OPTIMALISASI PENGGUNAAN *CMD* DAN *SYSINTERNALSUITS* SEBAGAI MALWARE DETECTION

Tri Yusnanto[1)],**Deny Lestiono**[2)]

[1)] *Manajemen Informatika STMIK Bina Patria*
[2)] *Manajemen Informatika STMIK Bina Patria*
Email : yusnanto@gmail.com[1)], DenyLestiono@gmail.com[2)]

Abstract

In this paper the author presents cmd optimization methods assisted by sysinternalsuits to hunt or search for malware on a computer that is running, to find a file or application that is considered suspicious in a network security. In using CMD, the cd \, dir, netstat commands are used while the sysinternalsuit runs tcpview, Rammap and process explorer to scan or look for files that are considered suspicious, especially malware hiding in directories or in programs that are running because the file usually runs after infect the victim's computer. By using this tool, it is expected to be able to help in the search for malware that we are looking for that is considered suspicious.

Keywords : cmd, tcpview, Rammap, proses explorer, malware

Abstrak

Dalam penelitian ini penulis meyajikan cara pengoptimalan cmd dibantu sysinternalsuits untuk memburu ataupun mencari malware didalam komputer yang sedang berjalan, guna mencari sebuah file ataupun aplikasi yang danggap mencurigakan didalam sebuah keamanan jaringan. Dalam menggunakan CMD digunakan perintah-perintah cd\, dir, netstat sedangkan pada sysinternalsuit dijalankan *tcpview, Rammap dan proses explorer* untuk memindai atau mencari file yang dianggap mencurigakan terutama malware yang bersembunyi didalam direktori ataupun didalam program yang sedang berjalan karena file tersebut biasanya kan berjalan setelah meninfeksi computer korban. Dengan mengguanakn *tool* tersebut diharapkan dapat membantu dalam pencarian malware yang kita cari yang danggap mencurigakan tersebut.

Kata Kunci:cmd, tcpview, Rammap, proses explorer, malware

1. Pendahuluan

Keamanan jaringan merupakan sebuah issu yang sangat cepat tumbuh berkembang seiring dengan cepatnya orang mengetahui kelemahan dari sebuah sistem komputer kemudian menyerangnya. Padahal Komputer merupakan alat modern yang tidak bisa lepas dari kehidupan kita sehari-hari. Mulai darikita dilingkungan keluaraga pekerjaan di kantor, multimedia digital, bahkan hiburan yang sela ini kita lihat ataupun kita dengarkan. Dewasa ini perkembangan sebuah komputer semakin berkembang dan masih akan terus berkembang tanpa batas.

Kita sebagai manusia mau tidak mau harus mengikuti perkembangan kemajuan teknologi khususnya bidang komputerisasi agar kita tidak termakan oleh alat yang dibuat oleh manusia untuk mempermudah dalam pekerjaan kita. komputer mengalami perubahan signifikan dari masa ke masa, baik dari bentuknya maupun spesifikasinya. Resiko yang kemungkinan bisa terjadi pada komputer seperti kerusakan – kerusakan dari bagian periperhal itu sendiri misal rusaksebuah perangkat hardisk, desktop terkena virus sehingga yang dapat menyebabkan hilangnya data, kebocoran data, rusaknya data dan resiko – resiko lainnya. Malware ataupun virus adalah program komputer yang diciptakan

oleh seseorang yang mempunyai maksud dan tujuan utama adalah mencari kelemahan dari suatu software ataupun aplikasi. Pada umumnya Malware diciptakan untuk membobol dan juga merusak suatu software atau operating sistem guna memperoleh sesuatu.

