REPOSITOR, Vol. 4, No. 1, Februari 2022, Pp. 83-94
ISSN : 2714-7975
E-ISSN : 2716-1382

Analisis Ransomware Wannacry Menggunakan Aplikasi Cuckoo Sandbox

Gratiyo Wahyu Wahidin*[1], Syaifuddin[2], Zamah Sari[3]
[1,2,3]Teknik Informatika, Universitas Muhammadiyah Malang
gratiyowahyu@gmail.com*[1], syaifuddin_skom@umm.ac.id[2], zamahsarii@umm.ac.id[3]

Abstrak

Ransomware mengakibatkan kerugian yang besar akhir-akhir ini, ransomware merupakan bagian dari malware yang melakukan enkripsi data pada targetnya. Malware tersebut kebanyakan menyerang instansi pemerintah dengan cara menyebar melalui jaringan lokal yang diawali dengan menyusup melalui email atau data yang tidak terpercaya. Untuk mengetahui hal apa saja yang dilakukan malware ketika sedang melakukan penyerangan perlunya untuk melakukan analisis baik menggunakan teknik statis maupun dinamis. Pada Cuckoo Sandbox terdapat teknik analisis dinamis dan statis, didalam analisis dinamis Cuckoo Sandbox menjalankan malware dalam lingkungan virtual sehingga dapat meminimalisir adanya penyebaran malware. Analisis statis dilakukan dengan cara melakukan dekompilasi malware tanpa melakukan uji coba secara langsung, sedangkan analisa dinamis melakukan uji malware dengan cara eksekusi cara langsung. Dengan perangkat lunak Cuckoo Sandbox informasi data yang didapat diharapkan dapat digunakan untuk mengetahui tentang aktivitas dan kebiasaan dari Ransomware. Beberapa dari ransomware mempunyai kebiasaan yang berbeda-beda, dalam analisis yang dilakukan oleh Cuckoo Sandbox terdapat pula hasil dari analisa kebiasaan dari malware, hasil yang didapat nantinya menjelaskan perilaku yang biasa dilakukan oleh malware sewaktu menginfeksi.

Kata Kunci: *Ransomware, Analisis Statis, Analisis Dinamis, Cuckoo Sandbox, Kebiasaan Malware*

Abstract

Ransomware has recently suffered significant damage, and Ransomware is part of the malware that performs data encryption. The program began primarily by attacking government agencies and breaking into email or data. To know what actions malicious code will take in the course of an attack, both static and dynamic techniques should be used to analyze them. Cuckoo Sandbox has dynamic and static analytics. Cuckoo Sandbox can minimize malware distribution by operating it in a virtual environment. Static analysis is conducted by integrating malicious code without conducting a direct test, and dynamic analysis analyzes malicious code by directly executing it. Cuckoo Sandbox software is expected to be available to learn about ransomware activities and habits or the other known is behavioral analysis. Some ransomware have different deployment method. The analysis conducted by Cuckoo Sandbox explains the results of the analysis of malicious code and explains how they do when they infect.

Keywords*: Ransomware, Static analysis, Dynamic analysis, Behavioral analysis, Cuckoo Sandbox*

1. Pendahuluan

Menurut data hasil survey yang dilaksanakan oleh IDCERT pada tahun 2015, Negara Indonesia menjadi negara yang paling sering diserang *malware* [1]. Serangan *malware* akhir – akhir ini lebih sering menyerang instansi besar seperti pemerintahan atau Rumah Sakit dengan cara masuk melalui celah *port* yang terbuka, selain itu penyebaran dapat terjadi melalui internet, *email*, dan aplikasi [2]. Hal tersebut terjadi karena jaringan pada instansi tersebut menggunakan *WAN*, perangkat lunak yang rentan, dan jaringan lokal di beberapa bagian, sehingga penyebaran *malware* dapat terjadi dengan cepat dan tidak terkendali.

Malware yang berjenis *Ransomware Wannacry* telah melakukan serangan secara masif ke seluruh penjuru dunia termasuk Negara Indonesia. *Malware* tersebut bekerja dengan cara melakukan enkripsi file dengan cepat serta menyebar pada data servernya, serta melakukan

pemindaian *port TCP* dan *UDP* 139 dan 445 (*SMB*) dari komputer, apabila *port* tersebut terbuka, maka *malware* akan menyebar secara otomatis yang dapat merugikan kinerja pengguna [3]. Enkripsi file yang digunakan pada malware tersebut adalah jenis *RSA-2048* sehingga sangat sulit untuk menemukan kode enkripsinya.

Ransomware termasuk salah satu bagian dari *malware*, berikut merupakan beberapa perbedaan antara *malware* biasa dengan *ransomware*. Perbedaan keduanya, jika malware aktivitasnya cenderung bersembunyi dan tidak mau menampakkan diri, sedangkan *ransomware* lebih menampakkan aktivitasnya sebagai virus. Sehingga pengguna dapat mengetahui apabila dirinya sedang terinfeksi oleh *ransomware* [4].

