INVESTIGASI SERANGAN *MALWARE NJRAT* PADA PC

Devi Rizky Septiani[1], Husni Mubarok[2], Nur Widyasono[3]
Fakultas Teknik Jurusan Teknik Informatika Universitas Siliwangi Tasikmalaya
Jl. Siliwangi 24 Tasikmalaya Jawa Barat
[1]devi.rizky@student.unsil.ac.id, [2]husni.mubarok@unsil.ac.id, [3]nur.widyasono@unsil.ac.id

ABSTRAK - *Malware* merupakan salah satu bentuk dari kejahatan komputer yang terjadi pada sebuah sistem jaringan komputer, *malware NjRAT* adalah salah satu dari *malware* yang sangat berbahaya karena besarnya dampak kerugian yang ditimbulkan, mulai dari pencurian data penting sampai mengubah hak akses pada *computer* korban. Aktivitas *malware* berkaitan erat dengan *memory computer*, *performance computer* dan juga aktifitas *network* pada *system computer*. Penelitian ini bertujuan untuk mengetahui cara kerja *malware NjRAT* dan melakukan investigasi terhadap *performance* pada *system computer*. Metodologi yang digunakan *dynamic analysis* dengan melakukan analisa *malware* pada suatu sistem dan melihat aktivitas atau proses yang diaktifkan oleh *malware* tersebut. Dampak perubahan yang terjadi pada PC Korban terlihat pada *performance* masing-masing PC yang telah disisipkan *malware.*

Kata kunci: Malware, NjRAT, System computer

I. Pendahuluan

Kejahatan dunia maya setiap tahunnya mengalami peningkatan yang sangat pesat, hal ini dikarenakan semakin berkembangnya teknologi komputer yang berdampak pada kehidupan manusia. Segala kemudahan yang didapat dari teknologi komputer pada kenyataannya tidak hanya berdampak baik bagi kehidupan manusia karena beberapa diantaranya ternyata juga ikut memberikan dampak yang buruk. Banyak orang yang memanfaatkan teknologi komputer sebagai media untuk melakukan tindak kejahatan yang bertentangan dengan hukum. Beragam tujuan yang dimiliki para pelaku ini beberapa diantaranya adalah untuk mencari kesenangan, mencari keuntungan. 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*. Virus komputer bekerja dengan cara menempel pada suatu *file* komputer yang biasanya berupa *file executable*, *trojan* bekerja dengan cara melakukan *social engineering file*s berbahaya dengan menampilkannya seperti *file*s yang terlihat tidak berbahaya, *spyware* adalah perangkat lunak yang disisipi kode untuk mendapatkan informasi penting dari pengguna seperti akun *bank*, *password*, dan informasi lainnya yang diinginkan oleh pembuatnya, sedangkan *worm* adalah perangkat lunak

jahat yang dibuat dengan memanfaatkan celah lubang keamanan pada sistem operasi untuk tujuan tertentu (Budhisantosa, 2014).

A. **Tujuan Penelitian**

Untuk mengetahui cara kerja *malware NjRAT* dan mengetahui *performance* PC apabila terinfeksi *malware* tersebut.

B. **Rumusan Masalah**

a. Bagaimana cara kerja *malware NjRAT* ?
b. Bagaimana *performance* PC apabila terinfeksi *malware NjRAT*?
c. Bagaimana penanganan *malware NjRAT?*

II. Kajian Pustaka

A. Malware

Malware (singkatan dari istilah Bahasa Inggris *malicious software*, yang berarti perangkat lunak yang mencurigakan) adalah program komputer yang diciptakan dengan maksud dan tujuan tertentu dari penciptanya dan merupakan program yang mencari kelemahan dari *software*. Umumnya *malware* diciptakan untuk membobol atau merusak suatu *software* atau sistem operasi melalui *script* yang disisipkan secara tersembunyi oleh pembuatnya (Asep, 2012)**.**

