DETEKSI *REMCOS REMOTE ACCESS TROJAN* (RAT) PADA *PHISHING EMAIL CORONA VIRUS* DENGAN METODE *REVERSE ENGINEERING*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

TARISSA FITRIANI
09011381823116

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

DETEKSI *REMCOS REMOTE ACCESS TROJAN* (RAT) PADA *PHISHING EMAIL CORONA VIRUS* DENGAN METODE *REVERSE ENGINEERING*

TUGAS AKHIR

Program Studi Sistem Komputer
Jenjang S1

Oleh

Tarissa fitriani
09011381823116

Palembang, 9 Januari 2023

Mengetahui,

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

ii

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa

Tanggal : 20 Desember 2022

Tim Penguji :

1. **Ketua** : **Sarmayanta Sembiring, M.T.**
2. **Sekretaris** : **Iman Saladin B. Azhar, M.MSI.**
3. **Pembimbing** : **Deris Stiawan, M.T., Ph.D.**
4. **Penguji** : **Ahmad Zarkasi, M.T**

Mengetahui, 5/1/23

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

iii

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Tarissa fitriani

NIM : 09011381823116

Judul : Deteksi *remcos remote access trojan* (RAT) pada *phising email corona virus* dengan metode *reverse engineering*

Hasil Pengecekan Software iThenticate/Turnitin : 5 %

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 tidak dipaksakan.

Palembang,6 Januari 2023

Tarissa fitriani
NIM. 09011381823116

iv

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Segala puji dan syukur atas kehadirat Tuhan Yang Maha Esa, yang atas segala berkat,kasih sayang,serta karunia-Nya penulis dapat menyelesaikan penulisan proposal tugas akhir ini yang berjudul "**Deteksi *remcos remote access trojan* (RAT) pada *phising email corona virus* dengan metode *reverse engineering***".

Pada penyusunan laporan ini, penulis banyak mendapatkan ide dan saran serta bantuan dari berbagai pihak baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Tuhan Yang Maha Esa dan terimakasih kepada yangterhormat:

1.Kedua orang tua, saudara, dan Keluarga Besar yang selalu mendoakan dan memberikan motivasi dan *support.*

2.Bapak Dr.Ir.Sukemi,M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer.

3. Bapak Huda Ubaya,M.T. Selaku Dosen Pembimbing Akademik

4.Bapak Jaidan Jauhari selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.

5. Bapak Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing Tugas Akhir.

6.Mba Sari selaku Administrasi Jurusan Sistem Komputer yang telah membantu melancarkan proses administrasi terkait Tugas Akhir

7.Seluruh staff dan pegawai jurusan sistem komputer beserta teman seperjuagan yang telah membersamai jalan juang.

8. Teman seperjuangan TA yaitu Viola Aqila Fawwaz dan Rika Fitriani yang membantu dan memberikan semangat dalam menyelesaikan laporan TA.

9.Teman – teman dan Adik Tingkat dari Grup Riset COMNETS yaitu Budiman Alfian, Chendy Maulana, Rifqi Abiyyu, Christoper Marlo, Garinnang Baiduri, Al-Mais, Ageng Raharjo, Arief Saifullah, Rizki Ridho, dll…

10. Dan semua pihak yang telah membantu..

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangatlah diharapkan penulis agar dapat segera diperbaiki sehingga laporan ini dapat dijadikan sebagai masukkan ide dan pemikiran yang bermanfaat bagi semua pihak dan menjadi tambahan bahan bacaan bagi yang tertarik dalam penelitian *reverse engineering*.

Wassalamualaikum Warahmatullahi Wabarakatuh

Palembang, 6 Januari 2023

Penulis,

Tarissa fitriani
NIM. 09011381823116

vi

REMOTE ACCESS TROJAN (RAT) DETECTION IN CORONAVIRUS PHISHING EMAIL USING REVERSE ENGINEERING METHOD

Tarissa Fitriani (09011381823116)

Department of Computer Systems, Faculty of Computer Science, Sriwijaya University
Email : tarissafitriani26@gmail.com

ABSTRACT

Remote Access Trojan (RAT) is a special type of remote access software commonly used for malicious purposes, in which the installation is performed without the user's consent, the remote control then performed silently, and the program hides in the system to avoid detection. Cyber attackers send phishing emails based on COVID-19 themes that attached with malware to disable networks or to steal data and credentials. This study uses reverse engineering and dynamic analysis methods to detect Remcos RAT malware. The results of this study indicate that the Remcos RAT malware used to control remote target computers. The malware infection method uses the TLSv1.2 protocol with RC4 encryption on port 1234 to communicate with the target computer. Malware activity then retrieves target computer information and the capabilities of creating, writing, deleting files, taking screenshots, and recording audio.

