Lembar Pengesahan Pembimbing

ANALISIS RANSOMWARE CRYPTOLOCKER MENGGUNAKAN METODE SURFACE ANALYSIS, RUNTIME ANALYSIS DAN STATIC CODE ANALYSIS UNTUK MENDUKUNG INVESTIGASI MALWARE FORENSICS

Nama: Luluk Usman

NIM: 12917118

Yogyakarta, April, 2017

Pembimbing I	Pembimbing II
Dr. Imam Riadi, M.Kom	Yudi Prayudi, S.Si.,M.Kom

Lembar Pengesahan Penguji

ANALISIS RANSOMWARE CRYPTOLOCKER MENGGUNAKAN METODE SURFACE ANALYSIS, RUNTIME ANALYSIS DAN STATIC CODE ANALYSIS UNTUK MENDUKUNG INVESTIGASI MALWARE FORENSICS

Nama: Luluk Usman

NIM: 12917118

Yogyakarta, April, 2017

Tim Penguji,

Dr. Imam Riadi, M.Kom
Ketua

Yudi Prayudi, S.Si.,M.Kom
Anggota I

Dr. Bambang Sugiantoro
Anggota II

Mengetahui,
Ketua Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia

Dr. R. Teduh Dirgahayu, ST.,M.Sc

Abstrak

Salah satu program jahat baru yang muncul beberapa tahun terakhir ini adalah Ransomware, mulai pada kuartal pertama 2014 Salah satu jenis ransomware dikenal dengan nama Cryptolocker. Para peneliti CTU menganggap Cryptolocker akan menjadi ransomware yang terbesar dan paling merusak di internet. Sampai dengan tahun 2017 ini, cryptolocker masih merelease varian terbarunya. Dalam penelitian ini menganalisa malware cryptolocker dengan tiga metode analisis malware yaitu surface analysis, runtime analysis dan static code analysis untuk mendukung malware forensic. Pada analisis malware dengan metode surface analysis dilakukan pengujian terhadap malware dengan cara scanning oleh antivirus, dilanjutkan dengan hashing pada malware, dan deteksi paket / obfuscated dilanjutkan dengan analisa Portable Executable dan analisa dengan malware sandbox. Sedangkan pada metode runtime analysis disiapkan sebauh environment atau lingkungan hidup malware kemudian malware dijalankan untuk selanjutnya dilakukan beberapa pengamatan perubahan registry, pengamatan aktifitas DNS, dan aktifitas komunikasi data jaringan. Pada penelitian dengan metode Static Code Analisis dilakukan pengujian untuk mencari hubungan penggunaan linked libraries dan function kemudian dilakukan pencarian string sebagai petunjuk langkah kerja dari malware, serta melakukan debugging pada malware untuk menelusuri lebih dalam perilaku malware. Dari penelitian ini didapatkan informasi tentang karakteristik dari malware dalam menyerang sistem. Pada analisa malware dengan metode surface analysis, malware mempunyai kemampuan perlindungan diri dengan terbungkus packed, pada analisa malware Runtime Analysis, malware melakukan perubahan registry, memantau aktifitas pada file system, proses dan thread yang terjadi, melakukan hubungan koneksi yang dilakukan oleh malware terhadap server malware, dan pada analisis static code dapat memberikan informasi yang sebelumnya tidak ditemukan dengan metode lain, yaitu malware mampu untuk berlindung dari pengawasan sistem keamanan komputer dan mematikannya seperti mematikan firewall, dan antivirus.

Kata kunci

malware, cryptolocker, surface , runtime, static code, forensic.

Abstract

One of the new malware that appears these last few years is Ransomware, starting in the first quarter of 2014 one type of ransomware known by the name Cryptolocker. Researchers CTU assume Cryptolocker will be the largest ransomware and most damaging on the internet. Up to the year 2017 is cryptolocker, still release the latest variant. In this study analyzes malware cryptolocker with three methods of malware analysis i.e. surface analysis, runtime analysis and static code analysis to support the malware forensic. On the analysis of malware with the method of surface analysis testing against malware by means of scanning by antivirus, followed by hashing on malware, and detection packages/obfuscated continued with the analysis of the Portable Executable and analysis with malware sandbox.While the malware analysis with runtime analysis methods the first step is setting up the environment for malware then run malware, further testing is performed to find out the changes to the registry, to know the DNS activity, and data communication networks,and on analysis of malware with Static Code Analysis method of testing done to find the relationship of the use of the linked libraries and function then do a search string as a work step instructions from malware, as well as perform debugging on malware to search deeper into the behavior of malware.From this research obtained information about the characteristics of malware in attacking the system.On malware analysis with the method of surface analysis, malware has the ability to self protection with wrapped packed, on the analysis of malware with the Runtime methods of Analysis, malware changes registry, monitor activity on a file system, process and thread that was going on, have the connections performed by malware against a server malware, and on analysis of static code can provide information not previously found by other methods, that the malware was able to shelter from surveillance computer security system and turn it off like turning off the firewall, and antivirus.

