RESEARCH PAPER
published: 24-08-2019
doi: 10.21070/jicte.v3i1.951

Wannacry Identification For Computer Data Security

Identifikasi Wannacry Untuk Keamanan Data Komputer

Alfan Hakim Wijaya*, Arif Senja Fitrani

Universitas Muhammadiyah Sidoarjo, Prodi Informatika, Fakultas Teknik

The purpose of this study is, to find out the features of the wanscry ransomware that have not been run and extract the Windows computer data system from wannacry in the scope of an interconnection network. To find out the behavior of wannacry ransomware after running on a Windows computer system and knowing how to use the ransomware

The method used in this research is Surface Analysis, Static Analysis, Runtime Analysis, and Intrusion Detection System. The research was carried out in the umsida informatics laboratory, data collection information about wannacry through journals, ebooks, and the internet. Identification techniques are carried out before ransomware is run on the system Windows operation, and after running.
The conclusion of this study is to identify the characteristics of wannacry ransomware outside with software strings, graphics, and to identify in depth with the OllyDbg, IdaPro software, and to identify when the ransomware is run the software used by TcpView, Procmon, ProcessExplore. Determine the exploitation technique of wannacry spread on computer systems. Along with ways to prevent the spread of infections in computer systems and networks using microtics

Keywords: ransomware, wannacry, eternablue exploit, windows, linux, wanancry ransomware analysis

Tujuan penelitian ini adalah, Untuk mengetahui ciri dari ransomware wanancry yang belum dijalankan dan mengamankan data sistem komputer windows dari penyebaran wannacry di lingkup yang terdapat sebuah jaringan interkoneksi. Untuk mengetahui perilaku ransomware wannacry setelah jalan di sistem komputer windows serta mengetahui exploit penyebaran ransomware tersebut.
Metode yang digunakan dalam penelitian ini adalah Surface Analysis, Static Analysis, Runtime Analysis, dan Intrusion Detection System, Penelitian dilakukan di laboratorium informatika umsida, Pengumpulan data informasi tentang wannacry melalui jurnal, ebook, daninternet.Teknik identifikasi dilakukan sebelum ransomware di jalankan di sistem operasi windows, dan setelah di jalankan.
Kesimpulan dari penelitian ini yaitu Mengindentifikasi ciri dari ransomware wannacry secara luar dengan software strings,pefram, serta mengindetifikasi secara dalam dengan software OllyDbg, IdaPro, Dan mengindetifikasi saat ransomware di jalankan software yang digunakan TcpView, Procmon, ProcessExplore. Mengetahui exploit teknik penyebaran wannacry di sistem komputer. Beserta cara untuk mencegah penyebaran infeksi

OPEN ACCESS
ISSN 2541-5107 (online)
Edited by:
Akbar Wiguna
Reviewed by:
Susilo Purnomo Hadi
****Correspondence:***
Alfan Hakim Wijaya
alfan.hakim@umsida.ac.id
Received: *01-07-2019*
Accepted: *14-07-2019*
Published: *24-08-2019*
Citation:
Wijaya AH and Fitrani AS (2019) Wannacry Identification For Computer Data Security. JICTE (Journal of Information and Computer Technology Education). 3:1. doi: 10.21070/jicte.v3i1.951

di sistem komputer maupun jaringan menggunakan mikrotik.

Keywords: ransomware, wannacry, exploit eternablue, windows, linux, analisis ransomware wanancry

PENDAHULUAN

Internet Security Theart Report dari symantec infeksi serangan perangkat lunak berbahaya yang menggunkan teknik kriptografi yang mengancam untuk mempubliskasikan data korban atau memblokir akses secara permanen dengan uang tebuasan atau disebut ransomware terus meningkat, dan pada mei 2017 di identifikasi ransomware baru yang mengenkripsi data, serta membuat salinan sendiri dan memberikan waktu untuk membayar, dengan memperingatkan bahwa file korban akan dihapus. ransomware jenis ini dikenal sebagai wannacry . Menurut tim Internet Security Theart Report menganggap ramsomware wannacry yang paling berbahaya dari pada ransomware petya atau notpetya dan ransomware badrabbit di tahun 2017 Aidan et al. (2017). hal ini terbukti sampai tahun 2017 ransomware Wannacy masih mengeluarkan varian terbarunya yaitu Wannacry 2.01 Nisha (2017) .