Malware menjadi ancaman yang sangat berbahaya karena mereka dapat bersembunyi didalam computer yang berjalan dan mengancam setiap saat, bahkan dapat berkembang biak sendiri dalam jangka waktu tertentu. Malware, merupakan salah satu ancaman utama di Internet saat ini. Sebuah program berbahaya, mulai dari virus komputer klasik seperti worm pada Internet dan jaringan, yang menargetkan pada sistem komputer yang terhubung ke dalam Internet. Ancaman ini didorong oleh kejahatan industri yang dimana menggunakan jaringan sebuah internet untuk tujuan ilegal, seperti mendistribusikan pesan spam yang sudah disusupkan program ilegal atau mengumpulkan data yang sangat penting atau rahasia (Franklin et al, 2007;. Holz et al, 2009.). Sayangnya, peningkatan jumlah dan keragaman malware membuat teknik keamanan klasik, seperti scanner anti-virus, tidak efektif dan, sebagai akibatnya, jutaan host di Internet saat ini terinfeksi, dengan perangkat lunak berbahaya (Microsoft, 2009; Symantec, 2009).

Oleh karena itu untuk melindungi dari malware di internet, pengembang perangkat lunak anti malware sangat bergantung pada analisis secara otomatis untukk menemukan varian baru guna merancang tindakan yang sesuai pertahanan yang di inginkan. menganalisis pergerakan sebuah malware merupakan sebuah kerja yang sangat susah, karena seorang pembuat malware sering kali menggunakan teknik-teknik tertentu guna mengelabuhi dari antivirus ataupun anti malware, seperti menggunakan kode biner, enkripsi, atau kod- kode tertentu ,tujuan ya hanyalah untuk menghalangi analisis dari gerak gerik yang mencurigakan.

Teknik ini sangat efektif terhadap analisis statis binari (Linn dan Debray, 2003; Christodorescu dan Jha, 2003; Kruegel et al., 2005;). Analisis dinamis saat run-time memungkinkan pemantauan perilaku malware. Oleh karena itu, sejumlah besar penelitian telah memfokuskan pada pengembangan alat untuk pengumpulan dan pemantauan malware (, Pouget et al, 2005;. Leita et al., 2006; Willems et al., 2007; Lanzi et al., 2009). karena sangat cepatnya perkembangan teknologi terutama yang berbasis pada internet maka kita harusselalu waspada pada setiap langkah baik dalam browsing atuapun saat mengsinstall suatu software,terutama software yang free download kita harus extra hati-hati. contoh dari *malware* adalah *worm, wabbit, keylogger, browser hijacker, trojan horse, spyware, backdoor, dialer, exploit dan rootkit* dsb.

2. Kajian Literatur

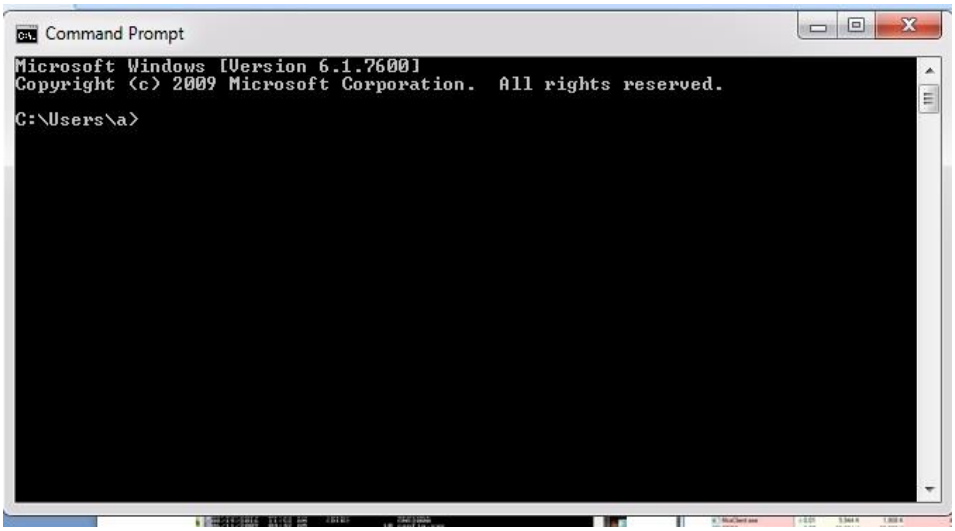
Dari kejian literature dijelaskan bahwa Malware adalah masalah pada keamanan komputer karena banyak sistem komputasi yang terhubung. Berbagai macam malware telah meningkat selama bertahun-tahun dan malware baru telah muncul, di mana varian baru mampu menghindari deteksi yang konvensional. Salah satu metode yang menjanjikan yang digunakan untuk mendeteksi malware adalah teknik *machine learning* (ML) (Ban Khammas .2018). Metode berdasarkan kinerja sebuah mesin sangat populer dalam mendeteksi malware yang tidak dikenal dan juga varian lainya yang mungkin berjalan didalamnya (Miao, Q., Liu, J., Cao, Y., Song, J. 2015). Karena varian malware baru berisi pola yang mirip dengan malware yang diamati, teknik mempelajari kinerja mesin dapat digunakan untuk mengidentifikasi malware baru yang mungkin berjalan didalam mesin tersebut (Khammas, B. M., Monemi, A., Joseph, S. B., Ismail, I., Mohd Nor, S., Marsono, M. N. 2015). Disisni penulis menggunakan pendeteksi bawaan micosoft sendiri yaitu CMD dan utilities lainya berupa *Sysinternalsuit* .

