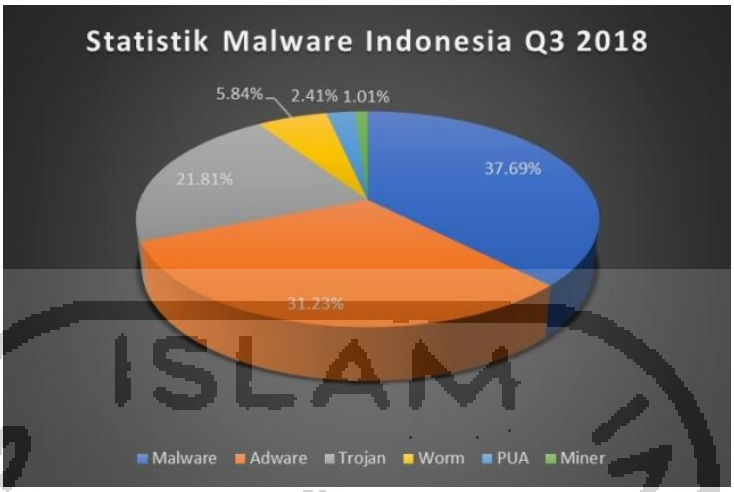
BAB 1
Pendahuluan

1.1 Latar Belakang

Teknologi memberikan tantangan dan menjadi ancaman bagi pengguna internet di dunia maya. Tingginya penyebaran internet menciptakan kejahatan tak hanya terjadi dalam dunia nyata, tetapi merambah ke dunia maya yang sering disebut sebagai *cyber crime*. Saat ini kejahatan di dunia maya antara *cybercrime* makin banyak jumlahnya, makin canggih modusnya, makin bervariasi karakteristik pelakunya dan makin serius akibatnya. Secara krimonologis, setiap kejahatan merupakan fenomena masyarakat (*social phenomenon*), karena eskalasi kerugian *cybercrime* bersifat global dan aktivitas pelakunya lintas-negara, maka *cybercrime* dianggap sebagai fenomena global. Secara sederhana, setiap kejahatan yang dilakukan mengarah pada *system computer* maupun menggunakan computer sebagai sarana melakukan kejahatan disebut *cybercrime* atau *computer-related crime*. Kejahatan tersebut tidak menggunakan kekerasan fisik. Hukum pidana yang mengatur kejahatan (tindak pidana) di dunia maya dikenal dengan istilah *cybercrime law*, dan jenis kejahatannya disebut *cybercrime*, pelakunya disebut *cybercriminal*. (Chandra, Hutauruk, Yulianto, & Satrya, 2016)

Cybercriminal adalah pelaku kejahatan di bidang teknologi informasi (*cybercrime*), baik pelaku secara langsung maupun pelaku yang turut serta melakukan *cybercrime*, ada atau tidaknya pelaku secara tidak langsung ditentukan oleh bentuk tindak pidana, karena didalamnya terkandung siapa saja yang dapat dipertanggungjawabkan secara pidana. Banyak cara yang dilakukan untuk mempermudah kegiatan kejahatan yang melibatkan teknologi komputer ini salah satunya adalah memanfaatkan kelemahan sistem jaringan komputer dengan menyusupkan program yang digunakan sebagai media untuk mencuri informasi dari sebuah sistem komputer, program ini disebut sebagai *malware*. *Malware* didefinisikan sebagai semua perangkat lunak jahat, program komputer jahat, atau perangkat lunak jahat, seperti virus (komputer), *trojans*, *spyware*, dan *worm*. (Septiani, Widiyasono, & Mubarok, 2017)

Berikut data statistik serangan *malware* dipaparkan dalam Gambar 1.1 :



Gambar 1.1 Grafik Serangan Malware

(*Sumber : Vaksin.com*)

