

**ANALISIS VIDEO VLC PLAYER YANG TERINFEKSI
MALWAREI**

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 disetujui 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 Syarifzal, 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 dibubuhkan 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, 23 Juni 2021

Yang Menyatakan,



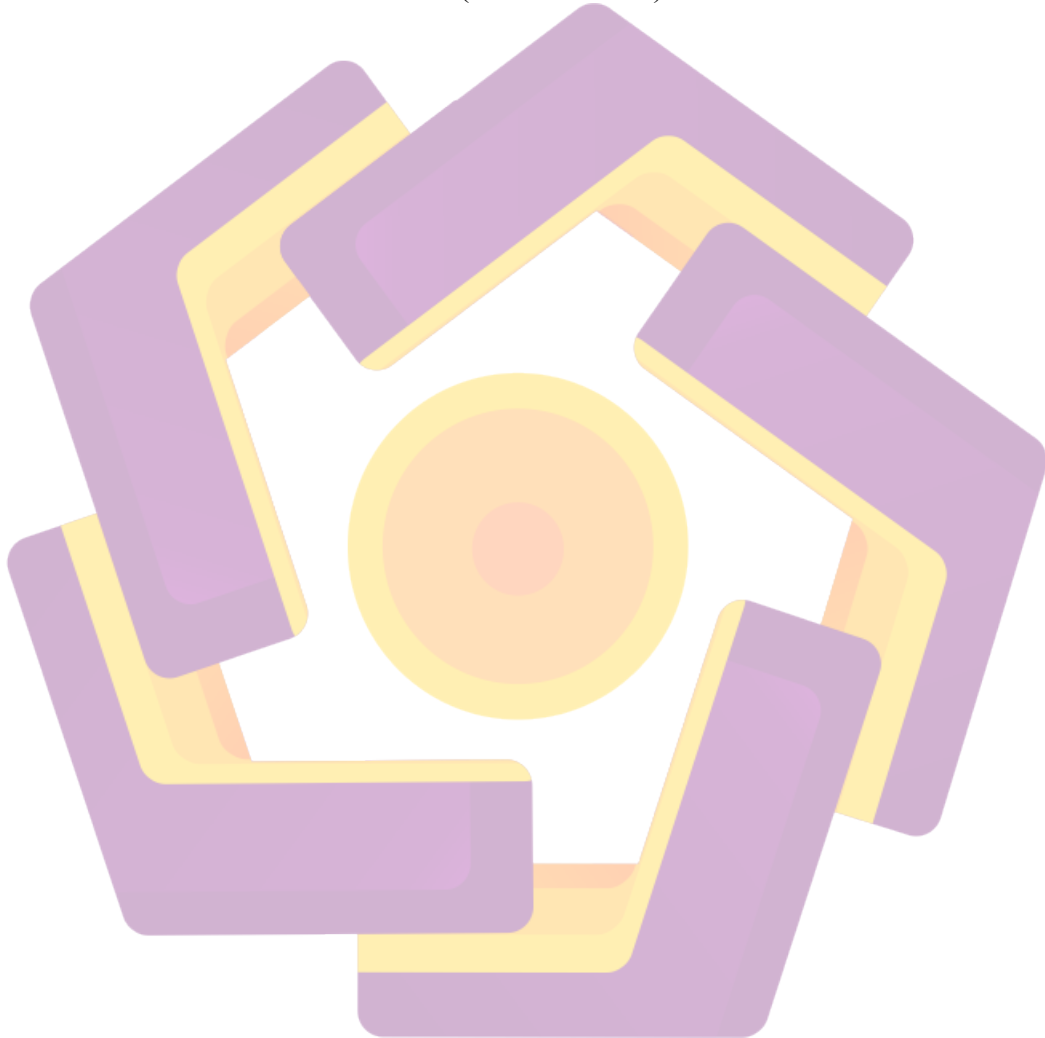
Ridho Utomo
NIM. 17.83.0011

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 ”