A. CMD

Command Prompt merupakan baris perintah pada aplikasi yang tersedia untuk sistem operasi Windows.dan kalu pada linux bias disebut sebagai root atau pemegangkendali penuh sebagai administrator. *Command Prompt* digunakan untuk menjalankan perintah ataupun masukan. Sebagian besar dari perintah yang digunakan untuk mengotomatisasi tugas-tugas melalui script dan file batch,dengan melakukan fungsi administratif m, dan untuk memecahkan masalah dan memecahkan beberapa jenis masalah yang biasa pada Windows. Command Prompt secara resmi disebut juga sebagai Windows Command Processor tetapi juga kadang-kadang disebut shell command atau dengan cmd.exe nama file-nya. Command Prompt tersedia pada setiap sistem operasi yang berbasis Windows NT yang meliputi Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, serta Windows Server 2012/2008/2003.

Sedangakan Windows Power Shell, merupakan baris perintah interpreter lebih maju /berkembang ini tersedia dalam versi Windows terbaru, dan terdapat berbagai cara dalam mengeksekusi perintah yang tersedia di Command Prompt. Oleh karena itu diharapkan Windows PowerShell dapat menggantikan Command Prompt dalam versi masa depan pada sebuah OS Windows.

Catatan: Command Prompt kadang-kadang salah disebut sebagai "DOS prompt" atau sebagai MS-DOS itu sendiri. Command Prompt adalah program Windows yang mengemulasi banyak kemampuan baris perintah yang tersedia di MS-DOS tetapi tidak benar-benar MS-DOS.



