ANALISIS VIDEO VLC PLAYER YANG TERINFEKSI MALWAREl

SKRIPSI

Disusun oleh:

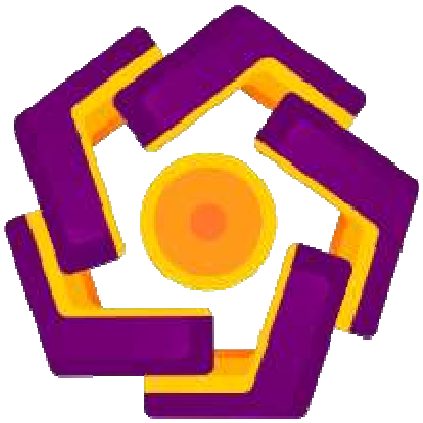
Ridho Utomo
17.83.0011

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

ANALISIS VIDEO VLC PLAYER YANG TERINFEKSI MALWARE

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:

Ridho Utomo
17.83.0011

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

PERSETUJUAN

SKRIPSI

ANALISIS VIDEO VLC PLAYER YANG TERINFEKSI MALWARE

yang dipersiapkan dan disusun oleh

Ridho Utomo

17.83.0011

telah disetujuai oleh Dosen Pembimbing Skripsi
pada tanggal 22 Juni 2021

Dosen Pembimbing,

Melwin Syafrizal, S.Kom., M.Eng.
NIK. 190302105

PENGESAHAN

SKRIPSI

ANALISIS VIDEO VLC PLAYER YANG TERINFEKSI MALWARE

yang dipersiapkan dan disusun oleh
Ridho Utomo

17.83.0011

telah dipertahankan di depan Dewan Penguji
pada tanggal 22 juni 2021

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Mulia Sulistiyono, M.Kom **NIK. 190302248**	
Dony Ariyus, M.Kom **NIK. 190302128**	
Melwin Syafrizal, S.Kom., M.Eng. **NIK. 190302105**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Juni 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.kom
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama : Ridho Utomo
NIM : 17.83.0011

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS VIDEO VLC PLAYER YANG TERINFEKSI MALWARE

Dosen Pembimbing : Melwin Syafrizal, S.Kom., M.Eng...

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, 22 Juni 2021

Yang Menyatakan,

Ridho Utomo

NIM. 17.83.0011

MOTTO

“Kesetiaan mereka akan terlihat di saat kamu tidak memiliki apa-apa dan menjadi bukan siapa-siapa

only your mother will always be with you ”

(**Ridho Utomo**)

PERSEMBAHAN

Segala puji bagi Allah SWT atas limpahan rahmat dan hidayah serta karunia-Nya sehingga skripsi ini selesai dengan sebaik-baiknya. Skripsi ini saya persembahkan untuk :

1. Kedua orang tua, Bapak Trisno Utomo dan Ibu Saminah Puji Lestari yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak Melwin Syafrizal, S.Kom., M.Eng.,. Selaku dosen pembimbing yang telah membantu dalam penyusunan skripsi ini.
3. Kepada Adik saya Naisya damayanti yang selalu memberikan semangat dan dukungan.
4. Kepada sahabat dan teman-teman yang ada disaat suka maupun duka selama masa perkuliahan saya.
5. Sesorang yang sangat berharga dan selalu memberikan saya semangat, Arliyanti Arifin. Trimakasih atas semuanya.

KATA PENGANTAR

Puji dan syukur dipanjatkan kehadirat Tuhan Yang Maha Esa atas karunia yang telah dianugerahkan kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Video Vlc Player Yang Terinfeksi Malware".

Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, skripsi ini tidak mungkin dapat terselesaikan. Oleh karena itu, penulis menyampaikan terima kasih kepada :

1. Allah SWT karena atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan mamfaat di kemudian hari.
2. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
3. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
4. Bapak Melwin Syafrizal, S.Kom., M.Eng.,. selaku Dosen Pembimbing yang telah bersedia memberikan pengarahan dan bimbingan dalam penyususnan Skripsi ini.
5. Segenap Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis di bangku kuliah dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.
6. Orang tua, saudara-saudara beserta keluarga yang selalu mendoakan dan memberikan dukungan penuh kepada penulis.
7. Serta kepada semua pihak yang telah membantu dalam penyusunan Skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Penulis berharap semoga skripsi ini dapat bermamfaat bagi semua pihak yang terkait dalam penulisan ini. Dalam penulisan skripsi ini penulis menyadari masih banyak kekurangan karena terbatasnya pengetahuan dan pengalaman penulis. Karena itu, dengan lapang hati penulis mengharapkan kritik dan saran yang membangun guna menyempurnakan skripsi ini.

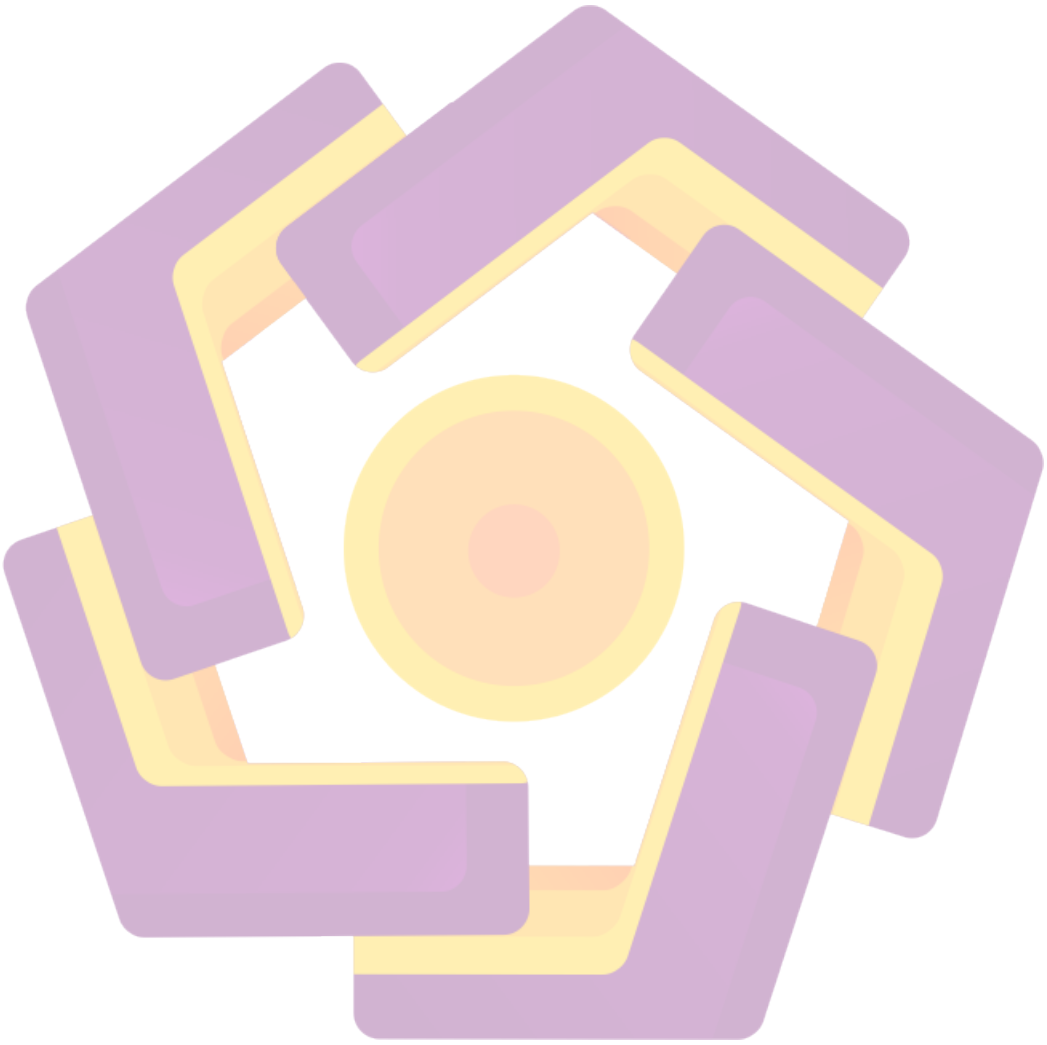
Yogyakarta, 22 juni 2021

Ridho Utomo

DAFTAR ISI

DAFTAR TABLE

DAFTAR GAMBAR



INTISARI

Malware yang ada saat ini sangat beragam dan berkembang dengan cepat, karena itu di butuhkan keahlian khusus untuk menganalisis malware. *VLC* Media player di buat untuk pemutar beragam file multimedia, baik video maupun audio dalam berbagai format, seperti *MPEG, DivX, Ogg*, *MKV,* dan lain-lain. Keamanan siber Jerman *CERT-Bund* metemukan celah kerentan terhatap *VLC* player yang dapat disisipkan malware dalam video yang berformat MKV, sehingga kerentanan terhadap *VLC* player di manfaatkan oleh hacker dengan cara membuat kode-kode yang nantinya akan di sisipkan di video yang berformat *MKV*. Sehingga video yang terinfeksi virus akan melakukan infeksi pada *VLC* player untuk menyerang windows korban

Untuk mengetahui bagaimana video ini bisa terinjeksi dan menyerang windows dengan memanfaatkan kerentan terhadap pemutar video *VLC* maka di perlukannya analisis. Analisis dilakukan dengan cara implementasi penyusupan malware terhadap file video yang nantinya akan di buka dengan *VLC* player. Penyusupan malware akan di lakukan dengan menggunakan msfconsole pada linux. Selanjutnya akan di lakukan analisis *dynamic* dengan melakukan analisa video yang sudah terinjeksi malware dengan *REMnux*, danmelihat aktivitas atau proses yang diaktifkan oleh malware tersebut dengan menggunakan tools *Prosess Explorer.*

