JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 4, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v7i4.2301
Hal 505-510

Investigasi Serangan *Backdoor Remote Access Trojan* (RAT) Terhadap *Smartphone*

M. Alvian H Nasution*, Agung Tri Laksono

Fakultas Ilmu Komputer, Program Studi Teknik Komputer, Universitas Amikom Yogyakarta, Sleman, Indonesia
Email: [1,*]Alvian.nasution@students.amikom.ac.id, [2]Agung.1998@students.amikom.ac.id
Submitted 26-06-2020; Accepted 16-08-2020; Published 31-08-2020

Abstrak

Smartphone merupakan salah satu kebutuhan bagi setiap orang untuk saat ini, terutama dalam hal komunikasi dengan sesama, namun dengan perkembangan teknologi yang juga semakin canggih terkadang kita sebagai user tidak mengetahui terdapat tindak kejahatan ataupun serangan yang bisa terjadi kepada smartphone kita dan mengancam informasi pribadi atau data diri yang ada didalamnya, terutama para pengguna android, dimana pada perangkat android bisa dilakukan penyisipan sebuah malware dengan jenis RAT atau sering kita sebut dengan Remote Access Trojan yang sengaja dibuat dengan menggunakan tools ngrok yang mana RAT tersebut dapat dibuat menggunakan berbagai macam ekstensi file seperti .jpg, .Mp4, ataupun .apk seperti yang dilakukan dan akan dibahas pada jurnal ini. Pada jurnal ini juga akan dilakukan percobaan melakukan penanaman RAT pada sebuah target yatu smarthone android yang mana pada akihrnya akan didapatkan akses penuh dari smartphone tersebut hingga didapatkan akses penuh pada setiap direktori yang ada sesaat setelah dilakukan penginstalan dari RAT yang disembunyikan dalam file bentuk .apk, selain itu dengan pengujian ini diharapkan para pengguna smarphone terutama pengguna android untuk tidak melakukan root secara pribdai, karena dengan melakukan root pada device dapat membuka celah keamanan dari device yang kita gunakan dan akan lebih mudah untuk dilakukan penyerangan dari pihak yang tidak bertanggung jawab

Kata Kunci: RAT, Malware, Android, Smartphone, Informasi

Abstract

The Smartphone is one of the needs for everyone at this time, especially in terms of communication with others, but with the development of technology that is also increasingly sophisticated, sometimes we as users do not know there are crimes or attacks that can occur to our smartphone and threaten personal information or data self that is in it, especially android users, where on Android devices can be inserted a malware with the type of RAT or often we call the Remote Access Trojan which is deliberately made using ngrok tools, where the RAT can be made using various file extensions such as. jpg,. MP4, or .apk as was done and will be discussed in this journal. In this journal, an experiment will also be carried out planting RATs on a target, namely an android smartphone which will finally get full access from the smartphone to get full access to any directory that exists shortly after the installation of the RAT hidden in the .apk form file, besides that with this test it is expected that smartphone users, especially Android users, do not root privately, because by rooting the device can open a security hole of the device that we are using and it will be easier to attack from irresponsible parties.

Keywords: RAT, Malware, Android, Smartphone, Information

1. PENDAHULUAN

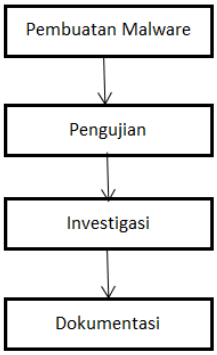
Dalam era teknologi seperti sekarang ini internet sudah menjadi hal yang lumrah, karena dapat membatu setiap kegiatan atau aktifitas setiap manusia. Sebagaimana sekarang ini semua dipermudahkan dengan internet, banyak komputer-komputer dan telepon genggam atau *smartphone* yang saling terhubung dengan menggunakan internet, internet banyak sekali manfaatnya bagi kehidupan manusia, namun dibalik banyaknya manfaatnya tersebut, internet juga dapat membawa malapetaka bagi penggunanya seperti penyebaran *malware* terhadap komputer atau *smartphone* melalui internet yang dimana *malware* ini dapat mengontrol *device* pengguna dan dapat melakukan pencurian data. *Malware* merupakan salah satu bentuk kejahatan pada sebuah jaringan komputer. *Backdoor* merupakan salah satu jenis virus *Trojan Horse* yang dimana virus ini dapat berkembang di dalam *device* yang terinfeksi kemudian memungkinkan *attacker* dapat memasuki sistem tanpa sepengetahuan pemiliknya.biasanya *malware* yang di install di dalam *backdoor* disebut dengan *Remote Access Trojan* (RAT) [1].

