DETEKSI MALWARE ADWARE PADA PLATFORM ANDROID DENGAN METODE REVERSE ENGINEERING

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

ALDO SAPRIANSYAH
09011181520035

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2021

HALAMAN PENGESAHAN

DETEKSI MALWARE ADWARE PADA PLATFORM ANDROID DENGAN METODE REVERSE ENGINEERING

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

ALDO SAPRIANSYAH
09011181520035

Indralaya, 31 Desember 2020

Pembimbing I	Pembimbing II
Deris Stiawan, M.T., Ph.D.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 197806172006041002	**NIP.198701222015041002**

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Pada hari Kamis 31 Desember 2020 telah dilaksanakan ujian sidang tugas akhir oleh Sarjana Ilmu Komputer, Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Aldo Sapriansyah

Nim 09011181520035

Judul : Deteksi Malware Adware Pada Platform Android Dengan Metode Reverse Engineering

Tim Penguji :

1. **Penguji**

   Huda Ubaya, M.T. (.....)

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Aldo Sapriansyah

Nim : 09011181520035

Jurusan : Sistem Komputer

Judul : Deteksi Malware Adware Pada Platform Android Dengan Metode Reverse Engineering

Hasil Pengecekan Software *iThenticate/Turnitin*: 18%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya 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 sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Indralaya, 6 Januari 2021

Aldo Sapriansyah

NIM.09011181520035

HALAMAN PERSEMBAHAN

“Selalu ada harapan bagi mereka yang sering berdoa dan selalu ada jalan bagi mereka yang gemar berusaha dan Tak perlu jadi hebat untuk memulai, tapi kita harus memulai untuk bisa menjadi hebat.” – Zig Ziglar

Tugas Akhir ini saya persembahkan untuk :

- **Kedua Orangtua, Kakak, Adik dan saudara-saudaraku**
- **Dosen Pembimbing dan Penguji**
- **Almamaterku (Universitas Sriwijaya)**
- **Teman Seperjuangan Sistem Komputer 2015**
- **Sahabat – sahabat saya**

KATA PENGANTAR

Alhamdulillahhirobbil'alamin Puji dan syukur penulis panjatkan kehadirat Allah Subhanahu Wa ta'ala , atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan tugas akhir ini dengan judul "Deteksi Malware Adware Pada Platform Android Dengan Metode Reverse Engineering" di susun untuk memenuhi sebagian persyaratan kelulusan untuk memperoleh gelar Sarjana Komputer pada jurusan Sistem Komputer Universitas Sriwijaya.

Pada kesempatan ini penulis menyadari keterbatasan dan kelemahan yang ada dalam menyelesaikan skripsi ini sehingga penulis ingin menyampaikan ucapan terimakasih kepada pihak-pihak yang telah memberikan dukungan, bimbingan dan motivasi kepada penulis untuk menyelasaikan tugas akhir ini, kepada:

1. Allah Subhanahu Wa Ta'ala, yang telah memberikan rahmat dan karunia-Nya sehingga penulisan tugas akhir ini dapat berjalan dengan lancar.
2. Kedua orang tua beserta keluarga yang selalu dan tak henti mendoakan serta memberikan motivasi dan semangat kepada saya.
3. Bapak Jaidan Jauhari, S.Pd., M.T. selaku dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T. sebagai Ketua Jurusan Sistem Komputer Universitas Sriwijaya.

5. Bapak Deris Stiawan, M.T., Ph.D. selaku pembimbing 1 tugas akhir yang telah meluangkan waktu, bantuan serta saran dan kritiknya dalam penyusunan tugas akhir ini.
6. Bapak Ahmad Heryanto, S.Kom., M.T. selaku pembimbing 2 tugas akhir yang telah meluangkan waktu, bantuan serta saran dan kritiknya dalam penyusunan tugas akhir ini.
7. Dosen-dosen pengajar yang telah memberikan ilmu bermanfaat kepada penulis selama menuntut ilmu di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Mba Winda Kurnia Sari selaku Administrator Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberi kemudahan dalam pengurusan administrasi.
9. Mba Renny Virgasari selaku Administrator Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberi kemudahan dalam pengurusan administrasi.
10. Seluruh teman-teman Jurusan Sistem Komputer Angkatan 2015 yang telah membantu dan memberikan semangat pada masa-masa perkuliahan.
11. Semua pihak yang telah memberi dukungan kepada penulis dan tidak bisa disebutkan satu-persatu.

Akhir kata, penulis menyadari bahwa tugas akhir ini masih banyak kekurangan baik dari isi maupun susunan. Semoga tugas akhir ini dapat bermanfaat untuk kita semua.