Penyebaran ransomware wannacry yang menyerang komputer dalam satu jaringan begitu cepat, Karena penyebaran wannacry menggunakan tools atau exploit dari National Security Agency (NSA). Exploit ini bernama eternalblue, yang memanfaatkan celah keamanan di sistem operasi Windows lewat eksekusi remote code SMBv1 serta menggunakan port 139/445 dan 3389 untuk menyerang sistem komputer .saat wannacry menginfeksi komputer yang terhubung jaringan menggunakan kabel LAN, worm dalam WannaCry secara otomatis akan mencari sendiri komputer lain di network yang rentan untuk diinfeksi2.[2]

Teknologi enkripsi yang digunakan Wannacry adalah enkripsi RSA 2048 yang digunakan oleh raksasa internet seperti Yahoo, Google, Facebook, industri keuangan dan e-commerce untuk melindungi lalu lintas data dari transaksi keuangan dan transaksi penting lainnya. Dimana kunci dekripsinya (Private Key) hanya dimiliki oleh pembuat ransomware, yang memiliki akses dan kontrol pada server yang digunakan untuk melakukan enkripsi. Namun, dalam banyak kasus, sekalipun uang tebusan (bitcoin) sudah dibayar, tidak ada jaminan bahwa dekripsi atas data yang dienkripsi akan berhasi3l.[3]

METODE PENELITIAN

Lokasi Penelitian

Penelitian ini dilakukan di Laboratorium Sistem Operasi, Jurusan Informatika, Fakultas Teknik, Universitas Muhammadiyah Sidoarjo

Alat Dan Bahan Penelitian

Analisis kebutuhan (Requirements Definition) adalah tahap yang menjadi dasar proses yang dibutuhkan dalam menganalisis wannacry dengan menggunakan metode Surface analysis, Static Analysis, Runtime Analysis Intrusion Detection System. Dari penjelasan tersebut, maka kebutuhan dari penggunaan aplikasi pada penelitian ini sebagai berikut :

a.Hardware

Hardware yang digunakan untuk melakukan analisis wannacry ini adalah personal computer/laptop dengan sebagai berikut :

1. Komputer server dengan sistem operasi linux backbox 64bit sebagai Intrusion Detection System Exploit EternalBlue.
2. Laptop dengan sistem operasi linux backbox 64bit dan sistem operasi virtual yaitu windows ultimate 32bit, untuk surface analysis dan static analysis.
3. Komputer dengan sistem operasi windows ultimate 32bit yang telah terinfeksi wannacry untuk Runtime Analysis.
4. Satu unit Switch Hub TP-LINK TL-SF1024
5. Satu Unit RB2011uias-2hnd-in (Mikrotik)
6. Kabel lan yang sudah terhubung jaringan

b. Software / Tool

Adapun software yang digunakan untuk melakukan analisis wannacry untuk mengidentifikasi jenis dan pola serangan wannacry.

1. Oracle VM VirtualBox Manager : Software gratis milik Oracle yang fungsi utamanya adalah mem-visualisasi- kan sebuah atau banyak Sistem Operasi (OS) di dalam Sistem Operasi utama.
2. Wireshark : Program Network Protocol Analyzer alias penganalisa protokol jaringan yang lengkap. Program ini dapat merakam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin.
3. Snort : Sebuah perangkat lunak yang berfungsi untuk mengamati aktivitas dalam suatu jaringan komputer.

Snort ini disebut juga sebagai NIDS (Network Intrusion Detection System) yang berskala ringan.

