SIMULASI DAN ANALISIS ENCRYPTION BASED RANSOMWARE UNTUK MEMETAKAN EVOLUSI RANSOMWARE

***Budi Ibnu Darmawan**, ****Fietyata Yudha**

Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia Kampus UII terpadu, Jl. Kaliurang km 14.5 Sleman, Yogyakarta

E-mail: *13523064@students.uii.ac.id, **yudha@uii.ac.id,

SARI

Penelitian dalam paper ini adalah untuk mensimulasikan dan menganalisis ransomware untuk memetakan evolusi dari ransomware tersebut, ransomware yang diteliti adalah WannaCry, Petya, NotPetya dan Badrabbit. tools yang digunakan dalam penelitian ini adalah cucko sandbox yang digunakan untuk menganalisis ransomware yang sedang berjalan, volatility yang digunakan untuk mengakses cpu load, kemudian cacty yang digunakan untuk memonitoring aktivitas ransomware setelah di injeksi

Kata Kunci : Ransomware, WannaCry, Petya, NotPetya, Badrabbit

I. PENDAHULUAN

Institusi yang memliki banyak pengguna internet pasti mempunyai beberapa masalah yang dihadapi oleh pengelola jaringan. Salah satunya adalah penyerangan dari orang yang memiliki niat jahat. Mereka yang melakukan itu untuk kepentingan dia sendiri seperti mengunci data *privasi* target, melakukan perusakan data atau *file.* Biasanya pelaku tersebut menyisipkan program yang telah dirancang untuk kepentingannya sendiri kedalam suatu jaringan atau bisa juga melalui aplikasi dan *file* program itu disebut dengan istilah *Malicious Software (*malware).

Malware merupakan *software* yang dirancang untuk mengumpulkan informasi yang sensitive, kebiasaan dari *malware,* baik itu ransomware, bad rabbit, dan notpetya. Kebiasaan dari *malware* tersebut menghentikan proses pada sistem dan menahan data dengan menggunakan sistem enkripsi yang dapat membahayakan data tersebut. Penyebaran dan evolusi *malware* tersebut juga beragam, oleh karena itu diperlukan analisis lebih lanjut terhadap malware tersebut. (Antonio pirozzi, 2017)

Untuk melakukan analisis, hal yang pertama kali dilakukan adalah membangun sebuah *sandbox.* S*andbox* adalah sebuah mekanisme keamanan untuk memmisahkan program yang sedang berjalan (Wikipedia). Artinya, program yang terindikasi *malware* dijalankan pada sebuah *sandbox* yang terisolasi untuk meminimalisir kerusakan yang

dihasilkan oleh *malware* tersebut. Tools yang akan digunakan dalam *sanboxing* yaitu Cuckoo *sandbox.* Cuckoo *sanbox* memungkinkan proses *dynamic dynamic* analisis yang dapat dimonitor secara *real-time.*

Hasil analisis nantinya akan menjadi perbandingan cara kerja *malware* pada perangkat. Hasil ini juga ingin membuktikan adanya penelitian tentang *malware* untuk memetakan evolusi *malware.* Diharapkan adanya penelitian tentang analisis *malware* ini dapat memberikan kontribusi pada bidang keilmuan *forensics* agar dapat berguna dikemudian hari.

II. LANDASAN TEORI

2.1. Ransomware

Ransomware adalah jenis perangkat lunak berbahaya yang mencegah pengguna mengakses atau membatasi akses mereka ke sistem atau file, baik dengan mengunci layar atau dengan mengenkripsi file, sampai meminta tebusan. Dalam banyaknya kasus, ransomware meninggalkan pengguna dengan sangat sedikit opsi, seperti hanya membolehkan korban untuk berkomunikasi dengan penyerang dan membayar tebusan.

2.2. Jenis jenis Ransomware

a. Wannacry

WannaCry pertama kali muncul pada tahun 2017 dimana virus ini menyerang beberapa perusahaan besar di Eropa. WannaCry adalah sebuah ransomware yang diciptakan oleh para hacker, yang menyerang sistem komputer melalui celah keamanan.

b. Petya

Petya merupakan ransomware pengenkripsi yang pertama kali ditemukan pada tahun 2016. Petya menyerang komputer dengan sistem operasi Windows. Dampak yang ditimbulkan dari perangkat pemeras ini adalah pengguna tidak dapat mengakses komputer dan semua berkas di dalamnya terkunci, kemudian perangkat tersebut meminta sejumlah tebusan yang dibayarkan menggunakan Bitcoin.

