ketika *malware* dijalankan.

3. Analisis Metode Hybrid

Analisis menggunakan metode hybrid menggabungkan keunggulan dari analisis statis dan analisis dinamis dengan cara melakukan pengecekan pada setiap signature *malware* setelah itu memonitor perilaku kode[18].

2.2.5 Sistem Operasi *Windows 10*

Sistem operasi windows 10 yang dikembangkan oleh microsoft digunakan sebagai host utama untuk melakukan analisis dinamis *malware* dan mengetahui karakteristik dari *malware ransomware locky*.

Gambar 2.1. *System Operasi Windows 10*

2.2.6 *Virtual machine*

Virtual machine windows 10 dan virtualbox adalah sistem yang dipakai untuk melakukan pengujian agar ketika menjalankan *malware* serangannya dapat diawasi dan dibatasi. Dengan menggunakan *virtualbox* serangan virus tidak akan menembus pada sistem utama tetapi akan merusak atau menginfeksi *virtual machine windows* 10.

Gambar 2.2. *Virtual machine*

2.2.7 *Framework Flarevm*

FlareVm adalah *framework* yang digunakan untuk melakukan analisis *malware*, beberapa standar dari *framework flarevm :*

1. Konfrehensip dan terintegritas
    - Alat Lengkap: *FLAREVM* menyertakan berbagai alat penting yang terintegrasi dengan baik, seperti IDA Pro, Ghidra, x64dbg, Wireshark, dnSpy, dan Volatility. Ini memastikan bahwa saya memiliki semua yang Anda butuhkan di satu tempat.
    - Otomasi: Banyak tugas rutin dapat diotomatisasi menggunakan skrip PowerShell dan Python, meningkatkan efisiensi dan konsistensi analisis.
2. Isolasi dan keamanan
    - Lingkungan Terisolasi: Berjalan di dalam mesin virtual memastikan bahwa analisis *malware* tidak membahayakan sistem utama atau jaringan.
    - Pengaturan Keamanan: Dapat diatur dengan jaringan host-only atau internal untuk mencegah komunikasi berbahaya dengan server eksternal.
3. Pembaharuan dan dukungan
    - Update Rutin: FLARE VM dan alat-alat di dalamnya diperbarui secara berkala untuk menambahkan fitur baru dan memperbaiki kerentanan.
    - Komunitas dan Dokumentasi: Didukung oleh komunitas keamanan yang aktif serta dokumentasi yang baik, menyediakan sumber daya tambahan untuk belajar dan mendapatkan bantuan.

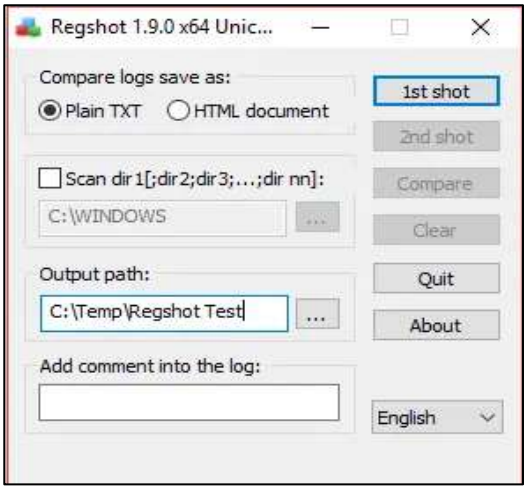
Gambar 2.3. *Flarevm*

2.2.8 Tools Flarevm

Disini saya akan menjelaskan alat-alat *flarevm* yang akan saya gunakan pada penelitian kali ini untuk menganalisis *malware ransomware locky* yaitu :

1. Regshot

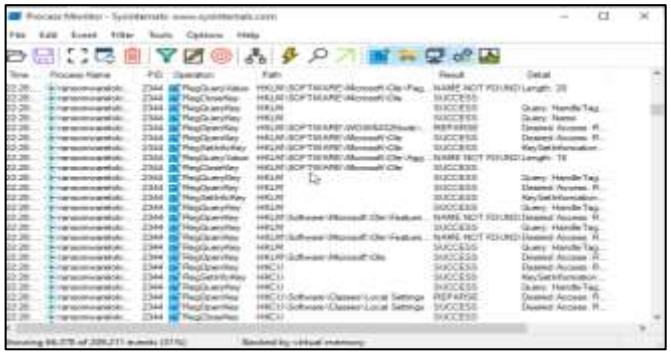
   Regshot adalah alat untuk melihat kecenderungan dari perilaku *malware* atau melihat aktivitas registry sementara :



Gambar 2.4. *Regshot*

2. Procmon

   Procmon adalah alat untuk melihat aktivitas reegistri secara *realtime* digunakan ketika melware dijalankan.



Gambar 2.5. *Procmon*

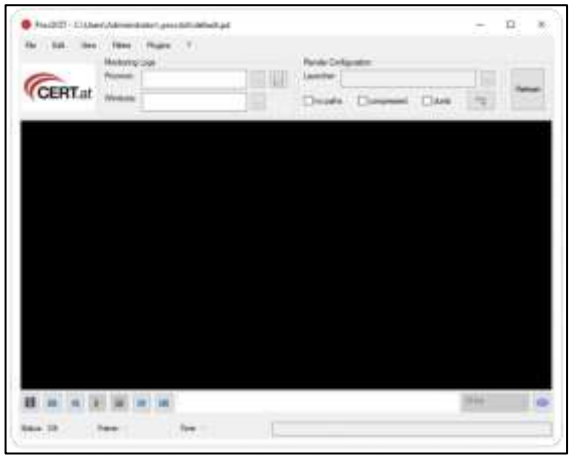
3. Fakenet

   Fakenet adalah alat untuk memantau dan menemukan ip yang dihubungi *malware* ketika dijalankan, fakenet juga berperan membuat jaringan palsu.

Gambar 2.6. *Fakenet*

4. Procdot

   Procdot adalah untuk melakukan virtualisasi dari dari hasil pencatatan dari procmon.



Gambar 2.7. *Procdot*

2.3 Kerangka Berpikir

Kerangka berfikir adalah struktur atau rencana yang disusun untuk mengatur secara garis besar haluan dari penelitia

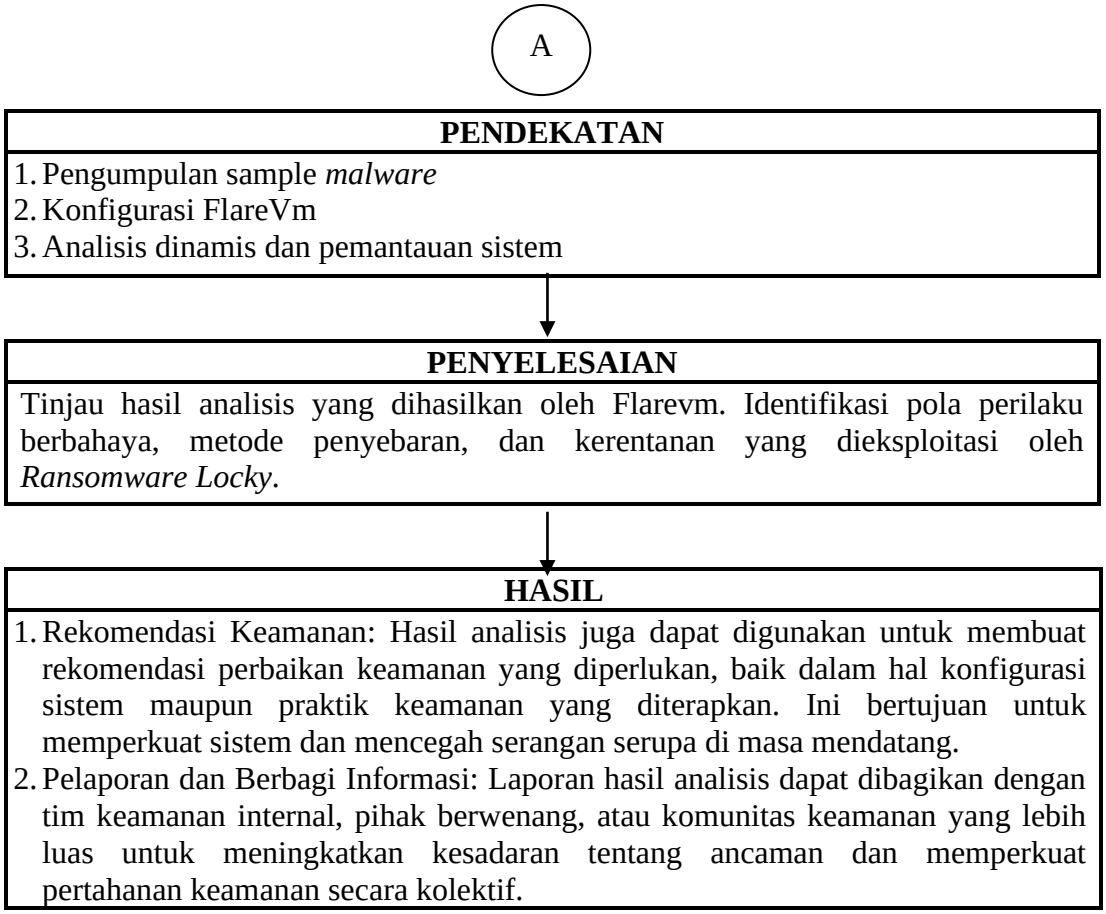
KESEMPATAN
1. Pemantauan dan analisis terhadap *malware* 2. Pemahaman terperinci pada perilaku *malware* **3.** Berbagi Informasi tentang temuan dengan komunitas keamanan yang lebih luas