4. Peframe : Software Opensource berbasis perintah (terminal) yang secara otomatis dapat mengekstrak file properti statis, menampilkan beberapa informasi yang dapat menjelajahi file secara interaktif.
5. Procmon : Aplikasi portable untuk merekam perilaku program yang sedang berjalan. Berbeda dengan Process Explorer yang merekam penggunaan sumber daya komputer, Process Monitor akan menangkap setiap ”perbuatan” program yang berjalan dari tiap proses.
6. Strings : Software perintah bawaan linux Backbox mirip dengan aplikasi peframe yaitu menjalankanya lewat terminal dan berfungsi untuk melihat code string suatu file.
7. OllyDbg : Aplikasi portable untuk analisa perilaku malware untuk melihat angka biner dan menjalan debugger.
8. Ida Pro : Aplikasi analisis perangkat lunak yang paling terkenal. yang merupakan standar de facto dalam industri keamanan perangkat lunak. aplikasi yang sangat diperlukan dalam analisa perangkat lunak, analisa biner yang serius dan analisa malware.
9. Tcpview : Sniffer jaringan yang menunjukkan semua informasi tentang paket TCP / UDP
10. Procexplore : Aplikasi Portable Mirip Task Manager bawaan windows namun dengan fungsi tambahan yang menjadikannya sebagai Advanced Task Manager, Process Explorer akan

menampilkan informasi tiap proses dengan lebih terperinci.
11. PeStudio : Software portabel GUI untuk statis memeriksa berbagai aspek dari file Windows executable yang mencurigakan, seperti nama fungsi impor dan ekspor dan strings.