Metode analisis malware dibagi menjadi 3 bagian, yaitu analisis statis, dinamis, dan hybrid. Metode analisis statis adalah analisa yang dilakukan dengan cara mengawasi secara langsung isi dari *source code* dengan menggunakan beberapa aplikasi *unpacker* tanpa melakukan eksekusi *malware* secara langsung. Dalam melihat dan mengamati bagian *source code malware* dapat menggunakan beberapa jenis program seperti program analisa, *debugger*, dan *disassembler*. Keuntungan dalam analisis statis yaitu data menjadi aman dan analisis juga cenderung cepat. Metode analisis dinamis adalah metode yang mengamati aktivitas pada malware dengan cara melakukan eksekusi secara langsung, sehingga tampak cara kerja atau perilaku *malware* sebelum dan sesudah melakukan infeksi. Metode ini menggunakan mesin *virtual*, sehingga dapat meminimalisir adanya penyebaran *malware*. Keuntungan analisis dinamis adalah mudah untuk mendeteksi *malware* yang sedang melakukan proses infeksi tentang cara kerja *malware* tersebut secara langsung. Analisis *hybrid* merupakan metode kombinasi atau gabungan dari analisis statis dengan analisis dinamis. Metode ini menggabungkan keunggulan dari analisis dinamis dan statis yaitu dengan melakukan pengecekan setiap signature malware jika ditemukan adanya kode tertentu disaat pemeriksaan dan *monitoring* perilaku kode pada *malware* tersebut [5].

Pada penelitian sebelumnya telah dilakukan analisis dinamis pada malware yang menggunakan bahasa *C#*, peneliti tersebut melakukan analisis *malware* hanya dengan teknik analisis dinamis tanpa membahas teknik analisis statis [6]. Untuk hasil dari analisis tersebut tidak jauh berbeda dengan proposal yang penulis lakukan. Perbedaannya, terletak pada bahasa pemrograman dimana penulis menggunakan *javascript* dan *python*, lalu kecepatan analisis *malware* cenderung lebih cepat. Pada penelitian lainnya yang berhubungan, penulis menganalisis *malware* yang terjangkit aplikasi *mobile*, penulis sebelumnya menganalisis *malware* dengan teknik analisis statis menggunakan teknik *decompile* aplikasi [7]. Dalam hal ini penulis menggunakan suatu aplikasi yang bernama *Cuckoo Sandbox*. Aplikasi tersebut ditanam dalam komputer dengan sistem operasi *ubuntu* 16.04 *LTS*. Penulis juga menggunakan *virtualbox host-only* dengan sistem operasi *windows* 7 32-bit untuk melihat hasil dari analisis *malware* yang dilakukan oleh aplikasi *Cuckoo Sandbox*.

2. Metode Penelitian

2.1 Ransomware Wannacry

Serangan *ransomware WannaCry* adalah serangan dunia maya global yang dimulai pada 12 Mei 2017, dan skalanya belum pernah terjadi sebelumnya dengan cepat memengaruhi lebih dari 200.000 komputer di lebih dari 150 negara. Secara umum, sindikat kejahatan transnasional "mengadaptasi model bisnis mereka dengan menggunakan apa yang disebut *'ransomware'* untuk mendapatkan kendali atas jaringan komputer dan kemudian meminta pembayaran sebagai imbalan untuk pemulihan." Virus *WannaCry* mengeksploitasi kerentanan di *Microsoft Windows* yang awalnya dikembangkan oleh Badan Keamanan Nasional AS dan beroperasi dengan mengenkripsi data korban dan menuntut pembayaran tebusan sebagai imbalan pemulihan data [8].

2.2 Analisis Statis

Terdapat beberapa metode pada analisis *malware*, salah satunya yaitu analisis *malware* dengan metode analisis statis. Metode statis pada analisis malware yaitu melakukan analisis *malware* dengan tidak menjalankan atau tidak mengeksekusi perangkat lunak yang terdapat *malware* didalamnya [9]. Analisis statis dilakukan dengan cara menganalisis dengan melihat *source code* dari perangkat lunak yang terinfeksi *malware*. *Source code* tersebut dapat diperoleh dengan memecah sampel *malware* dan kemudian mencari pola yang menarik dalam *source code* ini seperti adanya *code* yang berbahaya dan mencurigakan [7].

Jadi pada metode analisis statis ini akan didapatkan sebuah informasi tentang karakteristik dari *malware* berupa rangkaian kode yang berbahaya atau mencurigakan, susunan file "*API*" pada Ransomware.

2.3 Analisis Dinamis

Proses menganalisis perilaku atau tindakan yang dilakukan oleh aplikasi saat sedang menjalankannya disebut analisis dinamis. Analisis dinamis dapat dilakukan melalui pemantauan pemanggilan fungsi, pelacakan aliran informasi, analisis parameter fungsi, dan penelusuran instruksi. Umumnya mesin *virtual* atau *sandbox* digunakan untuk analisis ini; aplikasi yang diragukan biasanya dijalankan dalam lingkungan *virtual*. Jika aplikasi berperilaku tidak biasa, itu dikategorikan sebagai berbahaya. Saat ini, ada perangkat lunak pemblokiran perilaku, yang memblokir tindakan jahat program sebelum mereka menyerang [10].

2.4 Pengumpulan Data

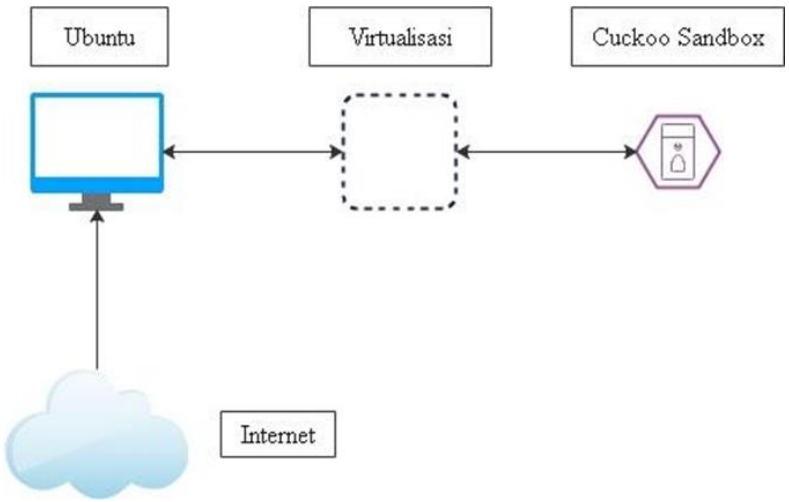
Beberapa pengguna ada yang sengaja untuk terinfeksi agar mendapatkan *sample* untuk keperluan penelitian, maka dari itu penulis sengaja mengunduh beberapa *malware* untuk dilakukan penelitian dengan analisis statis dan dinamis melalui *malware library* yang tersedia di beberapa *website*. Berikut merupakan Tabel 1 yang merupakan beberapa *malware* untuk keperluan penelitian penelitian:

Tabel 1. Sumber Jenis Mal ware yang akan digunakan untuk Penelitian

No	Jenis Malware	Sumber Sample Malware
1.	Ransomware.Wannacry	Github theZoo
2.	Ransomware.Cerber	Github theZoo
3.	Ransomware.TeslaCrypt	MalwareBazaar

2.5 Perancangan Sistem Analisis

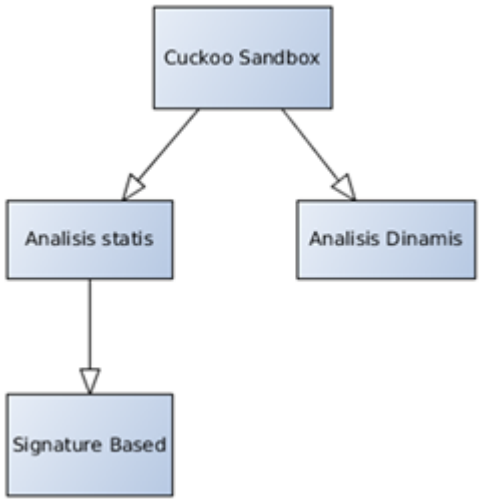
Pada bagian ini dijelaskan tahapan dalam melakukan perancangan *Cuckoo Sandbox* untuk melakukan proses analisis *malware*. Langkah dalam melakukan perancangan sistem akan dijelaskan pada Gambar 1



Gambar 1. Rancangan Sistem

Berdasarkan Gambar 1 yaitu rancangan sistem yang akan digunakan pada penelitian kali ini, dimana *malware* didapat dari internet akan diunduh oleh komputer *ubuntu*, untuk dilakukan uji analisis menggunakan perangkat lunak *Cuckoo Sandbox* dan diuji dengan *virtual* dengan menggunakan *virtualbox*.

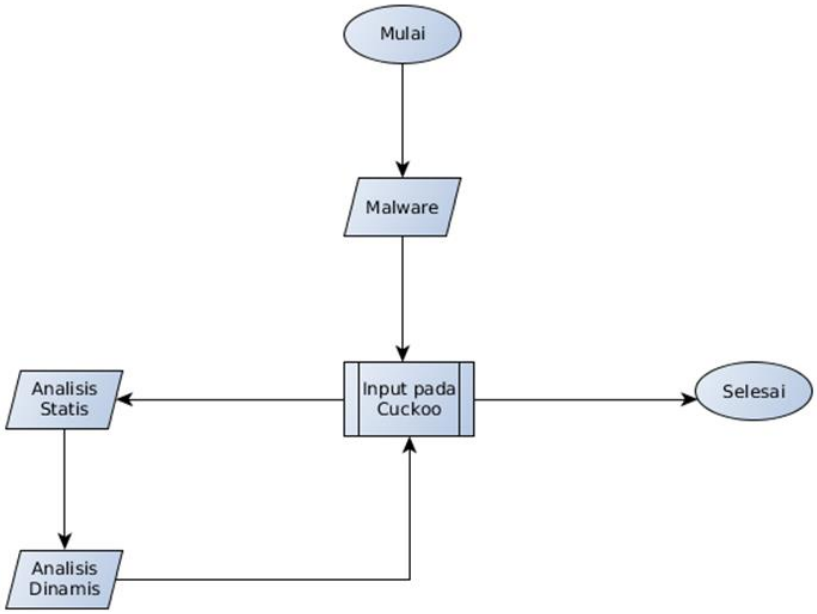
Pada perangkat lunak *Cuckoo Sandbox* itu sendiri terdapat analisis status, dinamis, serta kebiasaan dari malware tersebut. Analisis tersebut nantinya akan menguji *malware sample* yang sebelumnya telah diunduh oleh komputer. Berikut merupakan Gambar 2 tentang teknis analisis yang terdapat pada *Cuckoo Sandbox*



Gambar 2. Analisis pada Cuckoo Sandbox

2.6 Flowchart Proses analisis Malware

Berdasarkan pada Gambar 3, ditunjukkan *flowchart* dari proses *Ransomware Wannacry* di analisis melalui sistem yang telah dipasang yaitu *Cuckoo Sandbox*. Pada tahap pertama yaitu menyiapkan *malware* berjenis *Ransomware Wannacry* yang akan dianalisis seperti yang telah dijelaskan pada Tabel 1. Kemudian *malware* tersebut di *upload* pada sistem *Cuckoo Sandbox*, lalu melware tersebut dianalisis menggunakan metode analisis statis yang dimana akan menghasilkan *signature based*. Setelah melalui proses analisis statis maka akan muncul data berupa *hash*, *string*, *dll*, *registry edit*, dan komunikasi data *malware*.. Setelah melakukan proses analisis statis, *malware* akan di uji pada mesin *virtual*, yang dimana tersedia *virtualbox* dengan *windows* 7 64 *bit*. Proses analisis dinamis yaitu yang menandakan *malware* di uji secara *virtual* pada mesin *virtual* yang telah dipasang, dari analisis tersebut akan muncul data gambar berupa efek yang ditimbulkan dari *malware* tersebut.



