

Systematic Literature Review: Implementasi Metode Statis Dan Dinamis Pada Analisa Malware

Deni Prayitno^{a*}, Nugroho Adhi Santoso^b, Rifki Dwi Kurniawan^c,

^{abc} STMIK TEGAL

*Deni Prayitno, Alamat Email: deniprayitno33@gmail.com

Diterima : 19 Desember 2022 - Direview : 21 Desember 2022 - Diterbitkan : 31 Desember 2022

Intisari

Perkembangan teknologi yang terus menerus menciptakan peluang untuk kejahatan dunia maya menggunakan Internet. Salah satu jenis kejahatan dunia maya yang dapat merugikan individu atau bisnis adalah serangan malware. Malware adalah perangkat lunak yang sengaja dirancang untuk mencuri data, memanipulasinya, dan mendapatkan akses penuh ke server yang terinfeksi. Salah satu malware yang dapat menyusup ke komputer pengguna secara diam-diam dan jarak jauh adalah malware Poison Ivy, yang dikenal sebagai "Remote Acces Trojan" karena dapat mengambil kendali penuh melalui pintu belakang. Dalam proyek ini, malware Poison Ivy akan dianalisis untuk mengetahui cara kerja malware Poison Ivy. Analisis dilakukan dengan menggunakan metode analisis statis dan dinamis, bahwa kombinasi dari metode ini adalah kombinasi yang tepat untuk menganalisis aktivitas malware. Berdasarkan analisis metode kerja malware Poison Ivy, dapat disimpulkan bahwa jika ada beberapa signature, nama file dan string yang telah diperiksa, sebenarnya dapat melakukan proses remote login tanpa terdeteksi oleh pemilik.

Kata Kunci : Analisis Malware; Malware Statis; Malware Dinamis; Remote Acces Trojan

Abstract

The continuous development of technology creates opportunities for cybercrimes using the Internet. One type of cyber crime that can harm individuals or businesses is malware attacks. Malware is software that is intentionally designed to steal data, manipulate it, and gain full access to infected servers. One of the malware that can infiltrate a user's computer secretly and remotely is the Poison Ivy malware, which is known as a "remote access trojan" because it can take complete control through a back door. In this project, the Poison Ivy malware will be analyzed to find out how the Poison Ivy malware works. The analysis was carried out using static and dynamic analysis methods, that the combination of these methods is the right combination to analyze malware activity. Based on the analysis of the working method of the Poison Ivy malware, it can be concluded that if there are several signatures, file names and strings that have been checked, they can actually carry out the remote login process without being detected by the computer owner.

Keywords : Malware Analysis; Malware Dynamic; Malware Static; Remote Acces Trojan

1. Pendahuluan

Komputer membantu orang dalam pekerjaan mereka di era perkembangan teknologi yang konstan di mana kita hidup saat ini. Program yang berjalan di sistem operasi selama penggunaan memainkan peran penting dalam kinerja tugas pengguna. karena komputer dapat menjalankan perintah melalui program tersebut untuk membantu manusia dalam menjalankan tugasnya. Namun, tidak semua program dapat membantu pengguna dan mempermudah pekerjaan mereka. Beberapa perangkat lunak digolongkan sebagai (Malicious Software) karena dirancang untuk merugikan pengguna, atau sering disebut *Malware* (Amdani and Iqbal, 2021).

Di sebuah jaringan, dapat dengan mudah menyebar jika pengguna mengizinkannya. Karena versi baru sering dikembangkan menggunakan strategi yang berbeda untuk menghindari deteksi, sistem deteksi masih menjadi perhatian. Agar terdeteksi secara akurat, metode deteksi perlu ditingkatkan. sebagian besar ditujukan untuk memata-matai orang, mencuri data atau informasi pribadi orang lain (misalnya, di m-banking), membahayakan sistem keamanan,

dan lain-lain (Adenansi and Novarina, 2017). dikembangkan dengan tujuan semata-mata untuk perilaku jahat yang memiliki konsekuensi serius dan negatif bagi korban, seperti penyadapan dan pencurian data (Setia, Aldya and Widiyasono, 2019). Kemampuan untuk melakukan analisis untuk penyelidikan adalah prasyarat untuk setiap penyelidikan. Peningkatan dan evolusinya serta kemampuan beradaptasinya terhadap alat analisis yang digunakan (A. H. Muhammad, 2017).