Berdasarkan grafik statistik di atas menunjukkan bahwa tahun ke tahun *malware* mengalami peningkatan secara signifikan, salah satunya *malware Trojan Horse* yang banyak menyerang melalui windows, maka tentunya perlu adanya peningkatan keamanan data di komputer/laptop masing-masing. Salah satu serangan *malware trojan* yang berbahaya adalah serangan *Remote Access Trojan (RAT).*

Remote Access Trojan (RAT) adalah program *malware* yang mencakup pintu belakang (*backdoor*) untuk kontrol administratif atas komputer target. Pintu belakang yang dimaksud adalah berupa *port*. Apabila sang pembuat *backdoor* datang, maka *backdoor* akan membukakan pintu lalu mempersilahkan masuk dan melindunginya dari pengawasan keamanan, tentu setelah itu *hacker* dapat melakukan apa saja yang diinginkan dengan leluasa pada Laptop target. *Backdoor* merupakan metode yang digunakan untuk melewati autetifikasi normal *(login)* dan berusaha tidak terdeteksi. Dengan adanya *backdoor*, maka akan tercipta jalan masuk bagi seorang *hacker* yang seharusnya tidak memiliki hak masuk. Apabila seseorang yang tidak bertanggung jawab dapat masuk kedalam sistem, maka rang tersebut akan dapat melakukan pencurian terhadap informasi yang ada di dalam Laptop korban. RAT biasanya diunduh tanpa terlihat dengan program yang diminta pengguna, seperti permainan atau dikirim sebagai lampiran email, melalui USB dan *file sharing*. Setelah sistem *host* dikompromikan, penyusup dapat

menggunakannya untuk mendistribusikan RAT ke komputer lainnya yang rentan dan membuat *botnet*. *Botnet* adalah *malware* yang dapat melakukan serangan terhadap suatu jaringan secara terorganisir dimana *malware* ini juga dapat dikendalikan dari pusat atau *Command and Control (C&C)*. (Eko Indrajit, 2008)

Penelitian sebelumnya oleh Hutauruk, SCY et.al bahwa cara bagaimana *trojan* bekerja adalah dengan membuka jalur koneksi dari komputer yang terinfeksi ke penyerang. Data mengalir dari 2 (dua) arah, yakni dari korban dan penyerang dengan menggunakan *well-known protocol* dan *unusual port* untuk terhubung dengan korban. Tujuan yang dipaparkan pada penelitian ini menggunakan beberapa skenario pengujian dengan menyiapkan 4 (empat) buah sample *trojan malware* dan di analysis secara *static malware analysis* dan *dynamic malware analysis.*

Untuk membuktikan suatu *software* dikatakan *malware* adalah dengan mengetahui cara kerja program tersebut pada sistem komputer. Metode *malware analysis* dan *statis* merupakan kombinasi metode yang sesuai untuk menganalisa cara kerja *malware.*

Remote Access Trojan (RAT) adalah program *malware* yang berbahaya, namun cara kerja dari RAT hingga saat ini belum diketahui secara rinci bagaimana tahap-tahapannya. Dari beberapa penelitian yang sudah ada membahas tentang jenis-jenis RAT yang berbeda-beda cara serangan RAT. Trojan bekerja dengan membuka jalur koneksi komputer yang terinfeksi ke penyerang. Untuk itu mengetahui cara kerja RAT dalam penelitian ini berbeda dengan penelitian sebelumnya yang menyerang dari segi lain pada Laptop *user,* dan sangat penting untuk mengantisipasi dan mendeteksi pencegahannya. Dalam penelitian sebelumnya juga meneliti tentang investigasi dari jenis RAT yang membahas hal bagaimana RAT menyerang melalui jaringan user dan berbagai point-point penting di Laptop user, diantaranya bisa *remote desktop, remote cam, remote shell*, membuka menu *Manager, registry, keylogger, open folder, open chatting* pada *user, get passwords, open folder*, bisa melihat *Process Manager, Microphone* dari *user*. Cara kerja RAT perlu diteliti lebih lanjut karena ada point-point serangan yang belum dibahas di penelitian sebelumnya.

