DETEKSI POLA RANSOMWARE BERBASIS SIGNATURE MALWARE DENGAN MEMBANDINGKAN BEBERAPA ANTIVIRUS

TUGAS AKHIR

Oleh :

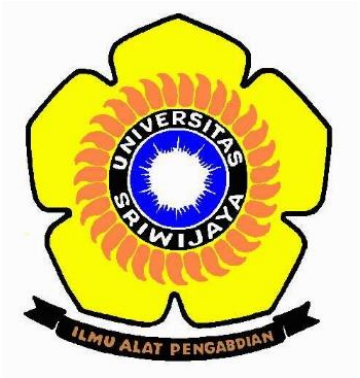
Kefin Pratama
09011181520020

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

DETEKSI POLA RANSOMWARE BERBASIS SIGNATURE MALWARE DENGAN MEMBANDINGKAN BEBERAPA ANTIVIRUS

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer



Oleh :

Kefin Pratama
09011181520020

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

HALAMAN PENGESAHAN

DETEKSI POLA RANSOMWARE BERBASIS SIGNATURE MALWARE DENGAN MEMBANDINGKAN BEBERAPA ANTIVIRUS

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

Kefiu Pratama
09011181520020

Indralaya, 31 Desember 20200

Pembimbing Tugas Akhir	**Mengetahui,** **Ketua Jurusan Sistem Komputer**
Deris Stiawan, M.T., Ph.D.	**Dr. Ir. H. Sukemi, M.T.**
NIP. 197806172006041002	**NIP. 196612032006041001**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Kamis

Tanggal : 31 Desemmber 2020

Tim Penguji :

1. **Ketua : Dr. Ir. H. Sukemi, M.T.** _____
2. **Anggota I : Deris Stiawan, M.T., Ph.D.** _____
3. **Anggota I : Ahmad Heryanto, M.T.** _____

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 19661203200641001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Kefin Pratama

NIM : 09011181520008

Judul : Deteksi Pola Ransomware Berbasis Signature Malware Dengan Membandingkan Beberapa Antivirus

Hasil Pengecekan *Software iThenticate/Turnitin* : 6%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya saya sendiri dan bukan hasil penjiplakan / plagiat. Apabila ditemukan unsur penjiplakan / plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun

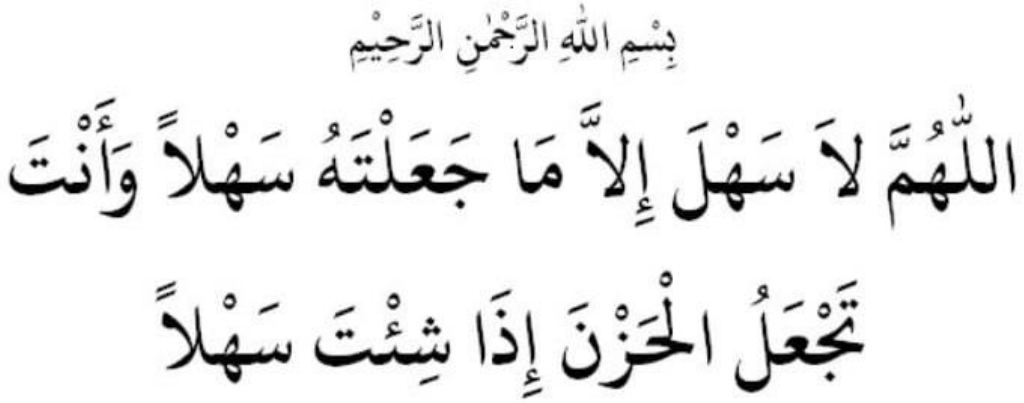
Palembang, 31 Desember 2020

Kefin Pratama

NIM. 09011181520020

HALAMAN PERSEMBAHAN

Doa Agar Dimudahkan Segala Urusan



"Ya Allah, tidak ada kemudahan kecuali yang engkau buat mudah. Dan engkau menjadi kesedihan (kesulitan), jika engkau kehendak pasti akan menjadi mudah"

Kupersembahkan khusus untuk yang sedang berjuang disana :

Untuk yang sedang berjuang semangat yaa, pasti bisa kok untuk menjalani kehidupan ini dan segala rintangan – rintangan yang diberikan. Tidak ada yang tidak bisa melewati ringan yang diberikan - Nya.

