Terbit online pada laman web jurnal: **https://ejurnalunsam.id/index.php/jicom/**

Jurnal Informatika dan Teknologi Komputer

Vol. 06 No. 02 (2025) 89 - 94 E-ISSN :2774-7115 P-ISSN: 2775-2089

Analisis Perilaku Dan Dampak Malware Ransomware Locky Metode Dinamis Framework Flarevm

Sahrul ismail Usman[1], Somantri[2], Anggun Fergina[3]

[1,2,3]Teknik Informatika, Fakultas Teknik, Komputer dan Desain, Universitas Nusa Putra

[1]sahrul.ismail_ti20@nusaputra.ac.id*, [2]somantri@nusaputra.ac.id, [3]anggun.fergina@nusaputra.ac.id

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: Dynamic Analysis, Malware, Ransomware Locky.

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 malwarenya 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 analisa 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).

Kata kunci: Analisis Dinamis, *Malware, Ransomware Locky*.

1. Pendahuluan

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 system[2] serta secara karakteristik dan perilakunya dapat dibedakan menjadi 2 yaitu crypto dan locker[3], varian crypto yang diluncurkan sebagai bagian dari langkah pemerasan dimana data di enkripsi untuk meminta korban membayar[4] yang selanjutnya disebut locky. locky adalah varian ransomware, locky ditemukan sekitar tahun 2016[5] yang memang perkembangannya terus-menerus tumbuh hingga sekarang, maka dari itu perlunya pemantauan serta analisis yang terus menerus dan berkelanjutan.

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 yang salah satu bentuk dari RaaS adalah locky, hal ini memungkinkan para penjahat yang tidak memiliki keterampilan terhadap pengembangan malware bisa meluncurkan serangan dengan cepat dan mudah[6]. menurut IEEE menyebutkan mereka meninjau penelitian yang ada

Diterima Redaksi : 12-07-2025 | Selesai Revisi : 25-07-2025 | Diterbitkan Online : 01-10-2025

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 pesatnya perkembangan malware 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 selama proses eksekusi dan infeksi malware[10], untuk mengetahui aktivitas registri[1], alamat yang dipanggil, dampak sistem yang terinfeksi serta fungsi parameter yang ada dan juga arus informasi yang dilakukan malware. Metode dinamis dibantu dengan beberapa tool yang akan menangkap setiap aktivitas yang dilakukan oleh malware, sehingga memungkinkan peneliti untuk mengamati dan mengidentifikasi secara mendalam terhadap perilaku malware ransomware locky.

Dengan beberapa referensi penelitian terdahulu sebagai bahan contoh panduan bagi peneliti yaitu meliputi "Analisis Perilaku Malware Malware Menggunakan Metode Analisis Dinamis" ditulis oleh Khalif Ibrahim dan kawan-kawan (2023) penelitian tersebut menunjukan tentang melakukan analisis karakteristik malware dan faktor-faktor yang dianalisa Ketika melakukan analisis malware penelitian diatas juga menunjukan tentang metode analisis dinamis pada malware dengan menjalankan malware itu sendiri[12], "Analisis Ransomware Wannacry Menggunakan Aplikasi Cuckoo Sandbox" disusun oleh Gratiyo Wahyu Wahidin, Syaifuddin, Zamah Sari (2022) penelitian tersebut memberi referensi terhadap penulis terhadap penggunaan framework karena untuk melakukan analisis malware ransomware sangat berbahaya dan beresiko sehingga harus ada benteng yang kuat yang dapat menjaga gerak dari ransomware itu sendiri.

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.

Adapun tujuan dari penelitian ini untuk melakukan analisis malware Ransomware Locky SHA 1 Hash : 97bae63417df5bde4a05cd44c6c523db50f6ab76 dengan menggunakan metode dinamis framework flarevm, Mengetahui aktivitas registry dan dampak pada sistem virtual machine windows 10 serta Mengetahui karakteristik malware ransomware locky.