↓

MASALAH
1. Perilaku dan dampak *malware* yang belum diketahui 2. Resiko penyerangan yang rentan terjadi **3.** Harus dilakukan peningkatan respon keamanan

↓

A



Gambar 2.8. Kerangka Berpikir

Penelitian ini dirancang untuk mengetahui karakteristik dan dampak yang dihasilkan oleh *ransomware locky*. Sehingga dapat bermanfaat di kemudian hari sebagai bahan analisis lanjutan serta pertimbangan untuk mengembangkan anti virus.

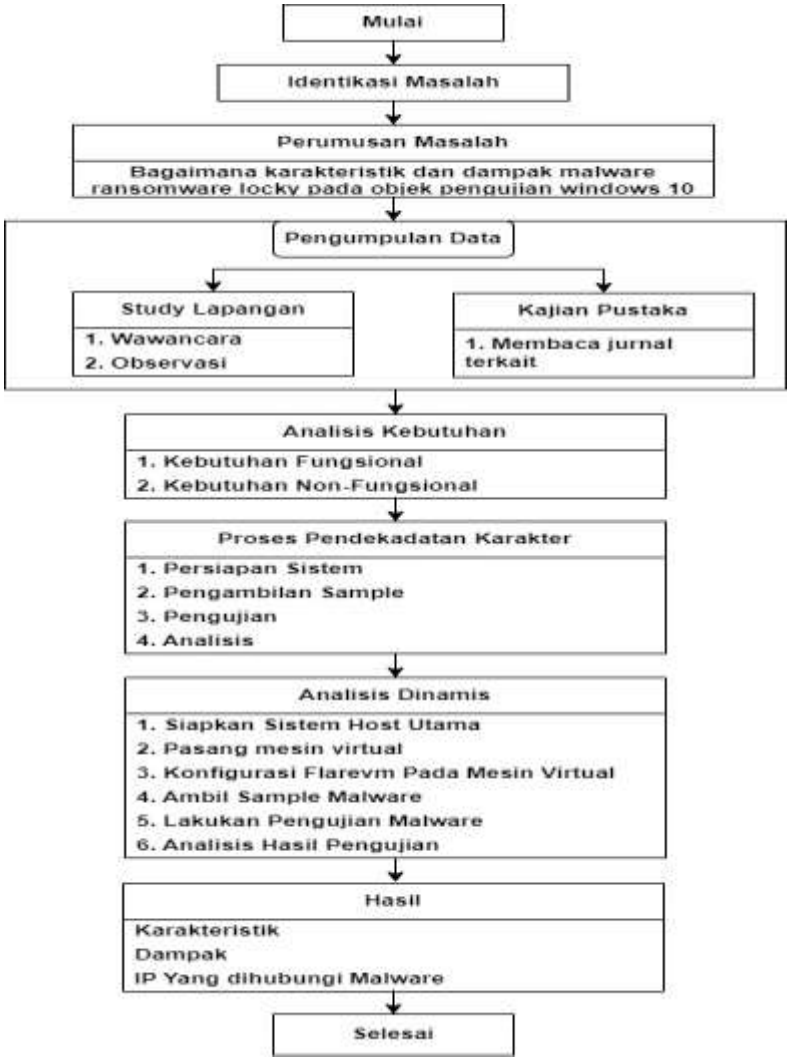
BAB III
METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metode penelitian ini adalah penelitian kualitatif yang bertujuan untuk memahami fenomena tentang apa yang dialami oleh subjek penelitian secara mendalam dan dapat melebar dapat berupa perilaku, perspektif ,tindakan motivasi dan lain-lain.

3.2 Tahapan Penelitian

Tahapan penelitian yang dilakukan oleh peneliti yaitu meliputi beberapa kegiatan yang divisualkan dalam *flowchart* :



Gambar 3.1. Tahapan Penelitian

3.3 Metode Pengumpulan Data

Dalam penelitian kali ini pengumpulan data terbagi menjadi 2 klasifikasi yaitu pengumpulan data fungsional dan non-fungsional :

3.3.1. Data Non-fungsional

Data non-fungsional yang dimaksud adalah data yang didapat sebagai bahan referensi terhadap penelitian ini dan sangat berguna bagi peneliti karena secara tidak langsung memiliki arahan yang jelas, namun data tersebut tidak membantu secara langsung proses analisis. Berikut upaya yang dilakukan adalah :

1. Observasi

   Observasi dilakukan secara online dengan mencari bahan penelitian tentang *cyber security*, Untuk menemukan referensi sebagai bahan dasar penelitian.

2. Wawancara

   Wawancara dilakukan kepada beberapa narasumber yang dianggap mahir dalam bidangnya dilakukan secara online maupum offline.

3. Studi Pustaka

   Studi pustaka dilakukan dengan menggali jurnal-jurnal terkait dengan rumusan masalah yang sudah ditentukan. Hal ini berguna untuk menentukan objek serta cara yang akan dilakukan oleh peneliti dalam mengatasi permasalahan yang ada.

3.3.2. Data Fungsional

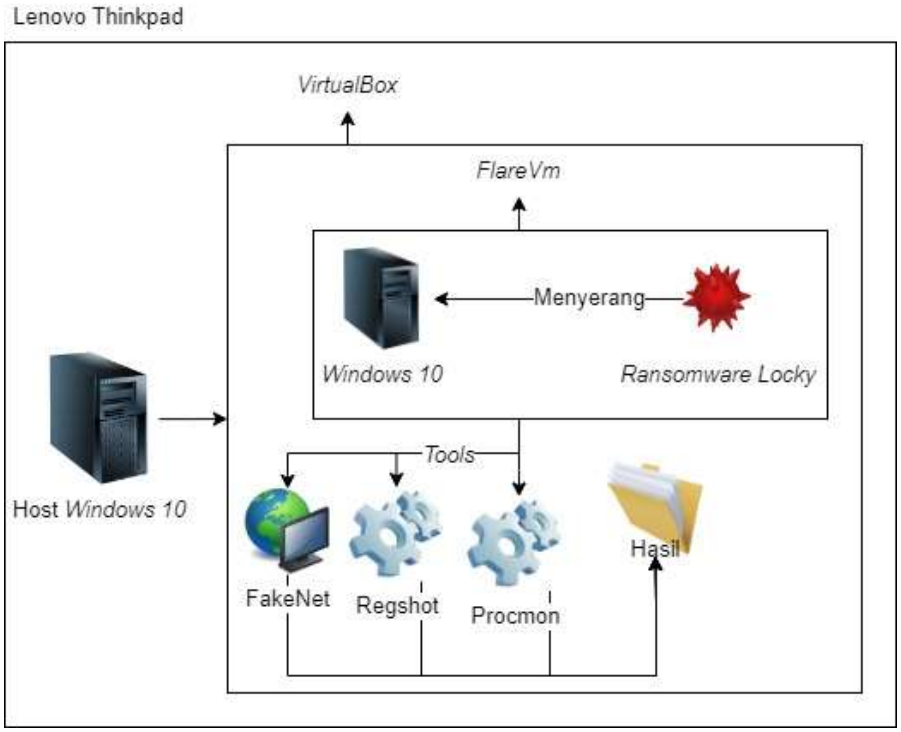
Pengumpulan data yang dilakukan dalam melakukan analisis *malware Ransomware Locky* adalah dengan metode studi kasus, dimana data yang dimaksud adalah data hasil pengujian *malware* yang menghasilkan aktivitas registry sistem dan dampak pada *virtual machine windows* yang terinfeksi *malware ransomware locky*.