KATA PENGANTAR

Puji syukur atas kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini dengan judul **"Deteksi Pola Ransomware Berbasis Signature Malware Dengan Mmembandingkan Beberapa Antivirus."**

Penulisan Proposal Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Adapun sebagai bahan penulisan, penulis mengambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mendukung dalam penulisan proposal ini. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril ataupun materil serta memberikan kemudahan, dorongan, saran dan kritik selama dalam proses penulisan Proposal Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. dan mengucapkan terima kasih kepada yang terhormat :

1. Orang Tua serta keluarga penulis tercinta, yang telah memberikan doa dan restu serta dukungan yang sangat besar selama mengikuti dan melaksanakan perkuliahan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya hingga dapat menyelesaikan Proposal Tugas Akhir ini.
2. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Reza Firsandaya Malik, M.T., selaku Dosen Pembimbing Akademik penulis di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Deris Stiawan, M.T., Ph.D., selaku Dosen Pembimbing Tugas Akhir penulis di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

1. Ibu Renny Virgasari selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
2. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Seluruh teman-teman seperjuangan angkatan 2015 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Almamater.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan Proposal Tugas Akhir ini. Karena sesungguhnya tak ada yang sempurna didunia ini. Untuk itu, segala saran dan kritik sangatlah penting bagi penulis. Akhir kata, semoga Proposal Tugas Akhir ini dapat bermanfaat dan berguna bagi khalayak.

Palembang, 31 Desember 2020

Penulis

Kefin Pratama

NIM. 09011181520020

DETEKSI POLA RANSOMWARE BERBASIS SIGNATURE MALWARE DENGAN MEMBANDING BEBERAPA ANTIVIRUS

Kefin Pratama (09011181520020)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : kefinpratama@gmail.com

ABSTRAK

Meskipun perangkat lunak antivirus telah berkembang pesat dekade terkahir ini, pencocokan signature klasik berdasarkan pola byte masih merupakan konsep umum untuk mengindentifikasi ancaman keamanan. Signature adalah mekanisme deteksi yang sederhana dan cepat yang dapat melengkapi strategi analisi yang lebih canggih. Oleh karena itu ancaman keamanan berbasis signature menjadi pilihan dari penelitian kali ini. Penelitian ini bertujuan untuk mengetahui manakah antivirus yang lebih tepat dalam memindai virus setelah itu di forensik pola ransomwarenya. Supaya kita bisa melihat log dan alert dari virus yang terkait dan kita lihat pula pola dari virus tersebut. Dalam penelitian ini untuk mengetahui log dan alart beserta mengetahui pola ransomware saya mengunakan metode bebasis signature malware menggunakan antivurus dan melihat pola pada ransomware menggunakan wireshark. Dalam melihat alert dan log virus yang terdeteksi ini saya memakai anti virus Sophos Home karena salam penelitian ini Sophos Home yang lebih jelas dalam memberikan informasi log dan alert dari virus tersebut. Dan juga untuk melihat pola ransomware ini saya menggunakan wireshark sebagai analisi dari pola yang di lakukan oleh virus tersebut.

Kata Kunci : Antivirus, Signature, Malware, Ransomware, Wireshark, Virus

SIGNATURE MALWARE BASED RANSOMWARE PATTERN DETECTION BY COMPARING SOME ANTIVIRUSES

Kefin Pratama (0901181520020)

Departement of Computer Engineering, Faculty of Computer Science, Sriwijaya University

Email: kefinpratama@gmail.com

ABSTRACT

Although antivirus software has grown rapidly in the past decade, classic signature matching based on a byte pattern is still a common concept for identifying security threats. Signature is a simple and fast detection mechanism that can complement more sophisticated analysis strategies. Therefore, signature-based security threats are the choice of this research. This study aims to determine which antivirus is more appropriate in scanning the virus after that in the forensic ransomware pattern. So that we can see the logs and alerts of related viruses and we can see the patterns of these viruses. In this research, to know log and alart along with knowing the ransomware pattern, I used the malware signature based method using antivurus and saw the pattern on the ransomware using wireshark. In viewing the alerts and logs of detected viruses, I use Sophos Home anti-virus because in this research, Sophos Home is more clear in providing log information and alerts for the virus. And also to see this ransomware pattern, I use wireshark as an analysis of the pattern carried out by the virus.