Keywords: *malware, remote access trojan, phishing, reverse engineering*

DETEKSI *REMCOS REMOTE ACCESS TROJAN* (RAT) PADA *PHISHING EMAIL CORONA VIRUS* DENGAN METODE *REVERSE ENGINEERING*

Tarissa Fitriani (09011381823116)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : tarissafitriani26@gmail.com

ABSTRAK

Remote Access Trojan (RAT) adalah jenis khusus perangkat lunak akses jarak jauh yang biasa digunakan untuk tujuan jahat, di mana penginstalan dilakukan tanpa persetujuan pengguna, kendali jarak jauh dilakukan secara diam-diam, dan program menyembunyikan dirinya sendiri dalam sistem untuk menghindari deteksi. Penyerang dunia maya mengirimkan *email phishing* berbasis tema COVID-19 yang melampirkan *malware* untuk menonaktifkan jaringan atau mencuri data dan kredensial. Penelitian ini menggunakan metode *reverse engineering* dan analisis dinamis untuk mendeteksi *malware Remcos RAT*. Hasil dari penelitian ini menunjukan bahwa *malware Remcos RAT* digunakan untuk mengendalikan komputer target jarak jauh. Metode infeksi yang dilakukan *malware* menggunakan protokol TLSv1.2 dengan enkripsi RC4 pada port 1234 untuk berkomunikasi dengan komputer target. Aktivitas *malware* mengambil informasi komputer target, kemampuan membuat, menulis, menghapus file, mengambil *screenshot* dan merekam audio.

Kata Kunci : *malware, remote access trojan, phishing, reverse engineering*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABLE

BAB I
PENDAHULUAN

1.1 Latar Belakang

Severe Acute Respiratory Syndrome Coronavirus-2 (SARS- CoV-2) adalah jenis baru dari penyakit *coronavirus* yang pertama kali terdeteksi pada manusia pada tahun 2019. Pada 11 Februari 2020, *World Health Organisation* (WHO) mengumumkan bahwa mereka akan menyebut penyakit tersebut sebagai COVID - 19. Menurut penelitian [1], Pandemi akibat penyebaran COVID-19 dengan cepat menjadi peristiwa krisis global, mengakibatkan karantina massal terhadap 100-an juta warga di berbagai negara di dunia.

Selama pandemi *virus corona* saat ini, penyerang dunia maya memanfaatkan kecemasan orang untuk mencuri informasi rahasia, mendistribusikan perangkat lunak berbahaya, melakukan serangan *ransomware*, dan menggunakan serangan rekayasa sosial lainnya. Dalam penelitian [2], penyerang dunia maya juga mengirim email phishing yang tampaknya berasal dari WHO atau organisasi kesehatan resmi mana pun kepada karyawan atau pengguna layanan kesehatan seperti email dengan lampiran PDF yang berisi informasi tentang langkah-langkah keamanan virus corona yang ditunjukkan.

Phishing adalah proses pengiriman email palsu yang tampaknya berasal dari sumber tepercaya yang tujuan utamanya adalah memperoleh data pribadi pengguna (sandi, kode PIN, detail perbankan, dll.), mengarahkan pengguna ke situs web palsu atau yang terinfeksi virus, meluncurkan perangkat lunak berbahaya di komputer pengguna. Saat melakukan serangan *phishing*, penyerang secara aktif menggunakan metode rekayasa sosial. Tahun 2021 dalam penelitian [3], rekayasa sosial adalah teknik manipulasi psikologis tindakan manusia berdasarkan penggunaan kelemahan dan karakteristik individu.