3.4 Metode Analisis

Metode dinamis digunakan untuk mengetahui perilaku *malware* dengan menjalankan *malware* itu sendiri dalam ruang lingkup yang diawasi[19], maka dari itu dibutuhkan *virtual machine* atau *virtualbox* untuk membatasi serangan dari *malware* tersebut. Tahap pertama *malware* diupload pada *Flarevm* dan *FlareVm* akan melakukan analisis secara otomatis[20], Setelah menjalankan *malware* pada sistem yang diawasi perlu beberapa *tool* untuk mencatat atau menangkap setiap

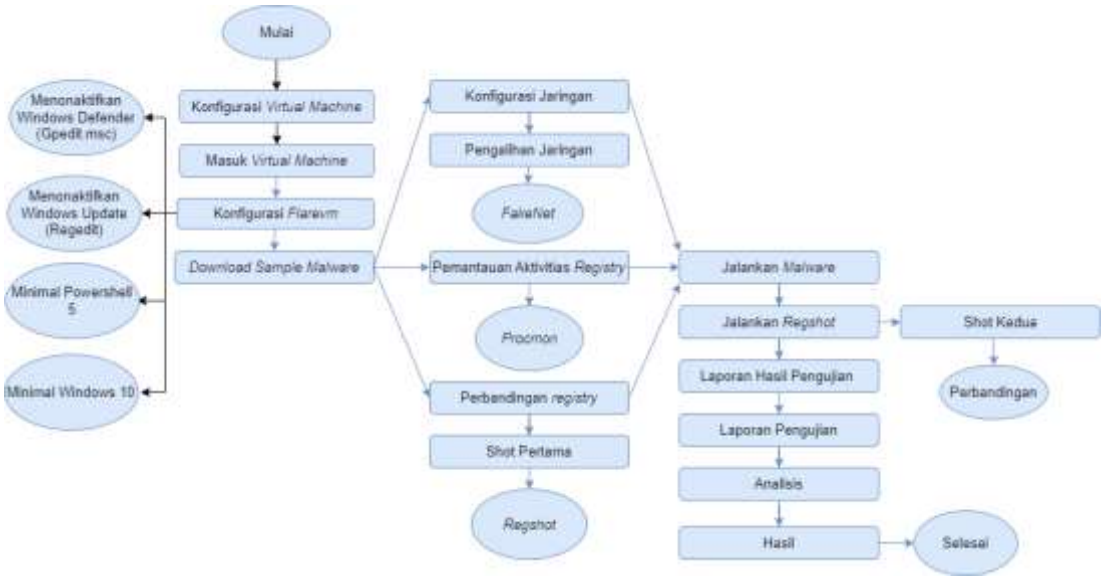
gerakan pada *malware* tersebut, dalam proses ini akan diperiksa proses secara menyeluruh seperti perubahan registry dan aktivitas komunikasi jaringan yang tercemar *malware*. Proses analisis terhadap perubahan pada sistem registry menggunakan program pendukung Regshot [8] dimana dilakukan perbandingan snapshot pada saat *malware* dijalankan dan tidak.

1. Desain Topologi



Gambar 3.2. Desain Topologi

2. Tahapan Analisis



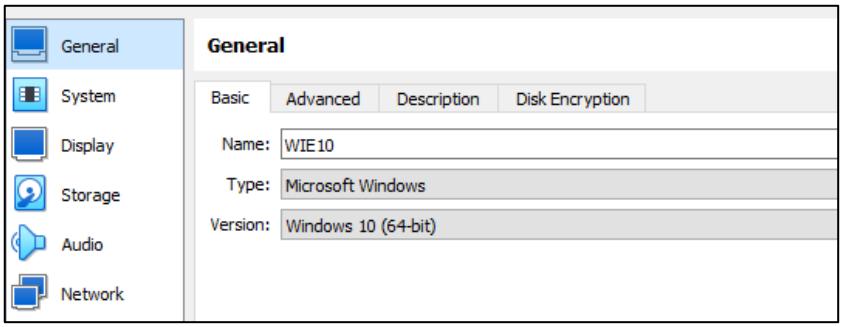
Gambar 3.3. Tahapan Analisis

Berdasarkan flowchart diatas menggambarkan serangkaian tahapan dalam melakukan analisis malware dengan langkah-langkah sebagai berikut :

a) Konfigurasi *Virtual Machine / Virtualbox*

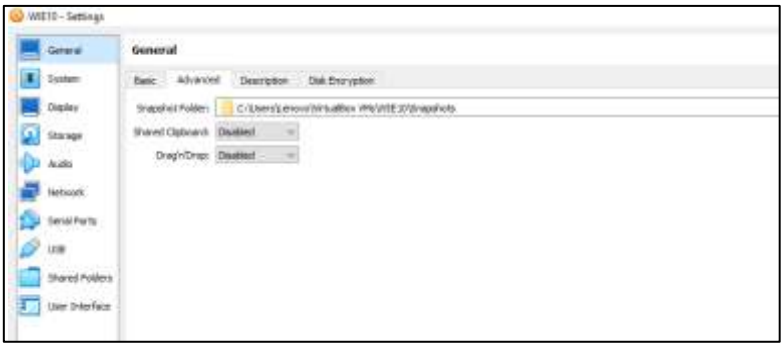
Pada bagian ini akan dijelaskan tentang beberapa pengaturan yang harus dilakukan pada *virtualbox* yang pada dasar menggunakan pengaturan biasa, berikut pengaturan yang perlu dipertimbangkan :

- Bagian *General*



Gambar 3.4. *General Basic*

Pada bagian ini versi windows yang digunakan menggunakan *windows 10 (64-bit)* untuk menyesuaikan segala bentuk dukungan baik dari performa, update dan kompabilitas.



Gambar 3.5. *General Advanced*

Bagian *shared clipboard* dan dragndrop di *disable* atau dimatikan untuk mencegah penyerangan serta sebagai upaya untuk meningkatkan keamanan.

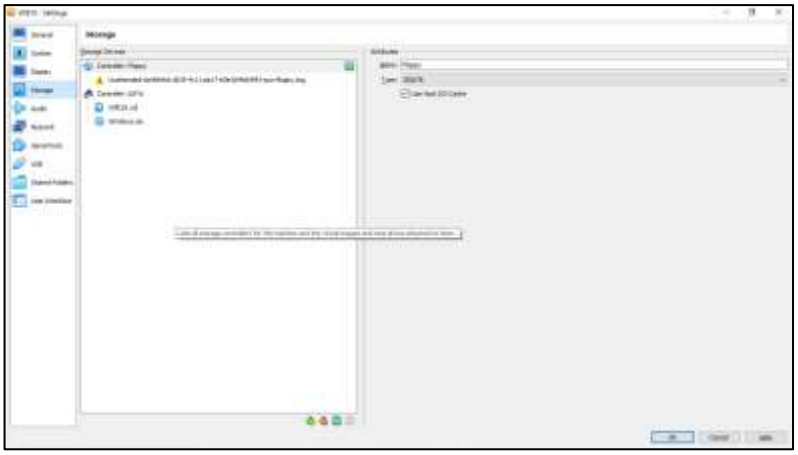
- Bagian *System*

Gambar 3.6. *System Motherboard*

Gambar 3.7. *System Processor*

Pada bagian *matherboard* dan Processor tingkatkan kapasitas semaksimal mungkin agar ketika *virtual machine* dijalankan dapat berjalan secara maksimal dan tidak menggangu proses analisis yang dilakukan.

