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.