c. NotPetya

NotPetya merupakan virus perangkat pemeras (ransomware) seperti Petya pada tahun 2016. Dampak yang ditimbulkan dari perangkat pemeras ini adalah pengguna tidak dapat mengakses komputer dan semua berkas di dalamnya terkunci, kemudian perangkat tersebut meminta sejumlah tebusan yang dibayarkan menggunakan Bitcoin.

d. Badrabbit

Bad Rabbit dibangun dari source code yang sama dengan Petya, namun Badrabbit tidak melakukan eksploitasi terhadap celah keamanan seperti yang dilakukan oleh WannaCry dan Petya, pada umumnya badRabbit melakukan rekayasa sosial di mana ia memalsukan dirinya sebagai update / installer Adobe Flash dan di injeksikan pada situs-situs yang tidak terkonfigurasi dengan aman sehingga pengakses situs yang tidak menyadari hal ini mengira mereka mengunduh Adobe Flash dan menjalankannya.

2.3. Sandbox

Sandbox adalah sebuah mekanisme keamanan untuk memisahkan program yang sedang berjalan. Sandbox ini sering digunakan untuk mengeksekusi kode yang belum teruji, atau program yang tidak dipercaya dari pihak pihak ketiga yang tidak diverifikasi, pemasok, pengguna yang tidak dipercaya dan situs yang tidak dipercaya (Bremer, 2018). Konsep ini juga berlaku untuk analisis malware sandboxing yang bertujuan untuk menjalankan aplikasi atau file yang tidak dikenal dan tidak dipercaya didalam lingkungan yang terisolasi dan mendapatkan informasi tentang apa yang dilakukannya.

2.4. Cucko Sandbox

Cuckoo sandbox adalah tool untuk melakukan analisis malware secara otomatis. Digunakan untuk menjalankan dan menganalisa file secara otomatis dan mengumpulkan hasil analisis komprehensif yang menguraikan apa yang dilakukan malware saat berjalan didalam sistem operasi.

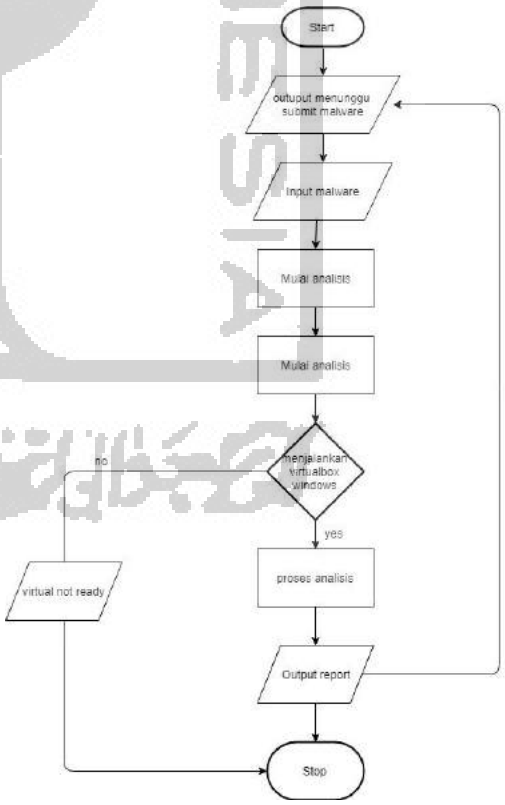
2.5. Volatility

Volatility framework adalah kumpulan tools yang diimplementasikan dengan python dibawah lisensi public-GNU, untuk ekstrak artefak digital dari sampel volatile memori (RAM).

III. METODOLOGI PENELITIAN

3.1. Langkah Penelitian

Langkah pertama yang harus dilakukan adalah membangun lingkungan penelitian. Lingkungan penelitian ini menggunakan mesin linux yaitu Ubuntu 16.04, Langkah selanjutnya adalah melakukan instalasi Cuckoo sandbox dari repository github milik Cuckoo, Setelah cuckoo sandbox telah diinstall, langkah selanjutnya adalah melakukan konfigurasi terhadap beberapa file didalam direktori cuckoo sandbox. Hal yang perlu dipersiapkan selanjutnya adalah Agent.py. pada penelitian ini, Agent.py adalah file ekstensi python yang nantinya akan digunakan dalam proses pengolahan malware.