- Bagian *Storage*



Gambar 3.8. Bagian *Storage*

Perlu dipertimbangkan ketika melakukan installasi *virtual machine windows 10* membutuhkan penyimpanan ± 200GB agar proses berjalannya sistem operasi dapat maksimal serta berguna untuk mengelabui *malware* ketika menyerang (tidak terdeteksi sebagai bahan analisis).

- Bagian *Network*

Gambar 3.9. Bagian *Network*

Jaringan merupakan alat komunikasi inti dari malware tetapi pada bagian pengaturan *virtualbox* tetap menggunakan NAT *(Network Addres Translation)* dimana akses jaringan tetap terhubung dengan server utama, namun saat

melakukan analisis harus dipastikan tidak ada koneksi internet yang terhubung baik *server* atau *machine virtual.*

b) Konfigurasi *Flarevm*

Framework flarevm merupakan alat yang dirancang untuk melakukan analisis *malware* dengan dukungan berbagai alat yang bisa digunakan ketika melakukan analisis, *flarevm* dipasang secara otomatis dengan mengikuti langkah-langkah yang sudah disediakan dalam *website* resmi *flarevm.* Namun ada beberapa hal yang perlu diperhatikan yaitu sebgai berikut :

- Nonaktifkan windows defender (Gpedit.msc)

Gambar 3.10. Penonaktifan *Windows Defender*

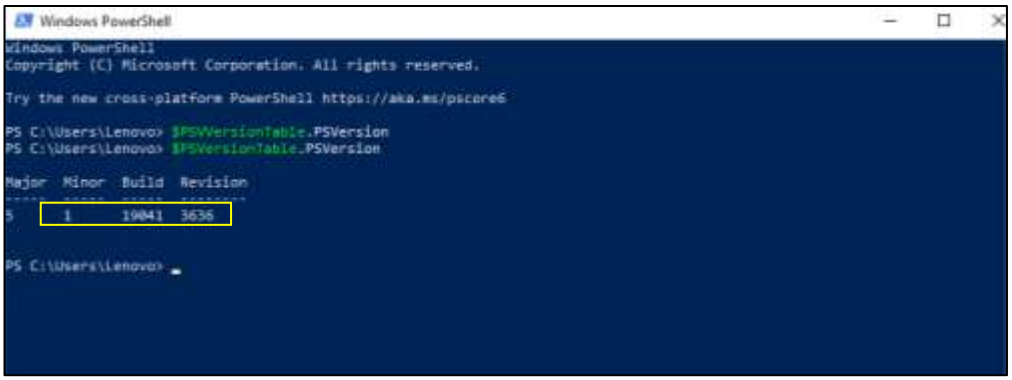
Penonaktifan *windows defender* dilakukan melalui akses Gpedit.msc dengan cara manual yang bisa dicari dalam internet.

- Nonaktifkan windows update (Regedit)

Gambar 3.11. Penonaktifan *Windows Update*

Penonaktifan windows *update* dilakukan secara manual melalui akses *regedit.*

- Minimal *Powershell 5*



Gambar 3.12. Tampilan *Powershell 5*

- Minimal Windows 10

Gambar 3.13 . Spesifikasi *Windows*

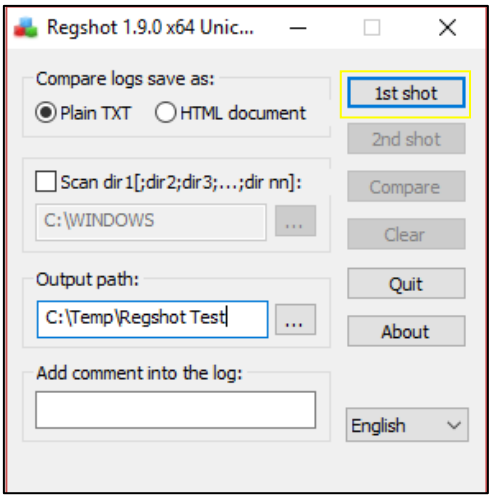
c) Konfigurasi Jaringan *Fakenet*

Berdasarkan pada konfigurasi diatas dengan melakukan penyesuaian pada *virtualbox* dengan menggunakan pengaturan jaringan NAT maka seharusnya tahap *ini virtual machine* bisa melakukan akses internet selama host menggunakan internet. Untuk melakukan konfigurasi jaringan menggunakan *fakenet* hal yang harus diperhatikan adalah untuk memutus koneksi internet dari server. Setelah itu cukup melakukan *running* file fakenet.exe melalui terminal

d) Langkah-langkah penggunaan *Regshot*

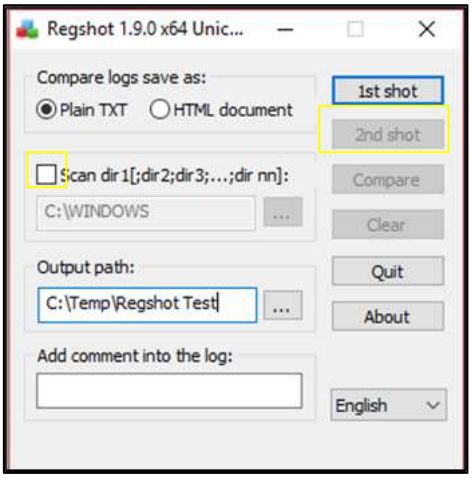
Regshot adalah alat yang digunakan untuk melakukan perbandingan aktivitas *registry* pertama sebelum sistem operasi terinfeksi dan setelah terinfeksi,

sebelum melakukan pengambilan shot pertama pastikan *virtual machine* sedang tidak melakukan aktivitas apapun untuk memaksimalkan penyesuaian perbandingan, setelah itu lakukan shot pertama dengan menekan 1st shot :



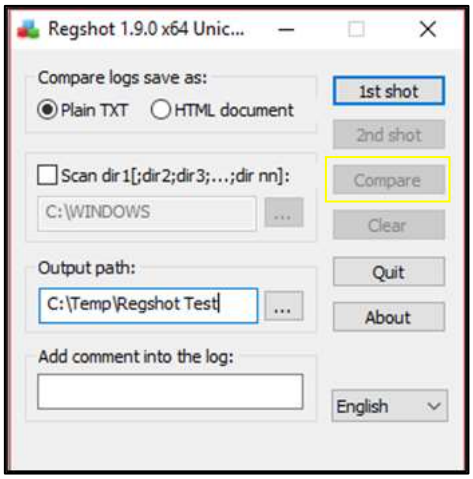
Gambar 3.14. Pengambilan Shot Pertama

Langkah selanjutnya yaitu menjalankan *malware*, setelah beberapa saat *malware* berjalan dan mengeksekusi dirinya sendiri lakukan shot kedua dengan menekan centang scan selanjutnya 2nd shot.



Gambar 3.15. Pengambilan Shot Kedua

Setelah proses kedua berhasil lalu lakukan perbandingan untuk mengukur seberapa jauh perubahan yang ada dengan menekan *compare* pada aplikasi *regshot.*

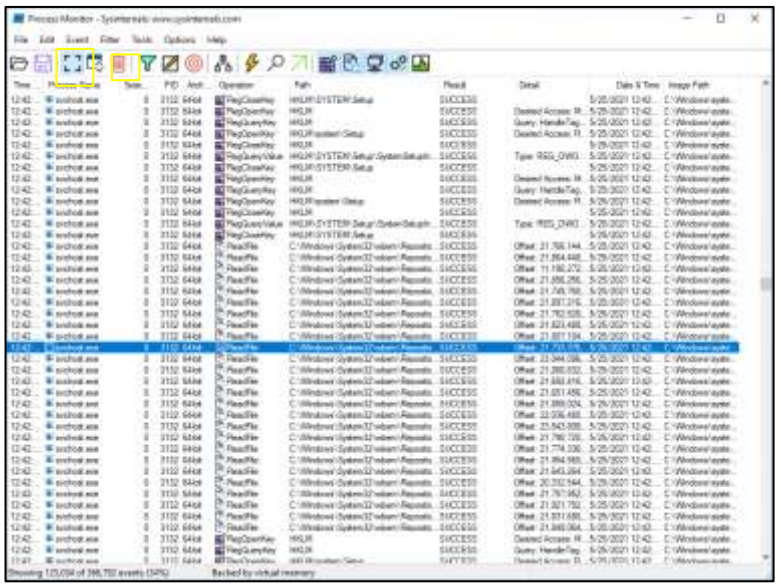


Gambar 3.16. Proses Perbandingan

e) Langkah-langkah penggunaan Procmon

Procmon adalah *tool* yang digunakan untuk menangkap aktivitas registry yang dihasilkan oleh *malware* sehingga memungkinkan untuk dapat melihat arah gerak dari *malware* serta memahami secara mendalam terhadap perilaku malware, berikut tahapan yang dilakukan dalam melakukan analisis menggunakan menggunakan procmon :

