Investigasi Serangan *Malware Njrat* Pada PC

Devi Rizky Septani[#1], Nur Widiyasono [*2], Husni Mubarok [#3]

[#]*Jurusan Teknik Informatika, Fakultas Teknik Universitas Siliwangi Tasikmalaya*

Jl. Siliwangi No. 24 Kota Tasikmalaya 46151

[1]devi.rizky@student.unsil.ac.id

[3]husni.mubarok@unsil.ac.id

[*]*Fakultas Teknik Universitas Siliwangi Tasikmalaya*

Jl. Siliwangi No. 24 Kota Tasikmalaya 46151

[2]nur.widiyasono@unsil.ac.id

Abstrak **—— *Malware* merupakan salah satu bentuk dari kejahatan komputer yang terjadi pada sebuah sistem jaringan komputer, *malware Njrat* termasuk jenis *Trojan horse*. *Trojan* adalah salah satu jenis *malware* yang ikut berkembang di dalamnya, yang memungkinkan *attacker* masuk ke dalam sistem tanpa diketahui oleh pemilik. Penggunaan *trojan* saat ini lebih ke arah kejahatan dunia maya (*cyber* crime), salah satu dari *malware* yang sangat berbahaya karena besarnya dampak kerugian yang ditimbulkan, mulai dari pencurian data penting sampai mengubah hak akses pada PC korban. Sasaran terbanyak penybaran *trojan* adalah pengguna sistem operasi *windows*. Penyebaran *trojan* ini dilakukan dengan metode *social engineering*, yaitu teknik yang menggunakan kelemahan manusia, sehingga *user* tanpa curiga langsung mengeksekusi sebuah program yang tidak dikenal. Aktivitas *malware* berkaitan erat dengan performa PC dan juga aktifitas *network* pada *system computer*. Penelitian ini bertujuan untuk mengetahui cara kerja *malware Njrat* dan melakukan investigasi terhadap performa 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 Target terlihat pada performa 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* [1].

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 [2].

Dampak yang terjadi apabila PC terinfeksi *malware* yaitu PC akan berjalan semakin lambat mesikpun menggunakan spesifikasi PC dengan processor bagus dan RAM dengan jumlah banyak, akan tetapi jika PC terinfeksi *malware* akan berjalan lambat dan pada performa *network* tidak stabil [3].

Solusi untuk penccegahan agar PC terhindar dari *malware* dapat menggunakan aniti virus dengan versi terbaru yang sangat bagus untuk mendeteksi berbagai jenis *malware*.

II. KAJIAN PUSTAKA

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 [4].

Berikut ini berbagai jenis *Malware* yang dinilai paling dominan menginfeksi komputer [5] :

ISSN 2460-0741

(1). 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.

(2). *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*.

(3). *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*.

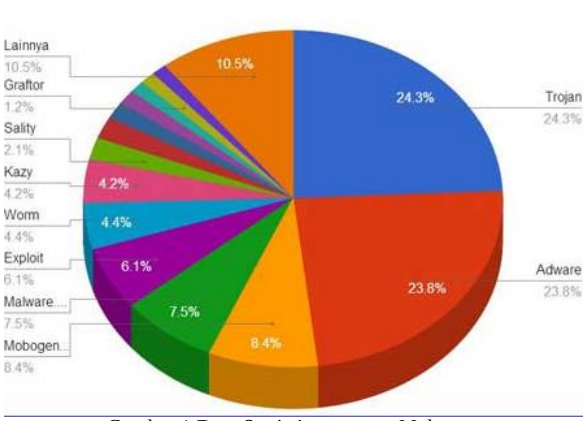
(4). *Spyware*

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.

(5). *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 1 Data *Statistic* serangan *Malware*

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 1 diatas [6].

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*.

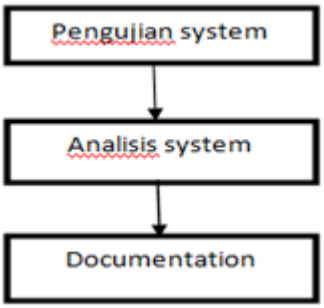
Sebuah layanan *DNS* dinamis adalah metode otomatis memperbarui *server* nama di *DNS*, sering secara *real time*, dengan konfigurasi *DNS* aktif *hostname* dikonfigurasi, alamat, atau informasi lainnya. Fitur ini memungkinkan

ISSN 2460-0741

penyerang tanpa IP statis khusus, seperti *DSL* atau koneksi *broadband*, untuk menggunakan nama *host* berbasis *DNS* [7].