Gambar 3. Flowchart Proses Analisis

2.7 Analisis Kebutuhan Sistem

Pada bagian ini menjelaskan kebutuhan yang diperlukan guna menunjang keberhasilan penelitian ini. Dari teknik analisis yang telah dijelaskan maka kebutuhan yang diperlukan untuk membantu proses analisis meliputi perangkat keras dan perangkat lunak.

a. Kebutuhan Perangkat Keras

Perangkat keras yang dibutuhkan pada proses analisis yakni sebagai berikut:

- Sistem Operasi : Ubuntu 16.04
- Processor : Intel Core i5-4210u 1.7 Ghz
- Memori : 8 GB RAM
- Penyimpanan : 250 GB Harddisk

b. Kebutuhan Perangkat Lunak

Perangkat lunak yang dibutuhkan pada proses analisis yakni sebagai berikut:

- *VirtualBox*
- *Linux*
- *Gedit*
- *Cuckoo Sandbox*
- *Windows* 7

3. Hasil Penelitian dan Pembahasan

Pada bagian ini akan dijelaskan bagaimana hasil yang didapatkan dari apa yang dilakukan pada bagian 2 sebelumnya dan bagaimana hasil tersebut dianalisis untuk mendapatkan informasi kebiasaan dari *Ransomware Wannacry*. Pada sub bab hasil akan dijabarkan apa saja yang ditemukan dari proses analisis *Ransomware* oleh perangkat lunak *Cuckoo Sandbox* berdasarkan kebiasaan *Ransomware* yang telah disebutkan sebelumnya. Pada proses pemasangan *Cuckoo Sandbox* dibutuhkan cara untuk memasang perangkat lunak dengan baik dan benar, hal ini bertujuan untuk memaksimalkan analisis yang diperoleh. Disini akan penulis tampilkan hasil dari analisis *Ransomware Wannacry* yang dilakukan oleh *Cuckoo Sandbox*, adapun md5 dari *malware* seperti pada Tabel 2 berikut.

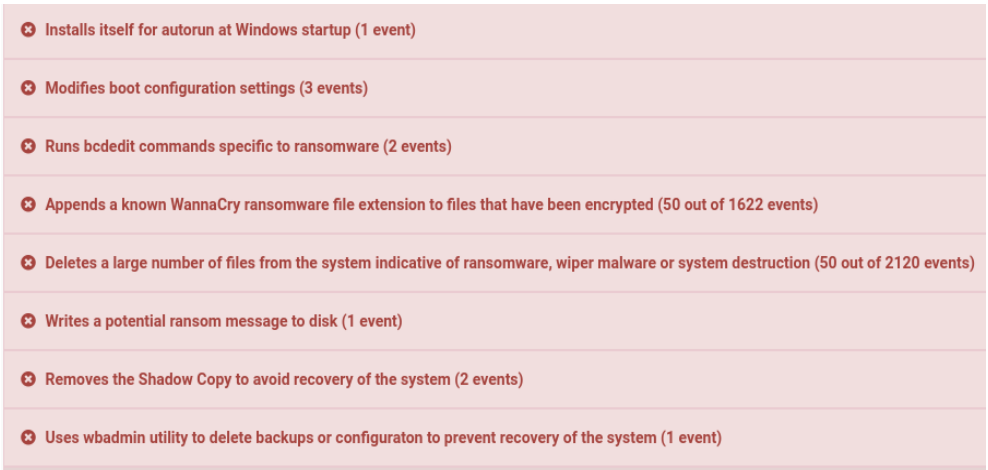
Tabel 2. md5 Malware yang akan di uji

No	Md5	Nama
1	84C82835A5D21BBCF75A61706D8AB54	Ransomware.Wannacry
2	8B6BC16FD137C09A08B02BBE1BB7D670	Ransomware Cerber
3	6D3D62A4CFF19B4f2CC7CE9027C33BE8	Ransomware TeslaCrypt

3.1. Hasil Analisis yang dilakukan dengan Cuckoo Sandbox

3.1.1 Analisis Dinamis Ransomware Wannacry

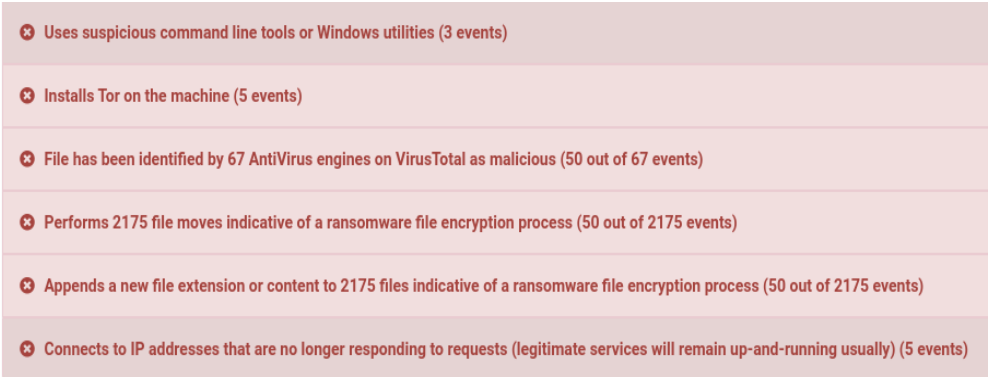
Pada hasil analisis dinamis ini akan ditampilkan beberapa gambar yang didapatkan sewaktu melakukan proses pengujian serta setelah selesai pengujian. Berikut hasil dari analisis *Ransomware Wannacry* yang dilakukan oleh *Cuckoo Sandbox*:



Gambar 4. Tampilan Hasil Analisis Ransomware.Wannacry pada Cuckoo Sandbox

Pada Gambar 4 *cuckoo sandbox* mendapat informasi bahwa *malware* melakukan instalasi *file* yang akan berjalan ketika *windows* sedang di aktifkan, lalu *malware* tersebut melakukan beberapa perubahan konfigurasi pada *windows booting*. Setelah proses tersebut *ransomware*

yang sedang di uji *cuckoo* melakukan proses enkripsi data dengan menggunakan perintah *bcdedit*, serta menulis pesan yang digunakan untuk mengancam pengguna, lalu setelah proses tersebut berjalan *malware* juga menghapus beberapa data dari sistem agar sistem tersebut tidak bisa dipulihkan secara manual.



Gambar 5. Tampilan Hasil Analisis Ransomware.Wannacry pada Cuckoo Sandbox

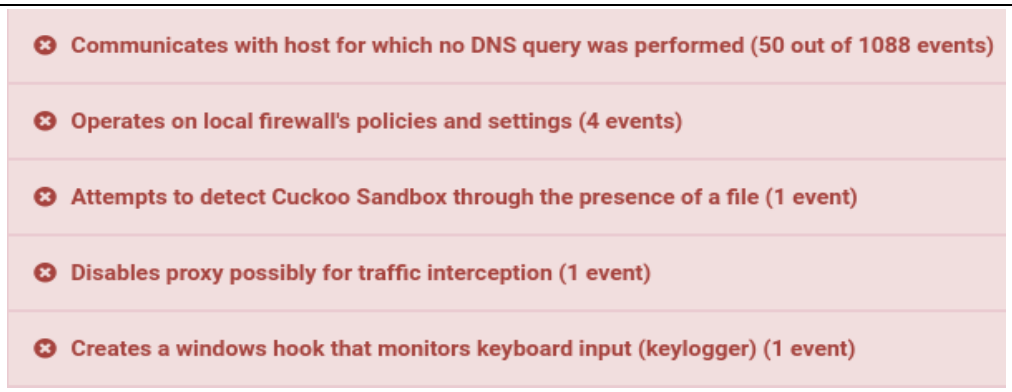
Pada Gambar 5 *cuckoo sandbox* mendeteksi adanya proses yang dilakukan oleh *malware* melaluli *cmd* yang tidak wajar, lalu *malware* tersebut melakukan pemasangan perangkat lunak *tor browser* yang digunakan untuk akses *domain* berbasis *union*. Setelah melakukan beberapa ekripsi data, *malware* tersebut melakukan akses ke situs yang berbahaya, akan tetapi pada *Ransomware Wannacry* ini situs tersebut tidak bisa di akses lagi.

Gambar 6. Tampilan Hasil Analisis Ransomware.Wannacry pada Cuckoo Sandbox

Pada Gambar 6 merupakan tampilan akhir dari terjangkitnya komputer oleh *Ransomware Wannacry*, pengguna dipaksa membayar untuk dilakukan deskripsi data, akan tetapi prosedur tersebut palsu menurut beberapa informasi dari Pemerintah, dan data pengguna akan tetap hilang dalam seminggu.

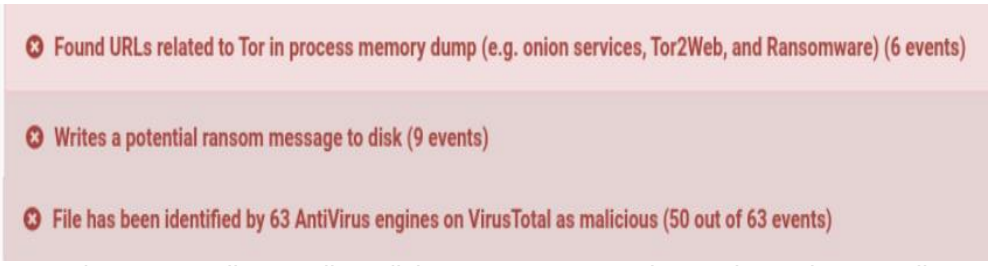
3.1.2 Analisis Dinamis Ransomware Cerber

Pada hasil analisis dinamis ini akan ditampilkan beberapa gambar yang didapatkan sewaktu melakukan proses pengujian serta setelah selesai pengujian. Berikut hasil dari analisis *Ransomware Cerber* yang dilakukan oleh *Cuckoo Sandbox*:



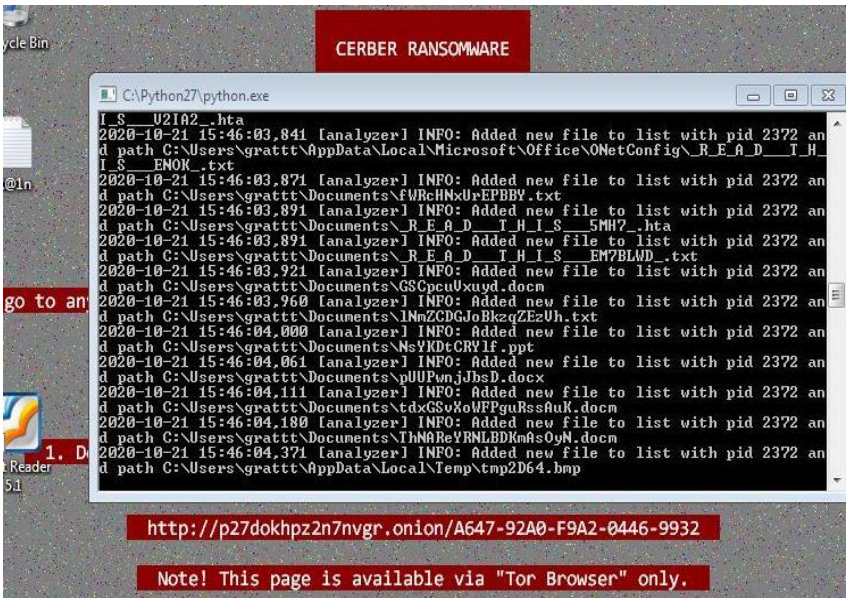
Gambar 7. Tampilan Hasil Analisis Ransomware.Cerber pada Cuckoo Sandbox