Keywords: *Antivirus, Signature, Malware, Ransomware, Wireshark, Virus*

DAFTAR ISI

DAFTAR GAMBAR

Daftar Tabel

LAMPIRAN

Lampiran 1. Berkas Revisi Tugas Akhir

Lampiran 2. Hasil Cek Plagiat

BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan kemajuan teknologi informasi, Internet terlibat di setiap area dalam kehidupan sehari-hari kita. Saat perangkat seluler dan teknologi komputasi awan mulai memainkan peran penting hidup kita, mereka menjadi lebih rentan terhadap serangan. Baru-baru ini, situs web phishing semakin berbahaya dan menjadi masalah yang serius di bidang keamanan jaringan. Penyerang menggunakan banyak pendekatan untuk menanamkan malware ke host target untuk mencuri data penting dan menyebabkan kerusakan besar. Pertumbuhan malware telah sangat cepat, dan tujuannya telah berubah dari kehancuran hingga penetrasi. Sehingga signature malware menjadi lebih sulit untuk dideteksi. Selain signature statis, malware juga mencoba menyembunyikan signature dinamis dari anti-virus inspeksi.[1]

Meskipun perangkat lunak anti-virus telah berkembang pesat dekade terakhir, pencocokan signature klasik berdasarkan byte pola masih merupakan konsep umum untuk mengidentifikasi keamanan ancaman. Signature anti-virus adalah mekanisme deteksi yang sederhana dan cepat yang dapat melengkapi strategi analisis yang lebih canggih. Namun, jika tanda tangan tidak dirancang dengan hati-hati, mereka dapat berubah dari mekanisme pertahanan menjadi instrumen serangan. Pada penelitian [2], menyajikan metode baru untuk secara otomatis memperoleh signature dari perangkat lunak anti-virus dan mendiskusikan bagaimana signature yang diekstrak dapat digunakan menyerang data yang masuk akal dengan bantuan pemindai virus itu sendiri.

Produk antivirus yang ada menggunakan berbagai jenis teknik untuk mendeteksi malware atau aktivitas yang mencurigakan. Mayoritas teknik semacam itu mengandalkan algoritma deteksi berbasis siganture. Namun, kecepatan algoritme

deteksi tersebut dapat berdampak buruk pada kinerja produk antivirus (misal Jika digunakan untuk pemindaian virus online). Dalam penelitian [3], meninjau penelitian yang mengusulkan adanya algoritma berbasis siganture yang cepat dan efisien untuk secara dinamis meningkatkan waktu dan akurasi deteksi virus. Dan mengklasifikasikan dan mendiskusikan algoritme yang berbeda sesuai dengan jenis analisis yang [3] lakukan (yaitu, statis, dinamis, atau hybrid). Selain itu, mengevaluasi algoritma deteksi virus yang ada menggunakan masalah desain dan kriteria kinerja yang berbeda, yaitu (a) biaya memori, (b) kompleksitas waktu, dan (c) tingkat deteksi. Selain itu, membahas bagaimana pilihan desain tertentu dari pendekatan berbasis signature hanya dapat diterapkan pada keadaan deteksi virus tertentu.

1.2 Tujuan

Adapun tujuan dari penelitian yang saya lakukan adalah :

1. Mendeteksi pola ransomwere
2. Mengetahui anti-virus mana yang belum update dari beberapa anti virus yang di tampilkan
3. Menerapkan metode signature malware untuk medeteksi pola yang tepat menggunakan beberapa anti-virus

1.3 Manfaat

Adapun manfaat yang dapat diambil dalam penelitian ini adalah :

1. Dapat memperlihatkan antivirus yang lebih tepat dalam memindai virus
2. Dapat mengetahui pola malware dengan menggunakan wireshark

1.4 Rumusan Masalah

Rumusan masalah dalam tugas akhir ini yaitu sebagai berikut :

1. Bagaimana mendeteksi pola ransomwere?

2. Bagaimana analisa antivirus yang lebih tepat dalam mendeteksi virus ransomere?

1.5 Batasan Masalah

Adapun batasan masalah dalam tugas akhir ini sebagai berikut :