Gambar 3. 1 Alur analisa cuckoo sandbox

3.2. Analisi Kebutuhan Sistem

a. Python 2.7

Python adalah Bahasa pemrograman yang dapat melakukan eksekusi sejumlah instruksi multiguna secara langsung (interpretative) dengan metode orientasi objek (Object Oriented Programming) serta menggunakan semantic dinamis untuk memberikan tingkat keterbacaan syntax (Advernesia,2018). Python yang digunakan adalah python dengan versi 2.7 dan diinstal pada system operasi Ubuntu.

b. CuckooSandbox

CuckooSandbox adalah tools yamg digunakan untuk menganalisis malware yang akan di eksekusi pada sistem operasi yang telah di injeksikan malware.

c. Volatility

Volatility Framework adalah kumpulan tools yamg diimplementasikan dengan python dibawah lisensi public GNU, untuk ekstraksi artefak digital dari sampel volatile memori (RAM).

d. Virtualbox

Virtualbox adalah software gratis milik Oracle yang fungsi utamanya adalah mem-visualisasi-kan sebuah atau banyak Sistem Operasi (OS) di dalam Sistem Operasi utama kita.

e. MongoDB

MongoDB adalah salah satu produk database noSQL Open Source yang menggunakan struktur data JSON untuk menyimpan datanya. MongoDB adalah merupakan database noSQL yang paling populer di internet. MongoDB sering dipakai untuk aplikasi berbasis Cloud, Grid Computing, atau Big Data.

f. Cacti

Cacti adalah salah satu software yang digunakan untuk keperluan monitoring yang banyak digunakan saat ini. Cacti menyimpan semua data / informasi yang diperlukan untuk membuat grafik dan mengumpulkannya dengan database MySQL. Untuk menjalankan cacti diperlukan software pendukung seperti MySQL, PHP, RRDTool, net-snmp, dan sebuah webserver yang support PHP seperti Apache atau IIS.

3.3. Analisis Kebutuhan Proses

Pada saat melakukan penelitian analisis ransomware menggunakan Cuckoo sandbox, terdapat beberapa proses yang terjadi. Proses berawal dari mengunduh sampel ransomware dari repository Github. Kemudian sampel ransomware yang telah di unduh tadi di submit kepada Cuckoo sandbox. Setelah proses submit selesai, selanjutnya Cuckoo sandbox akan menjalankan virtualbox untuk melakukan proses analisis. Setelah analisis selesai dilakukan, Cuckoo sandbox akan memproses hasil analisis yang telah didapatkan akan di tampilkan ke dalam report melalui halaman website.

Kemudian, proses untuk melakukan analisis ransomware pada file dengan membuka report, setelah itu akan ditampilkan halaman report pada website. Setelah itu kita masuk navigasi bar behavorial analisys, dan disitu kita bisa lihat kebiasaan dari ransomware yang telah kita analisis

3.4. Analisis Ransomware

Tujuan dari penelitian ini adalah untuk membuktikan apakah ransomware dapat mengakses file atau tidak. Maka, langkah awal dari penelitian ini adalah melakukan eksekusi file.exe yang diduga sebagai ransomware kedalam Cuckoo sandbox. Ransomware yang sama juga kita eksekusi pada sisi mesin virtual. Awal eksekusi pada Cuckoo sandbox adalah dengan melakukan submit pada website Cuckoo, kemudian Cuckoo sandbox akan mengeksekusi dan melakukan analisis secara otomatis.

Untuk analisis pada sisi virtual diawali dengan perangkat yang sudah diinjeksi ransomware. setelah file.exe dijalankan pada virtualbox yang sudah diinstal sistem operasi, akan dianalisis monitoring Cacti. Cara melakukan analisis dengan Cacti adalah dengan melihat live report dari proses berjalannya program dalam CPU.

Hasil akhir dari rencana analisis ini adalah diharapkan dapat menemukan dan membuktikan adanya ransomware mengakses file pada sisi virtualbox, serta memetakan evolusi ransomware dari hasil beberapa ransomware yang telah di jalankan pada Cuckoosandbox.