Perancangan Analisa Wannacry Dan Mencegah Penyebarannya

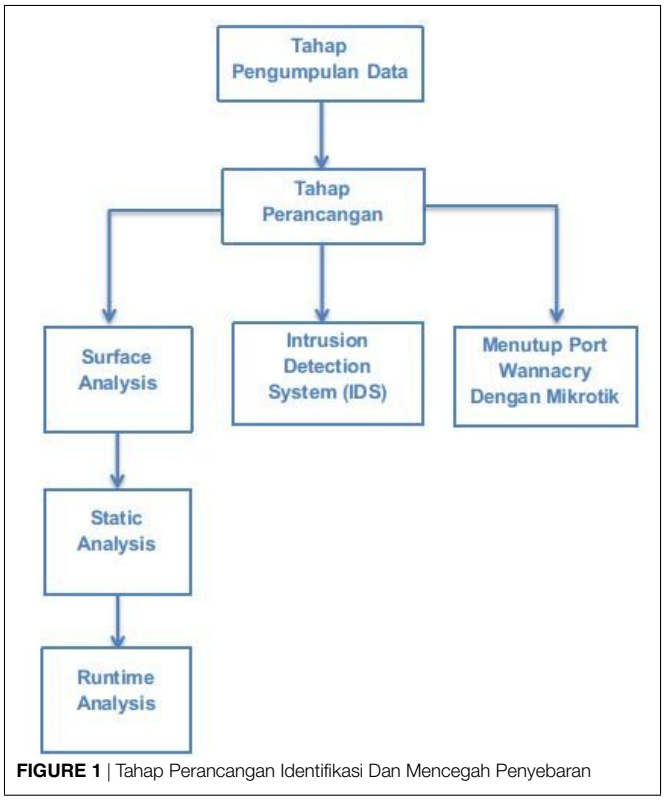

FIGURE 1 | Tahap Perancangan Identifikasi Dan Mencegah Penyebaran

Metode Surface Analysis

Berikut adalah bagan dari tools surface analysis wannacry dan fungsinya

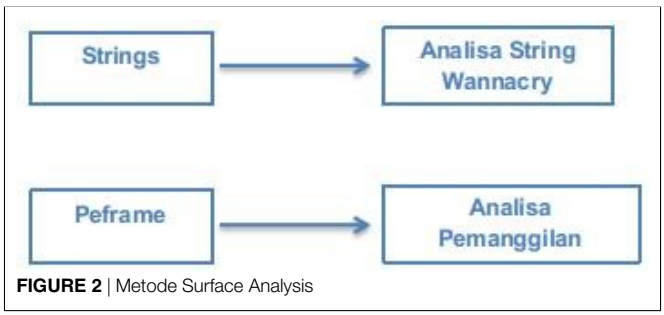

FIGURE 2 | Metode Surface Analysis

Metode Static Analysis

Berikut adalah bagan dari tools static analysis wannacry dan fungsinya

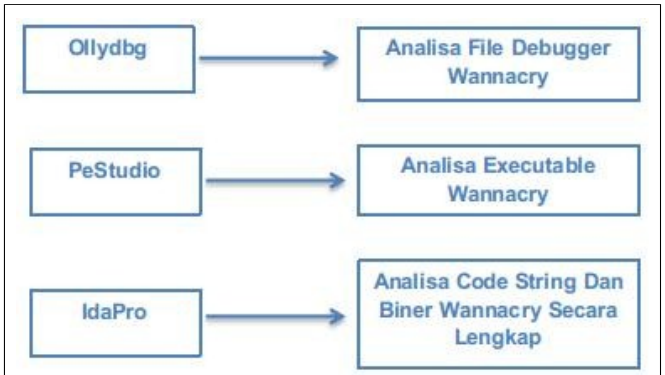

FIGURE 3 | Metode Static Analysis

Metode Runtime Analysis

Berikut adalah bagan dari tools runtime analysis wannacry dan fungsinya

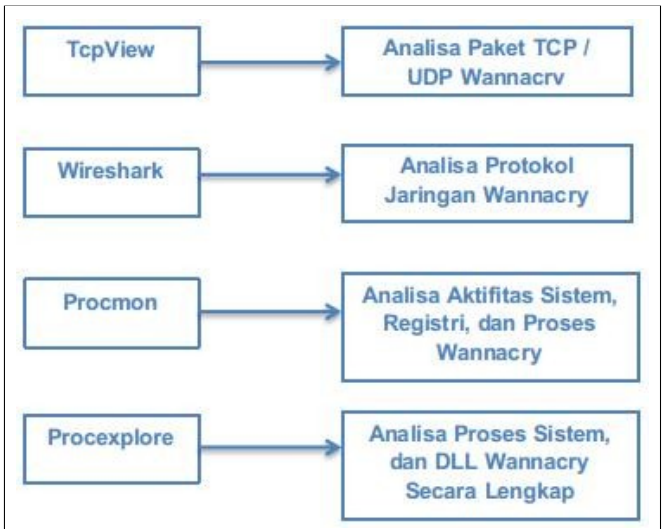

FIGURE 4 | Metode Runtime Analysis

Intrusion Detection System

Berikut adalah bagan dari toolsintrusion detection system dan fungsinya

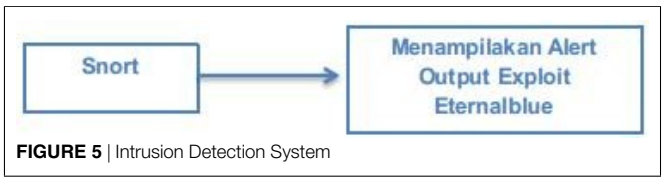

FIGURE 5 | Intrusion Detection System

Menutup Port Wannacry

Berikut adalah bagan dari Alat Mikrotik untuk menutup port wannacry

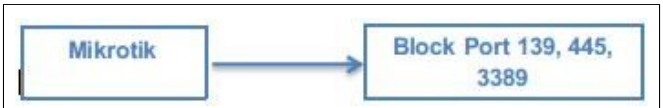

FIGURE 6 | Menutup Port Wannacry

PEMBAHASAN

Dalam mengidentifikasi program wannacry, diperlukan tahap pengujian yang dapat digunakan sebagai acuan dalam menentukan karakteristik dan menggali informasi terkait dari perilaku yang akan ditimbulkan oleh program wanancry tersebut.

