JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 4 Nomor. 2, Oktober 2019
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

PENINGKATAN KEAMANAN DATA TERHADAP SERANGAN *REMOTE ACCESS TROJAN* (RAT) PADA *CYBERCRIMINAL* MENGGUNAKAN METODE *DYNAMIC STATIC*

NANNY[1], YUDI PRAYUDI[2], IMAM RIADI[3]
Program Studi Teknik Informatika[1,2],
Universitas Islam Indonesia, Indonesia
[3)]Program Studi Sistem Informasi,
Universitas Ahmad Dahlan, Indonesia

E-mail : 13917154@students.uii.ac.id[1],
prayudi@uii.ac.id[2]
imam.riadi@is.uad.ac.id[3]

ABSTRAK

Remote Access Trojan (RAT) merupakan program *malware* jenis *Trojan Horse* yang mencakup pintu belakang (*backdoor*) untuk kontrol administratif atas komputer target. Penelitian ini melakukan skenario penyerangan untuk mengetahui cara kerja serangan RAT, melakukan serangan RAT dan meningkatkan keamanan data dari serangan RAT melalui simulasi dan manfaat dari MikroTik. Program *malware* jenis trojan njRAT sebagai media simulasi antara laptop attacker (penyerang) dan laptop victim (korban). Metode yang digunakan adalah metode *Dynamic Static,* dimana dalam pengaturan jaringan dengan menentukan IP Address, yaitu menghubungkan 2 (dua) MikroTik Router, Router RB951Ui Versi 6 di laptop attacker dan Router RB931-2nD di laptop korban. Beberapa tools forensik yang digunakan diantaranya Wireshark, Disk Investigator, Virus Total sebagai proses analisis.

Kata kunci : *firewall, njRAT, Remote Access Trojan (RAT), router*

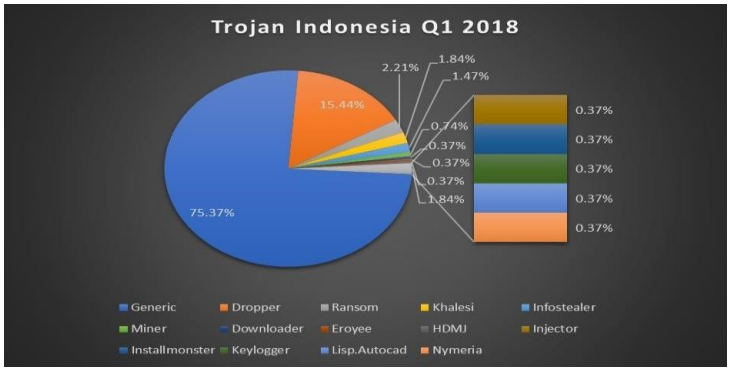
I. PENDAHULUAN

Tingginya penyebaran internet menciptakan kejahatan tak hanya terjadi dalam dunia nyata, tetapi merambah ke dunia maya yang sering disebut sebagai *cyber 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. 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

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 4 Nomor. 2, Oktober 2019
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

terkandung siapa saja yang dapat dipertanggungjawabkan secara pidana. *Malware* didefinisikan sebagai semua perangkat lunak jahat, program komputer jahat, atau perangkat lunak jahat, seperti virus (komputer), *trojans*, *spyware*, dan *worm*. 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*. *Backdoor* merupakan metode yang digunakan untuk melewati autetifikasi normal *(login)* dan berusaha tidak terdeteksi. Statistik perkembangan Trojan tahun 2018 yang merujuk pada Gambar 1.



Gambar 1. Statistik Perkembangan Trojan 2018 (*Sumber : Vaksin.com*)

Berdasarkan teknik dan metode yang digunakan, terdapat beberapa jenis *Trojan Horse*, antara lain: (Eko Indrajit, 2008)

a. *Remote Access Trojan (RAT)*, kerugian yang ditimbulkan adalah komputer korban dapat diakses secara *remote*;
b. *Password Sending Trojan*, kerugian yang ditimbulkan adalah *password* yang diketik oleh komputer korban akan dikirimkan melalui email tanpa sepengetahuan dari korban serangan;
c. *Keylogger*, kerugian yang ditimbulkan adalah ketikan atau input melalui keyboard akan dicatat dan dikirimkan via email kepada *hacker* yang memasang *keylogger*;
d. *Destructive Trojan*, kerugian yang ditimbulkan adalah file-file yang terhapus atau hard disk yang terformat;
e. *File Transfer Protocol (FTP) Trojan*, kerugian yang terjadi adalah dibukanya port 21 dalam sistem komputer tempat dilakukannya download dan upload file;