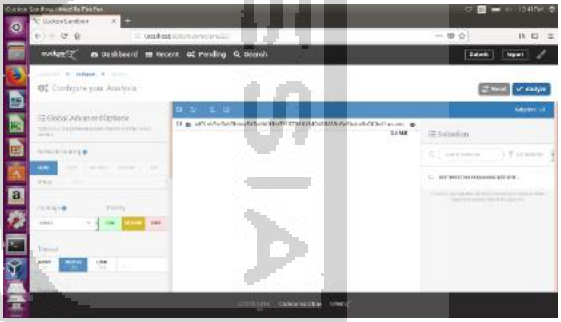
IV. IMPLEMENTASI DAN HASIL PENGUJIAN

4.1. Implementasi Analisis Cuckoo

Setelah proses membangun lingkungan kerja dan instalasi Cuckoo selesai dilakukan, penguji dapat memulai untuk melakukan pengujian terhadap sampel malware. Sampel malware yang akan diuji dan dianalisis adalah berikut :

1. Wannacry : ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
2. Petya : PetyaFix_2_0_766_127.exe
3. Notpetya : Svchost.exe
4. Badrabbit : 630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da.exe

Untuk melakukan analisis, cuckoo memerlukan sampel malware agar dieksekusi kedalam mesin guest. Sampel malware diunggah kedalam mesin host dengan menjalankan perintah cuckoo web pada direktori /opt/cuckoo pada terminal dan akan menampilkan web untuk memngunggah file tersebut

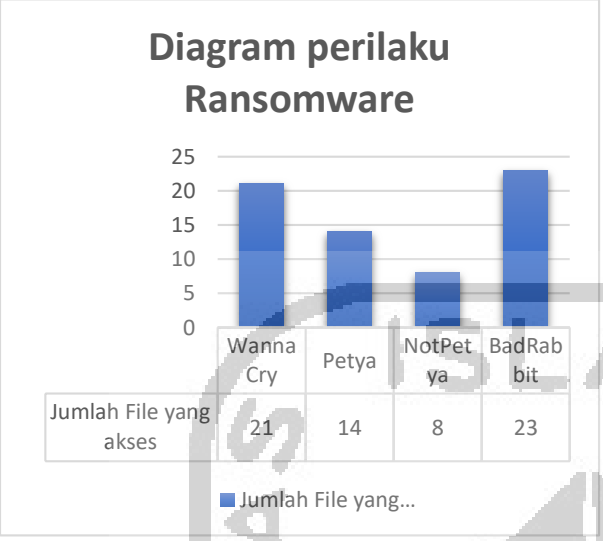


Gambar 4. 1 submit malware exe

4.2. Hasil Analisis Cuckoo

Pada kasus yang diteliti terdapat perbedaan mengenai tingkat perilaku suatu *Ransomware*. Perbedaan ini ditunjukan oleh banyaknya suatu file yang diakses oleh *Ransomware*. jumlah file yang diakses oleh *Ransomware* dapat ditunjukkan dengan menggunakan grafik batang. Gambar 4.22

menunjukan banyaknya file yang diakses oleh *Ransomware*.

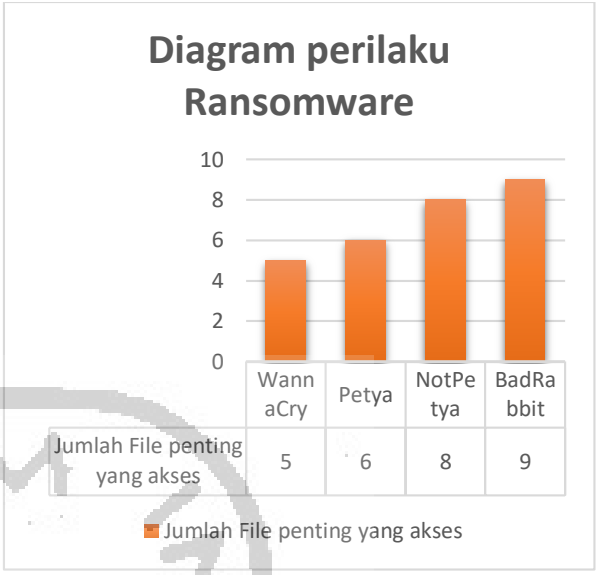


Gambar 4. 2 Diagram perilaku Ransomware berdasarkan jumlah file yang diakses dalam registry.

Berdasarkan empat *Ransomware* yang diteliti, terdapat perbedaan jumlah file yang diakses. Pada Wannacry jumlah file yang diakses sebanyak 21 file. Sedangkan untuk Petya jumlah file yang diakses sebanyak 14 file. Kemudian NotPetya jumlah file yang diakses sebanyak delapan file. Terakhir Badrabbit jumlah file yang diakses sebanyak 23 file.

