ANALISIS DAN DETEKSI MALWARE REMOTE ACCSESS TROJAN (RAT) MENGGUNAKAN METODE STATIS DAN DINAMIS

SKRIPSI

Disusun oleh:

Ansyuri Fadila
17.83.0016

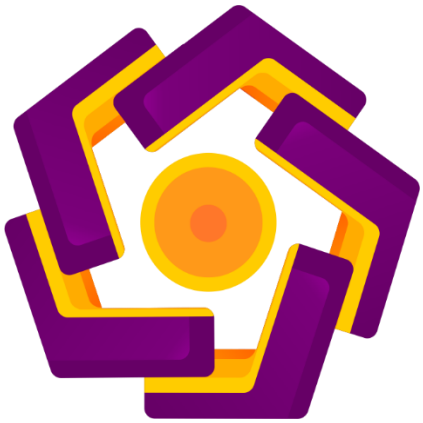
PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2021

ANALISIS DAN DETEKSI MALWARE REMOTE ACCSESS TROJAN (RAT) MENGGUNAKAN METODE STATIS DAN DINAMIS

SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer



Disusun oleh:

Ansyuri Fadila
17.83.0016

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS DETEKSI MALWARE REMOTE ACCSESS TROJAN (RAT) MENGGUNAKAN METODE DINAMIS DAN STATIS

yang dipersiapkan dan disusun oleh

Ansyuri Fadila

17.83.0016

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 10 Agustus 2021

Dosen Pembimbing,

Dony Ariyus, M.Kom
NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS DAN DETEKSI MALWARE REMOTE ACCSESS TROJAN (RAT) MENGGUNAKAN METODE STATIS DAN DINAMIS

Yang dipersiapkan dan disusun oleh

Ansyuri Fadila

17.83.0016

Telah dipertahankan di depan Dewan Penguji
pada tanggal 25 Agustus 2021

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Dony Ariyus, M.Kom **NIK. 190302128**	_____
Wahyu Sukestyastama Putra, S.T., M.Eng **NIK. 190302328**	_____
Senie Destya, M.Kom **NIK. 190302312**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 25 Agustus 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,M.Kom
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ansyuri Fadila
NIM : 17.83.0016

Menyatakan bahwa Skripsi dengan judul berikut

Analisis Dan Deteksi Malware Remote Accsess Trojan (RAT) Menggunakan Metode Statis Dan Dinamis

Dosen Pembimbing Dony Ariyus, M.kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 25 Agustus 2021

Yang Menyatakan,

Ansyuri Fadila

HALAMAN MOTTO

Tidak ada kata terlambat untuk kita bisa berubah. Masa lalu hanyalah proses pendewasaan untuk diri. Hidup tidak ditentukan oleh orang lain tapi kamu yang menentukanya.

Jangan salahkan dirimu atas keputusan yang salah. Setip orang pernah melakukanya. Jadikan mereka pelajaran untuk keputusan selanjutnya

Lakukan apapun dengan tepat, bukan hanya cepat. Keberhasilan tidak bisa dihalangi jika yang kamu lakukan tepat.

HALAMAN PERSEMBAHAN

Alhamdulillah, Segala puji dan syukur kepada Tuhan yang Maha Esa dan dukungan dan doa dari orang-orang tercinta, akhirnya skripsi ini dapat diselesaikan dengan baik. Oleh karena itu, dengan rasa bangga dan bahagia saya mengucapkan rasa syukur dan terimakasih saya kepada:

1. Allah SWT, Tuhan Yang Maha Esa karena hanya atas izin dan karunia-Nyalah, maka skripsi ini dapat dibuat dan selesai pada waktunya. Puji syukur yang tak terhingga pada Tuhan semesta alam yang meridhoi dan mengabulkan segala doa
2. Untuk kedua orang tua saya, Ibu Ramlah yang tidak pernah lelah dalam memberikan semangat supaya saya bisa menyelesaikan skripsi ini dan Bapak Yaeni Tabrin yang selalu mendo,akan disetiap sujudnya, memberikan motivasi hidup, memberikan begitu banyak pengorbanan yang tidak bisa saya balaskan. Terimakasih banyak saya ucapkan untuk keduanya yang tidak pernah lelah memberikan dukungan dan doa untuk saya
3. Bapak Dony Ariyus, M.kom, Selaku dosen pembimbing yang telah membantu dalam menyusun skripsi ini.
4. Bapak Banu Santoso, S.T.,M.Eng. Selaku Dosen wali yang telah memberikan arahan dan bimbingan selama 4 Tahun terakhir.
5. Kepada Adik saya Ainul Sabilah dan Annur Fafi Rahmah yang telah memberikan semangat serta dukunganya.
6. Kepada sahabat saya, Mega, Nita, Lisa, Mirna dan teman saya Tansen, Hardiansyah, Andrian, Ilham, Randika yang selalu membantu memberikan motivasi dan dukungan agar saya bisa menyelesaikan skripsi ini.
7. Rekan – rekan kelas 17 Teknik Komputer 1, yang telah memberikan saya dukungan, semangat serta menemani selama 4 tahun dalam satu kelas yang penuh dengan segala kondisi dalam hidup. Terimakasih atas kenangan-kenangan yang telah kita ukir bersama-sama. Semoga kita menjadi orang-orang yang bermanfaat dan dikenang menjadi pribadi yang baik, Aamiin.