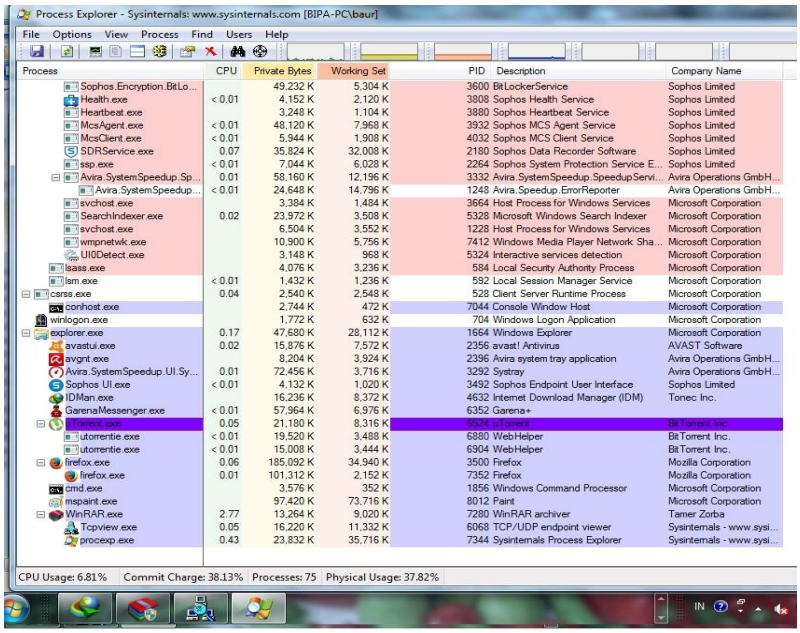
Gambar 1. Saat menjalankan CMD

B. SYSINTERNAL SUIT

Sysinternalsuit merupakan seperangkat alat atau set aplikasi yang terdapat pada Windows yang dapat didownload secara gratis dari situs web Microsoft TechNet. Sofware ini semua portabel, yang berarti bahwa kita tidak perlu menginstalnya, kita dapat menyimpanya di flash disk dan menggunakannya pada PC manapun. Bahkan, kita benar-benar dapat menjalankan mereka tanpa menginstal melalui *SysInternals* yang. Alat ini terdapat beberapa macam tool termasuk utilitas seperti *Process Explorer*, yang banyak seperti Task Manager dengan sejumlah fitur tambahan, atau Proses Monitor, yang memonitor PC kita untuk filesystem, registry, atau bahkan aktivitas jaringan dari hampir semua proses pada sistem kita. Autoruns membantu Kita berurusan dengan

proses startup. *TCPView* menunjukkan apa yang terhubung ke dalam di internet, dan ada banyak alat yang bisa dijalankan dari baris perintah untuk membantu Kita menangani proses, layanan, dan lain sebagainya.

Alat ini digunakan oleh setiap admin komputer terkemuka jika seumpama kita ingin memisahkan gandum dari sekam, hanya meminta admin untuk perbaikan PC lokal kita menggunakan *Proses Explorer*. Jika kita tidak memiliki petunjuk, maka kiata dapat meminta bantuan ke pada Microsoft techNet. Dengan menggunakan alat tersebut mungkin kita ingat waktu itu sony mencoba untuk menanamkan rootkit ke dalam cd musik mereka? utilitas sysinternals yang pertama kali mendeteksi masalah tersebut, dan sysinternals yang membuat pengumumankepada media masa. pada tahun 2006, microsoft akhirnya membeli perusahaan di belakang sysinternals, dan mereka terus memberikan utilitas gratis di situs web mereka

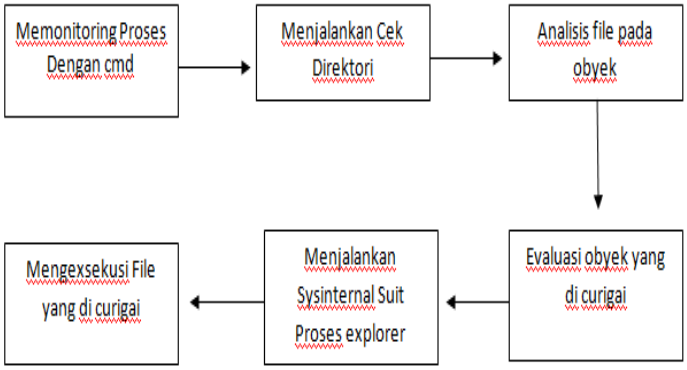


Gambar 2. Saat Menjalankan Sysinternalsuit

3. Metode Penelitian

Metode merupakan suatu prosedur atau cara untuk mengetahui sesuatu, yang mempunyai langkah-langkah sistematis. Sedangkan metodologi ialah suatu pengkajian dalam mempelajari peraturanperaturan suatu metode. Jadi, metodologi penelitian ialah suatu pengkajian dalam mempelajari peraturan-peraturan yang terdapat dalam penelitian (Husaini dan Purnomo, 2001: 42)

Jenis penelitian ini adalah eksperimental didalam penelitian ini yang dilakukan adalah melakukan pengamatan serta menganalisa komputer yang terkena malware.. Komputer yang dipakai untuk program ini menggunakan komputer dengan spesifikasi *Intel Pentium core i5 2320 Processor* 3.00 GHz, RAM 4 GB, dan AMD *Radeon* HD 5500 *memory size* 2048 MB.