III. METODOLOGI PENELITIAN

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

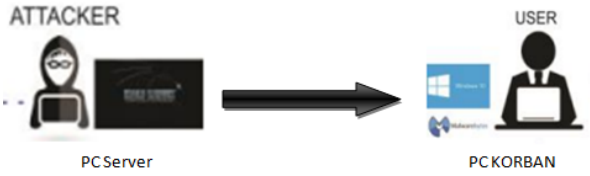


Gambar 2 Metodologi penelitian

Metode *dynamic analyisis* atau biasa disebut juga *behavior malware analysis*. Dynamic analisis *malware* adalah teknik melakukan analisa *malware* pada suatu sistem dan melihat aktivitas atau proses yang diaktifkan oleh *malware* tersebut [8].

IV. HASIL DAN PEMBAHASAN

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 3 Skema penyebaran *malware*

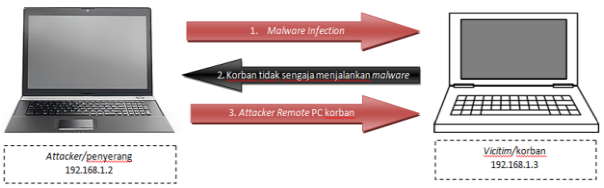
Proses penyebaran *malware Njrat* dilakukan oleh *attacker* dengan cara menyebarkan virus melalui *USB* ataupun *file sharing*. Pada PC satu tidak disisipkan *malware Njrat* tersebut dan untuk PC korban disisipkan *malware*, dengan cara menjalankan *malware* pada PC tersebut maka *attacker* atau PC server 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.

Jenis *malware Njrat* ini dijalankan secara manual untuk mengambil alih hak akses PC target. Sistem yang digunakan dengan cara *double* klik file sisipan *malware*, setelah *malware Njrat* berhasil menyerang PC target *attacker* langsung bisa melakukan hak akses apa saja terhadap PC target.

TABEL I
KARAKTERISTIK *MALWARE NJRAT*

NO	Kriteria
1	Tidak memiliki *verified signatured*
2	Memiliki kemampuan untuk melakukan file *duplication*
3	Memiliki *keylogger*
4	Memiliki kemampuan untuk menambahkan *registry* pada sistem
5	Memiliki kemampuan untuk *remote* perubahan *registry*
6	Memiliki kemampuan untuk melakukan akses *remote* terhadap folder korban
7	Memiliki kemampuan untuk *remote desktop* / *screen viewer*
8	Memiliki kemampuan untuk mengakses *remote shell* komputer korban

Attacker menyebarkan *malware Njrat* dengan menyebarkan *software* bajakan. Korban tidak mengetahui *software* tersebut berisi *malware* karena tidak ada perbedaan yang signifikan dari *software* tersebut. *Malware Njrat* ini dapat *meremote* PC target, dapat merusak file dan mencuri file penting pada PC target, dapat mengetahui aktivitas *user* target dengan menggunakan *remote camera attacker* dapat melihat *user* target.

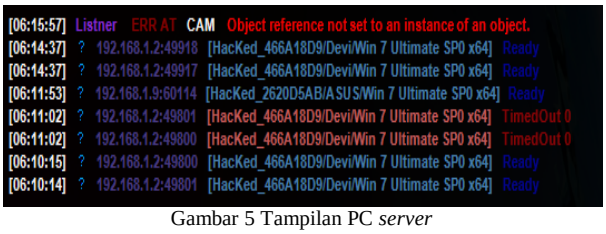


Gambar 4 Arsitektur *malware Njrat*

Penyebaran *malware* tersebut menggunakan teknik *social engineering* yaitu teknik yang menggunakan kelemahan manusia, sehingga *user* tanpa curiga langsung mengeksekusi sebuah program yang dianggapnya baik-baik saja.