- Buka procmon yang mesin virtual yang sudah dikonfigurasi dengan *flarevm* .
-



Gambar 3.17 . Tampilan Utama Procmon

Setelah dibuka hentikan perekaman serta bersihkan yang ada agar tidak menumpuk hasil analisis dari *malware* dengan menekan tombol yang sudah ditandai diatas. Selanjutnya setelah melakukan pembersihan dan sebelum menjalankan *malware* tekan Kembali tombol perekam dan setelah *malware* melakukan eksekusi pada dirinya sendiri hentikan tombol perekam. Setelah itu aktivitas *registry* yang dihasilkan *malware* akan terlihat dan perlu diingat agar tidak melakukan *close* terlebih dahulu sebelum melakukan *save* dari hasil semuanya.

3.5 Analisis Kebutuhan

Berikut beberapa kebutuhan yang diperlukan dalam proses analisis kali ini :

1) Spsesifikasi Sistem Target:

a. Sistem Operasi *Windows 10*

Tabel 3.1. Informasi Sistem Operasi *Windows 10*

No	Spesifikasi Target	Deskripsi
1.	Nama sistem : Sistem Operasi *Windows*	Sistem operasi *windows* dengan *update* terakhir Maret 2024
2.	Type : 64 Bit	Menggunakan arsitektur 64 bit. Memungkinkan untuk dapat menangani lebih banyak data.
3.	Varian : *Windows 10 Education*	Menggunakan *windows 10 education*, kelebihan memiliki akses lebih dalam seperti gpedit.msc dan regedit
4.	Versi : 2022	Memiliki versi 2022 merupakan versi terbaru dari windows

b. Spesifikasi *malware Ransomware Lokcy*

Tabel 3.2. Informasi *Malware Ransomware Locky*

No	Spesifikasi Subjek	Deskripsi
1.	Nama *Malware : Ransomware Locky*	Menggunakan *malware ransomware Locky* pertama dilihat pada 2024-05-22 23:11:24 UTC
2.	Jenis : *Ransowmare Crypto*	Jenis *Crypto malware* yang merusak serta mengenkripsi data penting
3.	SHA256 hash : 3329641a171508fa6b1ad7674b31431093d46be190d1a51acd77e486f42d9c8e	Memiliki SHA sebagai berikut
4.	Sumber : Malware Bazaar	Diunduh dari website malware bazaar link :

		https://bazaar.abuse.ch/sample/3329641a171508fa6b1ad7674b31431093d46be190d1a51acd77e486f42d9c8e/

c. Spesifikasi *Host* Utama

Table 3.3. Informasi *host* utama

No	Spesifikasi host	Deskripsi
1.	Nama Perangkat : *Lenovo Thinkpad*	Menggunakan perangkat *Lenovo thinkpad*
2.	Memori Perangkat :16384MB RAM	Perangkat memiliki 16GB RAM, sehingga memungkinkan untuk melakukan analisis secara maksimal
3.	Sistem Operasi : *Windows 10 Pro*	Menggunakan *windows 10 pro* dengan update terbaru Maret 2024
4.	Versi : 22H2	Memiliki versi 22H2 versi yang sudah mensuport berbagai *tools* termasuk analisis yang dilakukan

d. Spesifikasi *Virtualbox*

Tabel 3.4. Informasi Spesifikasi *Virtualbox*

No	Spesifikasi Aplikasi	Deskripsi
1.	Nama Aplikasi : *Virtualbox*	Menggunakan *virtualbox* dengan *update* pada Mei 2024
2.	Versi : *Virtualbox 7.0.18*	*Virtualbox 7.0.18* merupakan *update* terbaru saat ini.
3.	Jenis : *Windows Host*	Jenis *windows host* yang memungkinkan memberi dukungan pemasangan di *windows.*
4.	Sumber : *Website* resmi *virtualbox*	Diunduh dari virtualbox langsung link : https://www.virtualbox.org/wiki/Downloads

e. Spesifikasi *Tools* Perekam

Berikut adalah beberapa *tools* yang digunakan untuk melakukan analisis :

Tabel 3.5. Informasi *Tools* Perekam

No	Alat / *Tools*	Kegunaan
1.	*Procmon*	*Procmon* adalah alat yang digunakan untuk memantau aktivitas *registry* secara *realtime.*
2.	*Regshot*	*Regshot* adalah alat yang digunakan

		untuk melakukan perbanding sebelum terinfeksi dan sesudah terinfeksi.
3.	*FakeNet*	*FakeNet* digunakan untuk megelabui *malware* ketika menghubungi server melalu internet dan mencatatnya.
4.	*Procdot*	*Procdot* digunakan untuk melakukan virtualiasa dari hari *procmon* yang sudah disimpan

Pada table-tabel sudah dijelaskan spesifikasi serta kebutuhan yang akan digunakan pada analisis perilaku *malware ransomware locky*, *system* dan *tools* yang digunakan merupakan hasil dari pertimbangan kebutuhan dan keterbaruan.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Implementasi

Pada bab ini penulis akan melakukan pendekatan untuk mengetahui karakteristik dan dampak dari *malware Ransomware Locky* dengan cara menjalankan *malware* pada virtual machine *windows 10* sebagai objek penelitian, dengan didukung *framework Flarevm* sebagai standar keamanan dan alat analisis dengan konfigurasi yang sudah ditentukan agar ketika *malware* dijalankan tidak dapat menginfeksi tempat yang tidak diingin serta agar dapat menganalisis dari aktivitas registry dan alamat ip yang dihubungi.

4.2 Konfigurasi *Flarevm*

Dalam proses ini ada beberapa tahap yang harus diperhatikan sebelum pemasangan *flarevm*, walaupun penginstalan dilakukan secara otomatis. Ada beberapa hal yaitu :

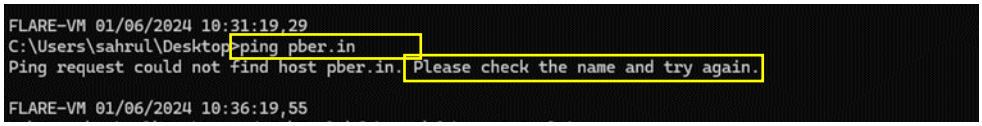
- Nonaktifkan windows defender (Gpedit.msc)
- Nonaktifkan windows update (Regedit)
- Powershell 5 Minimal
- Minimal Windows 10

Setelah beberapa hal diatas disesuaikan maka selanjutnya melakukan instalasi *flarevm* secara otomatis sesuai dengan panduan yang ada.