B. Jenis – jenis *Malware*

Menurut (Agung, 2011) berikut ini berbagai jenis *Malware* yang dinilai paling dominan menginfeksi komputer :

a. Virus

Virus merupakan program komputer yang bersifat mengganggu dan merugikan pengguna komputer. Virus adalah *Malware* pertama yang dikenalkan sebagai program yang memiliki kemampuan untuk mengganggu kinerja sistem komputer. Hingga saat ini biasanya masyarakat lebih populer dengan kata virus komputer dibandingkan dengan istilah *Malware* sendiri. Biasanya virus berbentuk *file* eksekusi (*executable*) yang baru akan beraktivitas bila *user* mengaktifkannya. Setelah diaktifkan virus akan menyerang *file* yang juga bertipe *executable* (*.exe*) atau juga tipe *file* lainnya sesuai dengan perintah yang dituliskan pembuatnya.

b. *Worm*

Worm yang berarti cacing merupakan *Malware* yang cukup berbahaya. *Worm* mampu untuk menyebar melalui jaringan komputer tanpa harus tereksekusi sebelumnya. Setelah masuk ke dalam sistem komputer, *Worm* memiliki kemampuan untuk mereplikasi diri sehingga mampu memperbanyak jumlahnya di dalam sistem komputer. Hal yang diakibatkan dari aktivitas *Worm* adalah merusak data dan memenuhi *memory* dengan *Worm* lainnya hasil dari penggandaan diri yang dilakukannya. Replikasi ini membuat memory akan menjadi penuh dan dapat menngakibatkan aktivitas komputer menjadi macet (hang). Kebiasaan komputer menjadi hang dapat menjadi gejala awal terdapatnya *Worm* pada komputer tersebut. Contoh *Worm* yang populer akhir-akhir ini adalah *Conficker*.

c. *Trojan Horse*

Teknik *Malware* ini terinspirasi dari kisah peperangan kerajaan Yunani kuno yang juga diangkat ke Hollywood dalam

film berjudul ‘Troy’. Modus dari *Trojan Horse* ini adalah menumpangi file biasa yang bila sudah dieksekusi akan menjalankan aktivitas lain yang merugikan sekalipun tidak menghilangkan fungsi utama file yang ditumpanginya. *Trojan Horse* merupakan *Malware* berbahaya, lebih dari sekedar keberadaannya tidak diketahui oleh pengguna komputer. *Trojan* dapat melakukan aktivitas tak terbatas bila sudah masuk ke dalam sistem komputer. Kegiatan yang biasa dilakukan adalah merusak sistem dan *file*, mencuri data, melihat aktivitas *user* (*spyware*), mengetahui apa saja yang diketikkan oleh *user* termasuk *password* (*keylogger*) bahkan menguasai sepenuhnya komputer yang telah terinfeksi *Trojan Horse*.

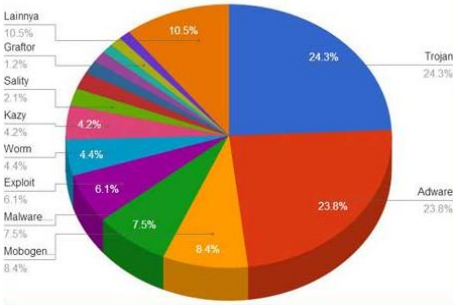
d. *Spyware*

Spyware merupakan *Malware* yang dirancang khusus untuk mengumpulkan segala informasi dari komputer yang telah dijangkitinya. Kegiatan *Spyware* jelas sangat merugikan *user* karena segala aktivitasnya yang mungkin menyangkut privasi telah diketahui oleh orang lain tanpa mendapat izin sebelumnya. Aktivitas *Spyware* terasa sangat berbahaya karena rentan terhadap pencurian *password*. Dari kegiatan ini juga akhirnya lahir istilah *Adware* yang merupakan iklan yang mampu muncul secara tiba-tiba di komputer korban hasil dari mempelajari aktivitas korban dalam kegiatan berkomputer. *Spam* yang muncul secara tak terduga di komputer juga merupakan salah satu dampak aktivitas *Spyware* yang dirasa sangat menjengkelkan.