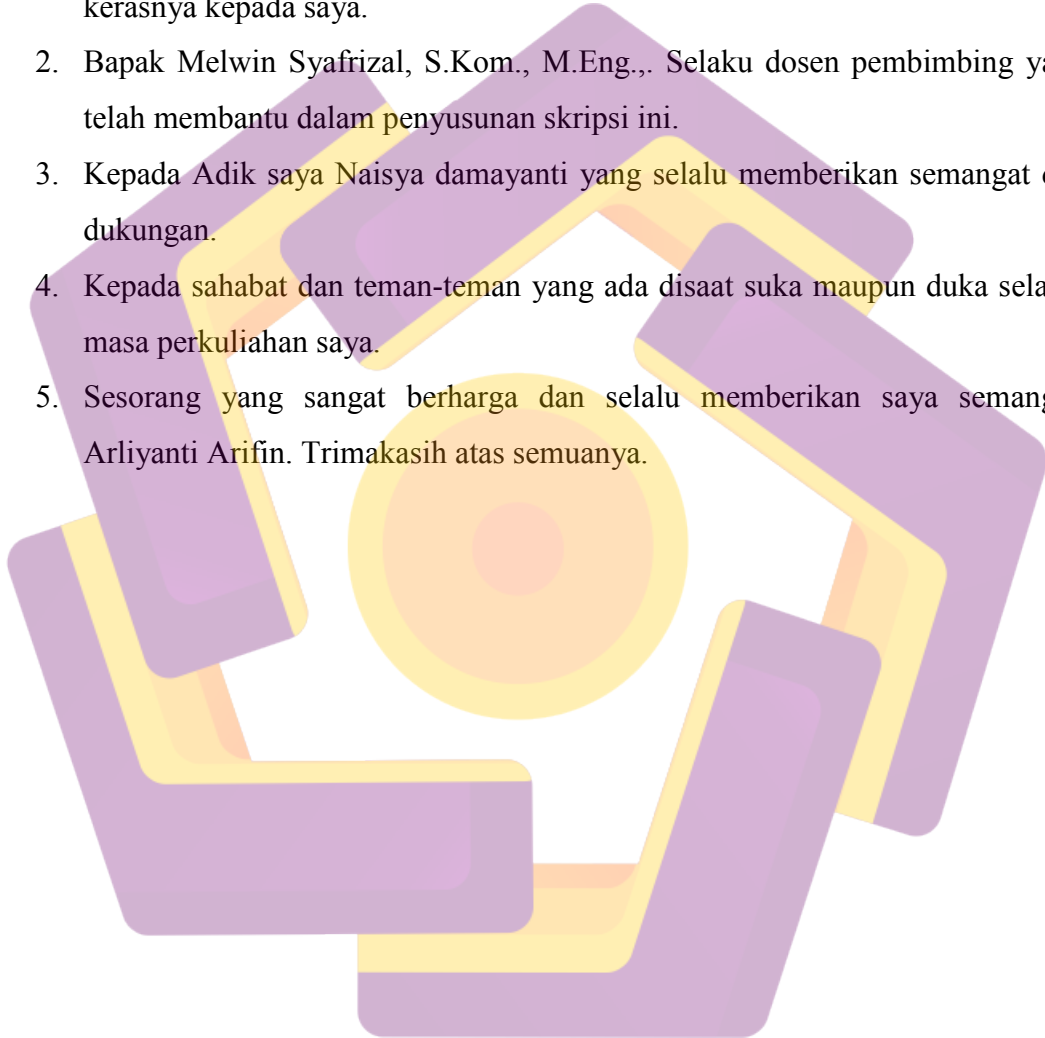
(Ridho Utomo)



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.