Analisis memudahkan untuk mengenali tanda tangan yang meluncurkan serangan, dikombinasikan dengan metode berbasis anomali dinamis yang dapat menyederhanakan klasifikasi dan kategorisasi. deteksi cepat. Metode anomali banyak digunakan sebagai pengobatan, yaitu dengan melakukan tindakan pencegahan dengan membaca pola serangan sehingga dapat memprediksi dari mana dan jenis serangan apa yang akan datang (Daniswara *et al.*, 2019). Analisis statis dilakukan dengan menguraikan kode sumber dan kemudian mempelajari dan memahami kode tersebut; dengan kata lain, tidak benar-benar dieksekusi selama proses

analisis. Perilaku kemudian dipelajari untuk mengumpulkan informasi tentang bagaimana dapat berevolusi atau memanipulasi dirinya sendiri, serta informasi tentang komponen sistem mana yang berinteraksi dengan , tidak seperti analisis dinamis, yang dalam proses analisisnya memerlukan salinan (Cahyanto, Wahanggara and Ramadana, 2017). Pada analisis dinamis menggunakan environment buatan seperti virtual machine dan juga sandbox. Dalam konsep identifikasi yang belum diketahui, analisis dinamis lebih baik dari pada analisis secara statis, namun analisis secara statis lebih cepat mengidentifikasi yang sudah diketahui (Aslan and Samet, 2018)

2. Kerangka Teori

2.1. Cybersecurity

Dengan banyaknya orang yang menggunakan internet saat ini, khususnya di Indonesia, sudah menjadi kebutuhan dasar manusia. Namun, dengan banyaknya orang yang menggunakan Internet, sejumlah kejahatan terjadi, sering disebut sebagai kejahatan Internet atau kejahatan dunia maya. Cybersecurity adalah teknologi atau subjek ilmiah yang membantu melindungi kita dari risiko kejahatan dunia maya dan mencegah kejahatan online (Riyandhika and Pratama, 2020). Kajian tentang kejahatan ini membutuhkan cybercriminology, yang merupakan kombinasi pengetahuan dari kriminologi, psikologi, sosiologi, ilmu komputer dan keamanan cyber untuk memberikan pemahaman yang mendalam tentang kejahatan dunia maya (Choi and Lee, 2018).

Untuk menjaga ketersediaan, kerahasiaan, dan integritas informasi, telah dikembangkan suatu metode yang disebut keamanan siber. Dan mekanisme pertahanan ini dirancang untuk melindunginya dari serangan cyber yang juga dikenal sebagai serangan internet. memiliki informasi rahasia yang tidak dapat diungkapkan kepada organisasi atau perusahaan terkait. Oleh karena itu, penting untuk menerapkan teknologi keamanan siber untuk melindungi informasi sensitif yang dimiliki oleh orang, organisasi, dan bisnis (Chairisda, 2020)

2.2. Poison Ivy RAT (Remote Access Trojan)

Poison Ivy RAT adalah program yang dapat terhubung dan mengambil kendali rahasia atas satu atau lebih perangkat komputer (Damage and Intelligence, no date). RAT Poison Ivy beroperasi melalui jaringan, baik lokal maupun publik, memungkinkannya untuk melakukannya dari jarak yang jauh. Poison Ivy RAT menggunakan arsitektur client-server. Dalam hal ini, server merupakan bagian dari aplikasi yang akan ditanamkan (backdoor) dan akan dijalankan pada perangkat korban, yang telah diberikan beberapa pengaturan seperti IP address dan port untuk dapat terhubung ke aplikasi utama (Call Home) (Nasution and Laksono, 2020).

