ANALISIS DAN DETEKSI *MALWARE* PADA PROTOKOL JARINGAN MENGGUNAKAN METODE *MALWARE* ANALISIS DINAMIS DAN *MALWARE* ANALISIS STATIS

SKRIPSI

Oleh
Vicram Renondo Sianipar
190210066

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2023

ANALISIS DAN DETEKSI *MALWARE* PADA PROTOKOL JARINGAN MENGGUNAKAN METODE *MALWARE* ANALISIS DINAMIS DAN *MALWARE* ANALISIS STATIS

SKRIPSI

Untuk memenuhi salah satu syarat
memperoleh gelar sarjana

Oleh
Vicram Renondo Sianipar
190210066

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2023

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini saya:

Nama	: Vicram Renondo Sianipar
NPM	: 190210066
Fakultas	: Teknik dan Komputer
Program Studi	: Teknik Informatika

Menyatakan bahwa **"Skripsi"** yang saya buat dengan judul:

ANALISIS DAN DETEKSI *MALWARE* PADA PROTOKOL JARINGAN MENGGUNAKAN METODE *MALWARE* ANALISIS DINAMIS DAN *MALWARE* ANALISIS STATIS

Adalah hasil karya sendiri dan bukan "duplikasi" dari karya orang lain. Sepengetahuan saya, didalam naskah Skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip didalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah Skripsi ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia naskah Skripsi ini digugurkan dan gelar akademik yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundangundangan yang berlaku.
Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun.

Batam, 27 Juli 2023

Vicram Renondo Sianipar
190210066

ANALISIS DAN DETEKSI *MALWARE* PADA PROTOKOL JARINGAN MENGGUNAKAN METODE *MALWARE* ANALISIS DINAMIS DAN *MALWARE* ANALISIS STATIS

SKRIPSI

Untuk memenuhi salah satu syarat
Guna memperoleh gelar sarjana

Oleh:
Vicram Renondo Sianipar
190210066

Telah disetujui oleh Pembimbing pada tanggal
Seperti tertera dibawah ini
Batam, 27 Juli 2023

Hotma Pangaribuan, S.Kom., M.SI
Pembimbing

ABSTRAK

Malware (perangkat lunak berbahaya) telah menjadi ancaman serius bagi keamanan jaringan dan komputer, dan terus mengalami perkembangan yang kompleks. Untuk menghadapi ancaman ini, metode analisis malware telah menjadi fokus utama dalam penelitian keamanan komputer. Dalam penelitian ini, kami mengusulkan pendekatan gabungan berdasarkan analisis dinamis dan analisis statis untuk mendeteksi malware yang menargetkan protokol jaringan. Pertama, kami melakukan analisis malware secara dinamis dengan menjalankan sampel malware pada lingkungan terkontrol dan memantau perilaku eksekusinya. Kami merekam berbagai aktivitas malware, termasuk perubahan sistem, koneksi jaringan, dan upaya menyembunyikan diri. Dari analisis dinamis ini, kami mendapatkan wawasan tentang perilaku malware yang dapat membantu mengidentifikasi tindakan jahatnya. Selanjutnya, kami melakukan analisis statis dengan mengamati kode sumber atau file eksekusi malware tanpa menjalankannya. Teknik ini memungkinkan kami untuk menganalisis struktur dan karakteristik file secara mendalam. Kami menggunakan teknik analisis statis seperti pengurai kode, analisis tanda tangan, dan pembandingan hash untuk mengklasifikasikan file sebagai malware atau non-malware. Selanjutnya, kami mengintegrasikan hasil analisis dinamis dan analisis statis untuk meningkatkan deteksi malware. Dengan memadukan informasi dari kedua metode analisis, kami dapat memperoleh pemahaman yang lebih lengkap tentang malware yang ditargetkan pada protokol jaringan tertentu. Ini membantu dalam mendeteksi varian malware yang sebelumnya tidak diketahui dan meningkatkan akurasi deteksi secara keseluruhan. Untuk menguji keefektifan pendekatan kami, kami melakukan serangkaian uji coba menggunakan berbagai sampel malware yang ada dan mengamati kinerja sistem deteksi kami. Hasil uji coba menunjukkan bahwa pendekatan gabungan kami berhasil mendeteksi dan mengidentifikasi malware pada protokol jaringan dengan tingkat keakuratan yang tinggi. Penelitian ini memberikan kontribusi penting dalam memperkuat pertahanan keamanan jaringan terhadap serangan malware. Dengan menggabungkan analisis dinamis dan analisis statis, sistem deteksi kami memiliki potensi untuk mengenali dan mengatasi ancaman malware masa depan dengan lebih efektif.