Berikutnya akan ditampilkan diagram perilaku dari keempat sampel *Ransomware*, dimana dari keempat sampel tersebut mengakses file di dalam *registry* setelah dieksekusi.

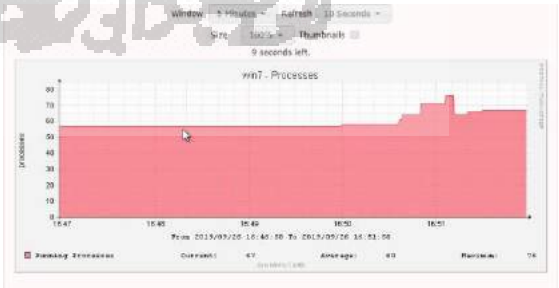
Dimana file yang diakses menunjukkan perilaku dari masing-masing sampel Ransomware, dimana sampel tersebut menghapus *file*,mengedit *file*,dan membuat *file*. Dan data dari perilaku bisa dilihat pada lampiran. Kemudian akan ditampilkan hasil diagram perilaku dari masing-masing *Ransomware* bisa dilihat pada gambar 4.23



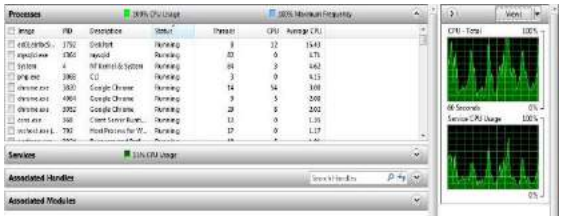
Gambar 4. 3 Diagram perilaku Ransomware berdasarkan jumlah file penting yang diakses dalam registy.

Berdasarkan empat *Ransomware* yang diteliti, terdapat perbedaan jumlah file penting yang diakses. Pada Wannacry jumlah file penting yang diakses sebanyak lima file penting. Sedangkan untuk Petya jumlah file penting yang diakses sebanyak enam file penting. Kemudian NotPetya jumlah file penting yang diakses sebanyak delapan file penting. Terakhir Badrabbit jumlah file yang diakses sebanyak sembilan file penting.

4.3. Hasil Monitoring cacti



Gambar 4. 4 hasil setelah ransomware dijalankan

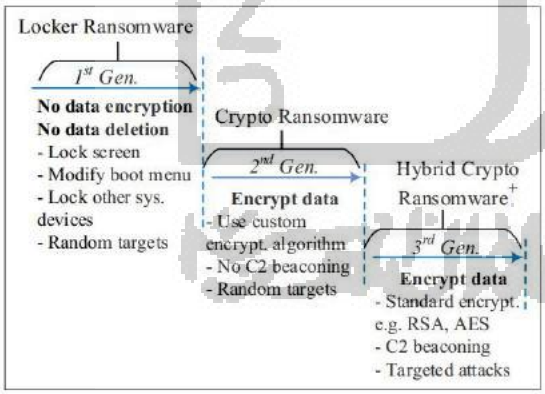


Gambar 4. 5 proses CPU dari task manager

Berdasarkan hasil yang ditunjukkan, proses yang di hasilkan menyebabkan menumpuknya proses pada mesin tempat dijalankannya ransomware tersebut. Dimana membuat kinerja dari mesin tersebut menjadi lambat dikarenakan menumpuknya proses pada CPU.

4.4. Evolusi Ransomware

Penulis menyajikan kerangka kerja yang mengklasifikasikan apa yang diberikan Ransomware generasi pertama, kedua, dan ketiga, dimana data ini saya dapatkan dari penelitian (Zimba & Chishimba, 2019). Kerangka tersebut didasarkan pada evolusi berbagai karakteristik struktur serangan Ransomware disajikan dalam Gambar 4.35.



Gambar 4. 6 Evolusi struktur serangan Ransomware

Dari gambar tersebut generasi pertama tidak menggunakan enkripsi dan pencegahan pemulihan data. generasi kedua menggunakan enkripsi, tetapi masih dapat dipulihkan karena kurangnya strategi implementasi. Dan generasi ketiga memasukkan enkripsi yang kuat serta komunikasi dengan server C2.