2.3. Analisis Statis

Dalam metode analisis statis ini, arsip berbahaya tidak diaktifkan secara eksklusif, tetapi dilacak, dicari, dan kemudian dianalisis berdasarkan kode sumber yang ditulis dalam Malware dengan melakukan operasi pada Malware. Proses yang paling mungkin adalah memverifikasi biner ini tanpa eksekusi (Rusdi, Widiyasono and Sulastri, 2019). Misalnya, jika kode sumber menyampaikan berita menarik

seperti struktur data, fungsi yang digunakan, dan grafik panggilan, panggilan dapat diekstraksi. Masalah ini hilang setelah mengkompilasi kode sumber menjadi biner yang dapat dieksekusi dan mencegah analisis lebih lanjut. Beberapa contoh metode analisis statis:

a. Teknik deteksi berbasis signature

Teknik ini menggunakan teknik pencocokan pola, string, atau tanda tangan. Penyerang menyuntikkan tanda tangan ke dalam perangkat lunak, dan tanda tangan ini digunakan untuk mengidentifikasi beberapa jenis Malware. Detektor Malware akan mencari tanda tangan yang ada untuk menemukan kode berbahaya (Dwi Nugraha, Budiono and Almaarif, 2019).

b. Teknik deteksi heuristic

Teknik ini juga dikenal sebagai teknik agresif. Teknik ini mirip dengan deteksi berbasis tanda tangan. Perbedaannya adalah heuristic ini mencari instruksi atau instruksi dalam suatu acara program. Apa yang akan terjadi pada akhir dari teknik ini adalah akan memudahkan penemuan varian baru yang semakin beragam (Aslan and Samet, 2018)

2.4. Analisis Dinamis

Dalam metode ini, file yang akan diuji diaktifkan di lingkungan yang aman pada mesin fisik yang telah disediakan sebagai lab Malware atau dalam bentuk virtual (mesin virtual) sehingga dapat diakses. di komputer ketika file berbahaya menjalankan proses. Analisa Malware dengan menggunakan Reverse engineering merupakan salah satu solusi yang bisa digunakan saat ini (Suryati and Budiono, 2020). Reverse engineering dalam analisis Malware berguna untuk ekstraksi data yang memuat informasi yang ada didalam Malware. Untuk dapat melihat apa yang dilakukan Malware saat berhasil menginfeksi computer . Tujuan utama dari sistem yang diusulkan adalah untuk mendeteksi secara otomatis dengan mengurangi tingkat kesalahan identifikasi Malware. Penggunaan analisis Malware dinamis adalah untuk mendeteksi adanya perilaku jahat. Sistem pertama-tama menangkap jejak eksekusi, sehingga mengidentifikasi jejak berbahaya (Sujoyothi and Acharya, 2017).

3. Metodologi

Cara untuk mengidentifikasi, mengevaluasi, dan menafsirkan penelitian apa pun yang terkait dengan pertanyaan penelitian, bidang, atau fenomena tertentu (Kitchenham, 2004). SLR telah menjadi metode standar untuk mendapatkan jawaban dengan melakukan tinjauan pustaka berdasarkan penelitian sebelumnya yang relevan (Aslan and Samet, 2018). dilakukan untuk berbagai tujuan, termasuk meringkas penelitian sebelumnya, mengidentifikasi informasi yang berguna tentang penelitian yang ada di lapangan, meninjau pertanyaan penelitian yang relevan, dan membuat laporan penelitian yang koheren (Rozi, 2020). Dalam melakukan penelitian, pemahaman yang menyeluruh tentang penelitian merupakan salah satu syarat yang harus dipenuhi oleh peneliti. SLR adalah metode yang memberikan pertanyaan untuk dijawab oleh peneliti. Dalam praktiknya, ini dilakukan dengan mengidentifikasi, memilih, dan mengevaluasi literatur penelitian yang relevan (Larasati, Yusril and Zukri, 2021)