Indralaya, 6 Januari 2021

Aldo Sapriansyah

DETEKSI MALWARE ADWARE PADA PLATFORM ANDROID DENGAN METODE REVERSE ENGINEERING

Aldo Sapriansyah(09011181520035)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer

Universitas Sriwijaya

E-mail: aldosapriansyah9@gmail.com

ABSTRAK

Malware bisa juga diartikan sebuah software yang dipasang dalam suatu sistem komputer tanpa sepengetahuan user atau pemilik sistem tersebut. Malware akan melakukan tindakan yang tidak diinginkan oleh pengguna, seperti mencuri informasi rahasia pengguna, perusakan pada suatu sistem yang diinfeksi, mendapatkan akses dari suatu komputer dan bisa menjalankan program pada komputer korban tersebut. *Malware* juga banyak ditemukan pada sistem android salah satunya jenis *adware*. *Adware* juga termasuk dalam jenis malware yang biasanya akan memberikan informasi kepada pengiklan tentang bagaimana kebiasaan browsing si pengguna, tentu saja pengiklan akan tahu informasi yang penting dalam sistem android pengguna.

Dengan menggunakan metode *reverse engineering* yang menggunakan metode analisis statis pada penulisan tugas akhir ini tentunya akan dapat mendeteksi keberadaan *malware adware* dari suatu aplikasi yang akan digunakan pada perangkat android. Dengan melihat izin pemasangan dan juga permission dari suatu aplikasi maka akan didapatkan hasil yang mendeteksi keberadaan dari *malware adware* tersebut.

Kata Kunci : Reverse Engineering, Analisis Statis, Malware Adware Android.

MALWARE ADWARE DETECTION ON ANDROID PLATFORM WITH REVERSE ENGINEERING METHOD

Aldo Sapriansyah(09011181520035)

Dept. of Computer Engineering, Faculty of Computer Science,

Sriwijaya University

E-mail: aldosapriansyah9@gmail.com

ABSTRACT

Malware can also be defined as software installed on a computer system without the knowledge of the user or owner of the system. Malware will perform actions that the user does not want, such as confidential user information, attack to an infected system, get access from a computer and can run programs on the victim's computer. Malware is also commonly found on Android systems, one type of adware. Adware is also included in a type of malware which will usually provide information to advertisers about how the user's browsing habits are, of course, advertisers will know important information in the user's Android system.

By using the reverse engineering method which uses the static analysis method in writing this thesis, of course, will be able to detect the presence of adware malware from an application that will be used on an Android device. By looking at the installation permission and also the permissions of an application, you will get results that detect the presence of the adware malware.

Keywords: Reverse Engineering, Static Analysis, Malware Adware Android.

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1. Latar Belakang

Malware mempunyai sistem pertahanan sendiri serta sangat dimungkinkan buat menyembunyikan diri dari antivirus ataupun apalagi menginfeksi antivirus itu sendiri[1]. Malware dapat ditangani dengan cara mengenali metode kerja kala telah melakukan serangan ke dalam sistem komputer pengguna. Dengan kata lain malware bisa ditangani ketika berhasil dianalisa serta mengenali data yang dibawa oleh malwarenya.

Pada penelitian[2], melakukan reverse engineering dari sampel malware botnet. Dari penelitiannya telah ditunjukan untuk bagaimana menentukan pendekatan yang paling dekat sebagai pencegahan dari serangan botnet. Pada proses yang telah terjadi inilah terjadinya gangguan yang merupakan aktivitas online ilegal dan juga dapat dikatakan sebagai aksi pencurian data dari sebuah organisasi dan perorangan hal ini tentunya dapat dicegah dengan pengembangan Sistem Intrusion Prevention yang lebih spesifik.

Pada penelitian[3], telah melakukan reverse engineering pada sampel malware Flawed ammyy rat. Kemudian dari riset yang telah dijalankan dengan analisis dinamis serta reverse engineering memakai sesi disassembly menampilkan pergerakan dari malware dimana malware ini tidak bisa berjalan pada sistem dalam kondisi fashion DOS. Malware ini akan memanipulasi system dengan metode melaksanakan aplikasi Ammyy Admin 3, sebab Amyy Admin ialah aplikasi yang nyaman hingga berikan akses pada malware tersebut. Malware RAT ini dicoba dengan metode basic analisis malware sebab tidak seluruh malware rat ini berjalan pada system. Malware rat ini wajib terkoneksi dengan attacker bagaikan tuan yang melaksanakan perintah berikutnya, semacam mengaktifkan keyloger, menggerakkan pointer korban, apalagi bisa mengaktifkan webcam korban tanpa sepengetahuan.