Gambar 4.1. Tampilan Utama *Flarevm*

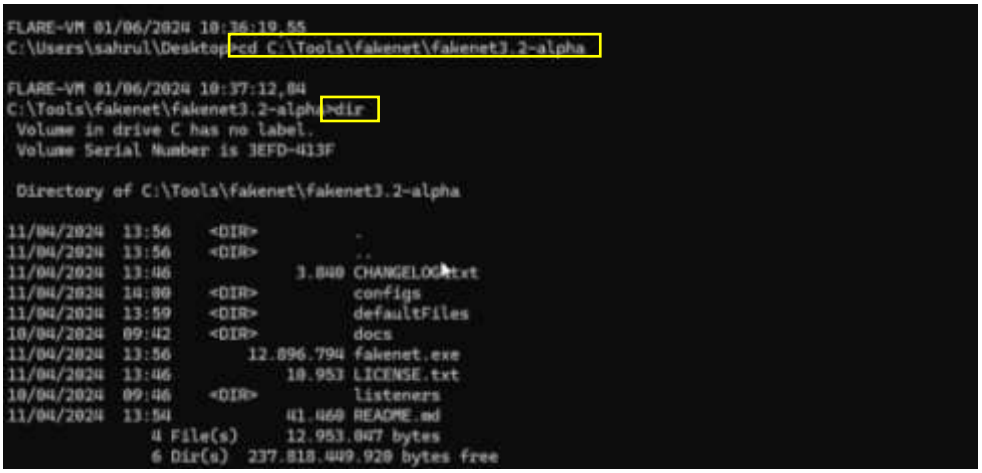
4.3 Konfigurasi jaringan

Konfigurasi jaringan disini menggunakan bantuan tools dari flarevm yaitu fakenet, dengan mengatur fakenet maka tidak memungkinan untuk *malware* bisa berkomunikasi dengan jaringan publik karena akan secara otomatis dialihkan kepada fakenet, berikut froses konfigurasi yang dilakukan :



Gambar 4.2. Memastikan Internet Terputus

Setelah memastik an koneksi internet terputus selanjunya kita pergi ke direktori Fakenet



Gambar 4.3. Konfigurasi Fakenet

Dan setelah itu run fakenet.exe serta output.log

Gambar 4.4. Fakenet Berhasil

4.4 Pengujian

Tahap pengujian *malware* kali ini terdapat beberapa kategori yang diambil dari hasil pengujian (Aktivitas Registri, Jaringan Lokal, Perbandingan) berikut hasil dari pengujian yang dilakukan :

4.4.1. Procmon

Procmon adalah untuk mencatat secara detail aktivitas *registry*, ketika *malware* dijalankan selanjutnya procmon dijalankan agar dapat menangkat dari setiap langkah yang dilakukan *malware*, berikut hasil laporan dari *procmon* :

Table 4.1. Hasil Procmon

- 08:06:26,6775980,"*Ransomwarelocky*.exe","3656","ReadFile","C:\Windows\SysWOW64\wininet.dll","SUCCESS","
- 08:06:26,6845131,"*Ransomwarelocky*.exe","3656","RegQueryKey","HKLM","SUCCESS
- 08:06:26,6607371,"*Ransomwarelocky*.exe","3656","RegOpenKey","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform","SUCCESS","
- 08:06:26,7071491,"*Ransomwarelocky*.exe","3656","CloseFile","C:\Windows\SysWOW64\ws2_32.dll","SUCCESS","","4000”
- 08:05:42,9663416,"svchost.exe","3184","LockFile","C:\Users\sahrul\AppData\Local\ConnectedDevicesPlatform\L.sahrul\ActivitiesCache.db-shm","SUCCESS","Exclusive: False, Offset: 124, Length: 1, Fail Immediately: True","1544"

Aktivitas *resgistry* yang dihasilkan *procmon* sekitar 43925, dan sample dari hasil diatas merupakan bentuk dominan yang dilakukan. Setelah data bersihkan dan dilakukan analisis berikut jumlah dominan dari perilaku malware :

Tabel 4.2. Hasil Perilaku *Malware*

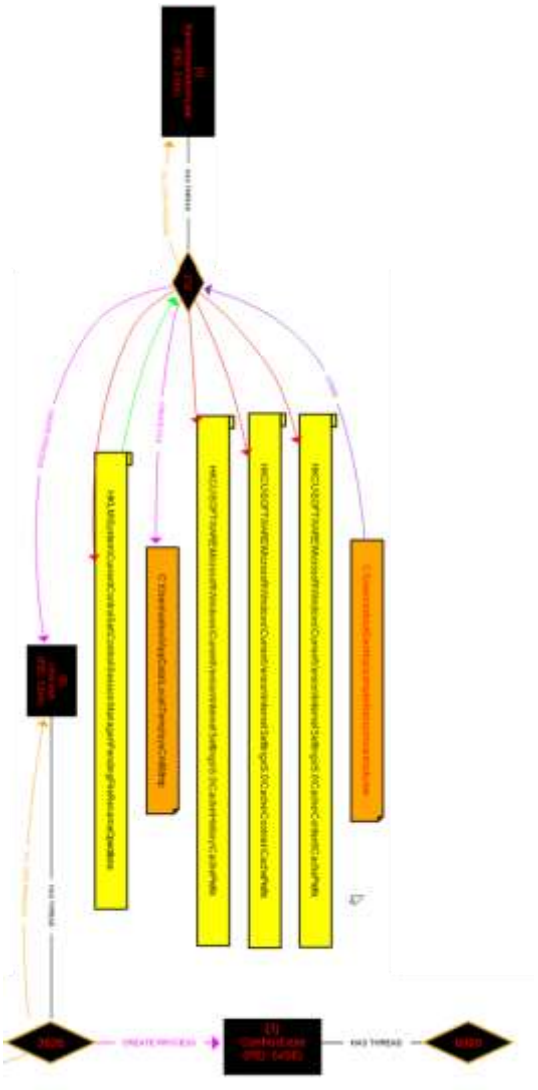
No	**Perintah**	**Jumlah**
1.	*RegOpenKey*	10733
2.	*RegQueryKey*	9972
3.	*RegQueryValue*	9502

4.	*CreateFile*	947
5.	*LockFile*	560

Karena tidak mungkin dibahasi satu persatu maka perlu bantuan alat yang bisa memvirtualisasi dari hasil aktivitas registri yang dilakukan yaitu menggunakan procdot.

4.4.2. *Procdot*

Dari hasil aktivitas *registry* yang berhasil ditangkap oleh procmon selanjutnya kita akan melakukan virtulalisasi dengan *procdot* agar lebih jelas dan terlihat kemana saja *malware* masuk :



Gambar 4.5. Proses *Malware* Menginfeksi Sistem

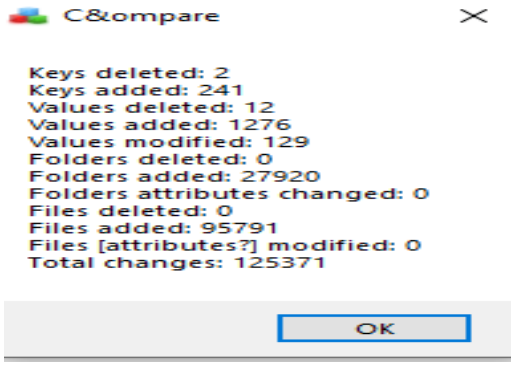
4.4.3. *Regshot*

Regshot adalah alat digunakan untuk membandingan registri sistem saat belum terkena *malware* dan saat sudah terinfeksi berikut hasil dari pengujian yang dilakukan. Berikut adalah hasil shot pertama :

Tabel 4.3. Pengambilan Shot Pertama

Hasil	Deskripsi
renderoption_registry = 1 renderoption_registry_nonautostart = 1 renderoption_registry_get = 1 renderoption_registry_set = 1 renderoption_files = 1 renderoption_files_bulkcategories = 1 renderoption_files_readonly = 0 renderoption_files_read = 1 renderoption_files_write = 1 renderoption_files_create = 1 renderoption_files_delete = 1 renderoption_files_basedon = 1 renderoption_files_loads = 1	Pada hasil shot pertama terlihat bahwa tidak ada perubahan *registry* yang siginifikan hal tersebut disebabkan karena sistem operasi masih berada didalam keadaan normal/belum terenkripsi malware.

Tahapan selanjutnya melakukan *shot* kedua dengan hasil perbandingan dari shot pertama yang sudah dilakukan. Berikut hasil dari perbandingannya :



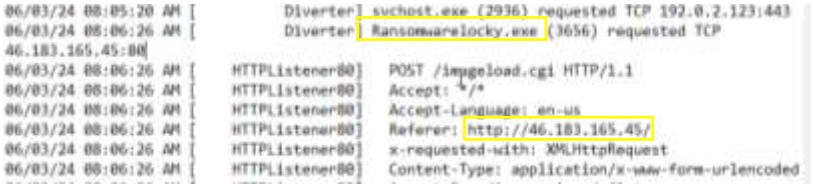
Gambar 4.6. Hasil *Regshot*

Berdasarkan dari hasil *compare*/perbandingan menggunakan regshot ketika *malware* sebelum menginfeksi dan sesudah mengimfeksi terlihat bahwa

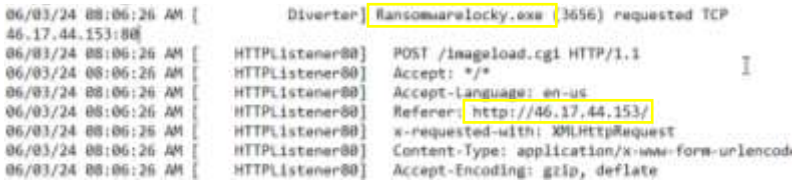
memang sistem terjadi begitu banyak penambahan file (*Added*). Oleh karena itu dampak dari *malware ransomware locky* dominan *Added* atau menambahkan *Key Registry* .