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 4 Nomor. 2, Oktober 2019
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

f. *Denial of Service (DoS) Trojan,* jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber *(resource)* yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar, sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

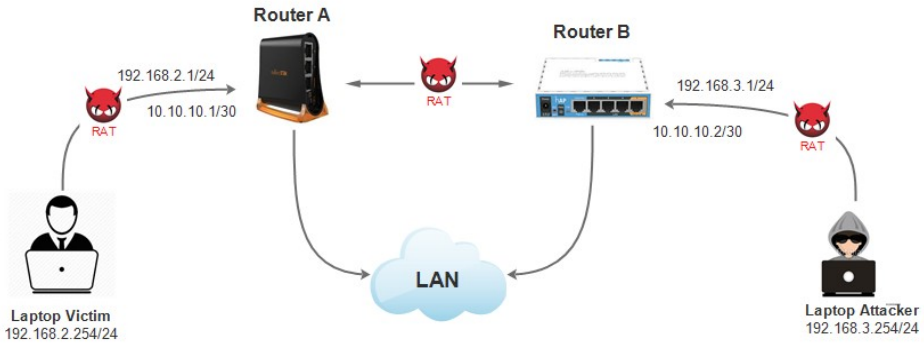
g. *Software Detection Killer*, kerugiannya dapat program-program keamanan, seperti zone alarm, anti-virus, dan aplikasi kemanan lainnya; dan

h. *Proxy Trojan*, kerugian yang ditimbulkan adalah di- "settingnya" komputer korban menjadi "*proxy server*" agar digunakan untuk melakukan "*anonymous telnet*", sehingga dimungkinkan dilakukan aktivitas belanja online dengan kartu kredit curian dimana yang terlacak nantinya adalah komputer korban, bukan komputer pelaku kejahatan.

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. Investigator dapat memasang sniffer paket untuk menangkap lalu lintas yang berjalan di jaringan dan menganalisisnya. (Hermaduanti & Riadi, 2016)

II. METODE PENELITIAN

Cara kerja serangan RAT dibahas dalam rangkaian topologi serangan *Remote Access Trojan* (RAT) yang ditujukan pada Gambar 2.



Gambar 2. Topologi Serangan RAT

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 4 Nomor. 2, Oktober 2019
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

IP address (Internet protokol address) adalah metode pengalamatan pada jaringan komputer dengan memberikan sederetan angka pada komputer (host), router atau peralatan jaringan lainnya.(Bhayangkara, 2014)

Berdasarkan topologi penelitian ini bagaimana serangan program *malware* jenis RAT terjadi diawali dari tindakan pelaku *attacker* yang melakukan penyerangan melalui jaringan LAN *(Local Area Network)* dengan mengirimkan program *malware* jenis RAT melalui via email, bisa lewat *file sharing,* atau media sosial dengan cara menanamkan program *malware* tersebut ke Laptop korban yang terhubung dengan jaringan router. Laptop korban akhirnya terjangkit yang mengakibatkan Laptop korban bisa diakses dalam jaringan LAN.

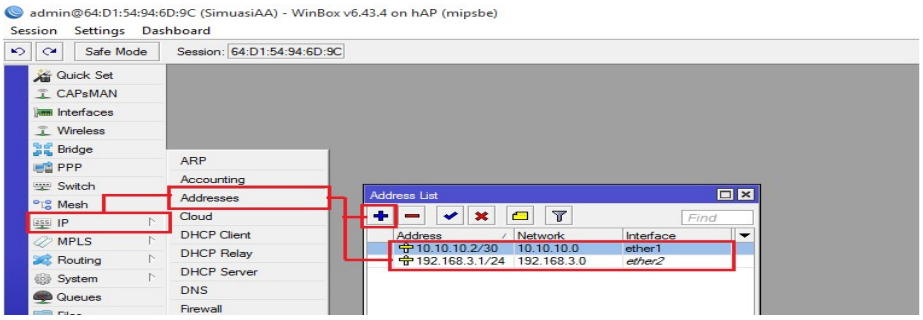
III. HASIL DAN PEMBAHASAN

a. Settingan Jaringan Router

Mikrotik pada hardware berbasis komputer komputer pribadi (PC) yang dikenal dengan stabilitas mereka, kontrol kualitas, dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses ini (routing). (Mazdadi, Riadi, & Luthfi, 2017)