Kata Kunci: Protokol Jaringan; Malware; Analisis Dinamis; Analisis Statis

ABSTRACT

Malware (malicious software) has become a serious threat to network and computer security, and continues to undergo complex development. To deal with this threat, malware analysis methods have become a major focus in computer security research. In this study, we propose a combined approach based on dynamic analysis and static analysis to detect malware targeting network protocols. First, we perform dynamic malware analysis by running malware samples in a controlled environment and monitoring their execution behavior. We recorded various malware activities, including system changes, network connections, and concealment attempts. From this dynamic analysis, we gain insights into the malware's behavior that can help identify its malicious actions. Next, we perform static analysis by observing the source code or executable file of the malware without running it. This technique allows us to analyze the structure and characteristics of the file in depth. We use static analysis techniques such as code parsing, signature analysis, and hash comparisons to classify files as malware or non-malware. Furthermore, we integrated the results of dynamic analysis and static analysis to improve malware detection. By combining information from both analysis methods, we were able to gain a more complete understanding of malware targeted at specific network protocols. This helps in detecting previously unknown malware variants and improves the overall detection accuracy. To test the effectiveness of our approach, we conducted a series of trials using various existing malware samples and observed the performance of our detection system. Experimental results show that our combined approach can successfully detect and identify malware on network protocols with a high degree of accuracy. This research makes an important contribution to strengthening network security defenses against malware attacks. By combining dynamic analysis and static analysis, our detection system has the potential to recognize and address future malware threats more effectively.

Keywords: Network Protocol; Malware; Dynamic Analysis; Static Analysis

KATA PENGANTAR

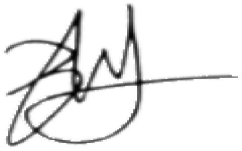
Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas segala berkat dan anugerahNya, sehingga penulis dapat menyelesaikan skripsi ini yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika di Universitas Putera Batam.

Dengan segala keterbatasan, penulis juga menyadari bahwa sksripsi inin takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terimakasih kepada:

1. Ibu Nur Elfi Husda, S.Kom., M.SI., selaku Rektor Universitas Putera Batam
2. Bapak Welly Sugianto, S.T., M.M., selaku Dekan Fakultas Teknik dan Komputer di Universitas Putera Batam
3. Bapak Andi Maslan, S.T., M.SI., selaku Ketua Program Studi Teknik Informatika di Universitas Putera Batam
4. Bapak Hotma Pangaribuan, S.Kom., M.SI., selaku Pembimbing Skripsi pada Program Studi Teknik Informatika di Universitas Putera Batam
5. Bapak Rahmat Fauzi, S.Kom., M.Kom., selaku Pembimbing Akademik pada Program Studi Teknik Informatika di Universitas Putera Batam
6. Seluruh Dosen dan Staff Universitas Putera Batam yang telah memberikan pengetahuan selama perkuliahan
7. Kedua Orangtua yang selalu mendoakan, mendukung, memberikan kasih sayang dan juga menyemangati penulis untuk menyelesaikan perkuliahan S1 ini

8. Zefly Haposan Gultom, S.Kom, selaku Staff *IT* di PT Nok Precision Component Batam yang memberikan izin penelitian ini
9. Almita Rumiris Sianipar, S.S, selaku Kakak yang selalu mendoakan serta memberikan masukan kepada peneliti
10. Erich Alamsyah Sianipar S.T, selaku Abang yang selalu mendoakan serta memberikan semangat kepada peneliti
11. Immanuel Sianipar selaku Adek yang turut serta mendoakan peneliti
12. Suwanda S.Kom, selaku Abang senior yang meluangkan waktunya dan juga memberikan masukan terhadap peneliti
13. Seluruh pihak yang telah banyak membantu dalam menyelesaikan penelitian ini yang tidak dapat penulis sebutkan satu persatu.

Batam, 27 Juli 2023



Vicram Renondo Sianipar

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL