SISTEM ANTI *VIRUS* DENGAN METODE PENCARIAN *HEADER FILE* DATA *SIZE OF CODE* DAN *ADDRESS OF ENTRY* DENGAN PERHITUNGAN *JACCARD SIMILARITY*

SKRIPSI

Oleh :

ZIRHAN ARFANDI

NIM : 2037080

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PASIR PENGARAIAN

2024

SISTEM ANTI *VIRUS* DENGAN METODE PENCARIAN *HEADER FILE* DATA *SIZE OF CODE* DAN *ADDRESS OF ENTRY* DENGAN PERHITUNGAN *JACCARD SIMILARITY*

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer

SKRIPSI

Oleh :
ZIRHAN ARFANDI
NIM : 2037080

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PASIR PENGARAIAN
2024

PERSETUJUAN PEMBIMBING

SISTEM ANTI *VIRUS* DENGAN METODE PENCARIAN *HEADER FILE* DATA *SIZE OF CODE* DAN *ADDRESS OF ENTRY* DENGAN PERHITUNGAN *JACCARD SIMILARITY*

Disetujui Oleh:

Pembimbing I	Pembimbing II
Asep Supriyanto S.T., M. Kom	Erni Rouza, S.T., M.Kom
NIDN. 1003108903	NIDN. 1009058707

Diketahui Oleh:

Ketua Program Studi Teknik Informatika

Basorudin, S.Pd., M.Kom

NIDN. 1020088702

PERSETUJUAN PENGUJI

PERSETUJUAN PENGUJI

Skripsi ini telah diuji oleh
Tim Penguji Ujian Sarjana Komputer
Program Studi Teknik Informatika
Fakultas Ilmu Komputer
Universitas Pasir Pengaraian
Pada Tanggal 14 Juni 2024

Tim Penguji :

1. Asep Supriyanto, S.T., M.Kom — Ketua ( )
   NIDN. 1003108903
2. Erni Rouza, S.T., M.Kom — Sekretaris ( )
   NIDN. 1009058707
3. Basorudin, S.Pd., M.Kom — Anggota ( )
   NIDN. 1020088702
4. Ir. Budi Yanto, S.T., M.Kom — Anggota ( )
   NIDN. 1029058301
5. Satria Riki Mustafa, S.Pd.,M.Si — Anggota ( )
   NIDN. 1001039301

Mengetahui
Dekan Fakultas Ilmu Komputer
Universitas Pasir Pengaraian

Hendri Maradona, M.Kom
NIDN. 1002038702

LEMBAR PERNYATAAN

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa Skripsi yang berjudul "Sistem *Anti Virus* Dengan Metode Pencarian *Header File Data Size Of Code* Dan *Address Of Entry* Dengan Perhitungan *Jaccard Similarity*.", benar hasil penelitian saya dengan arahan dosen pembimbing dan belum pernah diajukan dalam bentuk apapun untuk mendapatkan gelar kesarjanaan. Dalam Skripsi ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasi orang lain, kecuali secara tertulis dengan jelas dicantumkan dalam naskah dengan menyebutkan referensi yang dicantumkan dalam daftar pustaka. Pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena Tugas Akhir ini, serta lainnya sesuai norma yang berlaku di perguruan tinggi.

Pasir Pengaraian, 14 Juni 2024

Yang Membuat Pernyataan

ZIKHAN ARFANDI

NIM: 2037080

KATA PENGANTAR

Assalamu'alaikum wa rahmatullahi wa barakatuh.

Puji syukur *Alhamdulillah* kehadirat Allah SWT yang senantiasa melimpahkan rahmat dan karunia-Nya, sehingga penulis mampu menyelesaikan Skripsi ini dengan baik. Shalawat serta salam berucap buat junjungan alam kita Rasulullah Muhammad SAW karena telah membawa manusia dari zaman kebodohan ke zaman yang penuh dengan ilmu pengetahuan seperti sekarang ini.