e. *Backdoor*

Kerja dari *Backdoor* sangat berkaitan dengan aktivitas *hacking*. *Backdoor* merupakan metode yang digunakan untuk melewati *autentifikasi* normal (*login*) dan berusaha tidak terdeteksi. *Backdoor* sendiri sering kali disusupkan bersama dengan *Trojan* dan *Worm*. Dapat diartikan secara singkat *Backdoor* berarti masuk ke sistem komputer melalui jalur pintu belakang secara tidak sah. Dengan metode *Backdoor* maka akan sangat mudah untuk mengambil alih kendali dari komputer yang telah berhasil disusupi. Setelah berhasil masuk maka aktivitas yang dilakukan oleh *Backdoor* antara lain adalah mengacaukan lalu lintas jaringan, melakukan *brute force attack* untuk *mengcrack password* dan enkripsi dan mendistribusikan serangan *Distributed Denial of Service* (DDoS).

Data *statistic* penyebaran *malware* di Indonesia tiap tahun berubah persentasenya, dan berubah juga tahapan virus yang tersebarnya. Dapat dilihat pada gambar dibawah ini data *statistic malware* berbeda dengan tahun-tahun sebelumnya.



Gambar 2.1 Data *Statistic* serangan *Malware*
Sumber : (detik.com,2015)

Menurut (detik.com, 2015) *Malware* yang paling banyak terdeteksi sampai sekarang ini adalah jenis *Trojan* yang menguasai 24,30% serangan *malware* di Indonesia. Setelah *Trojan*, 23,8% jenis *Adware* menyerang pengguna computer.

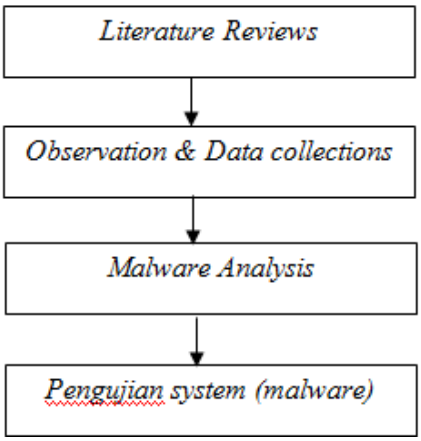
Selanjutnya diikuti oleh jenis lainnya seperti *Mobogen*, *exploit*, *worm*, *kazy*, dan lainnya yang memiliki hasil prsentase masing – masing yang dapat dilihat pada gambar 2.1 diatas.

C. *NjRAT*

NjRAT malware yang digunakan untuk *meremote* pc orang lain dengan jarak jauh. *RAT* digunakan untuk menghubungkan dan mengatur satu atau lebih komputer dengan berbagai kemampuan. Aspek utama dari *RAT* ini popularitasnya dengan sistem *Domain Name System* (*DNS*) layanan seperti *no-ip.com*. Sebuah layanan *DNS* dinamis adalah metode otomatis memperbarui *server* nama di *DNS*, sering secara *real time*, dengan konfigurasi *DNS* aktif *hostname* dikonfigurasi, alamat, atau informasi lainnya. Fitur ini memungkinkan penyerang tanpa IP statis khusus, seperti *DSL* atau koneksi *broadband*, untuk menggunakan nama *host* berbasis *DNS*.

III. Metodologi Penelitian

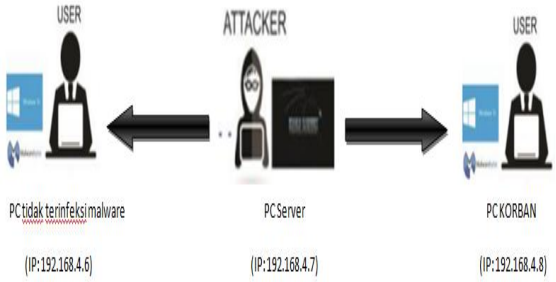
Adapun metodologi yang digunakan dalam penelitian ini adalah sebagai sebagai berikut :