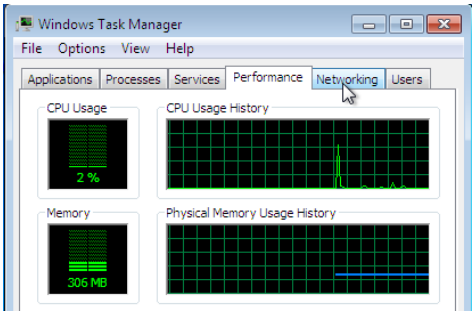
Virus komputer dibuat dengan tujuan yang tidak baik yaitu untuk pencurian data pada komputer tanpa sepengetahuan dari pemiliknya. banyak efek negatif yang ditimbulakan oleh virus komputer diantaranya rusaknya data dan program pada komputer sehingga data tersebut tidak dapat dibuka, ataupun program yang ada pada komputer tidak dapat berjalan.

ISSN 2460-0741



Gambar 5 Tampilan PC *server*

Tampilan pada PC *server* untuk *meremote* semua isi *computer* korban, dan bisa melakukan hak akses apapun terhadap PC korban setelah disisipkan *malware Njrat* tersebut.



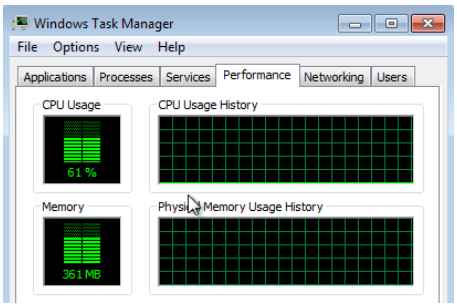
Gambar 6 Tampilan Performa PC 1

PC yang tidak terinfeksi *malware Njrat* dapat dilihat performa seperti pada gambar 6, maka trafik yang terjadi pada *system computer* tersebut akan lemah. Sama seperti trafik yang terjadi apabila semua PC belum terinfeksi *malware Njrat*.

TABEL II
KONSISTENSI PERFORMA PC SEBELUM TERINFEKSI *MALWARE NJRAT*

NO	Waktu	Penggunaan *memory*	Penggunaan CPU
1	1menit	49%	15%
2	5menit	45%	20%
3	8menit	45%	22%
4	10menit	43%	23%

Konsistensi waktu sebelum terinfeksi *malware Njrat* dari menit ke menit, penggunaan *memory* sebelum terinfeksi secara dinamis berjalan rata-rata 45% penggunaan untuk aplikasi yang sedang berjalan saja.



Gambar 7 Tampilan performa PC korban

Performa PC yang disispkan *malware Njrat*, 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.

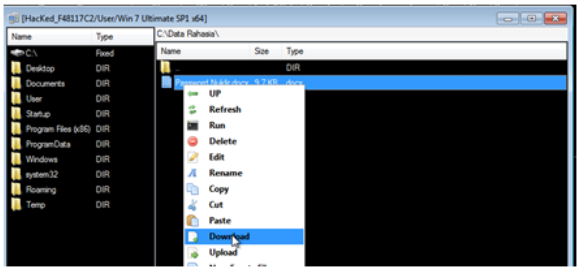
TABEL III
KONSISTENSI PC SETELAH TERINFEKSI *MALWARE NJRAT*

NO	Waktu	Penggunaan *memory*	Penggunaan CPU
1	1menit	41%	31%
2	5menit	51%	32%
3	8menit	51%	34%
4	10menit	53%	40%
5	25menit	55%	67%

Konsistensi waktu setelah terinfeksi *malware Njrat*. Perubahan yang terjadi setelah terinfeksi *malware* cukup meningkat menit demi menit, berjalan secara dinamis rata – rata penggunaan *memory* setelah terinfeksi *malware* menghabiskan sekitar 50%. Peningkatan trafik yang terjadi mengakibatkan PC dan jaringan menjadi lambat.