3.1. Pertanyaan Penelitian

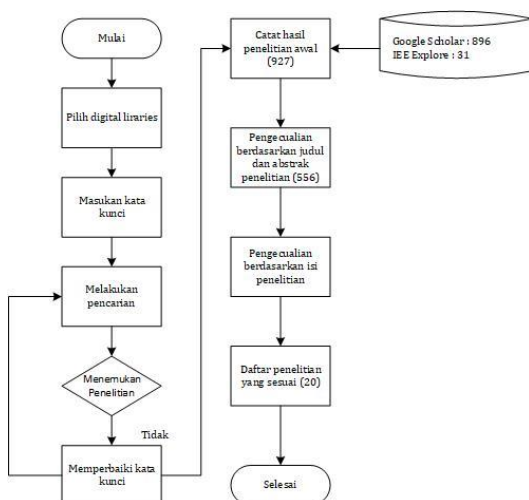
Tujuan dari tinjauan literatur dalam penelitian ini adalah untuk memahami topik penelitian, metode dan fungsi yang digunakan dalam analisis Malware (Triandini et al., 2019). mendapatkan hasil yang komprehensif, penelitian ini menggunakan sejumlah makalah yang dipublikasikan di jurnal database ternama seperti IEEE Xplore, ScienceDirect, Google Scholar dari tahun 2017 hingga 2022. Mereka dikelompokkan berdasarkan pertanyaan penelitian seperti yang ditunjukkan pada Tabel 1 di bawah ini.

Tabel 1. Pertanyaan Penelitian

Pertanyaan Penelitian	Motivasi
Apa saja tujuan topik riset pada bidang Analisis Malware? (RQ1)	Identifikasi tujuan topik riset pada bidang Analisis Malware
Apa saja metode yang digunakan pada Analisis Malware? (RQ2)	Identifikasi metode yang digunakan pada Analisis Malware
Apa saja kelebihan dan kekurangan pada metode yang digunakan? (RQ3)	Identifikasi kelebihan dan kekurangan pada metode yang digunakan

3.2 Seleksi Studi

Studi yang termasuk dalam SLR diterbitkan dalam 5 tahun terakhir dalam bentuk jurnal. Sebelum memulai pencarian, perlu untuk memilih kata kunci yang tepat untuk meningkatkan kemungkinan ditautkan ke artikel yang kita cari. Diskusi analisis dikumpulkan dari daftar database digital terpilih. Oleh karena itu, kata kunci yang digunakan adalah analisis, analisis statis, analisis dinamis, sehingga banyak pengguna keamanan komputer dan jaringan perlu menambahkan kata kunci CNS untuk mengklasifikasikan. Pencarian kata kunci fokus pada judul dan ringkasan. Tahapan proses pencarian dan jumlah penelitian yang teridentifikasi ditunjukkan pada Gambar 1. Pemilihan proses pencarian dilakukan dalam dua tahap, yaitu pemilihan judul dan pemilihan abstrak, serta pemilihan teks lengkap.



Gambar 1. Flowchart Proses Pencarian

Untuk mencapai tujuan penelitian perlu dirancang kriteria inklusi dan eksklusi seperti yang ditunjukkan pada tabel 2 untuk menghindari studi yang tidak sesuai dengan SLR.

Tabel 2. Kriteria Inklusi Dan Eksklusi

Kriteria Inklusi	Kriteria Eksklusi
Literatur yang berfokus pada analisis malware menggunakan metode statis dan dinamis	Literatur yang tidak berfokus pada analisis malware menggunakan metode statis dan dinamis
Literatur menggunakan Bahasa Indonesia dan Bahasa Inggris yang terbit dari tahun 2017 sampai 2022	Literatur yang terbit sebelum tahun 2017

4. Hasil dan Pembahasan

Dari hasil penelusuran publikasi ilmiah pada daftar database digital yang telah dipilih, terpilih beberapa publikasi ilmiah yang dapat dijadikan referensi bagi penulis untuk menjawab pertanyaan penelitian yang telah disusun. Terdapat publikasi ilmiah yang tidak dapat dijadikan sebagai referensi karena tidak secara khusus membahas metode statis dan dinamis untuk menganalisa Malware. Ringkasan hasil evaluasi dipaparkan pada penjelasan berikut.