Pada Gambar 7 ransomware cerber mencoba melakukan akses kepada host menggunakan dns tertentu seperti cloudflare, google, dan lainnya. Malware tersebut juga melakukan perubahan setting pada windows firewall, selain itu juga melakukan blokir proxy yang dapat digunakan pengguna untuk melakukan intersepsi pada jaringan secara manual. Cuckoo Sandbox juga mendapat informasi bahwa malware melakukan pencarian adanya cuckoo sandbox pada sistem atau tidak dan membuat beberapa proses yang digunakan untuk merekam aktivitas input devices dengan fungsi sama seperti keylogger.

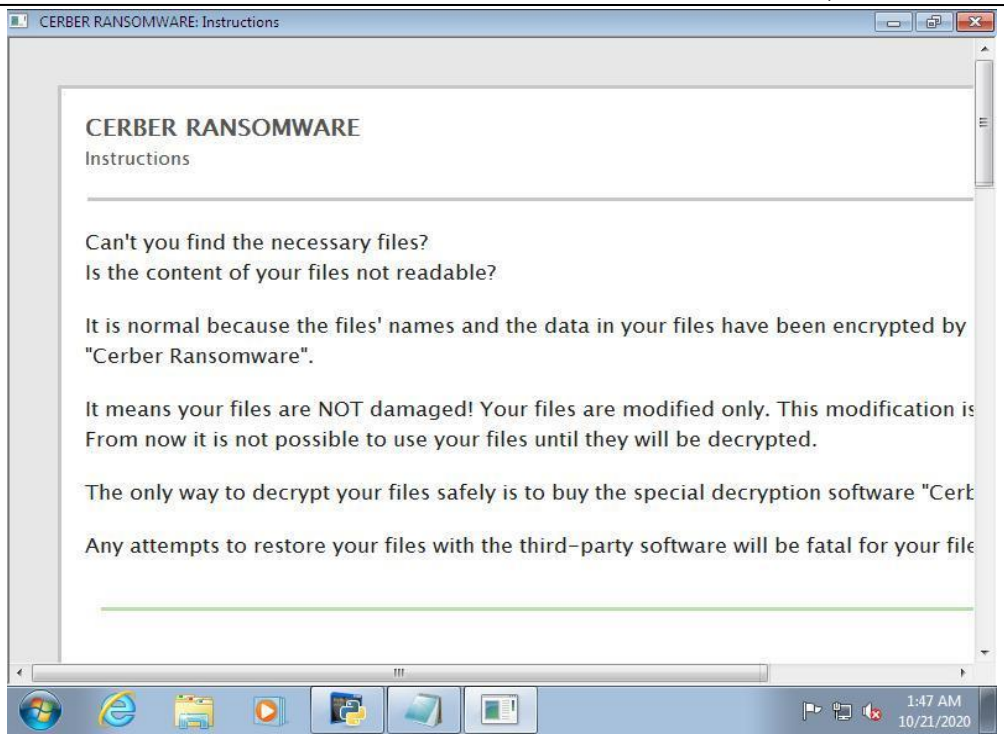


Gambar 8. Tampilan Hasil Analisis Ransomware Cerber pada Cuckoo Sandbox

Pada Gambar 8 Malware melakukan akses pada alamat situs yang berbahaya, akan tetapi situs tersebut hanya bisa dibuka oleh browser Tor. Ransomware Cerber juga menuliskan pesan yang digunakan untuk mengancam pengguna seperti halnya pada analisis Ransomware Wannacry sebelumnya.



Gambar 9. Tampilan Hasil Analisis Ransomware Cerber pada Cuckoo Sandbox



Gambar 10. Tampilan Hasil Analisis Ransomware Cerber pada Cuckoo Sandbox

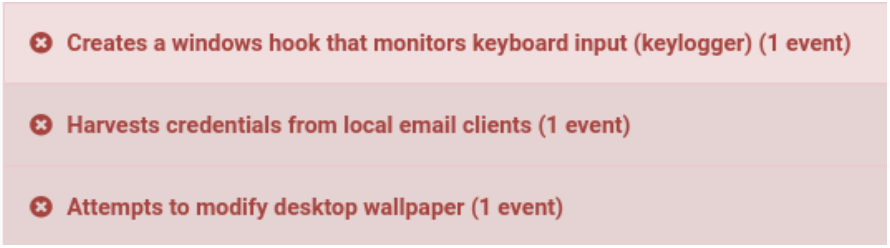
Pada Gambar 9 dan Gambar 10 merupakan tampilan *windows* ketika sudah terinfeksi oleh *Ransomware Cerber*, *malware* tersebut menuliskan pesan di jendela utama dan membuat file terpisah untuk melakukan ancaman tanpa hitungan mundur seperti *ransomware* biasanya.