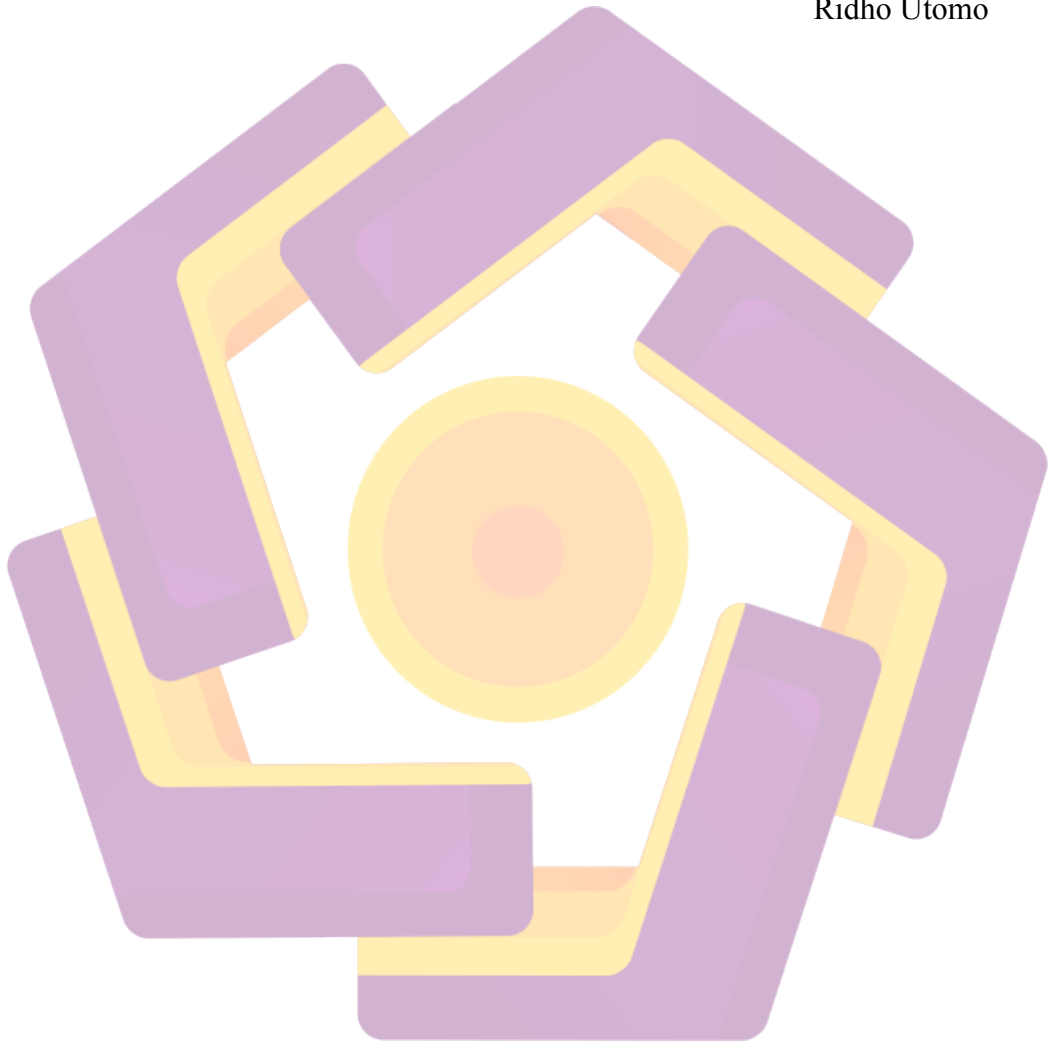
Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, skripsi ini tidak mungkin dapat terselesaikan. Oleh karena itu, penulis menyampaikan terima kasih kepada :

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 penyusunan 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

PERSETUJUAN	iii
PENGESAHAN	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	v
MOTTO	vi
PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR TABLE	xiii
DAFTAR GAMBAR	xiv
INTISARI.....	xvi
<i>ABSTRACT</i>	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	1
1.3 Batasan Masalah	1
1.4 Tujuan Penelitian	2
1.5 Metode penelitian.....	2
1.6 Sistematika Penulisan	3
BAB II.....	4
LANDASAN TEORI	4
2.1 Tinjauan Pustaka	4
2.2 Malware.....	7
2.3 Jenis Malware.....	7
2.3.1 Virus.....	7
2.3.2 Ransomware.....	7
2.3.3 Malicious Cryptominers.....	8
2.3.4 Rootkit.....	8
2.3.5 Worm	8
2.3.6 Spyware.....	8
2.3.7 Trojan	9
2.3.8 Adware	9
2.3.9 Keylogger.....	9
2.3.10 Backdoor	9

2.4	Perkembangan Teknik Kamufase Malware	10
2.4.1	Primitive Malware.....	10
2.4.2	Encrypted Malware	10
2.4.3	Oligomorfisme	11
2.4.4	Polimorfisme.....	12
2.4.5	Metamorfis	13
2.5	File MKV.....	13
2.6	Virtual Machine.....	14
2.7	Kali Linux.....	14
2.8	MSFconsole.....	14
2.9	Payload	15
2.10	Analisis dinamis	16
2.11	Cmd	16
2.12	Process Explorer.....	17
2.13	RENmux	17
2.14	String Analysis	17
2.15	Exploit	17
BAB III	18
METODOLOGI PENELITIAN	18
3.1	Gambaran Umum Penelitian	18
3.2	Analisis dengan Remnux.....	20
3.3	Analisis Dinamis	21
3.4.1	Perangkat Keras (<i>Hardware</i>)	22
3.4.2	Perangkat Lunak.....	22
3.4.3	Software Aplikasi Lain	24
BAB IV	25
PEMBAHASAN	25
4.1	Pembuatan Video malware yang akan di jadikan sample .	25
4.2.1	Proses Analisis Dengan Remnux	28
4.3	Proses Analisis Dinamis.....	32
4.3.1	Running Malware.....	32
4.3.2	Analisis Netstat	35
4.3.3	Analisis dengan <i>Process Explorer</i>	38
4.3.4	Analisis String dengan <i>Process Explorer</i>	41
4.4	Pencegahan Malware Yang sudah berjalan.....	47
4.5	Uji coba dengan anti virus.....	49
BAB V	51
PENUTUP	51
5.1	Kesimpulan	51