Performa *network* menjelaskan kinerja dari jaringan ketika proses pencurian data berlangsung. Perubahan trafik yang terjadi sebelum diinfeksi *malware Njrat* dapat dilihat dari *task manager*. performa *networking* sebelum terinfeksi *malware Njrat*. Penyerangan dilakukan melalui *wireless* adapter dengan kecepatan 65Mbps. *Network utilization* (penggunaan jaringan) dengan penggunaan jaringan sebesar 1,03% secara dinamis. Penggunaan *memory* sebesar 72%.

Performa *networking* setelah terinfeksi *malware Njrat*. Penyerangan dilakukan melalui *wireless* adapter dengan kecepatan 65Mbps. *Network utilization* (penggunaan jaringan) dengan penggunaan jaringan sebesar 3,26% secara dinamis. Penggunaan *memory* sebesar 67%. *Network* setelah terinfeksi *malware Njrat* berjalan menjadi lambat



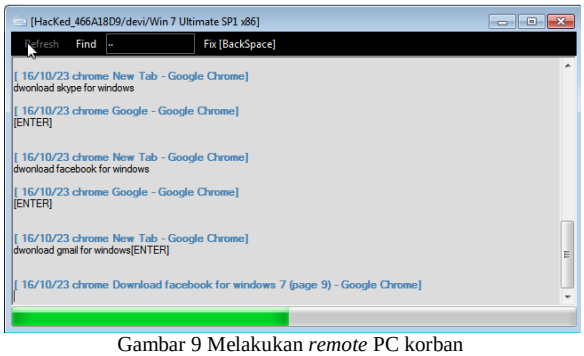
Gambar 8 Proses pencurian file

Pencurian *file* pada PC target dilakukan tanpa diketahui oleh *user*, pencurian *file*, mengganti nama *file* dan menghapus *file* dapat dilakukan oleh *attacker*. Dengan menggunakan teknik *social engineering* memanfaatkan kelemahan *user* dengan menjalankan aplikasi yang telah disisipkan *malware Njrat*.

File yang dicuri oleh *attacker* akan tersimpan otomatis pada PC server, melalui perintah *download*, *file* akan pindah ke PC *attacker*. Perintah *run* untuk mengendalikan PC target

ISSN 2460-0741

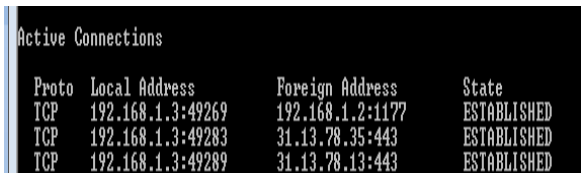
melalui *attacker*, misalnya dapat menjalankan atau membuka *file* yang diinginkan *attacker* tanpa diketahui oleh *user* target. Perintah *upload* untuk menambahkan *file* ke PC target, *file* akan ditambahkan oleh *attacker* tanpa diketahui target. Dapat melakukan hak akses apa saja pada *file* tersebut dan *attacker* juga dapat dengan bebas mengendalikan PC target dari jarak jauh. Pencurian *file* dapat terjadi berdasarkan kondisi jaringan.



Gambar 9 Melakukan *remote* PC korban

Malware Njrat dapat mengetahui segala aktifitas target yang sedang berjalan. Gambar 9 menjelaskan tentang aktifitas target yang sedang *mendownload* aplikasi yaitu *skype for windows, facebook for windows* dan *gmail for windows* melalui *google chrome* diakses pada tanggal 23 oktober 2016.

Username dan *password* dengan menggunakan perintah *keylogger* untuk dapat mengetahui aplikasi apa yang sedang dijalankan oleh target dan *password* yang telah tersimpan sebelumnya pada *history* PC target, dengan teknik *social engineering*, memanfaatkan teknik *trojan horse*, yaitu memanfaatkan rasa ingin tahu seseorang dan memberikan *malware* untuk keperluan apa saja. *Username* dan *password* diketahui oleh attacker setelah *Njrat* disisipkan melalui *keylogger*, *attacker* dapat mengetahui segala aktifitas yang sedang dilakukan termasuk mengetahui *username* dan *password*. . *Keylogger* dapat mengetahui *username* dan *password* PC target jika kondisi jaringan baik. Cara untuk mendapatkan *username* dan *password* ini dengan cara teknik *social engineering*. Pemanfaatan *social engineering* dengan cara *attacker* memanfaatkan celah *user* target dengan menyisipkan *software* bajakan yang berisi *malware*.