Pengguna *Trojan Horse* sekarang ini lebih ke arah kejahatan dunia maya (*cyber cryme)* , *malware* ini merupakan salah satu *malware* yang sangat berbahaya karena dampaknya sangat besar dan menimbulkan banyak kerugian. Seperti pencurian data dan penghubahan hak akses pada *device* korbannya[2]. Biasasnya *attacker* menyerang pada sistem operasi windows dan juga dapat menyerang pada *smartphone* atau android[3]. penyebaran *trojan horse* sendiri dengan mengandalkan kelemahan manusia atau dapat disebut dengan *sosial engineering* dengan kelemahan tersebut user tanpa curiga mengeksekusi sebuah program yang tidak dikenal yang dimana di dalam program tersebut telah disisipkan sebuah *malware* [4]. Aktivitas sebuah *malware* dapat mempengaruhi performa dari sebuah *device* yang dijalankan user dan dapat memperngaruhi sebuah jaringan komputer. Solusi untuk penanganan *malware* ini dengan menggunakan sebuah antivirus yang berbayar dan ter-update keunggulan anti virus yang terbaru dapat mendeteksi berbagai *malware*[5].

2. METODE PENELITIAN

Adapun metodologi yang digunakan dalam penelitian ini sebagai berikut:

JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 4, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v7i4.2301
Hal 505-510



Gambar 1. *Flowchart* penelitian

Metode *Dynamic* analisis *malware* adalah teknik melakukan analisa *malware* pada suatu sistem dan melihat aktivitas atau proses yang diaktifkan oleh *malware* tersebut. Pada metode ini sebuah *malware RAT* akan diperiksa dalam Virus Total yang telah disediakan sebagai laboratorium virtual *malware* untuk selanjutnya mampu dikumpulkan informasi-informasi mengenai efek terhadap *smartphone* ketika *file malware* dijalankan. Sehingga dapat diketahui kegiatan apa saja yang dilakukan oleh *malware* saat berhasil menginfeksi sebuah *smartphone*. Tahapan real nya , File *malware* akan di kirim kan ke sebuah *smartphone* yang telah disediakan untuk selanjutnya *malware* diuji ke sebuah *smartphone* yang masih aktif. Setelah itu efek dari *malware* akan mulai di investigasi, agar diketahui dampak yang terjadi jika sebuah *malware* RAT terinfeksi di sebuah *smartphone*, setelah proses investigasi selesai tahapan selanjutnya adalah dokumentasi dari hasil yang di dapat.

Malware merupakan perangkat lunak atau sebuah program komputer yang dibuat untuk tujuan tertentu seperti untuk mencari kelemahan sebuah *system/software*[6] . pada umumnya *malware* ini diciptakan untuk merusak dan membobol suatu *system/software* melalui program dan *script* yang disisipkan oleh pembuatnya[7].

Contoh-contoh *malware* sebagai berikut :

(1) Virus

Virus merupakan suatu jenis *malware* yang menyerang pada program yang berektensi (.exe)[8] biasanya virus ini memiliki kemampuan untuk mengganggu kinerja dari sistem komputer[9].

(2) *Worm*

Worm merupakan suatu jenis *malware* yang dapat menyebar melalui jaringan komputer kelebihan virus ini yaitu dapat memperbanyak jumlahnya dalam sebuah sistem komputer selain itu virus ini dapat merusak data dan file kemudian virus ini menyerang penyimpanan seperti memenuhi sebuah memory[10].