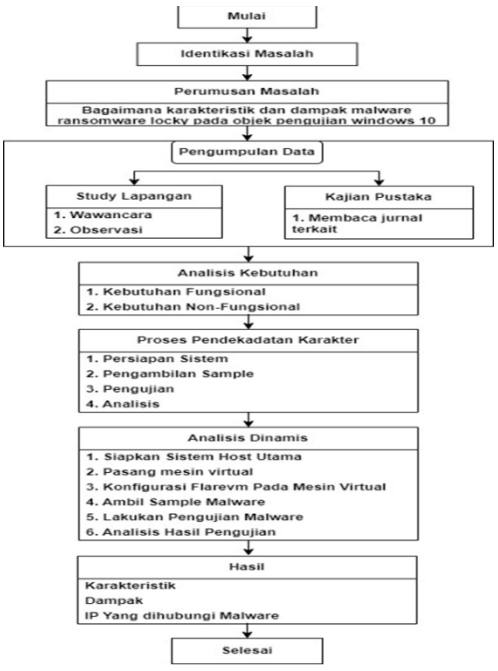
2. Metode Penelitian

2.1. Metode Pengumpulan Data

Metode penelitian yang digunakan 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.Metode dideskripsikan secara rinci yang memuat desain, populasi, sampel dan teknik pengambilan sampel, cara kerja penelitian, parameter yang diamati, serta teknis analisis. Metode ditulis dalam bentuk naratif dengan menyampaikan pentingnya cara penelitian dilakukan. Segala bentuk instruksi, manual atau manual teknis dalam kegiatan penelitian yang terlalu rinci tidak boleh dimasukkan.

2.2. Perencanaan Penelitian

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



Gambar 1. Tahapan Penelitian

2.3 Analisis Kebutuhan

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

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 :

a. Observasi

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

b. Wawancara

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

c. 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.

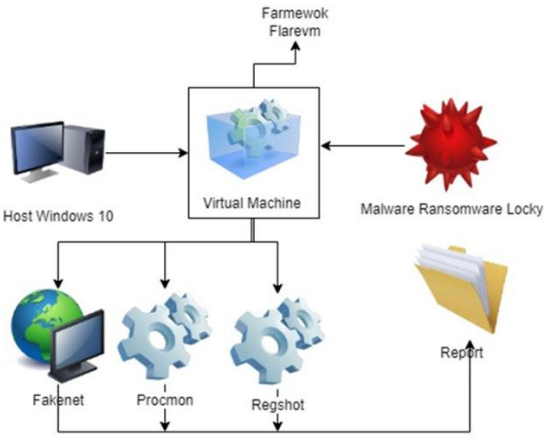
2. Data Fungsional

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.

2.4 Metode Analisis

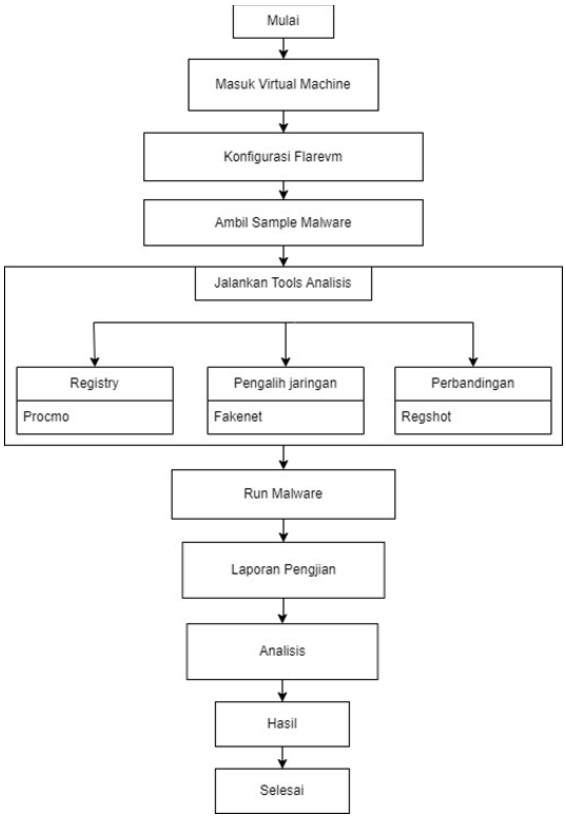
Metode dinamis digunakan untuk mengetahui perilaku malware dengan menjalankan malware itu sendiri dalam ruang lingkup yang diawasi[13], maka dari itu dibutuhkan virtual machine atau virtualbox untuk membatasi serangan dari malware tersebut. Tahap pertama malware diupload pada Flarevm dan FlareVm akan melakukan analisis secara otomatis, Setelah menjalankan malware pada sistem yang diawasi perlu beberapa tool untuk mencatat atau menangkap setiap gerakan pada malware tersebut[14], 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 dimana dilakukan perbandingan snapshot pada saat malware dijalankan dan tidak.

1. Desain Topologi



Gambar 2. Desain Topologi

2. Tahapan Analisis



Gambar 3. Tahapan Analisis

3. Hasil dan Pembahasan

3.1. 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.