4.4.4. *FakeNet*

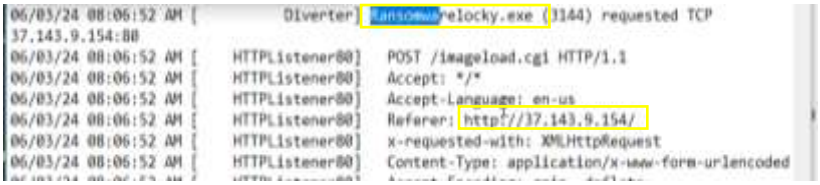
Fakenet digunakan untuk mengelola paket jaringan palsu, setiap *malware* yang berupaya memanggil alamat dari luar akan secara otomatis dialihkan pada *fakenet* dan hasilnya akan dicatat secara lengkap di *fakenet*, berikut hasil laporan dari *fakenet*.



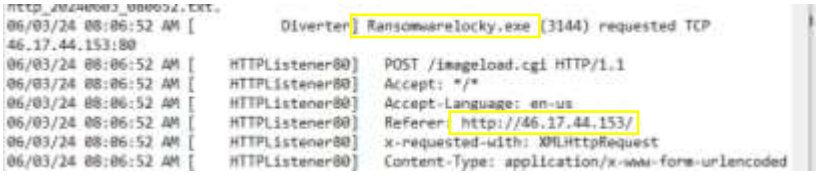
Gambar 4.7. Hasil Fakenet 1



Gambar 4.8. Hasil Faknet 2



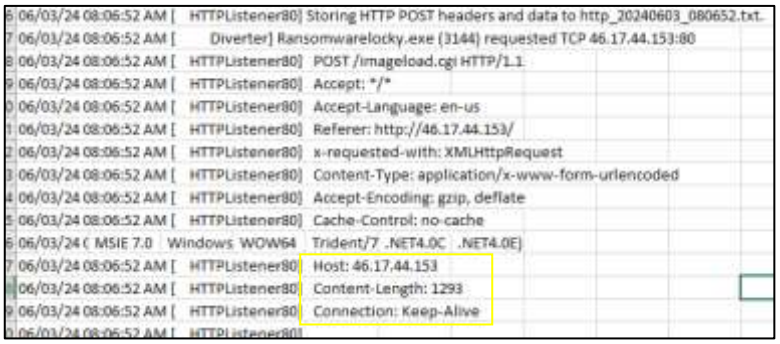
Gambar 4.9. Hasil Fakenet 3



Gambar 4.10. Hasil Faknet 4

Hasil dari pengujian fakenet terlihat bahwa *type* data yang dapat ditransmisikan dan kode perintah untuk mengirim dan menerima data, serta bagaimana transfer data terkonfirmasi dan tipe protol yang digunakan oleh *ransomware locky* adalah *TCP* (*Transmission Control Protocol*) dengan melakukan pemanggilan sebanyak 4 kali.

Berdasarkan hasil analisis jumlah data yang dikirimkan oleh *ransomware* dari ½ *second* itu sebanyak 1293 *byte*



Gambar 4.11. Jumlah *Byte* Pertama

Gambar 4.12. Jumlah *Byte* Kedua

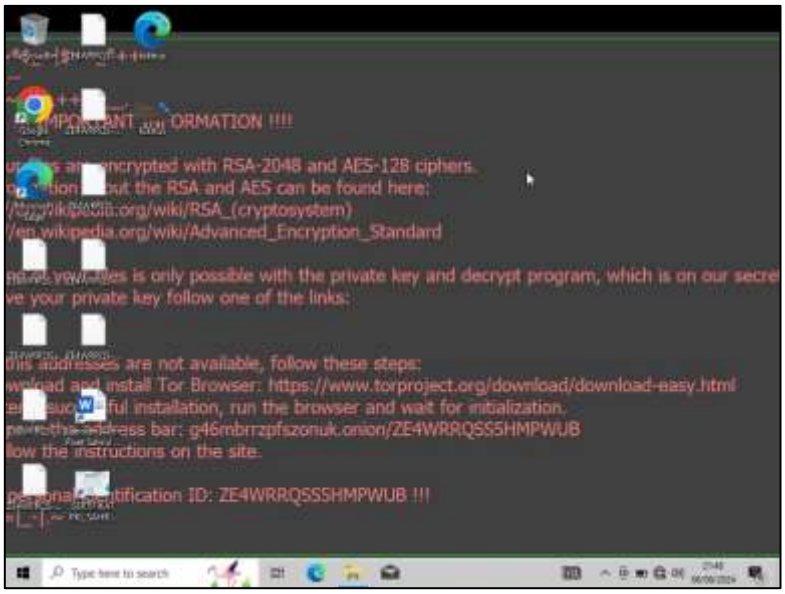
Pada gambar diatas dapat kita lihat untuk membuktikan bahwa kekuatan mengirim dan menerima data sangat kecil.

4.5 Dampak

Disini akan dijelaskan dampak pada sistem operasi windows 10 setelah dijalankan *malware* terlihat dampak yang signifikan terhadap sistem operasi windows yaitu :

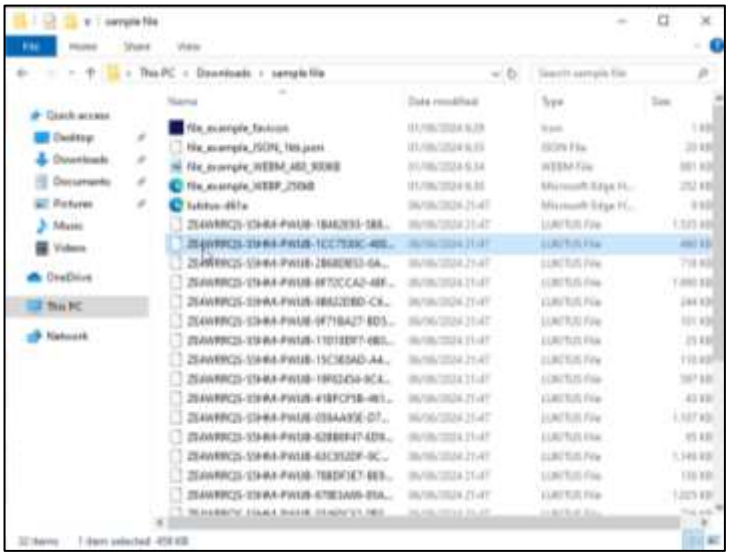
Gambar 4.11. Dampak Notifikasi

Setelah *malware* dijalankan selanjutnya *malware* akan memberi notifikasi bahwa file kita di enkripsi dan mengarahkan kita untuk melakukan pembayaran.



Gambar 4.12. Dampak *Wallpaper*

Dari gambar diatas terlihat dengan jelas bahwa setelah *malware* berjalan dan menginfeksi wallpaper kita akan berubah menjadi tampilan seperti diatas.



Gambar 4.13. Dampak Pada *File*

Semua file penting yang kita letakan di sistem operasi akan berubah nama nama menjadi (LUKITUS File), itu menandakan bahwa file berhasil dienkripsi dan harus dibayar untuk bisa membuka kembali.