Sistem pendeteksian *malware* terhadap serangan RAT masih menjadi masalah karena varian *malware* baru yang selalu berkembang dengan menggunakan teknik yang berbeda untuk menghindari metode pendeteksian. Untuk itu diperlukan pengembangan teknik pendeteksian serangan *malware* supaya *malware* dapat dideteksi secara akurat. Ada sebuah permasalahan yang juga belum dibahas dalam beberapa literatur, deteksi serangan RAT umumnya dilakukan dengan menggunakan bantuan beberapa tools, dan aplikasi forensics. Cara deteksi serangan RAT pada penelitian ini berbeda dengan penelitian sebelumnya yang mengetahui deteksi melalui aplikasi dari windows dan beberapa *tools forensics*.

Bagaimana meningkatkan keamanan data dari serangan RAT melalui simulasi, mengingat cara kerja dan deteksi RAT itu susah diketahui, maka perlu dilakukan simulasi. Simulasi ini digunakan untuk mengetahui bagaimana tahap-tahap cara kerja dari serangan RAT, maka dilakukan peningkatan keamanan data melalui proses melakukan settingan jaringan dan aplikasi windows yang digunakan, sehingga data client bisa terproteksi dari serangan RAT tersebut.

Berdasarkan latar belakang yang telah dipaparkan maka ranah dalam penelitian ini adalah melakukan skenario penyerangan dan deteksi serangan yang terdapat pada RAT dengan memanfaatkan jaringan MikroTik sebagai media dalam implementasi yang digunakan untuk keamanan data dengan metode simulasi. Untuk itu proses yang diharapkan dalam penelitian ini selain dimanfaatkan untuk meningkatkan keamanan data juga di kembangkan untuk manajemen dan keamanan data pada Laptop korban dalam sebuah jaringan komputer dengan metode simulasi serta korban terhindar dari serangan *cybercriminal*. Setelah itu dilakukan analisis pada hasil pengujian dari simulasi dengan tiap skenario penyerangan yang diajukan setelah mendapatkan hasil untuk di tarik sebagai kesimpulan.

1.2 Rumusan Masalah

Dari paparan latar belakang yang sudah ada, maka rumusan masalah pada penelitian ini adalah sebagai berikut :

a. Bagaimana cara kerja serangan *Remote Access Trojan (RAT)* melalui njRAT?

b. Bagaimana melakukan serangan RAT ?
c. Bagaimana meningkatkan keamanan data dari serangan RAT melalui simulasi dan manfaat dari MikroTik ?

1.3 Batasan Masalah

Dalam rangka mengarahkan penelitian berdasarkan rumusan masalah yang telah dipaparkan maka perlu adanya batasan masalah sebagai berikut :

a. Penelitian ini menggunakan *Remote Access Trojan (RAT)* sebagai proses dalam simulasi.
b. Cara kerja untuk mendeteksi serangan RAT melalui njRAT menggunakan aplikasi Winbox, Wireshark, Disk Investigator dan Virus Total.
c. Digunakan metode simulasi dengan cara kerja pada proses deteksi terkait serangan RAT.
d. Penelitian ini menggunakan jaringan MikroTik Router RB951Ui Versi 6 dan Router RB931-2nD.
e. Skenario simulasi serangan pada Laptop korban menggunakan salah satu program *malware.*
f. Penelitian ini dibatasi pada proses mendeteksi serangan RAT dan proses peningkatan keamanan data.

1.4 Tujuan Penelitian

Tujuan yang hendak dicapai pada penelitiaan ini yaitu :

a. Mengetahui cara kerja dalam serangan *Remote Access Trojan (RAT) melalui njRAT*.
b. Mengetahui simulasi keamanan data dalam sebuah manajemen *network* dengan menggunakan beberapa aplikasi, *tools forensics*.
c. Melakukan setting jaringan MikroTik Router RB951Ui Versi 6 dan Router RB931-2nD.
d. Skenario sebelum dan sesudah melakukan penyerangan pada Laptop korban
e. Mengetahui karakteristik bukti digital pada perangkat MikroTik Router untuk keperluan forensik.

f. Melakukan analisis dan pengujian atas metode yang digunakan untuk mendapatkan solusi dalam keamanan data.