Penelitian ini akan melakukan analisa terhadap file MKV yang terinfeksi malware dan menyerang kerentanan terhadap VLC player dengan menggunakan metode dynamic analisis. Hasil dari analisis pada file MKV ini di temukannya enkripsi pada malware trojan yang disisipkan ke video mkv setelah analis yang di lakukan dengan REMnux, namun setelah melakukan analisis dengan menggunakan Prosess Explorerr di temukannya aplikasi *werFault.exe, cmd.exe, vlc.exe dan conhost.exe* yang berjalan di belakang layer malware video mkv ini, dan di temukannya string stiting yang mencurigakan terhadap malware dan aplikasi yang berjalan di balik layer tersebut.

Kata kunci: *Malware, Video, Mkv, Vlc Player, Dynamic analiysis*

ABSTRACT

Malware is currently diverse and growing rapidly, because it requires special expertise to analyze malware. VLC Media player is made for playing various multimedia files, both video and audio in various formats, such as MPEG, DivX, Ogg, MKV, and others. The German cyber security CERT-Bund found vulnerabilities in the VLC player, which was inserted by malware in the MKV format video, so that hackers exploited the vulnerability to the VLC player by creating codes that would later be inserted in the MKV format video. So that a virus-infected video will infect the VLC player to attack the victim's windows

To find out how this video can be injected and attack windows by utilizing the vulnerability of the VLC video player, analysis is needed. The analysis was carried out by implementing malware infiltration of video files which will later be opened with the VLC player. Malware infiltration will be done using msfconsole on linux. Furthermore, dynamic analysis will be carried out by analyzing videos that have been injected with malware with REMnux, and seeing the activities or processes that are activated by the malware using the Process Explorer tool.

This research will analyze MKV files that are infected with malware and attack the vulnerability to VLC player using dynamic analysis method. The results of the analysis on this MKV file found encryption in trojan malware that was inserted into the mkv video after the analysis was carried out with REMnux, but after analyzing using Process Explorerr, werFault.exe, cmd.exe, vlc.exe and conhost applications were found. .exe running behind this mkv video malware layer, and finding suspicious stiting strings against malware and applications running behind the layer.

Keyword: *Malware, Video, Mkv, Vlc Player, Dynamic analiysis*