3.2. Konfigurasi Flarevm

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

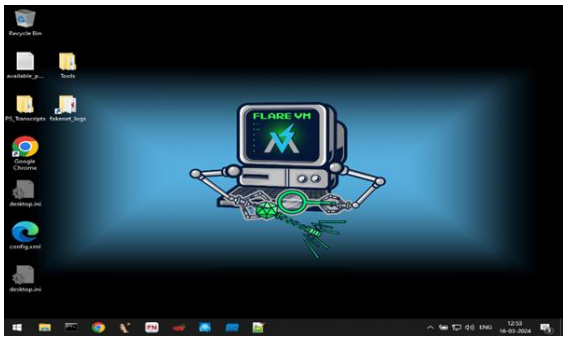
a. Nonaktifkan windows defender (Gpedit.msc)

b. Nonaktifkan windows update (Regedit)

c. Powershell 5 Minimal

d. Minimal Windows 10

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



Gambar 4. Tampilan Utama Flarevm

3.3. 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 5. Memastikan Internet Terputus

a. Setelah memastikan koneksi internet terputus selanjunya kita pergi ke direktori Fakenet



Gambar 6. Konfigurasi Fakenet

b. Dan setelah itu run fakenet.exe serta output.log



Gambar 7. Fakenet Berhasil

3.4. 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 :

3.3.1. Procmon

Procmon adalah alat untuk membantu dalam mengumpulkan, menganalisis, dan melaporkan indikator runtime malware[15], 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 :

- 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"

Gambar 8. Hasil Procmon

Aktivitas resgistri yang dihasilkan procmon sekitar 43925, dan sample dari hasil diatas merupakan bentuk dominan yang dilakukan. Karena tidak mungkin dipahasi satu persatu maka perlu bantuan alat yang bisa memvirtualisasi dari hasil aktivitas registri yang dilakukan yaitu menggunakan procdot.

3.3.2. Procdot

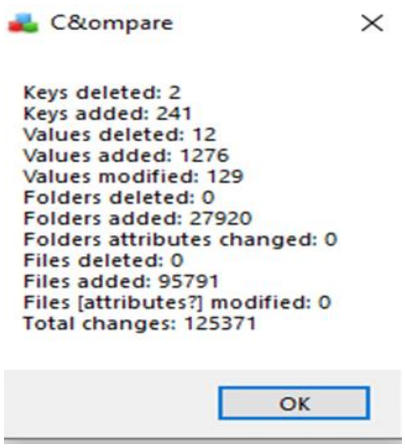
Dari hasil aktivitas registri yang berhasil ditangkap oleh procmon selanjutnya kita akan melakukan virtulalisasi dengan procdot agar lebih jelas dan terlihat kemana saja malware masuk :



Gambar 9. Proses Malware Menginfeksi Sistem

3.3.3. Regshot

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



Gambar 10. 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 karakteristik dari malware ransomware locky dominan Added atau menambahkan.

3.3.3. 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 11. Hasil Fakenet 1



Gambar 12. Hasil Fakenet 2



Gambar 13. Hasil Fakenet 3

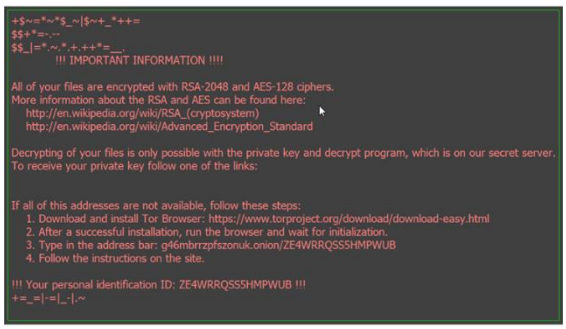


Gambar 14. Hasil fakenet 4

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 type protol yang digunakan oleh ransomware locky adalah TCP (Transmission Control Protocol) dengan melakukan pemanggilan sebanyak 4 kali.