Skripsi ini disusun sebagai salah satu syarat untuk mendapatkan kelulusan pada jurusan Teknik Informatika Universitas Pasir Pengaraian. Banyak sekali pihak yang telah membantu dalam penyusunan Skripsi ini, baik berupa bantuan materi maupun berupa motivasi dan dukungan kepada saya. Semua itu tentu terlalu banyak bagi saya untuk membalasnya, namun pada kesempatan ini saya hanya dapat mengucapkan terimakasih kepada:

1. Kepada Ayah dan Ibu tercinta, yang selalu memberikan doa, motivasi, bimbingan yang tiada hentinya, serta telah banyak berkorban demi keberhasilan anaknya dan merupakan motivasi saya untuk memberikan yang terbaik, terima kasih banyak.
2. Bapak Dr. Hardianto, M.Pd selaku Rektor Universitas Pasir Pengaraian.
3. Bapak Hendri Maradona, M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Pasir Pengaraian
4. Bapak Basorudin, M.Kom selaku Ketua Program Studi Teknik Informatika, sebagai penguji I saya yang telah memberi bimbingan, arahan, dan saran yang berharga dalam pengujian Skripsi ini.
5. Bapak Asep Supriyanto, S.T., M. Kom, sebagai pembimbing I saya yang telah memberi bimbingan, arahan, dan saran yang berharga dalam penyusunan Skripsi ini.

6. Ibuk Erni Rouza, S.T., M.Kom, sebagai pembimbing II saya yang telah memberi bimbingan, arahan, dan saran yang berharga dalam penyusunan Skripsi ini.
7. Teman–teman seperjuangan di Prodi Teknik informatika yang telah memberi semangat serta motivasi dalam penyusunan Skripsi ini.
8. Dan terima kasih kepada seseorang yang memberi saya semangat dan support.

Saya menyadari bahwa dalam penulisan Skripsi ini masih banyak kesalahan dan kekurangan, oleh karena itu kritik dan saran yang sifatnya membangun diharapkan untuk kesempurnaan Skripsi ini. Akhirnya saya berharap semoga Skripsi ini dapat memberikan sesuatu yang bermanfaat bagi siapa saja yang membacanya. Amin.

Wassalamu'alaikum wa rahmatullahi wa barakatuh

Pasir Pengaraian, 14 Juni 2024

Zirhan Arfandi
NIM. 2037080

ABSTRACT

Virus detection involves scanning the registry, startup programs, system services, active processes, and other elements. Portable executable files (PE) play an important role in detecting viruses, as they refer to the entry point of viruses. Therefore, information such as Size Of Code and Address Of Entry Point from PE are key in computer virus identification and detection efforts. This research aims to develop an effective protection system against computer virus threats using the Python programming language. The main method employed in this study involves monitoring header files and analyzing code size as well as entry point addresses. While common virus detection methods like CRC-32 (Cyclic Redundancy Code) have been widely utilized, their effectiveness becomes limited when confronted with virus adopting polymorphic techniques. Instances of local virus propagation employing polymorphic techniques have also been observed. Results from the developed system testing indicate that an approach focusing on header file analysis, particularly address Of Entry Point and size Of Code, enables accurate identification of virus. Despite modifications made to the virus's header files, essential data remains recognizable, and It takes about 3 minutes and 40 seconds to do a thorough scan.