1.5 Manfaat Penelitian

Berdasarkan latar belakang, rumusan masalah batasan masalah, dan tujuan dari penelitian yang telah disampaikan pada bagian sebelumnya, adapun manfaat yang ingin dicapai dalam penelitian ini yaitu :

a. Mengetahui bagaimana cara kerja serangan *Remote Access Trojan (RAT).*
b. Mengetahui proses deteksi serangan *Remote Access Trojan (RAT)* dalam metode simulasi
c. Memberikan solusi dalam keamanan data Laptop korban pada pencegahan serangan RAT.
d. Untuk mengetahui bagaimana settingan jaringan menggunakan MikroTik Router RB951Ui Versi 6 dan Router RB931-2nD.
e. Memberikan konstribusi pada proses bagaimana peningkatan keamanan data melalui pemblokiran jaringan *firewall traffic*.

1.6 Metode Penelitian

Adapun langkah-langkah yang akan ditempuh selama melakukan penelitian ini yaitu sebagai berikut :

a. Studi Literatur

   Penelitian ini dilakukan dengan melakukan studi kepustakaan yaitu dengan mengumpulkan bahan-bahan referensi yang terkait dengan penelitian, baik melalui buku, artikel, paper, jurnal, makalah, dan mengunjungi beberapa situs yang terdapat pada internet terkait dengan *Remote Access Trojan (RAT)*, serangan pada Router dan keamanan data dengan metode simulasi serta beberapa referensi lain yang dapat menunjang kegiatan penelitian yang dilakukan.

b. Pengambilan data

   Pada tahap pengambilan data *Remote Access Trojan (RAT)* peneliti menggunakan aplikasi Wireshark, Disk Investigator, Virustotal,

c. Konfigurasi Peningkatan Keamanan Data

Konfigurasi *Remote Access Trojan (RAT)* akan dimulai dari pekerjaan menonaktifkan anti virus si korban, menonaktifkan jaringan firewall windows, kemudian dilanjutkan dengan mengirimkan lewat USB, via email, *file sharing*, atau bisa lewat media sosial.

d. Simulasi Serangan dan Pengujian

Simulasi serangan dalam penelitian ini menggunakan *Remote Access Trojan (RAT)* untuk menyerang korban. Tahap yang dimaksud dalam simulasi dan pengujian ini bertujuan untuk mengetahui teknik pendeteksian *Remote Access Trojan (RAT)*, keberhasilan dalam penarikan data, dan informasi dari Router.

e. Analisis

Tahapan ini akan melakukan analisis terhadap point-point dalam program *malware Remote Access Trojan (RAT)* yang dapat bernilai bukti digital serta analisa penggunaan router yang dapat difungsikan untuk menarik data dari MikroTik melalui tools yang digunakan. Point-point apa saja yang ada dalam program *malware Remote Access Trojan (RAT)* sebagai bukti digital serangan.

f. Kesimpulan dan Laporan

Tahapan laporan adalah tahapan akhir yaitu penyampaian kesimpulan atas hasil dari penelitian ini.

1.7 Sistematika Penulisan

Tahapan ini adalah tahapan yang memberikan gambaran secara umum terkait dengan sistematika prosesan, dengan tujuan memberikan penjelasan secara ringkas terhadap kerangka dalam pemprosesan.

BAB I: PENDAHULUAN

Pendahuluan, merupakan pengantar terhadap permasalahan yang akan dibahas. Didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, sistematika penulisan yang dilakukan serta literatur review.

BAB II : LANDASAN TEORI

Pada Bab ini menjelaskan teori-teori yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang dibahas pada bagian ini merupakan teori yang berhubungan dengan program *malware Remote Access Trojan (RAT), network* dan *routing*.