Konfigurasi yang dilakukan ke sistem dengan menggunakan aplikasi WinBox versi 3.18. Dalam simulasi ini menggunakan 2 (dua) buah laptop yaitu laptop attacker (penyerang) dan laptop korban, juga menggunakan 2 (dua) buah MikroTik router jenis Router RB931-2nD sebagai Router A untuk laptop attacker dan RB951Ui Versi 6 untuk laptop attacker sebagai Router B untuk laptop korban. Settingan dimulai dengan aplikasi Winbox dengan membuat IP Address di laptop attacker dengan alamat IP Address adalah 192.168.3.1 dan IP Address pada laptop korban adalah 192.168.2.1 seperti rujukan pada Gambar 3.

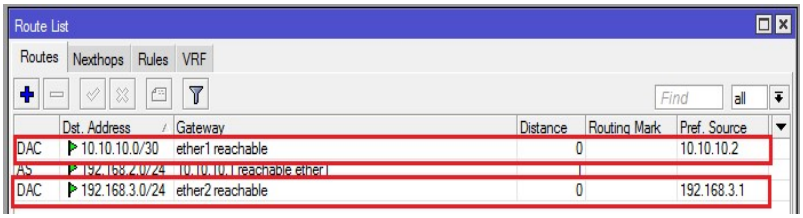
JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 4 Nomor. 2, Oktober 2019
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id



Gambar 3. Setting IP Address Laptop Attacker

Tahap selanjutnya kita akan menyambungkan ke IP router baik laptop korban dengan Destination-Address 192.168.3.0/24, Gateway 10.10.10.2 dan laptop attacker dengan Destination-Address 192.168.2.0/24, Gateway 10.10.10.1. Statis adalah tampilan kode aktual untuk mendapatkan pemahaman yang lebih baik tentang malware, sementara dinamika adalah untuk menganalisis perubahan ketika malware dieksekusi. (Usman, Prayudi, & Riadi, 2017)

Tahap berikutnya melakukan settingan jaringan IP Router baik pada Router A dengan IP Route 10.10.10.1/30 sebagai ether1 status DAC (*Dynamic Active Connected*) dan IP Route 192.168.2.1/24 sebagai ether2 status DAC dan Router B dengan IP Route 10.10.10.2/30 sebagai ether1 status DAC (*Dynamic Active Connected*) dan IP Route 192.168.3.1/24 sebagai ether2 status DAC. DAC artinya menunjukkan ether yang aktif dan mempunyai IP Route, sedangkan AC (*Active Static*) artinya ada sebuah *route static* yang ditujukan dalam Gambar 4.



Gambar 4. Hasil Setting IP Route

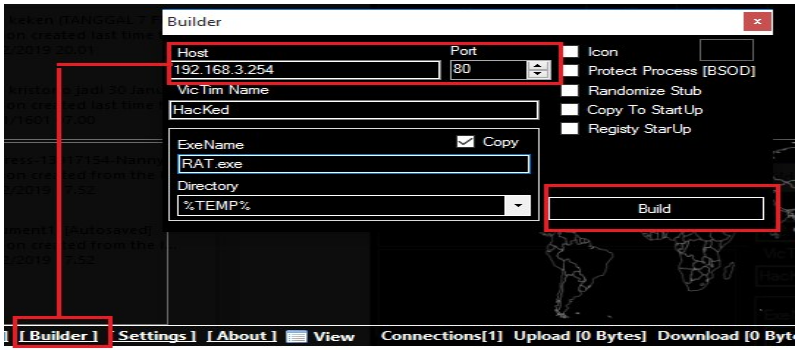
Setting jaringan diketahui dengan hasil yang dilakukan koneksi lokal dengan membuka Command Prompt lalu ping IP laptop baik laptop korban dan laptop *attacker*. Jika statusnya udah *reply* berarti settingannya sudah bisa diakses IP Address secara *static*. Selanjutnya dilakukan penyesuaian pada terminal di Winbox untuk mengetahui status daripada IP Host setelah dilakukan pembuatan IP Route di Laptop attacker. Untuk

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 4 Nomor. 2, Oktober 2019
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

mengetahui trafic port masing-masing jaringan dari Router A dan Router B melalui tab Interface List di Winbox, informasinya menunjukkan port di ether1 dan ether2 telah berjalan (Running) dalam kecepatan kbps port.