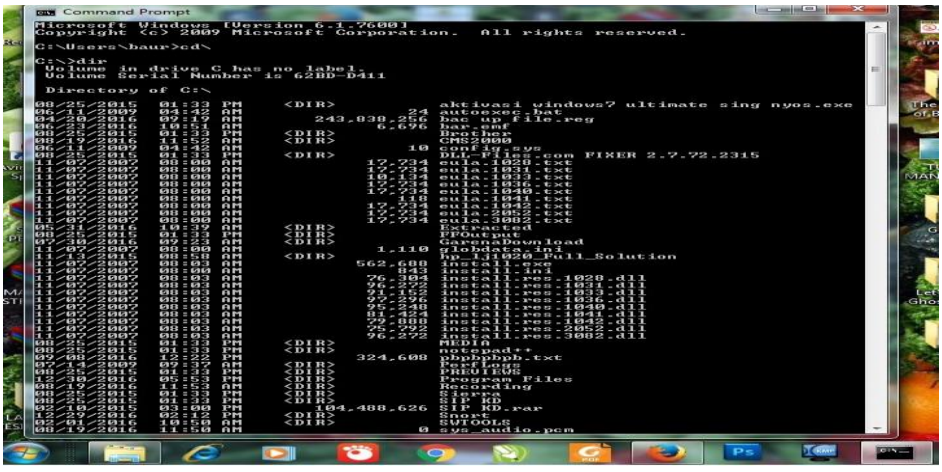


Gambar 3. kita dapat menggambarkan metode sebagai berikut:

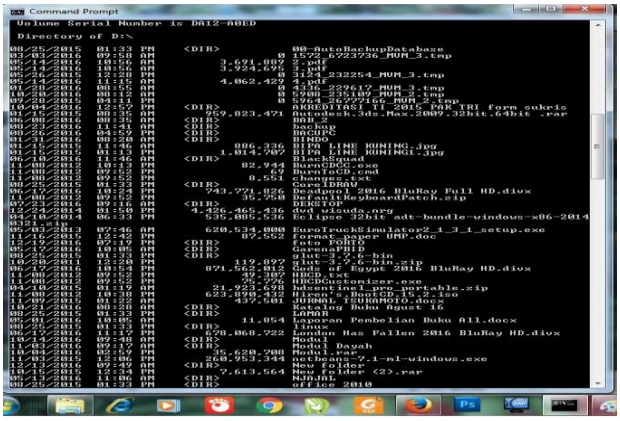
1. Monitoring dengan CMD
   Merupakan aktifitas yang dilakukan untuk memberikan informasi tentang sebab dan akibat dari suatu gejala tertentu dengan menggunakan CMD
2. Menjalankan Cek direktori
   Dengan menjalankan menjalankan cek direktori makan akan terlihat baik file yang terhiden atau yang tidak
3. Analisis File
   Merupakan cara untuk menidentivikasi file yang dinilai bermasalah atau yang patut dicurigai sebagai *malware*
4. Evaluasi File Yang dicurigai
   Evaluasi merupakan suatu proses yang sistematis untuk menentukan atau membuat keputusan apakah file tersebut malware atau bukan
5. Menjalankan Sysinternalsuit
   Dengan menjalakan program *sysinternalsuit* untuk pengecekan lebih lanjut
6. Mengeksekusi File yang dicurigai
   Ini merupakan proses penghapusan file yang dipastikan malware tersebut

4. Hasil dan Pembahasan

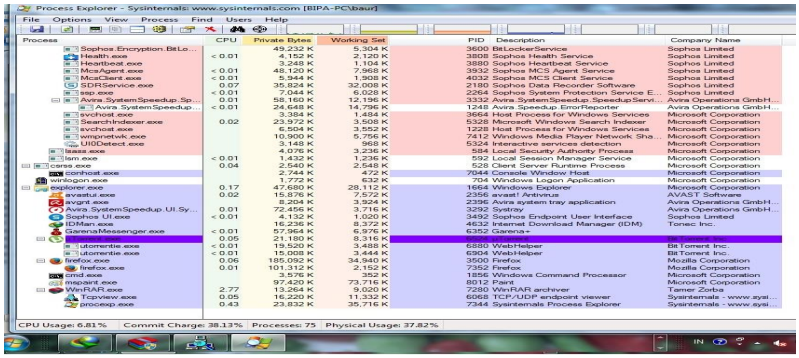
Di mana kita mulai memonitor dengan menjalankan perintah comand prompt langsung lewat acsesoris, dengan ini kita hampir sama kalau pada linux kita masuk kedalam root untuk menjalankan sebuah eksekusi sebelum menemukan sebuah file ataupun data yang kita cari.