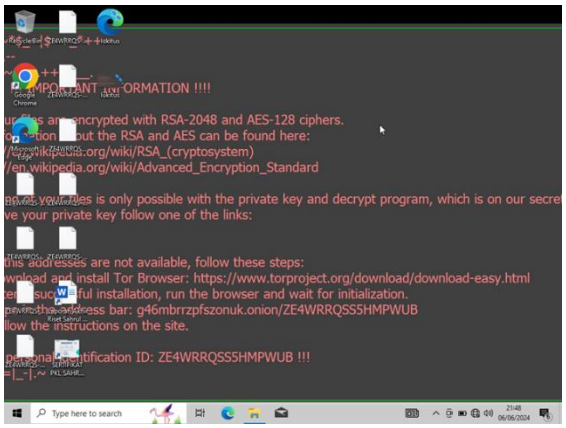
3.4. Pengujian

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



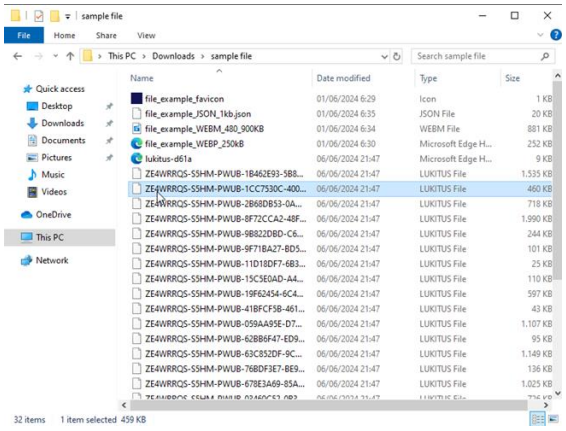
Gambar 15. Dampak Notifikasi

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



Gambar 16. Dampak Tampilan Layar

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



Gambar 17. File Terenkripsi

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. 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).Kesimpulan berisi ringkasan hasil pembahasan dan generalisasi atas hasil penelitian yang dilakukan.

Daftar Rujukan

[1] Novansyah, H., & Sutabri, T. (2023). Analisis Malware Dengan Metode Dinamik Menggunakan Framework Cuckoo Sandbox. Blantika : Multidisciplinary Journal, 2(1), 79–85. https://doi.org/10.57096/blantika.v2i1.15

[2] Rafrastara, F. A., Supriyanto, C., Paramita, C., & Astuti, Y. P. (2023). Deteksi Malware menggunakan Metode Stacking berbasis Ensemble. Jurnal Informatika: Jurnal Pengembangan IT, 8(1), 11–16. https://doi.org/10.30591/jpit.v8i1.4606

[3] Sistematis, T., & Sheldon, F. T. (2022). Survei Deteksi Serangan Crypto Ransomware Metodologi: Pandangan yang Berkembang.

[4] Peter, F., George, G., Mohammed, K., & Abubakar, U. B. (2022). Evaluation of Classification Algorithms on Locky Ransomware Using Weka Tool. Open Journal of Physical Science (ISSN: 2734-2123), 3(2), 23–34. https://doi.org/10.52417/ojps.v3i2.382

[5] Humayun, M. (2021). Machine Translated by Google Jurnal Informatika Mesir Internet of Things dan Ransomware : Evolusi , Mitigasi dan pencegahan Machine Translated by Google. 22, 105–117.

[6] Singh, A., Abosaq, H. A., Arif, S., Mushtaq, Z., Irfan, M., Abbas, G., Ali, A., & Mazroa, A. Al. (2024). Securing Cloud-Encrypted Data: Detecting Ransomware-as-a-Service (RaaS) Attacks through Deep Learning Ensemble. Computers, Materials and Continua, 79(1), 857–873. https://doi.org/10.32604/cmc.2024.048036

[7] Manoppo, V. A., Lumenta, A. S. ., & Karouw, S. D. . (2020). Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi. Teknik Elektro Dan Komputer, 9(3), 182.

[8] Fitria, K. M. (2023). Analisis Serangan Malware Dalam Perbankan Dan Perencanaan Solusi Keamanan. Jurnal Informatika Dan Teknik Elektro Terapan, 11(3). https://doi.org/10.23960/jitet.v11i3.3312

[9] Tjahjadi, E. V., & Santoso, B. (2023). Klasifikasi Malware Menggunakan Teknik Machine Learning. Jurnal Ilmiah Ilmu Komputer, 2(1), 60–70.

[10] Ibrahim, K. (2023). Analisis Perilaku Malware Malware Menggunakan Metode Analisis Dinamis. 10(5), 4122–4125.

[11] ASLAN, Ö., & AKİN, E. (2022). Malware Detection Method Based on File and Registry Operations Using Machine Learning. Sakarya University Journal of Computer and Information Sciences, 5(2), 134–146. https://doi.org/10.35377/saucis...1049798

[12] Qudamah, R., Widjajarto, A., & Almaarif, A. (2023). Analisis Karakteristik Antivirus Berdasarkan Metrik Sumber Daya Komputasi dan Indikator Pendeteksian. 10(5), 4765–4770. https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/21293

[13] Sianipar, V. R., & Pangaribuan, H. (2023). Analisis Dan Deteksi Malware Pada Protokol Jaringan Menggunakan Metode Malware Analisis Dinamis Dan Malware Analisis Statis. Computer and Science Industrial Engineering (COMASIE), 9(6). https://doi.org/10.33884/comasiejournal.v9i6.7833

[14] Denham, B., & Denham, B. (2022). ScholarWorks @ UARK Computer Science and Computer Engineering Ransomware and Malware Sandboxing..

[15] Aboud, M. A., & Mariyappn, K. (n.d.2022). Conducting Static and Dynamic analysis Techniques over Spyware.