Gambar 3.1 Diagram Alur Metodologi penelitian

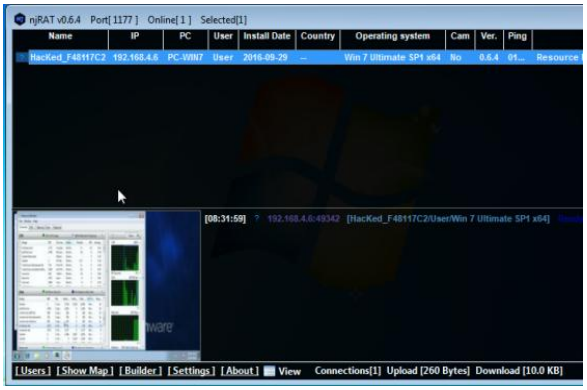
IV. Hasil dan Pembahasan

Bab ini merupakan uraian tentang hasil dan pembahasan, tujuannya adalah untuk mendapatkan jawaban atas semua permasalahan dari tema yang diangkat didalam penelitian. Proses analisis ini disusun dengan terstruktur untuk mendapatkan skema investigasi pada *performance* PC yang terinfeksi *malware*. Analisis dalam penelitian ini menggunakan *hardware* 3 PC dengan spesifikasi yang berbeda dan menggunakan *software VMware* sebagai alat untuk pengujian *malware* tersebut.



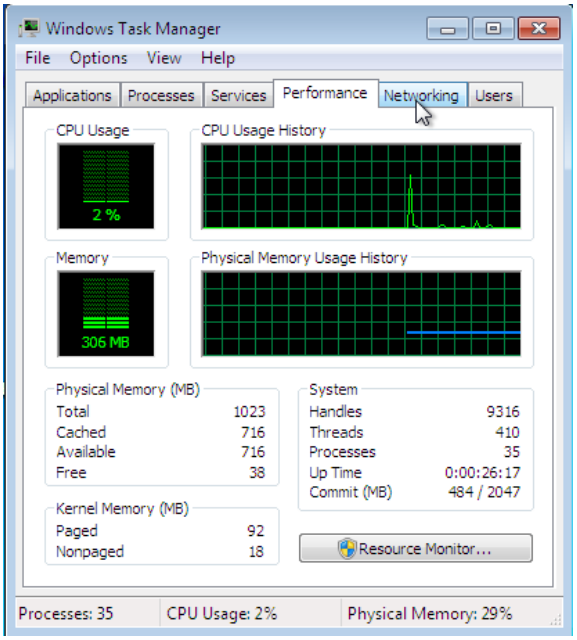
Gambar 4.1
Skema penyebaran *malware*

Proses penyebaran *malware* dilakukan oleh *attacker* dengan cara menyebarkan virus melalui *USB* ataupun *file sharing*. Pada PC satu tidak disisipkan *malware NjRAT* tersebut dan untuk PC korban disisipkan *malware*, dengan cara menjalankan *malware* pada PC tersebut maka *attacker* atau PC server dapat mengtahui aktifitas apa saja yang sedang dilakukan oleh PC korban dan juga untuk *server* bisa melakukan hak akses apapun terhadap PC korban tanpa diketahui oleh koban tersebut.



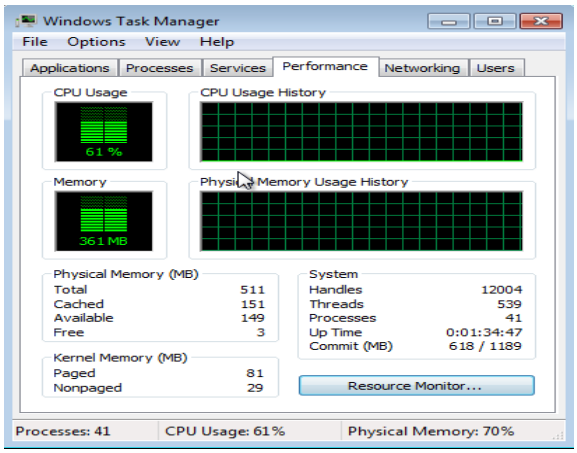
Gambar 4.2 Tampilan PC *server*

Gambar diatas ini adalah tampilan pada PC *server* untuk *meremote* semua isi *computer* korban, dan bisa melakukan hak akses apapun terhadap PC korban setelah disisipkan *malware* tersebut.