National Cyber Security Centre (NCSC) telah menghapus lebih dari 2.000 penipuan online terkait *virus corona*, termasuk 471 toko online palsu, 555 situs distribusi *malware*, 200 situs *phishing*, dan 832 penipuan uang muka. Google juga telah memblokir lebih dari 100 juta *email phishing* setiap hari, dan 18 juta *malware* dan *email phishing* terkait *virus corona* selama April 2020 [2]. WHO memperingatkan orang-orang tentang *phishing* yang tampaknya berasal dari WHO

dan meminta informasi sensitif seperti nama pengguna atau kata sandi, atau mengundang pembaca untuk mengklik tautan berbahaya atau membuka lampiran berbahaya.

Dalam bentuk *email phishing* dengan lampiran berbahaya, penyerang dunia maya meluncurkan serangan berbasis tema COVID-19 yang melampirkan *malware* untuk menonaktifkan jaringan atau mencuri data dan kredensial [4] . Salah satunya menggunakan malware jenis *remote access trojan.* Menurut penelitian [5], *Remote Access Trojan* (RAT) adalah jenis khusus perangkat lunak akses jarak jauh yang biasa digunakan untuk tujuan jahat, di mana penginstalan dilakukan tanpa persetujuan pengguna, kendali jarak jauh dilakukan secara diam-diam, dan program menyembunyikan dirinya sendiri dalam sistem untuk menghindari deteksi.

Dalam penelitian [6], penyerang mengirimkan *email phishing* yang berisi file *Remcos RAT Malware* yang dapat dieksekusi dengan nama "CoronaVirusSafetyMeasures_pdf[.]exe" . *Remcos RAT* pertama kali terlihat pada tahun 2016. Baik klien dan server ditulis dalam C++ sehingga ringan. *Remcos rat* menargetkan sistem operasi windows 32 bit dan 64 bit. Fungsinya termasuk mengunggah dan mengunduh file, manajemen sistem, dan *keylogger*.

Pada penelitian ini akan dilakukan *reverse engineering* dan analisis dinamis pada file yang bernama "Vaccinecovid19_pdf.exe". *Reverse engineering* untuk mendeteksi keberadaan *remote access trojan* dan mempelajari fungsi file tersebut. analisis dinamis dilakukan dengan cara menjalankan file *malware* dan menganalisa aktivitas yang dilakukan.

1.2 Tujuan

Adapun tujuan dari penulisan tugas akhir ini, yaitu :

1. Untuk mendeteksi keberadaan *malware remcos rat* pada file yang bernama "Vaccinecovid19_pdf.exe" menggunakan metode *reverse engineering*.
2. Memahami fungsi, jenis, metode infeksi, dan aktivitas *malware remcos rat* menggunakan *reverse engineering* dan analisis dinamis.
3. Dampak yang dihasilkan dari file *malware remcos rat* dan serangan *phising*.

1.3 Manfaat

Berikut manfaat dari penulisan tugas akhir ini, yaitu

1. Dapat mendeteksi keberadaan *malware remcos rat* yang dikirim melalui *email phising* corona virus.
2. Hasil analisis dapat digunakan untuk mengetahui fungsi, jenis, metode infeksi, dan aktivitas dan dampak dari file *malware remcos rat*.
3. Dapat mengetahui dan mempelajari source code dari file *malware remcos rat*
4. Dapat menjadi referensi untuk penelian selanjutnya

1.4 Perumusan Masalah

Berikut adalah rumusan masalah dalam penulisan Tugas Akhir ini:

1. Bagaimana cara mendeteksi keberadaan *malware remcos rat* pada file yang dikirim melalui *phising email corona virus*?
2. Bagaimana fungsi, jenis, metode infeksi, dan aktivitas dari file *malware remcos rat* tersebut?
3. Apa saja dampak yang ditimbulkan dari file yang bernama "Vaccinecovid19_pdf.exe"?

1.5 Batasan Masalah

Berikut batasan masalah dari tugas akhir ini, yaitu:

1. Tidak akan menangani lebih jauh tentang bagaimana aksi pencegahan dan penanganan dari *malware remcos rat* tersebut.
2. Hanya menganalisis *malware remcos rat* khususnya yang dikirimkan melalui *phising email corona virus*.
3. membahas cara mendeteksi serangan.