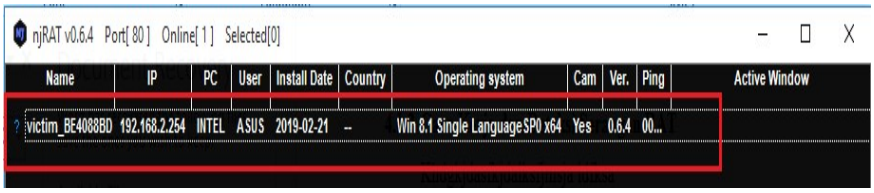
b. Simulasi *Remote Access Trojan (RAT)*

Mengetahui cara kerja dan deteksi serangan RAT dengan melakukan pembuatan *malware* jenis trojan dengan menggunakan tools njRAT v0.6.4. Tahap pembuatan *malware* jenis trojan ini dilakukan di laptop attacker dengan menggunakan alamat IP Address Host 192.168.3.254 dengan port 80 dan nama **Victim Hacked** dengan nama file .exe adalah **sss.exe**, yang ditujukan pada Gambar 5.



Gambar 5. Hasil Builder RAT

Tahap selanjutnya file **sss.exe** di copy ke laptop korban dengan double klik di desktop korban, maka akan tampil di tools njRAT dengan nama **?victim_BE4088BD**, IP Address 192.168.2.254, jenis PC Intel, User Asus, Tanggal Install tercantum dan informasi Operating System, yang merujuk pada Gambar 6.

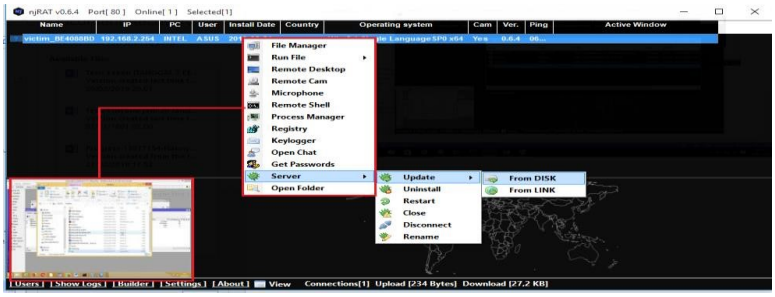


Gambar 6. Proses RAT Berhasil di Remote

Analisis *Remote Access Trojan* (RAT) dalam hal ini jenis *malware* njRAT pada laptop korban setelah berhasil di ambil alih oleh laptop attacker yang bisa meremote laptop korban, bukti digital yang didapatkan berupa data-data File Manager, Run File, Remote Desktop, Remote Cam, Microphone, Remote Shell, Process Manager, Registry, Keylogger, Open Chat, Get Password, Server (Update, Uninstall, Restart, Close,

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 4 Nomor. 2, Oktober 2019
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

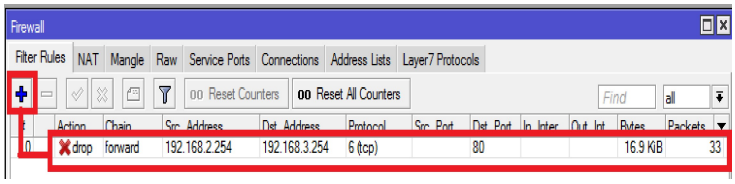
Disconnect, Rename), dan Open Folder. Hasil bukti digital Laptop Korban yang merujuk pada Gambar 7.



Gambar 7. Hasil Bukti Digital Laptop Korban

c. Konfigurasi Keamanan Data

Keamanan data laptop korban yang perlu dilakukan adalah memasang firewall di IP Address laptop korban dengan cara menentukan IP Address di aplikasi Winbox → IP → Firewall dengan IP Address Src Address : 192.168.2.254 adalah IP Address laptop korban, Destination Address 192.168.3.254 adalah IP Address laptop attacker dengan Destination Port 80 berdasarkan lokasi port yang bisa diakses oleh njRAT dan status di tab Action **drop**, terlihat pada Gambar 8.