5.2 Saran.....	52
DAFTAR PUSTAKA	54



DAFTAR TABLE

Tabel 2. 1 Penelitian yang terkait.....	5
Table 3.2 Spesifikasi Hardware	22
Tabel 3. 3 Spesifikasi Virtual Enviroment Kali Linux	22
Table 3.4 Spesifikasi <i>Virtual Enviroment</i> Windows 10.....	23
Table 3.5 Spesifikasi Virtual Enviroment REMNux	23
Table 3.6 Tools pendukung penelitian.....	24
Tabel 4.1 Merubah target	27
Tabel 4.2 File Attribute Analysis	29
Tabel 4.3 Hasil <i>Fuzzy Hashing</i>	30
Tabel 4.4 <i>Opsi</i> tambahan.....	34
Tabel 4.5 Keterangan options	36
Tabel 4.6 hasil dari netstat-ano	37
Tabel 4.7 Proses explorer setelah video di buka.....	39
Talel 4.8 Informasi aplikasi yang berjalan di <i>background</i>	40
Tabel 4.9 Parent yang terhubung langsung dengna malware.....	41
Tabel 4.10 Contoh Internal DOS	41
Tabel 4.11 Contoh external Dos.....	42
Tabel 4.12 Keterangan string malware cmd.exe.....	44
Tabel 4.13 Keterangan <i>string</i> malware <i>werfault.exe</i>	45
Tabel 4.14 Keterangan string malware vlc.exe.....	46

DAFTAR GAMBAR

Gambar 2. 1 Struktur dari virus terenkripsi [23].....	11
Gambar 2.2 Bentuk dan cara kerja dari oligomorphic[24]	12
Gambar 2.3 Struktur dan cara kerja <i>poliformisme</i> [24]	12
Gambar 2.4 Struktur dan cara kerja metamorfisme [24].....	13
Gambar 3.1 Diagram Alur Penelitian.....	19
Gambar 3.2 Proses analisis dengan Remnux	20
Gambar 3.3 Proses analisis dinamis.....	21
Gambar 4.1 <i>Msfconsole</i>	25
Gambar 4.2 <i>search mkv</i>	26
Gambar 4.3 <i>use exploit/windows/fileformat/vlc_mkv</i>	26
Gambar 4.4 perintah <i>Show options</i>	26
Gambar 4.5 <i>Cek show options</i> yang telah berhasil di set.....	27
Gambar 4.6 Perintah <i>run</i>	28
Gambar 4.7 Perintah <i>md5sum</i>	28
Gambar 4.8 Perintah <i>ssdeep</i>	28
Gambar 4.9 Menjalankan <i>hex</i>	29
Gambar 4.10 <i>Hasing</i> pada linux.....	30
Gambar 4.11 <i>Hasing</i> pada <i>remnux</i>	30
Gambar 4.12 <i>Hasing</i> windows 10.....	30
Gambar 4.13 analisa string otomatis.....	31
Gambar 4.14 Analisa <i>string</i> manual.....	32
Gambar 4.15 Skema Jaringan	33
Gambar 4.16 <i>Msfconsole</i>	33
Gambar 4.17 Use multi/handler	33
Gambar 4.18 <i>Set payload</i>	33
Gambar 4.17 <i>Show options</i>	34
Gambar 4.19 <i>Show options</i> sesudah di set.....	34
Gambar 4.20 <i>run</i>	34
Gambar 4.21 membuka malware <i>ridhomalware.mkv</i>	35
Gambar 4.22 Menjalankan <i>exploit</i>	35
Gambar 4.23 <i>netstat</i>	36
Gambar 4.24 <i>netstat -ano</i>	37
Gambar 4.25 Ilustrasi topologi jaringan.....	38
Gambar 4.26 Jalankan Program Proses Explorer.....	38
Gambar 4.27 proses yang berjalan di process explorer.....	38
Gambar 4.28 Properties aplikasi yang berjalan di balik layer	39
Gambar 4.29 Perintah <i>ping 192.168.56.10 -t</i>	43
Gambar 4.29 <i>string cmd.exe</i>	44
Gambar 4.30 <i>string WerFault.exe</i>	45
Gambar 4.31 <i>string vlc.exe</i>	46

Gambar 4.32 String perintah attacker	47
Gambar 4.33 netstat sessions 1	47
Gambar 4.44 Proses explorer search	48
Gambar 4.45 kill process.....	48
Gambar 4.46 session 1 close	49
Gambar 4.47 smart scanning.....	49
Gambar 4.48 Berjalannya malware ridhoutomo.mkv	50



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* menemukan celah kerentan terhadap *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*, dan melihat aktivitas atau proses yang diaktifkan oleh malware tersebut dengan menggunakan tools *Process 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 *Process Explorer* 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 analisis*

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 Explorer, 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*