JICTE (Journal of Information and Computer Technology Education)
Vol 3 No 1 (2019): August, 22-28
Articles

Wannacry Identification For Computer Data Security

Identifikasi Wannacry untuk Keamanan Data Komputer

Alfan Hakim Wijaya
Arif Senja
Program Studi Informatika, Fakultas Teknik, Universitas Muhammadiyah Sidoarjo

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

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[1] . Menurut tim Internet Security Theart Report menganggap ramsomware wannacry yang paling berbahaya dari pada ransomware petya atau notpetya dan ransomware badrabbit di tahun 2017[2]. hal ini terbukti sampai tahun 2017 ransomware Wannacy masih mengeluarkan varian terbarunya yaitu Wannacry 2.0[3] .

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 :

b. Software / Tool

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

References

1. https://habibahmadpurba.wordpress.com (2013), Jenis-jenis port untuk koneksi Data, email : habibahmadpurba@yahoo.co.id
2. Nisha, Farik (2017) a. “RSA Public Key Cryptography Algorithm –AReview”, Water Resources Research, VOLUME 6, ISSUE 07.
3. Bernardino Madaharsa Dito Adiwidya (2008), Algoritma AES (Advanced Encryption Standard) dan
4. Penggunaannya dalam Penyandian Pengompresian Data, Institut Teknologi Bandung, Bandung.
5. Karen Scarfone Dan Peter Mell (2007), Guide to Intrusion Detection and Prevention System (IDPS), National
6. Institute of Standards and Technology, USA.
7. http://ilmukomputer.org (2018), Pengenalan Dan Dasar Penggunaan Wireshark, Author: Annisa
8. Cahyaningtyas.
9. Aaron Zimba, Luckson Simukonda, Mumbi Chishimba (2017), “Demystifying Ransomware Attacks: Reverse Engineering and Dynamic Malware Analysis of WannaCry for Network and Information Security”, Water Resources Research, Vol. 1,No.1 hal. 35-40
10. Justin Jones, Narasimha Shashidhar (2017), “Ransomware Analysis and DefenseWannaCry and the Win32 environment”, Water Resource Research, Vol.6, No.4.
11. Suryadi Syamsu (2014), Modul Jaringan Komputer, BAB 4 Protokol Jaringan Komputer, STMIK AKBA.
12. Suryadi Syamsu, (2014), Modul Jaringan Komputer, BAB 1 Pengenalan Jaringan Komputer, STMIK AKBA.
13. Sean Dillon, Dylan Davis (2017), ETERNALBLUE Exploit Analysis and Port to Microsoft Windows 10, RiskSense, U.S. Department of Defense and U.S. Intelligence Community.
14. Computer Security Incident Response Team of Mauritius (2017), The Wannacry Ransomeware, CERT-MU, Port Louis.