(3) *Trojan Horse*

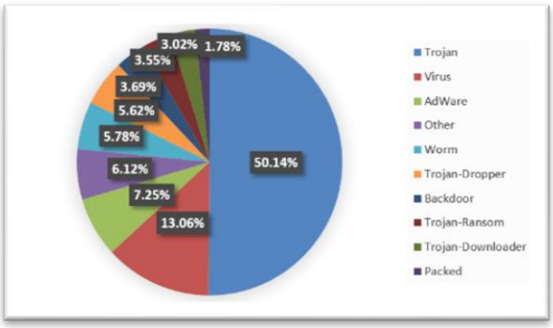
Trojan Horse merupakan suatu jenis *malware* yang menyerang pada sistem komputer biasanya trojan horse menyisipkan program-program yang jahat ke aplikasi-aplikasi yang lain misalnya menyisipkan virus, spyware,adware,keyloger dan *malware* lainnya untuk merusak dan mencuri data-data dan informasi seperti kartu kredit dan password[11].

(4) Spyware

Sypware merupakan suatu jenis *malware* yang yang bertugas untuk memata-matai kebiasaan pengguna komputer. Biasanya spyware ditemukan di pemasangan iklan seperti pop up yang ada di website.

(5) Backdoor

Backdoor merupakan suatu program yang dirancang untuk melewati authentifikasi normal (login) bisa juga disebut dengan mengakses dari pintu belakang dengan secara tidak sah, ketika *backdoor* ini sudah masuk kedalam sistem maka sangat mudah untuk mengambil alih komputer yang telah berhasil di susupi oleh backdoor ini.



Gambar 2. Data Statistik Serangan *Malware*

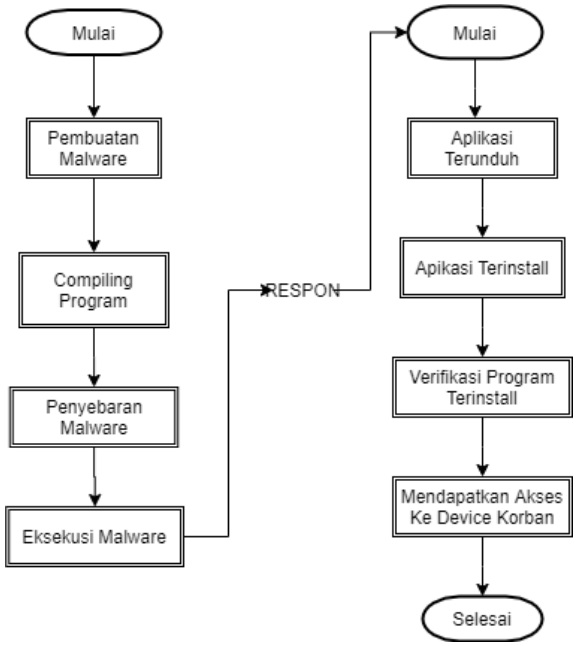
Dari data statistic pada gambar 1 virus Trojan yang unggul denggan menguasai 50.14%. dan setelah trojan virus dengan jumlah 13.06% . selajutnya diikuti dengan virus worm,backdoor yang dimana dapat dilihat di gambar no 1 diatas.

Remote Access Trojan (RAT) digunakan untuk melakukan akses jarak jauh dengan aspek dan kemampuannya mengontrol *devices* yang telah terinfeksi oleh *malware* yang telah di sisipkan backdoor sehinggan *attacker* dapat melakukan authentifikasi terhadap perangkat yang digunakan oleh korban.

JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 4, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v7i4.2301
Hal 505-510

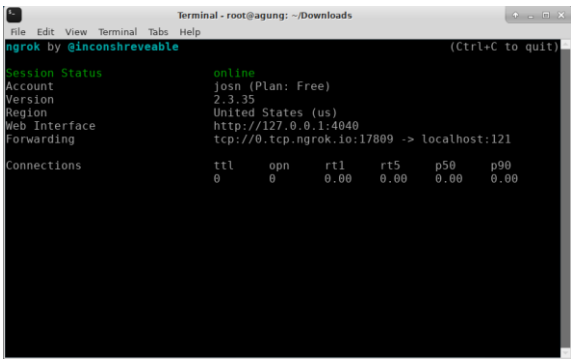
3. HASIL DAN PEMBAHASAN

Pada bagian pembahasan akan dijelaskan *flowchart* tentang alur yang akan dilakukan oleh *attacker* guna mendapatkan akses dari *device* target, dimana pada *flowchart* dibawah ini tergambar alur pembuatan serta respon yang akan didapatkan dalam proses serangan dengan *malware* yang akan di sisipkan dalam sebuah format file .apk yang sengaja di kirim melalui jejaring sosial untuk di install.