Pada penelitian[4], Menyamakan ketepatan deteksi antara aplikasi antivirus dengan metode analisis statis yang dicoba dengan metode mencari ciri malware yang diperoleh dari hasil scanning paling banyak pada Virus Total. Sehabis ciri malware ditemui, dilanjutkan dengan menganalisis value string pada ilustrasi

malware yang cocok dengan karateristik malware. Bila value string yang ditemui mewakili ciri malware, hingga hasil deteksi pada aplikasi antivirus bisa dikatakan pas serta cocok dengan hasil analisis yang dicoba dengan tata cara statis analisis.

Dari 10 ilustrasi malware yang diuji, cuma 3 ilustrasi malware yang bisa dianalisis. Buat ilustrasi awal yang ditemukan bagaikan spybot, seluruh karakteristiknya bisa dibuktikan dengan value string yang dihasilkan. Buat ilustrasi kedua yang ditemukan bagaikan trojan, cuma 6 dari 8 ciri trojan yang bisa dibuktikan dari value string yang dihasilkan. Buat ilustrasi ketiga, cuma 7 dari delapan ciri trojan yang bisa dibuktikan dari value string yang dihasilkan.

Ada dua cara untuk melakukan malware analisis, analisis statis dan analisis dinamis. Analisis statis dilakukan dengan cara kode malware akan dianalisis tanpa menjalankan malware tersebut, sementara analisis dinamis menjalankan malware secara langsung[2]. Menganalisa file exe dengan teknik analisis statis bisa menjelaskan beberapa informasi tentang Malware tanpa harus dijalankan pada virtual mesin. Analisis dinamis menjalankan Malware dan memeriksa perilakunya saat run-time dan tersedia lebih banyak informasi dan dapat meningkatkan kemampuan untuk mengidentifikasi malware yang dijalankan, bahkan untuk malware yang disamarkan. Analisis dinamis menjalankan malware pada lingkungan yang aman secara virtual dengan cermat aktivitasnya diawasi sambil memanfaatkan alat atau fitur yang canggih[3].

Berdasarkan latar belakang diatas dan penelitian-penelitian yang telah dilakukan dengan menggunakan metode reverse engineering untuk menganalisa dan mengetahui malware dalam sebuah sistem maka penulis akan mengikuti cara penelitian[4],dikarenakan objek yang akan saya teliti ini adalah sebuah program yang berjalan di platform android sementara pada penelitian[2][3] objek yang ditelitinya merupakan malware yang berjalan pada sistem komputer. Maka daripada itu penelitian ini akan menggunakan analisis statis, dan bagaimana mendeteksi serta analisa keberadaan malware adware jenis youmi dengan metode reverse engineering dengan cara menganalisa source code pada file androidmanifest.xml yang telah di ekstrak dari aplikasi CICAndMal2017 dan CIC dataset. Dengan melihat permission atau izin aplikasi tersebut.

2. Tujuan

Adapun tujuan dari dilakukannya penelitian ini adalah:

1. Mendeteksi keberadaan malware adware jenis youmi pada file androidmanifest.xml yang berupa permission atau izin pada aplikasi.
2. Membandingkan hasil deteksi menggunakan virus total dan dengan metode dan analisis reverse engineering dengan analisis statis.

3. Manfaat

Adapun manfaat dari penelitian ini diharapkan:

1. Dapat mengetahui cara kerja malware adware pada sistem android terutama pada file androidmanifest.
2. Dapat mempelajari source code sebuah aplikasi android.
3. Dapat menjadi referensi untuk penelitian selanjutnnya.

4. Batasan Masalah

Adapun batasan masalah pada penelitian ini:

1. Hanya menganalisis malware adware khususnya jenis youmi dari dataset "CICAndMal2017 dan CIC" yang terdapat pada source code file androidmanifest.
2. Tidak akan menangani lebih jauh tentang bagaimana aksi pencegahan dan penanganan dari malware tersebut.
3. Tidak dilakukannya uji sampel secara real-time.

5. Metodologi Penelitian

Dalam tugas akhir ini akan menggunakan metodologi dan melewati beberapa tahapan sebagai berikut:

1. Study Pustaka (Literatur)

Tahap ini ialah tahap yang mencari referensi atau literatur pada Keyword yang di angkat dari judul yang bertujuan untuk menunjang pada penelitian yang dilakukan.

2. Konsultasi

Pada tahap ini, peneliti berkonsultasi kepada orang-orang yang sudah dianggap memiliki pengalaman, pengetahuan terhadap permasalahan pada saat pembuatan Tugas Akhir ini.

3. Pengumpulan Data

Pada tahap ini, data yang diperoleh adalah dataset youmi malware yang termasuk dalam kategori adware pada android, sumber dataset didapatkan dari CICAndMal2017 dan CIC dataset.

4. Pengolahan Data

Pada tahapan ini, dilakukannya pengolahan data dengan cara diterapkan data ekstraksi dan juga seleksi dengan metode reverse engineering.