Gambar 4. pada saat manjalan CMD pada direktori c utuk di anallisa apakah ada file yang mencurigakan

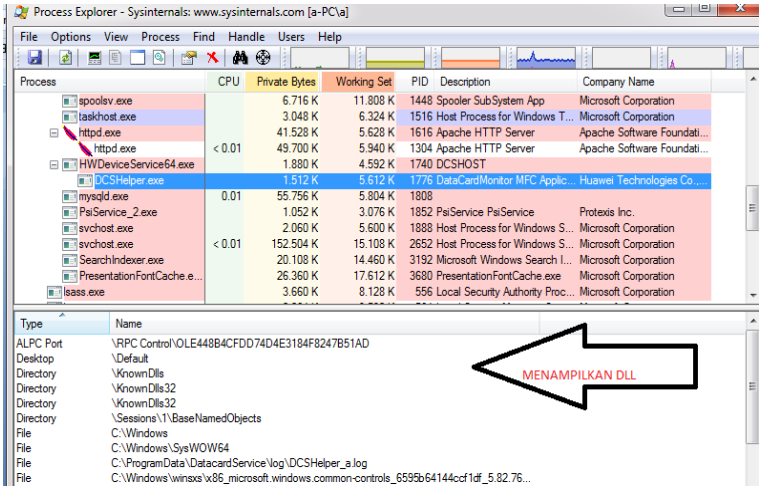


Gambar 5. kemudian dilanjutkan pada direktori d utuk di anallisa apakah ada file yang mencurigakan dan seterusnya sampai semua disk direktori dicek satu satu



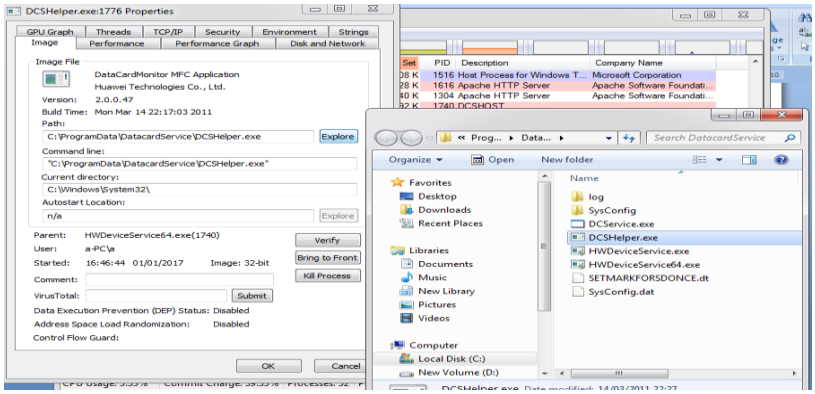
Gambar 6. di lanjutkan pada penggunaan sysinternal suit yaitu pada proses explorer

Dengan menggunakan Proses explorer kita dapat mengetahui apa yang sedang berjalan pada memori,dan juga pada network .dengan begitu apabila ada file yang dianggap mencurigakan kita dapat meneruskan memeriksanya dengan cara menepatkan kursor pada proses yang berjalan tadi dengan cara klik,maka akan tampil



Gambar 7. Menampilkan dll

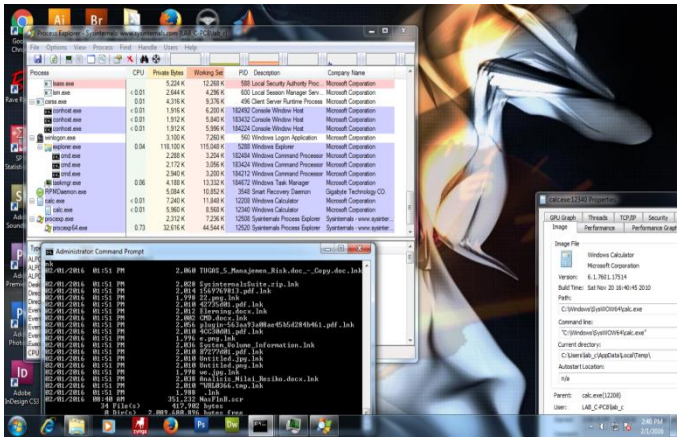
Untuk menampilakan dll atau proses yang berjalan pada sebuah proses maka kita pilh task bar view kemudian kita pilah show lower pine atau pakai short cut ctrl –L.Setelah memastikan bahwa proses tersebut benar-benar mencurigakan maka kita double klik pada proses tersebut .