Gambar 8. Pembuatan *Firewall Traffic*

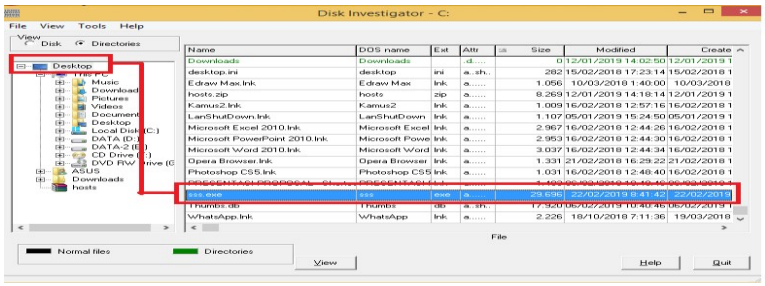
d. Hasil Pengujian *Remote Access Trojan (RAT)*

Pengujian dilakukan untuk membuktikan bahwa apakah pemblokiran *firewall traffic* berhasil atau tidaknya, maka dilakukan kembali pengujian penyerangan ke laptop korban dengan melakukan penyerangan dari laptop attacker ke laptop korban. Kemudian dilakukan pembuktian ternyata laptop korban sudah tidak bisa di deteksi lagi melalui file *malware* jenis njRAT, karena otomatis tidak bisa lagi menarik data-data atau meremote laptop korban.

Pengujian selanjutnya dilakukan menggunakan beberapa tool forensik diantaranya tools Disk Investigator yang membuktikan bahwa didalam disk terdapat file-file yang merupakan program *malware* jenis berbahaya yang berekstensi .exe. Disk Investigator

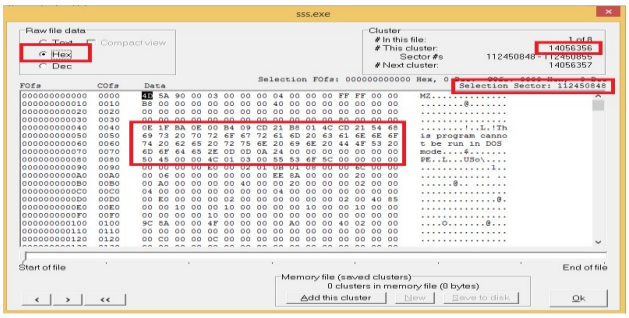
JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 4 Nomor. 2, Oktober 2019
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

menunjukkan file mana yang terdapat *malware* dengan memberikan tanda 2 (dua) warna yaitu hijau menunjukkan direktori atau folder dan warna hitam menunjukkan sebuah file. Jenis *malware* yang terjangkit di laptop korban dengan nama file **sss.exe** dengan size **29,696** sector, tanggal dan waktu (*timestamp*) penyerangan terjadi (*Modifed/Create*). Analisis Tools Disk Investigator merujuk pada Gambar 9.



Gambar 9. Analisis Tools Disk Investigator

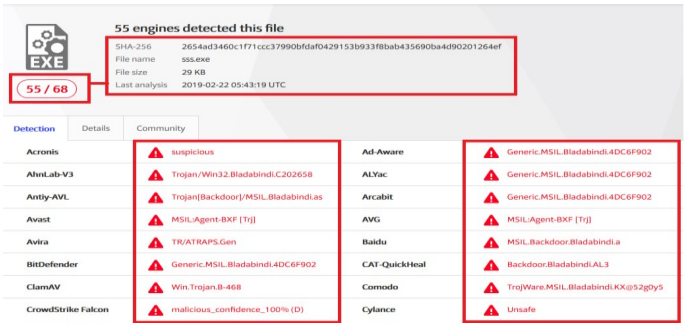
Untuk lebih jelas lagi diketahui dalam bentuk Heksadecimal di Raw file data yang diinformasikan dalam bentuk Cluster disk file *malware* tersebut yang dipaparkan dalam Gambar 10.



Gambar 10. Analisis Hasil Hexadecimal

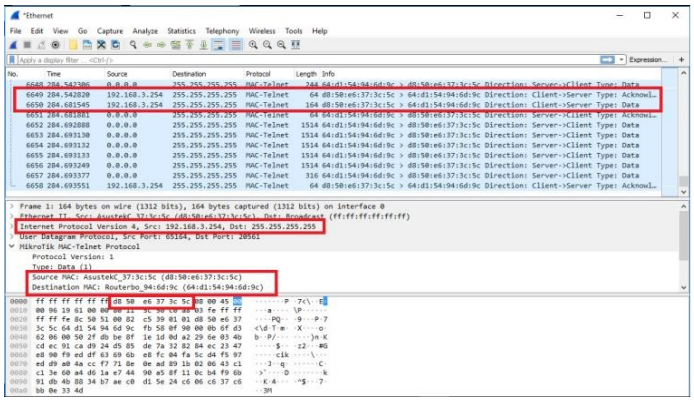
Selanjutnya analisis pada tools Virus Total yang membuktikan bahwa terdapat 55 file EXE jenis *malware* yang terdapat dalam file **sss.exe** yang berhasil dideteksi yang diinformasikan dalam Gambar 11.