5. Analisa

Pada tahap ini dilakukan analisa data yang telah dilakukan pengolahan.

6. Kesimpulan dan Saran

Pada tahap ini dilakukan penarikan kesimpulan dari analisa dan studi literatur serta saran jika ada untuk penulis selanjutnya mungkin bisa dijadikan bahan referensi.

DAFTAR PUSTAKA

[1] A. H. Lashkari, A. F. Akadir, H. Gonzalez, K. F. Mbah, and A. A. Ghorbani, "Towards a network-based framework for android malware detection and characterization," *Proc. - 2017 15th Annu. Conf. Privacy, Secur. Trust. PST 2017*, no. Cic, pp. 233–242, 2018, doi: 10.1109/PST.2017.00035.

[2] S. Alam, Z. Qu, R. Riley, Y. Chen, and V. Rastogi, "DroidNative: Automating and optimizing detection of Android native code malware variants," *Comput. Secur.*, vol. 65, no. July 2018, pp. 230–246, 2017, doi: 10.1016/j.cose.2016.11.011.

[3] D. J. Wu, C. H. Mao, T. E. Wei, H. M. Lee, and K. P. Wu, "DroidMat: Android malware detection through manifest and API calls tracing," *Proc. 2012 7th Asia Jt. Conf. Inf. Secur. AsiaJCIS 2012*, pp. 62–69, 2012, doi: 10.1109/AsiaJCIS.2012.18.

[4] Ö. Aslan, "Performance Comparison of Static Malware Analysis Tools Versus Antivirus Scanners To Detect Malware," 2017.

[5] A. Mylonas and D. Gritzalis, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software," *Comput. Secur.*, vol. 31, pp. 802–803, 2012, doi: 10.1016/j.cose.2012.05.004.

[6] C. Tsai, M. Lin, Y. Yang, and D. Rao, "Technique for false positives prevention in high availability network." 2014.

[7] Broadcom, "Symantec Endpoint Protection. Dikutip dari https://community.broadcom.com. Diakses pada tanggal 31 Desember 2020," 2020. [Online]. Available: https://community.broadcom.com/.

[8] M. Ignaio, H. Jose, Alberto, and D. L. S. Sergio, "On labeling Android malware signatures using minhashing and further classification with Structural Equation Models," *CEUR Workshop Proc.*, vol. 2657, no. 13 September 2017, pp. 1–16, 2020, doi: 10.1145/nnnnnnn.nnnnnnn.

[9] N. D. Birajdar, M. N. Dhuppe, T. M. Hegade, N. S. Jadhav, and M. D. Shelar, "Review Paper On Adware Detection Using Instruction Sequence

Generation," *Int. J. Eng. Tech.*, vol. 1, no. 6, pp. 25–28, 2015.

[10] L. K. Hatika, A. Budiyono, A. Almaarif, F. R. Industri, and U. Telkom, "ANALISIS KETEPATAN DETEKSI MALWARE PADA SOFTWARE ANTIVIRUS MENGGUNAKAN METODE ANALISIS STATIS ACCURACY ANALYSIS OF MALWARE DETECTION IN ANTIVIRUS SOFTWARE," vol. 6, no. 2, pp. 7812–7819, 2021.

[11] N. K. Gyamfi and E. Owusu, "Survey of Mobile Malware Analysis, Detection Techniques and Tool," *2018 IEEE 9th Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEMCON 2018*, no. May 2019, pp. 1101–1107, 2019, doi: 10.1109/IEMCON.2018.8614895.

[12] W. Zhang and F. Gao, "An Improvement to Naive Bayes for Text Classification," *Procedia Eng.*, vol. 15, pp. 2160–2164, 2011, doi: 10.1016/j.proeng.2011.08.404.

[13] V. Manjunath, "reverse engineering of malware on android," *SANS Inst. Inf. Secur. Read. Room*, 2020.

[14] P. Peng, L. Yang, L. Song, and G. Wang, "Opening the blackbox of virustotal: Analyzing online phishing scan engines," *Proc. ACM SIGCOMM Internet Meas. Conf. IMC*, pp. 478–485, 2019, doi: 10.1145/3355369.3355585.

[15] T. P. Setia, A. P. Aldya, and N. Widiyasono, "Reverse Engineering untuk Analisis Malware Remote Access Trojan," *J. Edukasi dan Penelit. Inform.*, vol. 5, no. 1, p. 40, 2019, doi: 10.26418/jp.v5i1.28214.

[16] H. A. Nugroho and Y. Prayudi, "Penggunaan Teknik Reverse Engineering Pada Malware Analysis Untuk Identifikasi Serangan," *Knsi*, pp. 27–28, 2014.