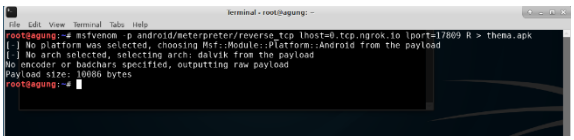
Gambar 3. *Flowchart* Responder

Pada *flowchart* diatas tergambar jelas bahwa alur yang ada sengaja dibuat untuk mendapatkan akses penuh dari *device* target yang menjadi sasaran, alur tersebut meliputi pembuatan *malware* hingga proses verifikasi dari program yang sudah berjalan dan bisa mendapatkan timbal balik dari program yang dikirim. Pembuatan dari program tersebut adalah dengan menggunakan tools bernama ngrok dan Metasploit dimana ngrok berguna untuk melakukan Metasploit pada *device* yang berbeda jaringan. Berikut adalah tampilan ngrok pada saat pembuatan *malware*



Gambar 4. Tampilan ngrok

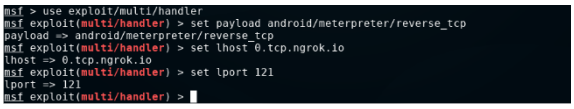
Tahap selanjutnya cara pembuatan program dengan menginputkan aplikas untuk di compile. berikut adalah proses tahan compiling program menggunakan msfvenom.



Gambar 5. Konfigurasi MSFvenom

Tahap selanjutnya kita akan melakukan setting LHOST dan LPORT dimana berfungsi supaya aplikasi yang telah dibuat dapat terhubung ke tools ngrok jadi dapat digunakan secara online. Beriku adalah tahap penambahan LHOST dan LPORT.

JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 4, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v7i4.2301
Hal 505-510

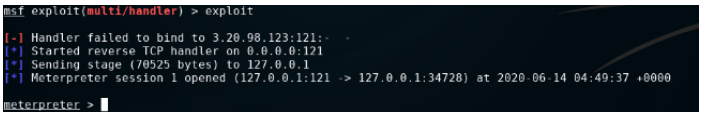


Gambar 6. Konfigurasi Metasploit

Tahap selanjutnya yaitu cara penyebaran virus dengan menggunakan platform WhatsApp , dimana *attacker* mengirimkan pesan singkat berupa ajakan dengan melampirkan apk (aplikasi) yang diberi nama thema.apk guna membujuk korban untuk melakukan installasi terhadap apk tersebut seperti pada gambar di bawah ini

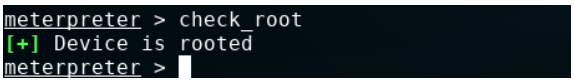
Gambar 7. Penyebaran *malware*

Tahap selanjutnya yaitu verifikasi program terinstall dengan menggunakan msf exploit dimana nantinya proses ini berfungsi untuk mendapatkan balasan dari aplikasi yang sudah terinstall sehingga mendapatkan session ID. Berikut adalah tahap verifikasi program terinstall.



Gambar 8. Proses exploit

Tahap selanjutnya yaitu mendapatkan akses kepada *device* korban dimana cara melakukan test terhadap akses dengan melakukan check_*root* pada bagian meterpreter, apabila sudah mendapatkan akses akan muncul respon berupa kalimat "*Device is rooted*". Seperti pada gambar dibawah ini



Gambar 9. Cek informasi *device*

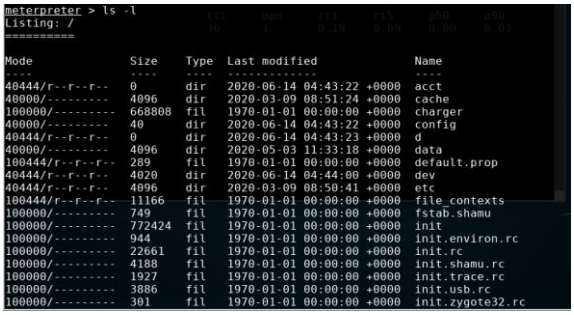
Setelah mendapatkan akses terhadap *device* kita akan melakukan pengecekan informasi yang terdapat pada *device* dengan menginputkan perintah "*sysinfo*" seperti pada gambar dibawah ini

Gambar 10. Cek informasi *device*

Selanjutnya kita akan melakukan pengambilan akses *device* secara penuh dengan masuk ke *system root* pada *device*. Seperti pada gambar dibawah.