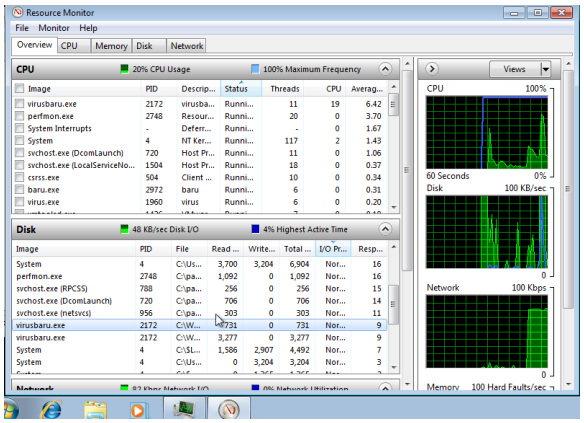
Gambar 4.3 Tampilan *Performance* PC 1

PC yang tidak terinfeksi *malware* dapat dilihat pada *performancenya* seperti pada gambar diatas, maka trafik yang terjadi pada *system computer* tersebut akan lemah. Sama seperti trafik yang terjadi apabila semua PC belum terinfeksi *malware*.



Gambar 4.4 Tampilan *performance* PC korban

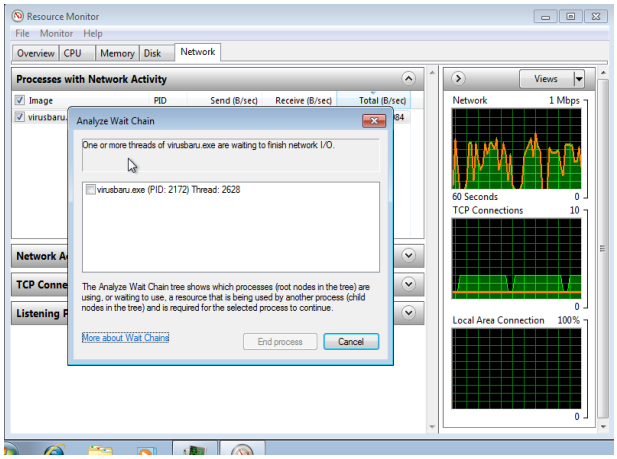
Gambar diatas dapat dilihat pada *performance* PC yang disispkan *malware*, grafik yang terjadi pada *CPU* terus meningkat tinggi dibandingkan dengan sebelum dan yang tidak ternfeksi *malware*, sama seperti grafik pada *memory* semakin lama semakin tinggi jumlahnya. Trafik *CPU* dan *memory* yang terinfeksi *malware* dapat dilihat pada gambar dibawah ini.



Gambar 4.5 *Overview computer* korban

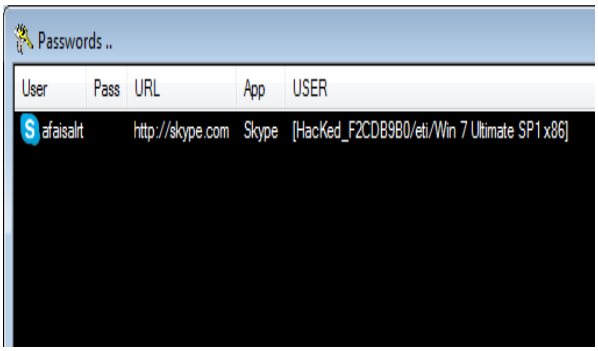
Performance yang terjadi pada *CPU* menunjukan ada *virusbaru.exe* berhasil masuk pada *system omputer* tersebut, dan trafik pada *CPU* juga terus meningkat dengan adanya *malware*. *Virusbaru.exe* pada disk tersimpan pada *registry C/windows*,

artinya virus masuk pada *local disk C* pada *system computer* tersebut. Dalam *network* juga dapat dilihat serangan yang terjadi setelah di sisipkan *malware*, dapat dilihat pada gambar selanjutnya.