1. Deteksi pola yang dilakukan dengan mengambil beberapa virus yang di deteksi dengan beberapa antivirus
2. Menganalisa mana antivirus yang tempat untuk mendeteksi virus yang ada
3. Pengujian akan dilakukan menggunakan virtual box dengan system operasi windows
4. Pengujian akan dibuktikan melalui beberapa anti virus
5. Pengamatan akan difokuskan kepada pola – pola ransomware

1.6 Metode Penelitian

Metodologi yang akan digunakan dalam penilitian ini yaitu:

1. Tahap Pertama (Studi Pustaka/Literatur)

   Dalam tahap ini penulis mencari informasi yang diperlukan melalui media pembelajaran seperti jurnal ilmiah, buku, internet, serta artikel-artikel terkait yang mendukung penulisan Proposal Tugas Akhir ini.

2. Tahap Kedua (Perancangan Sistem)

   Pada tahap ini dimana penulis menentukan perangkat keras maupun perangkat lunak yang dipakai dalam penelitian ini.

3. Tahap Ketiga (Pengujian)

   Dalam tahap ini berupa pengujian yang sesuai dengan parameter yang ditentukan oleh batasan masalah.

4. Tahap Keempat (Hasil dan Analisa)

   Tahapan ini berisi hasil pengujian pada penelitian tersebut kemudian diketahui pola – pola ransomwere dari hasil deteksi antivirus yang sudah terdeteksi.

5. Tahap Kelima (Kesimpulan dan Saran)

   Tahapan terakhir berisi tentang kesimpulan dan saran dari hasil studi pustaka, perancangan sistem dan analisa pada penelitian tersebut. Pada saran berisi poin-poin dari penulis untuk penelitian selanjutnya.

1.7 Sistematika Penelitian

Penyusunan tugas akhir ini dibuat sistematika penulisan untuk memudahkan dan menjelaskan inti dari tiap bab yang dijelaskan sebagai berikut :

BAB I PENDAHULUAN

Bab ini terdiri dari Latar Belakang, Tujuan, Manfaat, Rumusan Masalah, Batasan Masalah, Metodologi Penelitian, dan Sistematika Penelitian yang mengacu pada landasan topik penelitian

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang dasar teori yang berhubungan dengan penelitian tugas akhir.

BAB III METODE PENELITIAN

Bab ini berisi penjelasan secara sistematis mengenai bagaimana proses penelitian dilakukan, tahapan perancangan sistem, dan penerapan metode penelitian.

BAB IV PENGUJIAN DAN ANALISIS

Bab ini menjelaskan tentang hasil pengujian yang dilakukan serta menganalisa dari hasil data yang didapat.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil pengujian yang dilakukan, menjawab tujuan yang dicapai dari BAB I (Pendahuluan), dan saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] Fan, C. I., Hsiao, H. W., Chou, C. H., & Tseng, Y. F. (2015). Malware detection systems based on API log data mining. *Proceedings - International Computer Software and Applications Conference*, *3*, 255–260. https://doi.org/10.1109/COMPSAC.2015.241

[2] Wressnegger, C., Freeman, K., Yamaguchi, F., & Rieck, K. (2017). Automatically inferring malware signatures for anti-virus assisted attacks. *ASIA CCS 2017 - Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security*, 587–598. https://doi.org/10.1145/3052973.3053002

[3] Scott, J. (2017). Signature Based Malware Detection is Dead. *Cybersecurity Think Tank, Institute for Critical Infrastructure Technology*, (February).

[4] Ferdiansyah. (2018). Analisis Aktivitas Dan Pola Jaringan Terhadap Eternal Blue Dan Wannacry Ransomware. *JUSIFO (Jurnal Sistem Informasi)*, *2*(1), 44–59. Retrieved from http://eprints.binadarma.ac.id/3873/1/Ferdiansyah-Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue dan Wannacry Ransomware.pdf

[5] Nieuwenhuizen, D. (2017). A behavioural-based approach to ransomware detection. *Whitepaper. MWR Labs Whitepaper*. Retrieved from https://labs.mwrinfosecurity.com/assets/resourceFiles/mwri-behavioural-ransomware-detection-2017-04-5.pdf