Metode Surface Analysis

Pada Metode Surface Analysis menggunakan software strings, dan peframe yang sudah disiapkan di linux backbox. Tampilan Password WNcry@2ol7 untuk membuka isi file dari si wannacry.exe menggunkan software strings lewat terminal linux backbox.

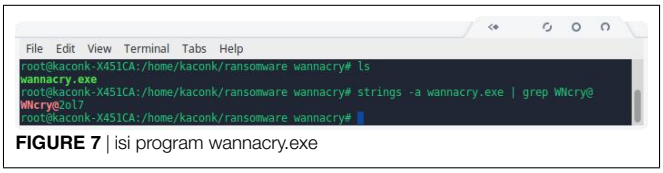

FIGURE 7 | isi program wannacry.exe

Metode Static Analysis

Pada Metode Static Analysis menggunakan software OllyDbg, PeStudio, yang sudah di siapkan di mesin virtual windows 7 dan software IdaPro yang sudah terinstall di linux backbox. Menggunakan Aplikasi OllyDbg, Di Bawah ini Hex Dump dan ASCII, di temukan Hex 40 dan ASCII MZ yang dimaksud file wannacry di jalankan secara portable dengan jenis file PE (Preinstallation Environment).

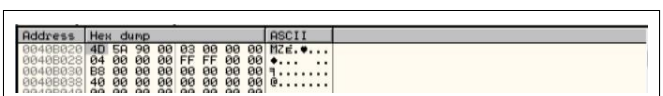

FIGURE 8 | . Identifikasi hex dan ASCII

Tampilan URL kill switch file wannacry menggunakan ollydbg, yang saat dijalankan pertama kali memanggil URL dan jika tidak ada respon dari URL, malware terus dijalankan. Link URL wannacry, http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

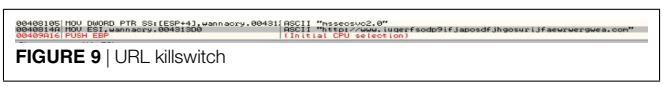

FIGURE 9 | URL killswitch

Metode Static Analysis juga menggunakan Linux Backbox dengan aplikasi Ida Pro yang sudah terinstall. Identifikasi lanjut yaitu wannacry memanggil fungsi API di memori untuk merujuk ke file korban. Seperti memanggil API CreateProcessA, CreateFileA, WriteFile, dan CloseHandle.

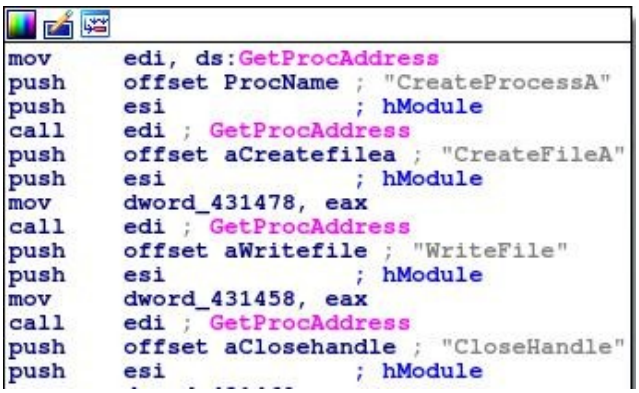

FIGURE 10 | Pemanggilan API

Metode Runtime Analysis

Pada Metode Runtime Analysis menggunakan software portable TcpView, Procmon, dan ProcessExplore yang sudah di siapkan di mesin virtual windows 7 dan juga wireshark yang sudah terinstall di linux Backbox. TcpView Aplikasi Portable yang bertugas untuk menangkap paket TCP/UDP port wanancry yang aktif di sistem

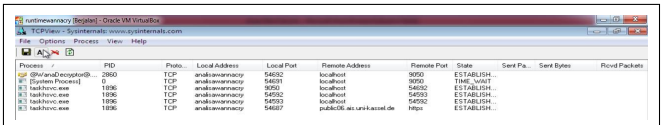

FIGURE 11 | Paket TCP yang berjalan

Procmon melihat aktifitas perubahan registry dan penyerangan system dll wannacry di windows seperti sistem kerne32.dll, aplikasi ini portable sehingga ringan an cepat saat digunakan untuk analisa runtime malware.