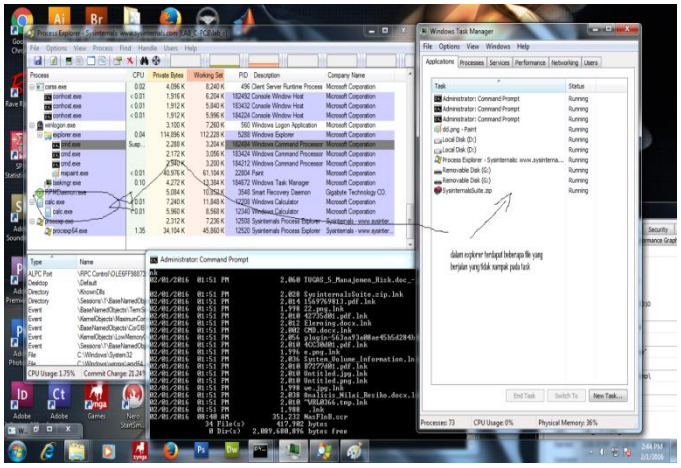
Gambar 8. Rinci file dengan Explorer

Dengan begitu kita akan lebih rinci masuk kedalam file yang berjalan dan akan terlihat beberapa file yang berada didalam folder tersebut.dari situ kitabisa memilih salah satu file terutama yang berexktensi dll untuk kemudian kita temukan apakah file tersebut sama dengan file yang lainya baik tanggal maupun tahun pembuatan file tersebut, karena apabila berbeda bias di pastikan itu sebuah crapware yang menyusup. Walaupun kedalam legitimate windows executables,jadi kita harus jeli untuk mengamati file yang diangap mencurigakan sebelum terlambat.

Dalam percobaan dengan cmd didapatkan file yang diangap virus dalam direktri c .percobaan ini dilakukan kedalam sebuah laboratorium komputer yang ada di stmik binapatria. File tersebuat berextensi inf yang biasanyaberbentuk shot cut kalau ber ada di dalam flash disk hasilnya kan tampak pad gambar dibawah ini

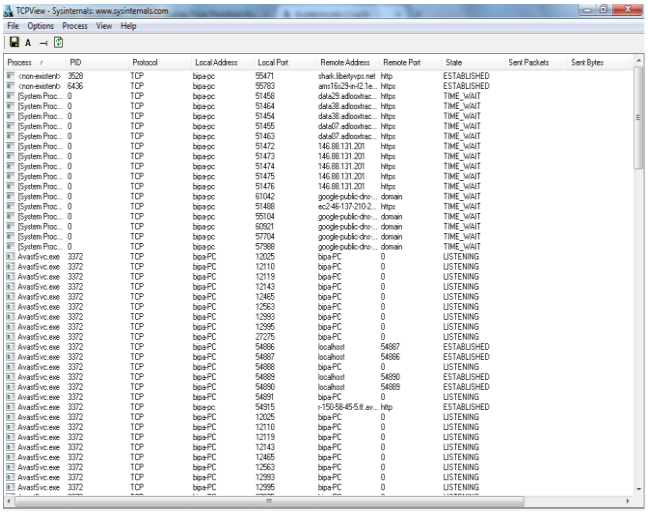


Gambar 9. Dari dir C pada sebuah pc lab c



Gambar 10. Explorer sysinternalsuit

Dari situ didapat beberepa file yang bias kita analisa, apakah file tersebut mencurigakan atau tidak jadi kita bias mengetahui lebih dalam karena ad kelengkapan fitur find dll pada explorer



Gambar11. Tcp view

Dari tcp view didapatkan beberapa koneksi jaringan yang estabelised, dari situ dimukinkan adanya spyware ataupun backdoor yang terhibung kejaringan kita apabila kita tidah mengenali dari koneksi tersebut makan bias kita klik kanan pada proses yang berjalann tersebut kita pilah *who is* maka akan tampil dari aman asal jaringan dan detail jaringan tersebut.