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Dengan mengucapkan Syukur kepada Allah SWT, yang telah memberikan Karunia dan Rahmat-nya, penulis bisa menyelesaikan skripsi yang berjudul: *"Analisis Dan Deteksi Malware Remote Access Trojan (RAT) Menggunakan Metode Statis Dan Dinamis".* Tujuan skripsi ini adalah untuk memenuhi salah satu persyaratan ujian guna untuk mendapatkan gelar sarjana komputer (S.Kom) pada program studi Teknik Komputer, Fakultas ilmu Komputer, Universitas AMIKOM Yogyakarta.

Dalam menyelesaikan skripsi ini telah melibatkan beberapa pihak yang sangat membantu dalam segala hal. Oleh karena itu penulis menyampaikan banyak terimakasih sedalam-dalamnya kepada:

1. Allah SWT, Tuhan Yang Maha Esa karena atas izin dan karunia-Nyalah, skripsi ini dapat selesai pada waktunya.
2. Prof. Dr. M. Suyanto, MM selaku rektor Universitas AMIKOM Yogyakarta
3. Ibu Krisnawati, S.Si., M.T. selaku Dekan Fakultas Ilmu Komputer dan Ketua Program Studi S1 Sistem Informasi.
4. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta
5. Kedua orang tua, yang selalu memberikan dukungan baik materi maupun doa.
6. Bapak dan Ibu Universitas AMIKOM Yogyakarta yang telah memberikan ilmunya selama penulis kuliah.
7. Keluarga besar kelas S1 Teknik Komputer 01 angkatan 2017.Serta semua pihak yang telah membantu dalam proses penyusunan skripsi ini yang tidak dapat disebutkan satu per satu.

Akhirnya dengan kerendahan hati penulis mengucapkan terimakasih dan semoga skripsi ini dapat bermanfaat bagi penulis maupun pembaca.

Wassalamualaikum Warahmatullahi Wabarakatuh

Yogyakarta, 10 Agustus 2021

Ansyuri Fadila

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Saat ini para pengguna aktif di internet banyak yang melakukan kegiatan pengunduhan, baik saat mengakses informasi, bisnis maupun informasi lainnya secara legal maupun ilegal. Namun tanpa disadari saat melakukan aktivitas pengunduhan secara ilegal banyak sekali kerugian yang didapatkan salah satunya yaitu malware yang disisipkan pada aplikasi atau trojan. Ancaman yang timbul dari program jahat ini sangatlah berbahaya karena program jahat ini mampu mengontrol sistem komputer khususnya penguna windows dari jarak jauh atau yang biasa disebut *Remote Access Trojan* (RAT). RAT mulai dimanfaatkan oleh pembuat malware untuk disisipkan pada *software* seperti pada *file* dengan ekstensi .EXE.

Analisis akan dilakukan dari pembuatan malware pada *software* njRAT yang kemudian malware tersebut dianalisa oleh Virus Total, dan *tools* Cuckoo, hasil dari analisis statis dan dinamis yang di lakukan oleh *tools* Cuckoo secara otomatis akan dikaji ulang untuk menentukan alur dari malware njRAT bekerja, selain kedua *tools* tersebut peneliti juga melakukan analisis dengan tools Wireshark untuk menganalisis jaringan dari malware tersebut.

Hasil implementasi dari malware njRAT yang berhasil di konfigurasi dan dibentuk menjadi trojan (*server.exe*) dapat di deteksi oleh Virus Total dengan rasio 59 dari 70 anti-malware. Kemudian dari analisis dinamis Cuckoo, terekam juga aktivitas mencurigakan seperti proses pengaksesan dan pengantian *registry*, serta pembuatan dan duplikasi pada direktori yang berbeda yang diduga merupakan *path* asli dari malware tersebut berada. Hasil dari *network analysis* menggunakan wireshare ditemukan *ip controller* serta *port* yang digunakan oleh malware ketika menginfeksi.

Kata kunci: Malware, Remote access Trojan (RAT), Analisi Statis, Analisis Dinamis, Network Analisis.

ABSTRACT

Currently, there are many active users on the internet who carry out downloading activities, both when accessing information, business and other information legally or illegally. However, without realizing it, when carrying out illegal downloading activities, there are a lot of losses, one of which is malware that is inserted into the application or trojan. Threats that arise from this malicious program are very dangerous because this malicious program is able to control computer systems, especially Windows users remotely or commonly called Remote Access Trojan (RAT). RAT began to be used by malware makers to be inserted into software such as files with the .EXE extension.

The analysis will be carried out from the creation of malware on the njRAT software which is then analyzed by Virus Total, and the Cuckoo tools, the results of the static and dynamic analysis carried out by the Cuckoo tools will automatically be reviewed to determine the flow of the njRAT malware working, in addition to the two tools The researchers also conducted an analysis with Wireshark tools to analyze the network from the malware.

The results of the implementation of the successfully configured njRAT malware and formed into a trojan (server.exe) can be detected by Virus Total with a ratio of 59 out of 70 anti-malware. Then from Cuckoo's dynamic analysis, suspicious activity was also recorded, such as the process of accessing and changing the registry, as well as creating and duplicating in different directories which are suspected to be the original path of the malware. The results of the network analysis using wireshare found the IP controller and the port used by the malware when it infected.

Keywords: *Malware, Remote access Trojan (RAT), Static Analysis, Dynamic Analysis, Network Analysis.*