Gambar 10 *command line* PC korban

Virus yang masuk ke dalam PC target, virus masuk dengan menggunakan *port* asing yaitu :1177, 192.168.1.2:1177 adalah IP *address* penyerang menggunakan port :1177 menyerang PC target, dengan perintah *netstat-n* pada *Command line*. Perintah *netstat -n* untuk memunculkan daftar IP *address* mana saja yang masuk ke dalam *system*.

Proto menjelaskan protokol, *Local address* menjelaskan tentang IP *address* dan *port* yang sedang berjalan pada PC target, PC target dengan IP 192.168.1.3. *Forgein address* menujukan koneksi yang sedang dituju oleh PC target, 192.168.1.2 adalah IP *address attacker* dengan *port* :1177 masuk ke *system* PC target, dengan status *ESTABLISHED* maksudnya terhubung dengan PC lain yaitu PC *attacker*.

Menghilangkan semua *malware Njrat* yang ada pada *system* komputer dengan menghapus *virusbaru.exe*, *parampaa.exe* pada *registry*, *task manager*, dan pada semua *system* yang ada pada komputer. Penanganan melalaui Anti virus juga digunakan untuk membantu PC mendeteksi keadaan *system*, mendeteksi semua isi yang ada pada komputer. Mengetahui keadaan komputer tersebut aman atau tidaknya dari serangan virus.

Hasil scanning dengan menggunakan 4 anti virus yang berbeda. Percobaan yang dilakukan menghasilkan hasil yang berbeda. Dengan menggunakan anti virus Avast dan AVG, file yang dibuat dengan nama parampaa.exe berhasil terdeteksi sebagai virus dengan tingkat keparahan yang tinggi, terdeteksi sebagai *malware* yang berjenis kuda troya (*Trojan horse*).

TABEL IV
TABEL HASIL PENANGANAN ANTI VIRUS TERHADAP *MALWARE NJRAT*

Nama Virus	Nama Anti Virus	Deteksi	Status
Parampaa.exe	Avast	Terdeteksi	*High*
Parampaa.exe	AVG	Terdeteksi	*High*
Parampaa.exe	Smadav	Tidak	-
Parampaa.exe	Avira	Tidak	-

Dua anti virus lainnya yaitu Smadav dan Avira file parampaa.exe tidak terdeteksi sebagai *malware*, karena oleh anti virus ini tidak terjadi kesamaan signature *malware*, maka hasilnya file ini baik-baik saja.

Berikut kerugian yang ditimbulkan oleh *malware Njrat*:

- *File* yang diserang dapat dihapus
- Hak akses pada PC target dapat diambil alih oleh *attacker*
- Mendapatkan tangkapan gambar target tanpa diketahui
- Mendapatkan *username* dan *password* dari PC target

Berikut dampak dari perilaku *malware Njrat:*

- PC cenderung berjalan semakin lambat
- Data rahasia seseorang dapat diketahui juga dapat dicuri oleh *attacker*
- *File* pada PC target akan menjadi rusak bahkan hilang
- Dapat *login* aplikasi yang sedang berjalan pada PC target
- PC target dapat dikendalikan oleh *attacker*

ISSN 2460-0741

V. KESIMPULAN DAN SARAN

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*)

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

REFERENSI

[1]. Mathur, K. Teknik pendeteksi dini dan analisis mallware. *Jurnal internasional software engginerring, 2013.*

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

[3]. Elanda, A. Tren *malware* dan teknologi deteksi. In A. Elanda, *Tren Malware dan teknologi deteksi.* Bandung. 2015.

[4]. Agung, M. F. *Jenis-jenis Mallware dan pencegahannya*. Bogor. 2011.

[5]. Gandotra, B., & Sanjeev, D. Analisis dan klasifikasi mallware. *Jurnal internasional*. 2014.

[6]. Agung, M. F. (2011). Konsep dasar *malware* analisis. *Jurnal Teknik informatika* .

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

[8]. Babu. Metodologi Penelitian pada pertambangan Web untuk deteksi Mallware. *Jurnal Internasional*. 2014.

ISSN 2460-0741