3.1.3 Analisis Dinamis Ransomware TeslaCrypt

Pada hasil analisis dinamis ini akan ditampilkan beberapa gambar yang didapatkan sewaktu melakukan proses pengujian serta setelah selesai pengujian. Berikut hasil dari analisis *Ransomware TeslaCrypt* yang dilakukan oleh *Cuckoo Sandbox*:

Gambar 11. Tampilan Hasil Analisis Ransomware TeslaCrypt pada Cuckoo Sandbox

Pada Gambar 11 File yang dijalankan oleh *malware* terdeteksi sebagai packer yang dikenali oleh *cuckoo sandbox*. *Malware* melakukan akses ke situs ber domain tor serta mengganti konfigurasi keamanan *browser* bawaan. *Malware* juga mencari informasi *antivirus* yang terpasang pada perangkat, hal tersebut biasanya digunakan untuk melakukan blokir akses *antivirus* kepada *file* atau proses yang sedang berjalan dan juga memasang aplikasi yang akan berjalan ketika windows sedang dijalankan. Lalu *Malware* mencoba mendeteksi adanya *cuckoo sandbox* melalui scan file ke beberapa direktori tertentu.

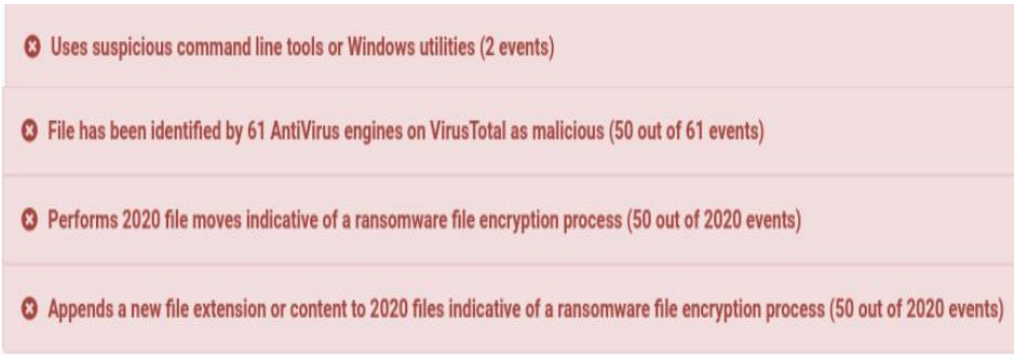


Gambar 12. Tampilan Hasil Analisis Ransomware TeslaCrypt pada Cuckoo Sandbox

Pada Gambar 12 terdapat proses Perekaman data yang dihasilkan dari perangkat keras berupa *mouse*, *keyboard* atau *input device* lainnya, *Malware* tersebut juga mencari dan menggali beberapa data privasi yang berhubungan dengan *email* dari perangkat. *Malware* mencoba untuk mengganti tampilan utama dari *windows.*

Gambar 13 Tampilan Hasil Analisis Ransomware TeslaCrypt pada Cuckoo Sandbox

Pada Gambar 13 terdapat proses dimana *Malware* membuat file yang berisi panduan deskripsi palsu yang digunakan untuk mengecoh dan mengancam pengguna, serta menulis beberapa ancaman pada beberapa *file* tertentu. *Malware* membuat file yang berkaitan dengan deskripsi file, akan tetapi file tersebut dikenali oleh *cuckoo sandbox* dan palsu. Pada saat itu juga *Cuckoo* juga mendeteksi adanya proses yang digunakan untuk *malware* untuk membersihkan jejak digitalnya, serta menghapus cadangan data yang terdapat pada perangkat lunak.



Gambar 14. Tampilan Hasil Analisis Ransomware TeslaCrypt pada Cuckoo Sandbox

Pada Gambar 14 terdapat proses yang *Cuckoo* mendeteksi adanya penggunaan *command line* yang tidak wajar pada *windows. File* yang telah dilakukan enkripsi oleh *malware* dipindahkan kedalam direktori khusus yang dibuat oleh *Ransomware TeslaCrypt.* Proses enkripsi secara terus menerus kepada *file* perangkat lunak yang di uji, proses tersebut berjalan menggunakan *cmd* yang telah di atur oleh *malware.*

Gambar 15 Tampilan Hasil Analisis Ransomware TeslaCrypt pada Cuckoo Sandbox

Pada Gambar 15 merupakan tampilan layar ketika *windows* sudah terinfeksi oleh *Ransomware TeslaCrypt*, di tampilan tersebut terdapat beberapa link, *bitcoin*, dan waktu ketika *file* telah ter enkripsi sempurna.

3.1.4 Analisis Kebiasaan Ransomware

Setiap malware berjenis *ransomware* memiliki kebiasaan yang cenderung hampir sama. Pada 3 contoh *ransomware Wannacry*, *Cerber*, dan *TeslaCrypt* diantaranya selalu melakukan pencarian data pengguna di awal prosesnya diantaranya informasi nama komputer, informasi perangkat lunak, informasi perangkat keras, lalu menggunakan *cmd* yang tidak jauh bebeda, membuat beberapa *file executable*, *office*, dan menggunakan konsep yang sama dalam menghapus jejak digital. Akan tetapi *malware* tersebut menggunakan hak akses situs yang berbeda beda karena mereka dibuat oleh orang yang berbeda pula, dan pola ancaman yang berbeda juga. *Ransomware* melakukan penyebaran secara lokal dengan cepat, dimana hal tersebut terbukti dengan analisis dinamis sebelumnya berupa setiap *malware* selalu melakukan percobaan akses ke dalam jaringan lokal. Berikut merupakan Tabel 3 persamaan kebiasaan *Ransomware Wannacry*, *Cerber*, *Teslacrypt*:

Tabel 9. Aktivitas Ransomware Wannacry yang terekam pada Cuckoo Sandbox

Kebiasaan Malware	Wannacry	Cerber	TeslaCrypt
Melakukan pencarian Informasi yang berhubungan dengan perangkat	✓ Dinamis Gambar 4.3.1.3	✓ Dinamis Gambar 4.3.2.3	✓ Dinamis Gambar 4.3.3.3
Memodifikasi *Boot windows*	✓ Dinamis Gambar 4.3.1.6 Gambar 4.3.1.7	✗	✓ Dinamis Gambar 4.3.3.4 Gambar 4.3.3.5
Membuat *File* ekstensi *office*	✓ Dinamis dan Statis Tabel 4.2.1.6 Gambar 4.3.1.6	✓ Dinamis dan Statis Tabel 4.2.2.6 Gambar 4.3.2.5	✓ Dinamis dan Statis Tabel 4.2.3.6 Gambar 4.3.3.4
Melakukan percobaan koneksi jaringan lokal atau jaringan TOR	✓ Dinamis dan	✓ Dinamis dan	✓ Dinamis dan Statis

	Statis Tabel 4.2.1.5 Gambar 4.3.1.5	Statis Tabel 4.2.2.5 Gambar 4.3.2.4	Tabel 4.2.3.5 Gambar 4.3.3.4
Melakukan Enkripsi Data	✓ Dinamis Gambar 4.3.1.8	✓ Dinamis Gambar 4.3.2.8	✓ Dinamis Gambar 4.3.3.8
Melakukan pencurian data berupa *email* pada korban	×	×	✓ Dinamis Gambar 4.3.3.6

4. Kesimpulan

Dengan melakukan analisis malware melalui *Cuckoo sandbox* pada *malware Ransomware Wannacry* menggunakan analisis statis dan dinamis maka akan mendapatkan data karakter dari malware tersebut. Data tersebut berupa informasi yang penting untuk menggali rekam jejak dari apa saja yang dilakukan *malware* pada perangkat lunak yang terinfeksi, seperti halnya pada analisis yang telah dilakukan malware melakukan akses dan merubah beberapa komponen penting pada proses komputer. Proses tersebut meliputi memodifikasi *registry* pada sistem, akses ke jaringan atau situs tertentu, merubah setting *firewall*, menghapus cadangan data pada perangkat lunak, serta mencuri informasi *email* dan perangkat keras. Hal tersebut sangat berbahaya apabila dilakukan modifikasi karena dapat mempengaruhi kinerja sistem. Dampak yang berbahaya apabila terinfeksi oleh *Ransomware* adalah file akan terenkripsi sehingga beberapa data yang ada tidak bisa di akses lagi, sehingga besar kemungkinan melakukan pemasangan ulang *windows* merupakan jalan yang paling cepat dengan resiko kehilangan semua data yang terdapat pada *hardisk*. *Ransomware* melakukan penyebaran melalui koneksi lokal, *email*, serta program yang tidak terpercaya, hal tersebut sangat mudah menyebar karena melihat beberapa pengguna jarang melakukan pembaruan perangkat lunak dan antivirus.

Dari penjelasan yang telah ditulis sebelumnya, akan berbahaya jika tidak melakukan blokir beberapa *port* yang jarang dipakai seperti *port* 139, 445 untuk mencegah mudahnya menyebar malware secara *local*. Pengguna perangkat lunak juga disarankan untuk melakukan pembaruan perangkat lunak dan memasang antivirus tambahan.

Referensi

[1] ID-SIRTII, “Laporan Survey Malware Periode Januari-Mei Daftar Isi,” p. 30, 2015, [Online]. Available: https://www.cert.or.id/media/files/survey_malware_report_juni15.pdf.

[2] ID-SIRTII, “Indonesia Cyber Security Monitoring Report 2018,” *Indonesia Security Incident Response Team On Internet Infrastructure*, ID-SIRTII, p. 42, 2018.

[3] Symantec Security Center, “Wannacry Ransomware Write-up,” vol. 0, no. May, pp. 1–18, 2017, [Online]. Available: https://www.symantec.com/security-center/writeup/2017-051310-3522-99.

[4] N. Hampton, Z. Baig, and S. Zeadally, “Ransomware behavioural analysis on windows platforms,” *J. Inf. Secur. Appl.*, vol. 40, pp. 44–51, 2018, doi: 10.1016/j.jisa.2018.02.008.

[5] R. Adenansi and L. A. Novarina, “Malware dynamic,” *J. Educ. Inf. Commun. Technol.*, vol. 1, no. 1, pp. 37–43, 2017.

[6] A. H. Fitrasani, “Aplikasi pendeteksi malware dengan teknik analisis dinamis,” 2017.

[7] Y. I. Rizqony, D. R. Akbi, and F. D. S. Setiawan, “Analisis Karakteristik Malware Joker Berdasarkan Fitur Menggunakan Metode Statik Pada Platform Android,” *J. Repos.*, vol. 2, no. 10, pp. 1368–1379, 2020, doi: 10.22219/repositor.v2i10.1145.

[8] L. J. Trautman and P. Ormerod, “Wannacry, Ransomware, and the Emerging Threat to Corporations,” *SSRN Electron. J.*, no. April, 2018, doi: 10.2139/ssrn.3238293.

[9] D. Ucci, L. Aniello, and R. Baldoni, “Survey of machine learning techniques for malware analysis,” *Comput. Secur.*, vol. 81, no. December, pp. 123–147, 2019, doi: 10.1016/j.cose.2018.11.001.

[10] D. Uppal, V. Mehra, and V. Verma, “Basic survey on Malware Analysis, Tools and Techniques,” *Int. J. Comput. Sci. Appl.*, vol. 4, no. 1, pp. 103–112, 2014, doi: 10.5121/ijcsa.2014.4110.