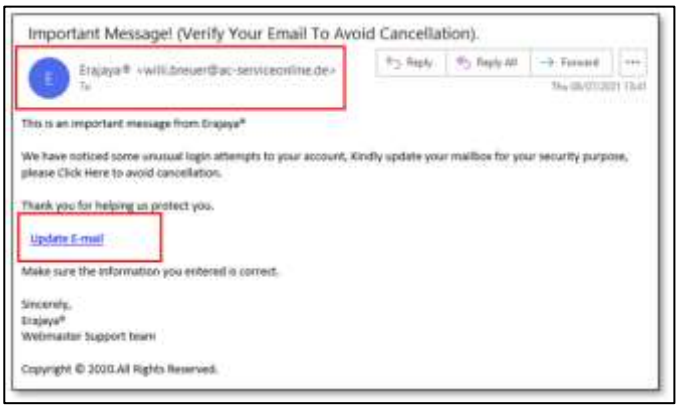
4.6 Hasil Rekomendasi Peningkatan Keamanan

Hasil rekomendasi ini didapatkan berdasarkan hasil analisis, diharapkan Dengan mengimplementasikan rekomendasi ini, baik pengguna biasa sebagai user maupun pengembang dapat meningkatkan tingkat keamanan sistem mereka terhadap ancaman seperti ransomware dan serangan malware lainnya. Langkah preventif yang tepat dapat mengurangi risiko dan dampak dari serangan keamanan komputer.

4.6.1. Untuk Pengguna Biasa

Sebagai pengguna biasa, langkah-langkah berikut dapat membantu meningkatkan keamanan komputer Anda:

1. Aktifkan *Windows Defender* dan Perbarui Secara Berkala: sebaiknya aktifkan dan pastikan *update* definisi virus terbaru telah diinstal untuk perlindungan terhadap *malware* termasuk *ransomware* seperti *locky*.
2. Perbarui Sistem Operasi dan Aplikasi Secara Teratur: Pastikan sistem operasi *Windows* dan aplikasi yang Anda gunakan selalu diperbarui dengan *patch* keamanan terbaru. Ini membantu dalam menutup celah keamanan yang dapat dieksploitasi oleh *malware*.
3. Waspadai *Email Phishing*: Jangan mengklik tautan atau lampiran dari *email* yang tidak dikenal atau mencurigakan. *Ransomware* sering kali menyebar melalui *email phishing*.



Gambar 4.14. Contoh *Email Phising*

4. *Backup* Data Secara Berkala: Simpan salinan cadangan data penting Anda di luar perangkat yang terhubung secara langsung ke *internet*. Jika terinfeksi

ransomware, Anda memiliki salinan data yang dapat dipulihkan tanpa membayar tebusan.

5. Gunakan Aplikasi Keamanan: Instal dan aktifkan perangkat lunak keamanan yang terpercaya, termasuk *firewall* dan aplikasi anti-malware.

BAB V
KESIMPULAN

5.1. Kesimpulan

Berdasarkan hasil pengujian dengan analisis dinamis *framework flarevm* yang sudah dilakukan di penelitian skripsi ini dapat disimpulkan bahwa :

1. *Malware ransomware locky* adalah jenis *malware* yang sangat berbahaya, karena dapat mengenkripsi semua file yang ada sistem dan minta tebusan untuk bisa mengaksesnya kembali.
2. Kecenderungan atau perilaku dari *malware ransomware locky* ketika mengenkripsi *windows 10* itu menambahkan (menambahkan value atau key agar file yang terinfeksi tidak dapat dibuka).
3. Protokol internet yang digunakan untuk mengirim dan menerima data oleh *malware ransomware locky* adalah TCP (*Transmission Control Protocol*).

5.2. Saran

Maka sangat disarankan bagi pengguna leptop atau komputer agar lebih berhati-hati baik dalam hal mengakses internet, link tidak jelas, dokumen tidak jelas dan hal-hal lain yang sifatnya mencurigan. mengingat penyebaran *malware* sangat cepat sehingga sebisa mungkin lakukan pencegahan sebelum terjadi.

DAFTAR PUSTAKA

[1] H. Novansyah and T. Sutabri, "Analisis Malware Dengan Metode Dinamik Menggunakan Framework Cuckoo Sandbox," *Blantika Multidiscip. J.*, vol. 2, no. 1, pp. 79–85, 2023, doi: 10.57096/blantika.v2i1.15.

[2] F. A. Rafrastara, C. Supriyanto, C. Paramita, and Y. P. Astuti, "Deteksi Malware menggunakan Metode Stacking berbasis Ensemble," *J. Inform. J. Pengemb. IT*, vol. 8, no. 1, pp. 11–16, 2023, doi: 10.30591/jpit.v8i1.4606.

[3] F. Peter, G. George, K. Mohammed, and U. B. Abubakar, "Evaluation of Classification Algorithms on Locky Ransomware Using Weka Tool," *Open J. Phys. Sci. (ISSN 2734-2123)*, vol. 3, no. 2, pp. 23–34, 2022, doi: 10.52417/ojps.v3i2.382.

[4] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: Evolution, mitigation and prevention," *Egypt. Informatics J.*, vol. 22, no. 1, pp. 105–117, 2021, doi: 10.1016/j.eij.2020.05.003.

[5] Gilang Ramadhan, "Perlindungan Hukum Bagi Korban Ransomware Wannacry Tindak Pidana Ransomware," *J. Kaji. Kontemporer Huk. Dan Masy.*, pp. 1–15, 2023, doi: 10.11111/dassollen.xxxxxxx.

[6] A. Singh *et al.*, "Securing Cloud-Encrypted Data: Detecting Ransomware-as-a-Service (RaaS) Attacks through Deep Learning Ensemble," *Comput. Mater. Contin.*, vol. 79, no. 1, pp. 857–873, 2024, doi: 10.32604/cmc.2024.048036.

[7] V. A. Manoppo, A. S. . Lumenta, and S. D. . Karouw, "Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi," *Tek. Elektro Dan Komput.*, vol. 9, no. 3, p. 182, 2020.

[8] K. M. Fitria, "Analisis Serangan Malware Dalam Perbankan Dan Perencanaan Solusi Keamanan," *J. Inform. dan Tek. Elektro Terap.*, vol. 11, no. 3, 2023, doi: 10.23960/jitet.v11i3.3312.

[9] E. V. Tjahjadi and B. Santoso, "Klasifikasi Malware Menggunakan Teknik Machine Learning," *J. Ilm. Ilmu Komput.*, vol. 2, no. 1, pp. 60–70, 2023.

[10] K. Ibrahim, "Analisis Perilaku Malware Malware Menggunakan Metode Analisis Dinamis," vol. 10, no. 5, pp. 4122–4125, 2023.

[11] Ley 25.632, “済無No Title No Title No Title,” vol. 5, no. 2, pp. 207–217, 2002.

[12] 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

[13] 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.

[14] R. B. Hadiprakoso, W. R. Aditya, and F. N. Pramitha, “Analisis Statis Deteksi Malware Android Menggunakan Algoritma Supervised Machine Learning,” *Cyber Secur. dan Forensik Digit.*, vol. 5, no. 1, pp. 1–5, 2022, doi: 10.14421/csecurity.2022.5.1.3116.

[15] M. Santonario, Frenvol De. Moises, “Analisis Malware Android Menggunakan Reverse Engineering,” vol. 1, no. 2, pp. 41–53, 2023.

[16] N. K. T. Srilaksmi, M. Erkamim, N. Dzakiah, N. K. A. Suardana, and N. K. S. D. P. Swambini, “An Examination of Cybercrimes Leading to Vulnerabilities in Energy, Transportation, and Financial Systems,” *J. Digit. Law Policy*, vol. 3, no. 1, pp. 38–51, 2023, doi: 10.58982/jdlp.v3i1.509.

[17] A. R. Damanik, H. B. Seta, and T. Theresiawati, “Analisis Trojan Dan Spyware Menggunakan Metode Hybrid Analysis,” *J. Ilm. Matrik*, vol. 25, no. 1, pp. 89–97, 2023, doi: 10.33557/jurnalmatrik.v25i1.2327.

[18] N. Qomariah, E. I. Alwi, and M. A. Asis, “Analisis Malware Hummingbad Dan Copycat Pada Android Menggunakan Metode Hybrid Analysis Of Hummingbad And Copycat Malware On Android Using Hybrid Methods,” vol. 6, no. 2, pp. 39–47, 2023.

[19] T. Survei, M. N. Olaimat, B. A. S. Al-rimy, and S. Komputasi, “Anti-Analisis dan Penghindaran Ransomware,” 2022.

[20] Y. Kishon, “Ransomware Victims and Network Access Sales in Q1 2022,” 2023.