Apa saja tujuan topik riset pada bidang Analisis Malware? (RQ1)

Penelitian ini dilakukan untuk memahami bagaimana koneksi client-server bekerja, bagaimana server Posison Ivy berkomunikasi dengan klien, dan bagaimana perilaku sistem operasi yang berjalan (Adenansi and Novarina, 2017).

Langkah-langkah analisa dinamis ini akan memeriksa seluruh komputer, seperti proses yang berjalan di komputer, perubahan registri, koneksi internet, dan kejadian aneh lainnya yang mungkin terjadi saat komputer terinfeksi Malware (Cahyanto, Wahanggara and Ramadana, 2017).

Penyebaran Malware ada banyak bentuknya mulai dari social-engineering attack yang memanfaatkan kondisi psikis dari suatu individu, file download fraud guna menipu user untuk men-download secara tidak sengaja, dan email phishing menipu user dengan spam email yang menarik perhatian user (Daniswara et al., 2019). Dalam penelitian ini, penulis berbicara tentang bagaimana Malware didistribusikan oleh penyerang dan bagaimana ditemukan di komputer (Adenansi and Novarina, 2017).

Penelitian ini menggunakan pengelompokan dan klasifikasi laporan perilaku Malware yang disematkan untuk mengidentifikasi keberadaan perilaku berbahaya (Sujyothi and Acharya, 2017).

Apa saja metode yang digunakan pada Analisis Malware? (RQ2)

Untuk memahami bagaimana fungsi malware Poison Ivy, proyek ini akan menganalisisnya. Metode analisis statis dan dinamis digunakan dalam penelitian ini, dimana kombinasi kedua metode tersebut merupakan cara yang paling efektif untuk mengkaji aktivitas malware (Adenansi and Novarina, 2017).

Analisis Malware Statis Tidak seperti analisis Malware dinamis, dalam analisis statis ini, file berbahaya tidak langsung diaktifkan, melainkan dilacak, dicari, dan dianalisis. Informasi yang diperoleh sangat lengkap dan dapat memberikan gambaran yang sangat detail tentang mekanisme aksi program jahat secara keseluruhan (Cahyanto, Wahanggara and Ramadana, 2017).

Banyak cara penanganan yang dapat dilakukan namun salah satu cara mengatasinya adalah dengan melakukan analisis, cara pencegahan ini merupakan cara yang cukup handal dalam mengatasi karna dapat membaca pola serangan yang tepat jika analisisnya juga tepat (Daniswara *et al.*, 2019).

Artikel ini ditulis untuk membantu pengguna komputer lebih memahami bagaimana Malware disebarkan oleh penyerang dan bagaimana mempersiapkan serangan yang semakin bervariasi (Adenansi and Novarina, 2017).

Malware canggih ditargetkan, tidak diketahui, tersembunyi, dipersonalisasi, dan nol hari dibandingkan dengan Malware tradisional yang luas, dikenal, terbuka, dan satu kali (Sujoyothi and Acharya, 2017).

Apa saja kelebihan dan kekurangan pada metode yang digunakan? (RQ3)

Menurut penelitian ini, Poison Ivy membajak sistem operasi target dengan menyuntikkan file dll, khususnya loadlibrary.dll, dan kemudian menambahkan file dan entri registri saat server terhubung ke komputer target. Poison Ivy melakukan proses perbandingan kata sandi sebelum menghubungkan virus, dan jika kata sandi cocok, server dapat mengakses komputer target (Amdani and Iqbal, 2021).

Saat menggunakan metode analisis Malware statis ini, perlu memahami bahasa mesin, terutama arsitektur program, karena ini akan sangat berguna untuk menganalisis komposisi kode perangkat lunak. Malware mengacu pada informasi yang dikumpulkan dari perilaku yang disebabkan oleh Malwarenya (Cahyanto, Wahanggara and Ramadana, 2017).