BAB III : METODE PENELITIAN

Bab ini membahas tentang kerangka konsep penelitian dan gambaran umum langkah penyelesaian yang akan dilakukan. Bagan proses investigasi dibuat berdasarkan referensi yang didapat, untuk menyelesaikan penelitian dilakukan pembuatan rancangan simulasi untuk membuktikan bagan proses cara kerja dan teknik pendeteksian yang dikembangkan.

BAB IV : HASIL DAN ANALISA

Bab ini membahas bagaimana simulasi yang sudah dirancang pada bab sebelumnya pada sistem yang sebenarnya. Hasil yang didapat pada tahap simulasi ini apakah sesuai dengan yang diharapkan dan dilakukan pembahasan terkait dengan penelitian yang dibuat.

BAB V : KESIMPULAN DAN SARAN

Tahapan ini adalah tahapan terakhir yang dilakukuan dalam penelitian ini dan memuat tentang kesimpulan dari keseluruhan uraian dari Bab-bab sebelumnya, serta memberikan saran terkait dengan kekurangan yang diperoleh dalam penelitian untuk pengembangan ilmu pengetahuan di kemudian hari.

1.8 Literatur Review

Rangkuman dari literature review terhadap penelitian-penelitian yang telah dipaparkan secara singkat dapat dilihat pada Tabel 1.1 dimana akan menunjukkan perbandingan dari beberapa penelitian sebelumnya.

Tabel 1. 1 Literatur Review

No.	Nama	Metode yang digunakan	Jenis RAT	Alat yang digunakan	Bentuk Output	Kelemahan	Saran
1.	(Hutauruk SCY., Yulianto FA., Satrya GB., 2016)	- Static malware analysis - Dynamic malware anlysis	Trojan	Sistem operasi Windows	Deteksi trojan	-	- Mendeteksi *malware* jenis lain - *Malware analysis* dalam Linux - Sistem operasi versi 64bit
2.	(Cahyanto TA., Wahanggara V., Ramadana D., 2017)	Dynamic malware anlysis	Poison Ivy RAT	Tool Regshot, Wireshark	Kebenaran informasi program *malware* Poison Ivy RAT	- Informasi melalui kode-kode *hexa*, *string* dan *binary*	- Pengetahuan lebih mendalam membaca program berbahasa mesin *(assembly langguage)* - Teknik analisis program *malware* dengan *Reverse Engineering*
3.	(Harjono, 2013)	Simulasi Identifikasi serangan *malware*	Win32.Worm.Downadup.Gen (*Malware Worm*)	Sistem Operasi Linux Ubuntu 10.04	Penerapan *Dionaea* dalam jaringan lokal UMP	Tidak adanya sistem untuk mendeteksi adanya serangan *malware*	-
4.	(Septani DR., Widiyasono N., Mubarok H., 2016)	Dynamic analysis	njRAT	PC, windows task manager	Cara kerja *malware*	-	Mendalami cara kerja dan pola serangan *malware* dengan lebih dari satu jenis *malware*
5.	(Syarif YS., Yudi P.,	Static and Dynamic	*Malware*	Tools forensik	Analisis malware menggunakan	Terjangkit Malware	Lebih detail lagi tentang Malware

	Imam R., 2015)	Analysis Method			beberapa tools forensik		Analisis
6.	(Kristono, I. Riyadi, Y. Prayudi, 2018)	Simulasi	DDoS (Denial of Service)	- MikroTik RB951Ui - Access Point TP-Link MR3020 - Switch TP-Link - Modem ADSL	- Melakukan setting metarouter dan keamanan data - Melakukan simulasi eksplorasi metarouter	- Harus bisa terhubung dengan internet - Routerboard belum bisa terupdate secara otomatis	- Router bisa terupdate secara otomatis - Metarouter laiinya bisa membangun keamanan data jaringan yang lebih baik kedepannya