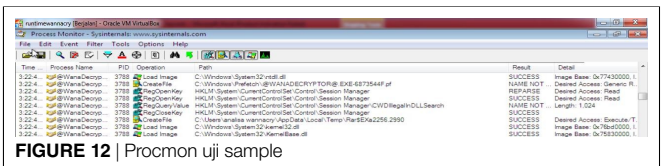

FIGURE 12 | Procmon uji sample

Process Explore aplikasi portable terakhir dalam runtime analysis untuk menganalisa prosess berjalannya wannacry saat di komputer. Diidentifikasi terdapat file bawaan dari wannacry seperti file taskhsvc.exe yang membuat data berisi tor klien, untuk mengkoneksikan ke server wannacry. dan juga membuat file bernama @WannDecryptor@.exe yang berfungsi

untuk memanggil fungsi api enkripsi, serta pembayaran dan cara menggunakan bitcoin.

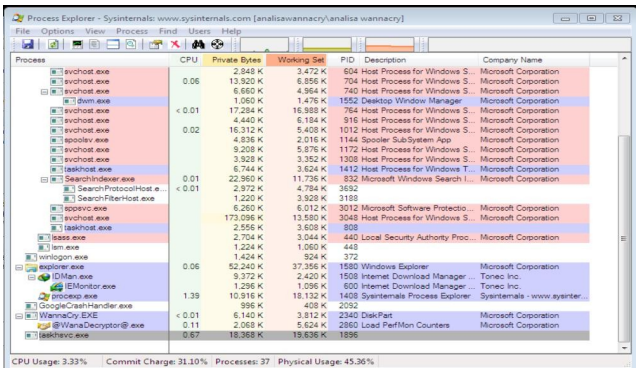

FIGURE 13 | ProcessExplorer uji sample

Wireshark aplikasi bawaan linux Backbox untuk menganalisa trafik jalannya wannacry di sistem. Wireshark menangkap dns killswitch, dan karena dns sudah offline dns tidak tercapai ke server.kemudian wireshark menganalisa wanancry yang menscan ip yang mempunyai port 445 untuk smb di windows.

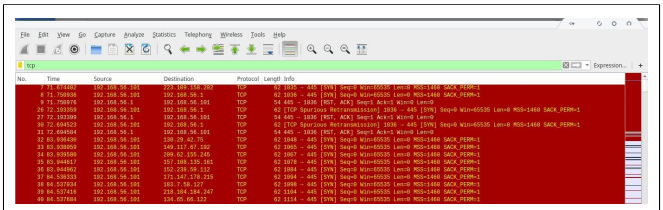

FIGURE 14 | Wireshark deteksi port 445 vulnerability

Intrusion Detection System

Identifikasi yang digunakan untuk melihat penyebaran wannacry melalui exploit Eternalblue & DoublePulsar yang menyerang sistem SMB di windows. Dengan software ids snort yang sudah terinstall dan dikonfigurasi mendeteksi exploit eternalblue yang menyerang sistem SMB windows dapat ditangkap.