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 4 Nomor. 2, Oktober 2019
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id



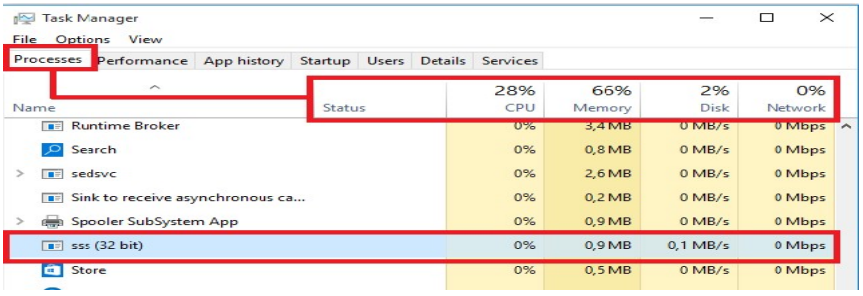
Gambar 11. Hasil Analisis Virus Total

Hasil analisis selanjutnya dengan menggunakan aplikasi Wireshark yang memberikan informasi bagaimana akses penyerangan terjadi. Dalam Wireshark terlihat alamat IP Address yang menyerang laptop korban dengan Mikrotik Router yang tanpa akses internet. Hasil analisis penyerangan ditujukan pada Gambar 12.



Gambar 12. Hasil Analisis Penyerangan

Hasil pada tahap pengujian mengenai keamanan pemblokiran *firewall traffic* dapat dilihat pada gambar pada proses Task Manager yang ditujukan pada Gambar 13.



Gambar 13. Proses Task Manager

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 4 Nomor. 2, Oktober 2019
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

IV. KESIMPULAN

1. Simulasi pada Laptop Attacker dan Laptop Korban yang dilakukan, maka dapat ditarik kesimpulan bahwa deteksi serangan RAT jenis *malware* njRAT, dari proses penyerangan yang dilakukan dapat diperoleh informasi bahwa serangan RAT memiliki karakteristik yang dapat mengendalikan atau meremote laptop korban yang bisa menghapus data, *disconnect* laptop, pengambilan *log data*, mengganti nama *file/folder*, dapat merubah data-data korban, mengetahui *password*, mengetahui aktivitas yang dilakukan pada laptop korban.
2. Hasil penelitian ini membuktikan bahwa serangan *malware* jenis njRAT ini bisa dilakukan tanpa akses internet dan bukti digital di laptop korban. Simulasi ini memberikan pembelajaran bahwa MikroTik Router dapat membantu mencegah penyerangan program *malware* jenis njRAT ini melalui pemblokiran paket data dengan menentukan *firewall traffic*.

V. DAFTAR PUSTAKA

Bhayangkara, F. J. & I. R. (2014). Implementasi Proxy Server Dan Load Balancing Menggunakan Metode Per Connection Classifier (Pcc) Berbasis Mikrotik. *Implementasi Proxy Server Dan Load Balancing Menggunakan Metode Per Connection Classifier (Pcc) Berbasis Mikrotik*, *2*(2), 133–134. Retrieved from http://journal.uad.ac.id/index.php/JSTIF/article/view/2729

Chandra, S., Hutauruk, Y., Yulianto, F. A., & Satrya, G. B. (2016). Malware Analysis Pada Windows Operating System Untuk Mendeteksi Trojan Malware Analysis on Windows Operating System To Detect Trojan, *3*(2), 3590–3595.

Eko Indrajit, P. R. (2008). *Aneka Ragam Serangan di Dunia Maya*.

Hermaduanti, N., & Riadi, I. (2016). Automation framework for rogue access point mitigation in ieee 802.1X-based WLAN. *Journal of Theoretical and Applied Information Technology*, *93*(2), 287–296.

Usman, L., Prayudi, Y., & Riadi, I. (2017). Ransomware analysis based on the surface, runtime and static code method. *Journal of Theoretical and Applied Information Technology*, *95*(11), 2426–2433.

Kurniawan, A.; Riadi, I.; Luthfi, A. (2017). Forensic Analysis and Prevent of Cross Site Scripting in Single Victim Attack Using Open Web Application Security Project (Owasp). *Search.Ebscohost.Com*, *95*(6), 1363–1371.

Mazdadi, M. I., Riadi, I., & Luthfi, A. (2017). Live Forensics on RouterOS using API Services to Investigate Network Attacks. *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(2), 406–410.