V. KESIMPULAN

Setelah melakukan penelitan menggunakan tools Cuckoo Sandbox dengan objek *Ransomware* Wannacry, Petya, NotPetya dan Badrabbit penguji menarik kesimpulan. penulis berhasil membangun lingkungan penelitian menggunakan sistem operasi Ubuntu 16.04 LTS. Cuckoo Sandbox dapat dipasang dan dapat terintegrasi dengan baik kepada mesin Virtualbox sebagai wadah eksekusi dan analisis sampel *Ransomware* Wannacry, Petya, NotPetya dan Badrabbit. Kemudian penulis berhasil mengimplementasikan sampel *Ransomware* pada perangkat Windows melalui Virtualbox. Dan menganalisis hasil dari tiap *Ransomware* dengan menggunakan Cuckoo Sandbox dan monitoring Cacti.

Hasil dari analisis sampel *Ransomware* dapat diketahui, perilaku dari *Ransomware* yang dilihat dari jumlah *file* dan *file* penting yang diakses pada *registry*, dan dari tahun 2016 sampai 2017 peningkatan kerusakan kebanyakan dari generasi ketiga, dengan *CAT5* yang menunjukan tingkat kerusakan sangat tinggi yang sebelumnya telah di klasifikasi. Dan dari generasi ketiga menunjukkan mereka bisa masuk ke seluruh struktur jaringan yang kemudian menginfeksi setiap host yang rentan untuk diserang.

Kemudian hasil monitoring CPU menggunakan Cacti menunjukkan adanya penambahan proses pada CPU setelah *Ransomware* Petya dan Wannacry di jalankan.

REFERENSI

Akbanov, M., Vassilios G. Vassilakis, & Michael D. Logothetis. (2019). Static

and Dynamic Analysis of WannaCry Ransomware. *Information and Communication Technology*, 12.

Burnap, P., French, R., Turne, F., & Jones, K. (2018). Malware classification using self organising feature maps and machine activity data. *c o m p u t e r s & s e c u r i t y*, 12.

detik inet. (2019, october 11). Retrieved from detik.com: https://inet.detik.com/konsultasi-internet-security/d-3703943/mengenal-bad-rabbit-si-kelinci-nakal

Jagat Review. (2019, october 11). Retrieved from Jagat Review: jagatreview.com/2017/05/5-hal-yang-perlu-kamu-tahu-dari-ransomware-wannacry/

KARDILE, A. B. (2017). CRYPTO RANSOMWARE ANALYSIS AND DETECTION USING PROCESS MONITOR. *THE UNIVERSITY OF TEXAS AT ARLINGTON*, 49.

Labs, L. R. (2017). notpetya technical analisys. *The Security Intelligence Company*, 12.

Muhammad, A. H., Sugiantoro, B., & Luthfi, A. (2017). METODE KLASIFIKASI DAN ANALISIS KARAKTERISTIK MALWARE MENGGUNAKAN KONSEP ONTOLOGI. *Magister Teknik Informatika Universitas Islam Indonesia*, 14.

Pirozzi, A. (2018). Malware Analysis Report: A new variant of Mobef Ransomware. *Cybaze Group*, 10.

Sharma, A., & Sahay, S. K. (2014). Evolution and Detection of Polymorphic and Metamorphic Malwares: A Survey. *International Journal of Computer Applications (0975 – 8887)*, 5.

Tedyyana, A., & Supria. (2018). Perancangan Sistem Pendeteksi Dan Pencegahan Penyebaran Malware Melalui SMS Gateway. *JURNAL INOVTEK POLBENG - SERI INFORMATIKA*, 7.

virus, T. (2019, october 11). Retrieved from Tanpavirus.com: http://tanpavirus.web.id/virus-petya/

virustotal. (2019, 10 22). Retrieved from virustotal.com: https://www.virustotal.com/gui/file/55504677f82981962d85495231695d3a92aa0b31ec35a957bd9cbbef618658e3/detection

Zimba, A., & Chishimba, M. (2019). Understanding the Evolution of Ransomware:Paradigm Shifts in Attack Structures. *Computer Network and Information Security*, 39.

jagatreview.com/2017/05/5-hal-yang-perlu-kamu-tahu-dari-ransomware-wannacry/

[7] 7KARDILE, A. B. (2017). CRYPTO RANSOMWARE ANALYSIS. 49.

[8] 8log Rythm Labs. (2017). notpetya technical analisys. 12.

[9] Pete Burnap, Richard French, Frederick Turne, & Kevin Jones. (2018). Malware classification using self organising feature maps and machine activity data. 12.

[10] Tedyyana, A., & Supria. (2018). Perancangan Sistem Pendeteksi Dan Pencegahan. 7.

[11] virus, T. (2019, october 11). Retrieved from Tanpavirus.com: http://tanpavirus.web.id/virus-petya/