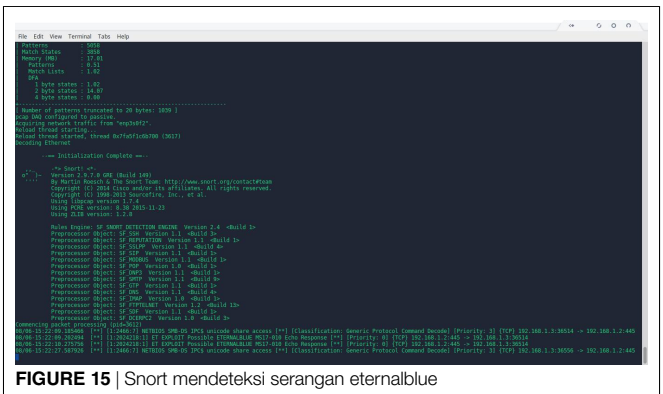

FIGURE 15 | Snort mendeteksi serangan eternalblue

Menutup Port Wannacry

Mencegah penyebaran wannacry di jaringan komputer dengan menutup port 137,445,3389 dengan mikrotik menggunakan fitur firewall.

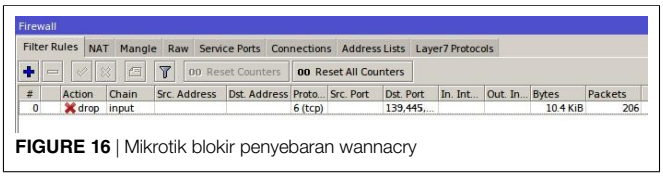

FIGURE 16 | Mikrotik blokir penyebaran wannacry

KESIMPULAN

Identifikasi yang dirancang untuk mengetahui ciri dari ransomware wannacry. Identifikasi yang dirancang diketahui bahwa format file yang terinfeksi wannacry yaitu :123, .jpeg , .rb , .602 , .jpg , .rtf , .doc , .js , .sch , .3dm , .jsp , .sh , .3ds , .key , .sldm , .3g2 , .lay , .sldm , . 3gp , .lay6 , .sldx , .7z , .ldf , .slk , .accdb , .m3u , .sln , .aes , .m4u , .snt , .ai , .max , .sql , .ARC , .mdb , .sqlite 3 , .asc , .mdf , .sqlitedb , .asf , .mid , .stc , .asm , .mkv , .std , .asp , .mml , .sti , .avi , .mov , .stw , .backup , .mp3 , .suo , .bak , .mp4 , .svg , .bat , .mpeg , .swf , .bmp , .mpg , .sxc , .brd , .msg , .sxd , .bz2 , .myd , .sxi , .c , .m yi , .sxm , .cgm , .nef , .sxw , .class , .odb , .tar , .cmd , .odg , .tbk , .cpp , .odp , .tgz , .crt , .ods , .tif , .cs , .odt , . tiff , .csr , .onetoc2 , .txt , .csv , .ost , .uop , .db , .otg , .uot , .dbf , .otp , .vb , .dch , .ots , .vbs , .der" , .ott , .vcd .dif , .p12 , .vdi , .dip , .PAQ , .vmdk , .djvu , .pas , .vmx , .docb , .pdf , .vob , .docm , .pem , .vsd , .docx , .pfx, .vsdx , .dot , .php , .wav , .dotm , .pl , .wb2 , .dotx , .png , .wk1 , .dwg , .pot , .wks , .edb , .potm , .wma , .eml, .potx , .wmv , .fla , .ppam , .xlc , .flv , .pps , .xlm , .frm , .ppsm , .xls , .gif , .ppsx , .xlsb , .gpg , .ppt , .xlsm , . gz , .pptm , .xlsx , .h , .pptx , .xlt , .hwp , .ps1 , .xltm , .ibd , .psd , .xltx , .iso , .pst , .xlw , .jar , .rar , .zip , .java , .raw. Identifikasi yang dirancang dapat mengetahui bagaimana penyebaran wannacry terhadap sistem operasi komputer, terutama windows. Memblokir penyebaran wannacry dengan mikrotik.

REFERENCES

Aidan, J. S., Verma, H. K., and Awasthi, L. K. (2017). Comprehensive Survey on Petya Ransomware Attack. *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*, 122–125.

Nisha, F. (2017). RSA Public Key Cryptography Algorithm -AReview". *Water Resources Research* 6, 7–7.

Conflict of Interest Statement: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.