Analisis mempermudah untuk mengenali tanda-tanda suatu Malware akan melancarkan sebuah serangan, ditambah lagi dengan metode dinamis berbasis anomaly yang dapat mempermudah klasifikasi dan pengkategorian, selain itu keuntungan yang juga didapatkan ketika implementasi metode ini adalah deteksi suatu pola akan terasa lebih mudah dan lebih cepat deteksi nya (Daniswara *et al.*, 2019).

Tujuan Malware diciptakan oleh penyerang untuk merusak atau membobol suatu sistem operasi melalui script rahasia atau dapat dikatakan disisipkan oleh penyerang secara tersembunyi (Adenansi and Novarina, 2017).

Dengan demikian, analisis Malware dinamis otomatis menjadi teknik yang disukai secara luas untuk mengidentifikasi Malware yang tidak dikenal (Sujoyothi and Acharya, 2017)

5. Simpulan

Menurut hasil pencarian yang dilakukan, ditemukan berbagai macam berita menarik di berbagai majalah yang diteliti. Metode yang digunakan dalam penelitian ini, terutama analisis statis dan dinamis Malware, merupakan model penelitian yang paling sulit untuk diterapkan karena melibatkan proses peninjauan dan penjelajahan skenario perangkat lunak (kotak putih) selama analisis, untuk ini peneliti menyarankan untuk menyiapkan strategi yang lebih

intensif dalam kajian metode ini, terutama pada level sumber daya manusia, yang harus memiliki pengetahuan dan pengalaman bekerja dengan bahasa pemrograman.

SLR ini membahas berbagai klasifikasi jenis Malware yang digunakan oleh penyerang. Peretas menggunakan berbagai kerentanan untuk menginfeksi pengguna dengan Malware. Dengan banyaknya jenis Malware, penyerang selalu berusaha memanfaatkan orang. Untuk mencegah Malware menyerang komputer Anda, penting untuk selalu waspada, melindungi, dan menangani Malware di komputer Anda. Salah satu langkah keamanan adalah memindai komputer Anda secara teratur dengan perangkat lunak anti-virus. Pengetahuan tentang Malware juga diperlukan untuk memprediksi penyebaran Malware yang semakin canggih dengan berbagai cara. Pemindaian Malware digunakan untuk mendeteksi Malware terhadap program yang kemungkinan besar terinfeksi Malware. Malware dinamis dapat menggunakan beberapa alat yang menambah pengetahuan penting bagi pengguna komputer. Malware masih menjadi topik terbuka, sehingga peneliti juga menyarankan untuk mengembangkan metode untuk menganalisis Malware menggunakan metode analisis fundamental yang disebut Reverse Engineering.

Daftar Pustaka

- A. H. Muhammad, B.S. And A.L. (2017) “Metode Klasifikasi Dan Analisis Karakteristik Malware Menggunakan Konsep Ontologi”, *Tenomatika*, Vol. 1x(1), Pp. 16–28.
- Adenansi, R. And Novarina, L.A. (2017) ‘Malware Dynamic’, *Jurnal Of Education And Information Communication Technology*, 1(1), Pp. 37–43.
- Amdani, R.T. And Iqbal, M. (2021) ‘Analisis Dan Deteksi Malware Poison Ivy Malware Analisis Statis Analysis And Detection Of Malware Poison Ivy With Malware Dynamic Analysis Method And Malware Static Analysis’, 7(2), Pp. 178–191.
- Aslan, O. And Samet, R. (2018) ‘Investigation Of Possibilities To Detect Malware Using Existing Tools’, *Proceedings Of Ieee/Acs International Conference On Computer Systems And Applications, Aiccsa*, 2017-Octob, Pp. 1277–1284. Available At: <https://doi.org/10.1109/Aiccsa.2017.24>.
- Cahyanto, T.A., Wahanggara, V. And Ramadana, D. (2017) ‘Analisis Dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis Dan Malware Analisis Statis’, *Justindo, Jurnal Sistem & Teknologi Informasi Indonesia*, 2(1), Pp. 19–30. Available At: <http://jurnal.unmuhjember.ac.id/index.php/justindo/article/view/1037>.
- Chairisda, N.R.P. (2020) ‘Optimalisasi Satgas Cyber Patrol Polres Banyumas Dalam Menghadapi Pemilu 2019’, *Police Studies Review*, 4(January), Pp. 243–296. Available At: <http://journal.akademikepolisian.com/index.php/psr/article/view/86>.
- Choi, K. And Lee, C.S. (2018) ‘The Present And Future Of