Keywords

malware, cryptolocker, surface , runtime, static code, forensic.

Pernyataan keaslian tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Untuk material yang membutuhkan izin, saya juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan material tersebut dalam tesis ini.

Yogyakarta, April, 2017

Luluk Usman, ST

Publikasi selama masa studi

Usman, L., Prayudi, Y., & Riadi, I. (2017). RANSOMWARE ANALYSIS BASED ON THE SURFACE, RUNTIME AND STATIC CODE METHOD. *JOURNAL OF THEORETICAL AND APPLIED INFORMATION TECHNOLOGY (E-ISSN 1817-3195 / ISSN 1992-8645)*.

Publikasi yang menjadi bagian dari tesis

Kontributor	Jenis Kontribusi
Luluk Usman	Mendesain eksperimen (70%) Menulis *paper* (70%)
Dr. Imam Riadi, M.Kom	Mendesain eksperimen (10 %) Menulis dan mengedit *paper* (15%)
Yudi Prayudi, S.Si.,M.Kom	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (15%)

Kontribusi yang diberikan oleh pihak lain dalam tesis ini

Tidak ada kontribusi dari pihak lain

Halaman Persembahan

BISMILLAHIRRAHMANIRRAHIM...

Kupersembahkan karyaku ini kepada orang-orang yang telah membimbingku memaknai hakikat kehidupan.

- Ibuku yang Tercinta
- Ibuku yang kusayang dan selalu mendoakan dalam setiap proses sulit yang kuhadapi
- Ibuku yang terkasih dan tak henti memberikan semangat dan motivasi agar aku tidak menyerah.
- Bapakku yang juga memerikan support dan selalu mengingatkanku dalam mendekatkan diri kepada Allah SWT, mengingatkanku untuk selalu bisa bertahan dalam kondisi sesulit apapun.
- Adik-adik ku yang menjadi motivasiku untuk menjadi orang yang hebat agar kelak aku bisa menjadi contoh yang layak untuk kalian ikuti.
- Istriku tercinta yang menemaniku dan memberi motivasi dalam penelitian siang malam

Dengan segala ketulusan hati,

Luluk Usman

Kata Pengantar

Assalamualaikum, Wr, Wb

Alhamdulillah, puji syukur kehadirat Allah SWT atas segala nikmat, karunianya sehingga tesis yang berjudul " ANALISIS RANSOMWARE CRYPTOLOCKER MENGGUNAKAN METODE SURFACE ANALYSIS, RUNTIME ANALYSIS DAN STATIC CODE ANALYSIS UNTUK MENDUKUNG INVESTIGASI MALWARE FORENSICS" dapat diselesaikan. Tesis ini disusun sebagai salah satu syarat untuk meraih gelar Magister Komputer pada program studi Magister Teknik informatika, Program Pascasarjana Fakultas Teknologi Industri, Universitas Islam Indonesia, disusun sebagai sarana untuk menerapkan ilmu yang telah didapatkan selama masa perkuliahan dengan konsentrasi Forensik Digital. Dalam penyusunan laporan ini tidak lepas dari dukungan pihak terkait, oleh karena itu pada kesempatan ini penulis dengan kerendahan hati ingin menyampaikan rasa terima kasihnya kepada:

- Allah SWT, tiada tuhan selain Allah, Muhammad utusan-Nya.
- Ibu & Bapak atas doa dan restunya.
- Istri tercinta.
- Adik-adikku.
- Bapak Dr. Imam Riadi, M.Kom selaku Dosen Pembimbing I.
- Bapak Yudi Prayudi, S. Si, M. Kom selaku Dosen Pembiming II.
- Ketua Program Pascasarjana FTI UII & seluruh formasinya.
- Dosen Magister Teknik Informatika khususnya untuk konsentrasi forensik digital.
- Teman-teman Forensik Digital angkatan 6.
- Dr. Ganjar Alfian atas masukan-masukannya tentang model penelitian.
- Pihak-pihak anonim yang langsung maupun tidak langsung memberikan dukungan.

Akhir kata semoga laporan ini dapat berguna bagi kemajuan bidang ilmu forensikdigital. Aamiin.

Wassalamualaikum, Wr. Wb

Yogyakarta, Februari 2017

Luluk Usman