1.6 Metodelogi Penelitian

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

1. Tahap Pertama (Studi Pustaka / Literatur)

   Tahapan ini dimulai setelah masalah yang telah di bahas sesuai dengan

penelitian sebelumnya yang mengacu banyaknya artikel, paper, jurnal dan buku yang berhubungan dengan penelitian ini yang berjudul "Deteksi *remcos remote access trojan* (RAT) pada *phising email corona virus* dengan metode *reverse engineering*".

2. Tahap Kedua (Perancangan Sistem)

   Tahapan ini merupakan tahapan untuk menentukan perangkat-perangkat yang dibutuhkan pada penelitian, berupa perangkat keras ataupun lunak.

3. Tahap Ketiga (Pengujian)

   Tahapan ketiga ialah pengujian yang sesuai dengan parameter serangan yang ditentukan oleh batasan masalah.

4. Tahap Keempat (Hasil dan Analisa)

   Tahapan keempat mencakup hasil pengujian pada penelitian ini kemudian Hasil penelitian dianalisa untuk mengetahui kelebihan dan kekurangan rancangan penelitian beserta faktor yang mempengaruhi.

5. Tahap Kelima (Kesimpulan dan Saran)

   Tahapan terakhir meliputi kesimpulan dan saran dari hasil studi pustaka dan literatur, perancangan sistem dan analisa pada penelitian. Pada saran berisi poin-poin dari penulis untuk penelitian berikutnya.

1.7 Sistematika Penulisan

Dalam memudahkan penyusunan Tugas Akhir ini dan juga untuk memperjelas isi dari setiap bab dari tugas akhir ini, dilakukan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pada bab pertama membahas tentang Latar Belakang Masalah, Tujuan dan Manfaat, Perumusan dan Batasan Masalah, Metode Penelitian, dan Sistematika Penulisan dari penelitian yang dilakukan sebagai dasar penelitian ini.

BAB II TINJAUAN PUSTAKA

Bab kedua menjelaskan Dasar Teori, Konsep dan Prinsip Dasar yang diperlukan untuk memecahkan masalah dalam penelitian ini.

BAB III METODOLOGI

Bab ketiga ialah metodologi yang diterapkan akan dibahas secara rinci tentang teknik, metode, dan alur proses yang dilakukan dalam penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab keempat ialah hasil pengujian dan analisis yang telah diperoleh dari penelitian ini dan pembahasan terhadap hasil yang telah dicapai meliputi kelebihan dan kekurangan dari penelitian.

BAB V KESIMPULAN DAN SARAN

Pada bab kelima ialah kesimpulan yang bersumber dari hasil penelitian yang telah dilakukan dan juga saran untuk penelitian selanjutnya khususnya tentang Tugas Akhir yang dikerjakan.

DAFTAR PUSTAKA

[1] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput. Secur.*, vol. 105, p. 102248, 2021, doi: 10.1016/j.cose.2021.102248.

[2] A. Alzahrani, "Coronavirus social engineering attacks: Issues and recommendations," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 5, pp. 154–161, 2020, doi: 10.14569/IJACSA.2020.0110523.

[3] M. A. Ivanov, B. V. Kliuchnikova, I. V. Chugunkov, and A. M. Plaksina, "Phishing Attacks and Protection against Them," *Proc. 2021 IEEE Conf. Russ. Young Res. Electr. Electron. Eng. ElConRus 2021*, pp. 425–428, 2021, doi: 10.1109/ElConRus51938.2021.9396693.

[4] M. Baz, H. Alhakami, A. Agrawal, A. Baz, and R. A. Khan, "Impact of covid-19 pandemic: A cybersecurity perspective," *Intell. Autom. Soft Comput.*, vol. 27, no. 3, pp. 641–652, 2021, doi: 10.32604/IASC.2021.015845.

[5] V. Valeros and S. Garcia, "Growth and Commoditization of Remote Access Trojans," *Proc. - 5th IEEE Eur. Symp. Secur. Priv. Work. Euro S PW 2020*, pp. 454–462, 2020, doi: 10.1109/EuroSPW51379.2020.00067.