Keywords**:** *Entry Point Address, Computer virus. Python, Virus Detection.*

ABSTRAK

Pendeteksian *virus* melibatkan proses pemindaian *registry, program startup*, layanan sistem, proses aktif, dan elemen lainnya. Berkas *Portable Executable* (*PE*) memainkan peran penting dalam mendeteksi *virus*, karena merujuk ke titik masuk (*entry point*) dari *virus*. Oleh karena itu, informasi seperti *Size Of Code* dan *Address Of Entry Point* dari *PE* menjadi kunci dalam upaya identifikasi dan deteksi *virus* komputer. Penelitian ini bertujuan untuk mengembangkan sistem perlindungan yang efektif terhadap ancaman *virus* menggunakan bahasa pemrograman *Python*. Metode utama yang digunakan dalam penelitian ini adalah memantau *header file* dan menganalisis ukuran kode serta alamat titik masuk. Meskipun metode pencarian virus yang umum seperti *CRC-32* (*Cyclic Redundancy Code*) telah banyak digunakan, namun ketika dihadapkan dengan virus yang mengadopsi teknik *polymorphic* keefektifannya menjadi terbatas. Hasil pengujian sistem yang dikembangkan Dengan menganalisis nilai-nilai heksadesimal dari *Address of Entry Point* dan *Size of Code* menunjukkan bahwa pendekatan yang memfokuskan pada analisis *header file*, khususnya *Address of Entry Point* dan *Size of Code*, memungkinkan untuk mengidentifikasi *virus* dengan akurat. Meskipun *virus* telah melakukan perubahan pada *header file*, data esensial tetap dapat dikenali, bahkan jika virus telah menggunakan Teknik *polymorphic* atau pengacakan kode, dan dibutuhkan waktu sekitar 3 menit 40 detik untuk melakukan pemindaian secara menyeluruh.

Kata Kunci: Deteksi *Virus, Entry Point Address, Python, Virus.*

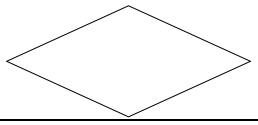
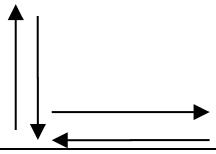
DAFTAR ISI

DAFTAR GAMBAR

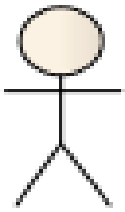
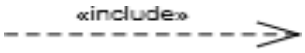
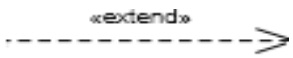
DAFTAR TABEL

DAFTAR SIMBOL

Simbol *Flowchart:*

	TERMINAL Digunakan untuk menggambarkan awal dan akhir dari suatu kegiatan.
	*DECISION* Digunakan untuk menggambarkan proses pengujian suatu kondisi yang ada.
	*FLOW LINE* Digunakan untuk menggambarkan hubungan proses dari suatu proses ke proses lainnya.
	*INPUT/OUTPUT* Digunakan untuk menggambarkan proses masukan data yang berupa pembicaraan data dan sekaligus proses keluaran yang berupa pencetakan data.
	*Stored* Data Simbol yang menunjukkan objek penyimpanan data umum yang digunakan dalam alur proses contohnya hardisk, flashdisk atau perangkat penyimpanan lainnya.
	*PROCESS* Digunakan untuk menggambarkan proses yang sedang dieksekusi.
	*Document* Simbol yang menyatakan langkah proses yang akan menghasilkan dokumen.

SIMBOL *USE CASE DIAGRAM*

Simbol	Deskripsi
Use case 	*Use Case* menggambarkan fungsionalitas yang disediakan sistem sebagai unit-unit yang bertukar pesan antar unit dengan aktor, yang dinyatakan dengan menggunakan kata kerja
Aktor / *actor* 	*Actor* atau Aktor adalah *Abstraction* dari orang atau sistem yang lain yang mengaktifkan fungsi dari target sistem. Orang atau sistem bisa muncul dalam beberapa peran. Perlu dicatat bahwa aktor berinteraksi dengan *Use Case*, tetapi tidak memiliki kontrol terhadap *use case*
Asosiasi / *association*	Asosiasi antara aktor dan *use case*, digambarkan dengan garis tanpa panah yang mengindikasikan siapa atau apa yang meminta interaksi secara langsung dan bukannya mengindikasikan data
Asosiasi / *association* 	Asosiasi antara aktor dengan *use case* yang menggunakan panah terbuka untuk mengindikasikan bila aktor berinteraksi secara pasif dengan sistem
Include 	*Include*, merupakan di dalam *use case* lain (*required*) atau pemanggilan *use case* oleh *use case* contohnya adalah pemanggilan sebuah fungsi program
Extend 	*Extend*, merupakan perluasan dari *use case* lain jika kondisi atau syarat terpenuhi