- Cybercrime, Cyberterrorism, And Cybersecurity', *The International Journal Of Cybersecurity Intelligence And Cybercrime*, 1(1), Pp. 1–4. Available At: <https://doi.org/10.52306/01010218yxgw4012>.
- Damage, A. And Intelligence, E. (No Date) 'Security'.
- Daniswara, D.A. *Et Al.* (2019) 'Analisis Deteksi Malicious Activity Menggunakan Metode Analisis Malware Dinamis Berbasis Anomali Detection Analysis Of Malicious Activity Using Anomaly-Based Dynamic Malware Analysis Method', 6(2), Pp. 7796–7803.
- Dwi Nugraha, J., Budiono, A. And Almaarif, A. (2019) 'Analisis Malware Berdasarkan Api Call Memory Dengan Metode Deteksi Signature-Based Malware Alaysis Based On Call Memory Api With Signature-Based Detection Method', 6(2), Pp. 7820–7827.
- Kitchenham, B. (2004) 'Procedures For Performing Systematic Reviews, Version 1.0', *Empirical Software Engineering*, 33(2004), Pp. 1–26.
- Larasati, I., Yusril, A.N. And Zukri, P. Al (2021) 'Systematic Literature Review Analisis Metode Agile Dalam Pengembangan Aplikasi Mobile', *Sistemasi*, 10(2), P. 369. Available At: <https://doi.org/10.32520/Stmsi.V10i2.1237>.
- Nasution, M.A.H. And Laksono, A.T. (2020) 'Investigasi Serangan Backdoor Remote Access Trojan (Rat) Terhadap Smartphone', 7(4), Pp. 505–510. Available At: <https://doi.org/10.30865/Jurikom.V7i4.2301>.
- Riyandhika, R. And Pratama, R. (2020) 'Analisis Kesadaran Cybersecurity Pada Kalangan Mahasiswa Di Indonesia', *Uii*, 1(2), P. 1.
- Rozi, F. (2020) 'Systematic Literature Review Pada Analisis Prediktif Dengan Iot: Tren Riset, Metode, Dan Arsitektur', *Jurnal Sistem Cerdas*, 3(1), Pp. 43–53. Available At: <https://doi.org/10.37396/Jsc.V3i1.53>.
- Rusdi, A.S., Widiyasono, N. And Sulastri, H. (2019) 'Analisis Infeksi Malware Pada Perangkat Android Dengan Metode Hybrid Analysis', (24).
- Setia, T.P., Aldya, A.P. And Widiyasono, N. (2019) 'Reverse Engineering Untuk Analisis Malware Remote Access Trojan', *Jurnal Edukasi Dan Penelitian Informatika (Jepin)*, 5(1), P. 40. Available At: <https://doi.org/10.26418/Jp.V5i1.28214>.
- Sujyothi, A. And Acharya, S. (2017) 'Dynamic Malware Analysis And Detection In Virtual Environment', *International Journal Of Modern Education And Computer Science*, 9(3), Pp. 48–55. Available At: <https://doi.org/10.5815/Ijmecs.2017.03.06>.
- Suryati, O.T. And Budiono, A. (2020) 'Impact Analysis Of Malware Based On Call Network Api With Heuristic Detection Method', *International Journal Of Advances In Data And Information Systems*, 1(1), Pp. 1–8. Available At: <https://doi.org/10.25008/Ijadis.V1i1.176>.
- Triandini, E. *Et Al.* (2019) 'Systematic Literature Review Method For Identifying Platforms And Methods For Information System Development In Indonesia', *Indonesian Journal Of Information Systems*, 1(2), P. 63.