[6] A. Sharma, P. Gupta, A. Professor, and A. Professor, "Covid 19 Pandemic: Impact on Business and Cyber Security Challenges," *J. Emerg. Technol. Innov. Res.*, vol. 7, no. 7, p. 52, 2020, [Online]. Available: www.jetir.org

[7] T. Pajar Setia, N. Widiyasono, and A. Putra Aldya, "Analysis Malware Flawed Ammyy RAT Dengan Metode Reverse Engineering," *J. Inform. J. Pengemb. IT*, vol. 3, no. 3, pp. 371–379, 2018, doi: 10.30591/jpit.v3i3.1019.

[8] S. Megira, A. R. Pangesti, and F. W. Wibowo, "Malware Analysis and Detection Using Reverse Engineering Technique," *J. Phys. Conf. Ser.*, vol. 1140, no. 1, 2018, doi: 10.1088/1742-6596/1140/1/012042.

[9] İ. Kara and M. Aydos, "the Ghost in the System: Technical Analysis of Remote Access Trojan," *Int. J. Inf. Technol. Secur. №*, vol. 1, no. January 2020, p. 2019, 2019.

[10] H. Agarwal, F. Husain, and P. Saini, *Ransomware Analysis Using Reverse Engineering*, vol. 1046, no. July. Springer Singapore, 2019. doi: 10.1007/978-981-13-9942-8.

[11] M. Hazri, "Analisis Malware PlasmaRAT dengan Metode Reverse Engineering," *J. Rekayasa Teknol. Inf.*, vol. 4, no. 2, 2020, [Online]. Available: http://e-journals.unmul.ac.id/index.php/INF/article/view/4131

[12] B. Akram and D. Ogi, "The Making of Indicator of Compromise using Malware Reverse Engineering Techniques," *7th Int. Conf. ICT Smart Soc. AIoT Smart Soc. ICISS 2020 - Proceeding*, pp. 11–16, 2020, doi: 10.1109/ICISS50791.2020.9307581.

[13] R. T. Amdani and M. Iqbal, "Analisis dan Deteksi Malware Poison Ivy Dengan Malware Analisis Dinamis dan Malware Analisis Statis," vol. 7, no. 2, pp. 178–191, 2021.

[14] A. Amiruddin, P. N. H. Suryani, S. D. Santoso, and M. Y. B. Setiadji, "Malware Analysis Model using Reverse Engineering Technique," *Sci. J. Informatics*, vol. 8, no. 2, pp. 222–229, 2021, doi: 10.15294/sji.v8i2.24755.

[15] W. Jiang, X. Wu, X. Cui, and C. Liu, "A highly efficient remote access Trojan detection method," *Int. J. Digit. Crime Forensics*, vol. 11, no. 4, pp. 1–13, 2019, doi: 10.4018/IJDCF.2019100101.

[16] A. P. Namanya, A. Cullen, I. U. Awan, and J. P. Disso, "The World of Malware: An Overview," *Proc. - 2018 IEEE 6th Int. Conf. Futur. Internet Things Cloud, FiCloud 2018*, pp. 420–427, 2018, doi: 10.1109/FiCloud.2018.00067.

[17] C. Aguado, C. Sanchez, D. Díaz López, and J. Garcia, "Using Reverse Engineering to Face Malware," *J. Eng. Educ.*, vol. 14, no. 21, pp. 107–121, 2019, [Online]. Available: https://drive.google.com/open?id=1tS5LgtluBp6pIK5PKAKAEcB35PEgZcdw

[18] R. Nurhidayati and Salauddin Muis, "Analysis Of Voice Data Security Security By Using The Rc4 Algorithm," *J. Info Sains Inform. dan Sains*, vol. 11, no. 2, pp. 22–28, 2021, doi: 10.54209/infosains.v11i2.44.

[19] J. Zhang, H. Liu, and L. Ni, "A Secure Energy-Saving Communication and

Encrypted Storage Model Based on RC4 for EHR," *IEEE Access*, vol. 8, pp. 38995–39012, 2020, doi: 10.1109/ACCESS.2020.2975208.

[20] S. M. Hameed, H. A. Sa'adoon, and M. Al-Ani, "Image encryption using DNA encoding and RC4 algorithm," *Iraqi J. Sci.*, vol. 59, no. 1B, pp. 434–446, 2018, doi: 10.24996/IJS.2018.59.1B.24.