Gambar 4.6 *Performance* pada *network*

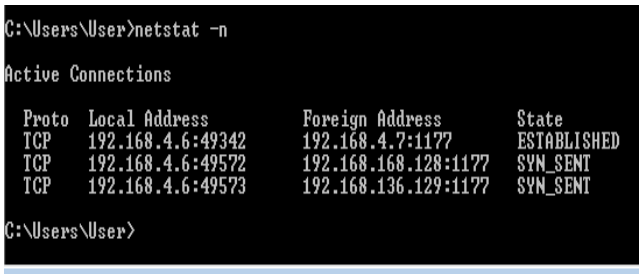
Network activity pada *system computer* korban mempengaruhi pada kecepatan internet menjadi semakin lemah dan tidak stabil kecepatan */mbps. Virusbaru.exe is running normally. Malware* tersebut menyerang masuk pada *network computer* korban sehingga *server* dapat *meremote website* yang ada pada PC korban.



Gambar 4.7 *Get password* PC korban

Gambar diatas menjelaskan tentang serangan virus *malware* tersebut dapat mengetahui *website* yang ada pada PC korban. Aplikasi yang sedang aktif pada PC korban yaitu *skype* dengan *username* afaislrt dan *url* http://skype.com.

Matikan semua *AV* yang ada dan juga harus matikan *firewall* agar virus yang disisipkan tidak langsung terdeteksi pada *system* komputer



Gambar 4.8 *Test netstat* CMD PC korban

Tampilan diatas menjelaskan bahwa benar pada PC korban diserang oleh virus *malware*. *Port* 1177 adalah *port* asing yang masuk ke dalam *system* pada PC korban dan status *port* tersebut berjalan normal masuk tanpa diketahui oleh *user* PC korban.

V. Kesimpulan

Cara kerja *malware NjRAT* sifatnya sangat berbahaya sehingga *attacker* dapat melakukan hak akses apa saja terhadap PC korban bahkan untuk membobol *web* dan juga *passwordnya* dapat dilakukan dengan adanya serangan *malware* yang terjadi.

Perubahan trafik *performance* yang terjadi pada PC yang disisipkan *malware* semakin lama semakin cepat tetapi pada *performance* di *network* semakin melemah (*loading*)

Penanganan agar tidak terinfeksi *malware* baik *local* ataupun tidak dapat dilakukan pemasangan *Antivirus* dan juga menghidupkan *firewall* pada *system computer*, menutup seluruh *port* yang ada pada PC tersebut.

Saran

Sebaiknya penelitian selanjutnya lebih mendalami cara kerja dan pola serangan *malware* dengan berbagai jenis *malware* lainnya lebih dari satu jenis *malware*

VI. DAFTAR PUSTAKA

Agung, M. F. (2011). *Jenis-jenis Mallware dan pencegahannya.* Bogor.

Budhisantosa, N. (2014). Analisis modifikasi konfigurasi Accsess Control List pada USB studi kasus pada penyebaran mallware trojan shortcut. *Ilmu komputer* .

Elanda, A. (2015). Tren malware dan teknologi deteksi. In A. Elanda, *Tren Malware dan teknologi deteksi.* Bandung.

Mathur, K. (2013). Teknik pendeteksi dini dan analisis mallware. *Jurnal internasional software engginerring* .

Thakkar, N. (2014, Agustus 05). *Blog Central*. Retrieved from blogs.mcafee.com: https://blogs.mcafee.com/mcafee-labs/trail-njrat/

Fedler, R., & Julian, S. (2013). Efektifitas mallware pada android. *Jurnal internasional* .

Gandotra, B., & Sanjeev, D. (2014). Analisis dan klasifikasi mallware. *Jurnal internasional* .

Indrajit, R. E. (2013). Analisa mallware.

Jyoti, L. (2013). Teknik deteksi Mallware. *Jurnal Internasional* .

Kramer, S. (2013). Pengenalan kerangka mallware. *Jurnal internasional* .