5. Kesimpulan

Dari hasil tersebut maka apabila kita lebih jeli dan teliti dalam mengetahui sebuah file yang dianggap asing ,maka kita akan terhidar dari serangan malware yang berbahaya ,walupun menggunakan tooll bawan dari Microsoft ataupun windows itu sendiri. Dengan menggunakan sysinternalsuit akan lebih detail untuk mengetahui malware tersebut dan segera mengeksekusinya agar tidak menimbulkan dampak yang lebih berbahayaapabila tidak segera ditangani.

.

Daftar Pustaka

Alan Calder (2005). A business guide to information security_ how to protect your company's IT assets, reduce risks and understand the law.Kogan

Ban Khammas .(2018) Malware Detection using Sub-Signatures and Machine Learning .

Journal of Information Security Research . https://doi.org/ 10.6025/jisr/2018/9/3/96-106.

Bazrafshan Z., Hashemi H., Fard S., Hamzeh A. (2013)., A survey on heuristic malware detection techniques. In 5th Conf. Information and Knowledge Technology, IKT

Bhuyan M. H., Bhattacharyya D., Kalita j.(2011) Surveying port scans and their detection methodologies. The Computer Journal 54, 10 (Oct.).

Bo Y, Ying F, Qiang Y, Yong T, Liu L (2017). A survey of malware behavior description and analysis. Yu et al. / Front Inform Technol Electron Eng 2018 19(5):583-603

Christodorescu and S. Jha. Static analysis of executables to detect malicious patterns. In Proceedings of USENIX Security Symposium, pages 12–22, Washington, DC, USA, 2003.USENIX Association.

Ismail, I., Marsono, M. N., Khammas, B. M., Nor. S. M. (2015). Incorporating known malware signatures to classify new malware variants in network traffic," International Journal of Network Management, 25 (6) 471–489.

Khammas, B. M., Monemi, A., Joseph, S. B., Ismail, I., Mohd Nor, S., Marsono, M. N. (2015). Feature selection and machine learning classification for malware detection, Jurnal Teknologi, 77 (1) 234–250.

Miao, Q., Liu, J., Cao, Y., Song, J. (2015). Malware detection using bilayer behavior abstraction and improved one-class support vector machines, International Journal of Information Security, 1–19.

Misra, A., Verma, M., Sharma, A. (2014). Capturing the interplay between malware and anti-malware in a computer network, Applied Mathematics and Computation, 229, 340–349.

Santos, I., Brezo, F., Ugarte-Pedrero, X., Bringas, P. G. (2013). Opcode sequences as representation of executables for datamining-based unknown malware detection, Information Sciences, 231, p 64–82

Wang, W., Zhang, X., Gombault, S. (2009). Constructing attribute weights from computer audit data for effective intrusion detection, Journal of Systems and Software, 82 (12) 1974–1981

Vinod, P., Laxmi, V., Gaur, M. S. (2012). Reform: relevant features for malware analysis, In: 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2012, p 738–744, IEEE

Buku :

O. Digit and IMuhardianto (2013). Cuckoo Malware Analysis, Birmingham: Packt Publishing.

Prosiding seminar:

I. Goldberg, D. Wagner, R. Thomas and E. Brewer(1996) "A Secure Environment for Untrusted Helper Applications (Confining the Wily Hacker)," in Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California.

Santos, I., Nieves, J., Bringas, P. G. (2011). Semi-supervised learning for unknown malware detection, International Symposium on Distributed Computing and Artificial Intelligence, p. 415–422, Springer.

Shabtai, A., Moskovitch, C., Feher, C., Dolev, S., Elovici, Y. (2012). Detecting unknown malicious code by applying classification techniques on opcode patterns," Security Informatics, 1 (1) 1–22.