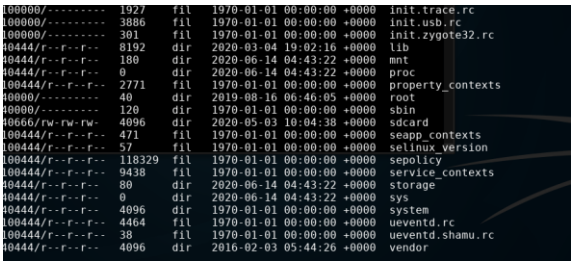
Gambar 11. Cek informasi *device*

Selanjutnya setelah mendapatkan akses *root* kita melakukan cek direktori dengan menginputkan perintah ls -l dimana hasil dari perintah tersebut menandakan bahwa kita dapat mengakses seluruh daftar list direktori yang ada dimana list direktori dari target adalah seperti gambar dibawah ini



Gambar 12. Cek informasi *device*

JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 4, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v7i4.2301
Hal 505-510

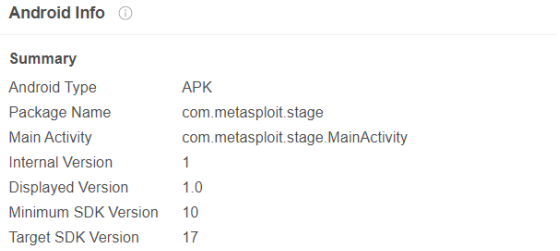


Gambar 13. Cek informasi *device*

Selanjutnya akan dilakukan analisis *malware* secara *dynamic* dengan bantuan website virustotal dimana nantinya kita akan mencoba melakukan analisis terhadap malwar RAT yang sudah dibuat.

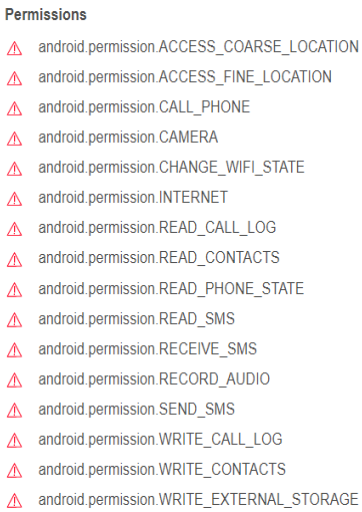
Gambar 14. Analisis *malware*

Pada gambar diatas terdapat bagian dasar dari *malware* yang dibuat dimana pada bagian tersebut mencangkup keaslian file berupa MD5,SHA-1,SHA 250, vhash, SSDEEP, selain itu terdapat juga file type sasaran yaitu Android, file magic dimana file tersebut bertujuan untuk mengubah extensi php menjadi .apk untuk android serta terdapat juga informasi berupa ukuran dari *malware* sebesar 9.85 KB (10086 bytes)



Gambar 15. Analisis *malware*

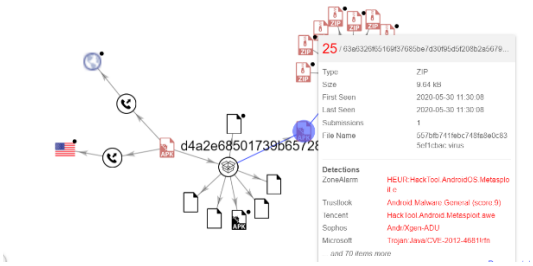
Pada gambar diatas didapatkan informasi berupa ringkasan dari *malware* tersebut berupa android type, package name, main activity, internal version, displayed version, minimum SDK version, target SDK version. Dimana informasi yang didapat mencangkup target sasaran yaitu android.



Gambar 16. Analisis *malware*

Pada gambar diatas terdapat informasi berupa akses yang didapatkan oleh *malware* dari serangan terhadap target diantaranya *malware* dapat melakukan akses terhadap kamera, membaca kontak korban, membaca SMS, Menerima SMS, Mengirim SMS, *Record* audio, dan Membaca log panggilan.

JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 4, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v7i4.2301
Hal 505-510



Gambar 17. Analisis *malware*

Selanjutnya kita akan melihat relasi dari file RAT yang telah dibuat, pada gambar diatas dapat dilihat bahwa relasi dari file RAT yang ada mengandung beberapa *engine* yang membahayakan *system* android seperti android OS Hack Tool Android OS.Metasploit.e dimana *engine* tersebut bertujuan untuk melakukan *exploit* terhadap target

4. KESIMPULAN

Setelah dilakukan pembahasan pada jurnal diatas didapatkan kesimpulan bahwa serangan RAT dapat terjadi dan menyerang *system* dari sebuah android dimana pada serangan RAT *attacker* dapat melakukan akses terhadap *system* secara penuh oleh karena itu sebagai user sebaiknya kita melakukan tindak preventif/pencegahan terhadap pengunduhan maupun installasi terhadap aplikasi yang dikirim/didapatkan dari pihak yang tidak diketahui kredibilitasnya. Selain itu melakukan pengamanan terhadap *device* yang digunakan dengan tidak melakukan *root* secara tidak sah dimana dengan melakukan *root* terhadap *device* membuka celah keamanan dari *device* untuk dilakukan serangan dari pihak ketiga.

REFERENCES

[1] D. R. Septiani, N. Widiyasono, and H. Mubarok, "Investigasi Serangan *Malware* Njrat Pada PC," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 2, pp. 123–128, 2016, doi: 10.26418/jp.v2i2.16736.

[2] R. Novrianda, Y. N. Kunang, and P. . Shaksono, "Analisis Forensik Pada Platform Android," *Konf. Nas. ilmu Komput.*, pp. 141–148, 2014.

[3] A. Kartono, A. Sularsa, and S. J. I. Ismail, "Membangun Sistem Pengujian Keamanan Aplikasi Android Menggunakan Mobsf," vol. 5, no. 1, pp. 146–151, 2019.

[4] N. Setiawan, "Kasus kejahatan siber pada telepon seluler android," *CyberSecurity dan Forensik Digit.*, vol. 2, no. 1, pp. 24–29, 2019.

[5] Y. A. Utomo *et al.*, "Membangun Sistem Analisis *Malware* Pada Aplikasi Android Dengan Metode Reverse Engineering Menggunakan Remnux," vol. 4, no. 3, pp. 2000–2012, 2018.

[6] H. Abualola, H. Alhawai, M. Kadadha, H. Otrok, and A. Mourad, "An Android-based Trojan Spyware to Study the NotificationListener Service Vulnerability," *Procedia Computer Science*, vol. 83. pp. 465–471, 2016, doi: 10.1016/j.procs.2016.04.210.

[7] A. S. Rusdi, N. Widiyasono, and H. Sulastri, "Analisis Infeksi *Malware* Pada Perangkat Android Dengan Metode Hybrid Analysis," no. 24, 2019.

[8] W. C. Hsieh, C. C. Wu, and Y. W. Kao, "A study of android *malware* detection technology evolution," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2015-January, pp. 135–140, 2016, doi: 10.1109/CCST.2015.7389671.

[9] T. A. Cahyanto, V. Wahanggara, and D. Ramadana, "Analisis dan Deteksi *Malware* Menggunakan Metode *Malware* Analisis Dinamis dan *Malware* Analisis Statis," *Justindo, J. Sist. Teknol. Inf. Indones.*, vol. 2, no. 1, pp. 19–30, 2017.

[10] E. J. Victorius, A. Budiyono, A. Almaarif, and S. Kom, "Analisis Deteksi *Malware Remote Access Trojan* Menggunakan *Dynamic Malware* Analysis Detection Tools Berbasis Behaviour *Malware* Detection Analysis of *Remote Access Trojan* With Behaviour-Based *Dynamic Malware* Analysis Detection Tools," vol. 6, no. 2, pp. 7804–7811, 2019.

[11] A. F. Muhtadi and A. Almaarif, "Analysis of *Malware* Impact on Network Traffic using Behavior-based Detection Technique," *Int. J. Adv. Data Inf. Syst.*, vol. 1, no. 1, pp. 17–25, 2020, doi: 10.25008/ijadis.v1i1.14.