Journal of the Korea Academia-Industrial cooperation Society
Vol. 20, No. 4 pp. 50-55, 2019

https://doi.org/10.5762/KAIS.2019.20.4.50
ISSN 1975-4701 / eISSN 2288-4688

데이터 복원이 가능한 사용자 요구사항 분석기반 랜섬웨어 탐지 시스템에 관한 연구

고용선[1*], 박재표[2]
[1]숭실대학교 대학원 IT정책경영학과, [2]숭실대학교 정보과학대학원 정보보호학과

A Study on the Ransomware Detection System Based on User Requirements Analysis for Data Restoration

Yong-Sun Ko[1*], Jae-Pyo Park[2]
[1]Department of IT Policy Management, Graduate School, Soongsil University
[2]Department of Information Security, Graduate School of Information Sciences, Soongsil University

요 약 최근 랜섬웨어의 공격은 끊임없이 증가하고 있으며, 기본 백신으로는 탐지하기 어려운 신종 랜섬웨어도 지속적으로 늘어나고 있는 추세이다. 이로 인해 랜섬웨어 대응 솔루션이 개발되고 있지만, 기존 랜섬웨어 솔루션의 단점과 한계로 인해 그 피해가 감소하지 않고 있는 실정이다. 랜섬웨어는 윈도우, 리눅스, 서버, IoT 장비, 블록체인 등 플랫폼을 가리지 않고 다양하게 공격을 하고 있지만, 대부분의 기존 랜섬웨어 대응 솔루션은 다양한 플랫폼에 적용이 어려우며, 특정 플랫폼에서만 종속되어 동작하는 한계가 있다. 본 연구는 이러한 기존 랜섬웨어 탐지 솔루션이 가지고 있는 문제점에 대해서 분석하고, 사용자 관점에서 실제로 랜섬웨어에 의한 피해를 줄일 수 있는 요구사항 분석을 통해 필요한 요소 기능을 정의한 후 사전 설치 없이도 다양한 OS를 지원하고 감염 이후에도 데이터 복원이 가능한 탑재형 모듈 기반의 랜섬웨어 탐지 시스템을 제안한다. 제안한 시스템의 각 기능이 구현 가능한지에 대해 기존 기술의 분석을 통해서 확인하고, 실제 제안한 기법들이 사용자의 보안 요구사항에 부합한지에 대한 적합성을 개인과 기업의 PC 사용자 총 264명을 대상으로 설문 조사를 통해 검증하였다. 설문 결과를 통계적으로 분석한 결과, 제안 시스템 도입의사의 점수가 7점 만점에 6.3 이상으로 매우 양호한 것으로 나타났고, 기존 솔루션에서 제안 시스템으로의 변경의사 점수도 6.0 이상으로 매우 높은 것으로 나타났다.

Abstract Recently Ransomware attacks are continuously increasing, and new Ransomware, which is difficult to detect just with a basic vaccine, continuously has its upward trend. Various solutions for Ransomware have been developed and applied. However, due to the disadvantages and limitations of existing solutions, damage caused by Ransomware has not been reduced. Ransomware is attacking various platforms no matter what platform it is, such as Windows, Linux, servers, IoT devices, and block chains. However, most existing solutions for Ransomware are difficult to apply to various platforms, and there is a limit that they are dependent on only some specific platforms while operating. This study analyzes the problems of existing Ransomware detection solutions and proposes the onboard module based Ransomware detection system; after the system defines the function of necessary elements through analyzing requirements that can actually reduce the damage caused by the Ransomware from the viewpoint of users, it supports various OS without pre-installation and is able to restore data even after being infected. We checked the feasibility of each function of the proposed system through the analysis of the existing technology and verified the suitability of the proposed techniques to meet the user's requirements through the questionnaire survey of a total of 264 users of personal and corporate PC users. As a result of statistical analysis of the questionnaire results, it was found that the score of intent to introduce the system was at 6.3 or more which appeared to be good, and the score of intent to change from existing solution to the proposed system was at 6.0 which appeared to be very high.

Keywords : Ransomeware, SSD, Garbage Collection, Delayed Deletion, Restore Data

*Corresponding Author : Yong-Sun Ko(Soongsil Univ.)
Tel: +82-2-323-8463 email: 3238463@hanmail.net
Received February 14, 2019 Revised March 25, 2019
Accepted April 5, 2019 Published April 30, 2019

1. 서론

최근 랜섬웨어의 공격이 IT산업에서 심각한 문제로 대두되고 있다. 2017년에 큰 피해를 일으킨 랜섬웨어인 워나크라이(WannaCry)는 이제 대중에게도 랜섬웨어의 위협이 무엇인지 알리는 계기가 되었다[1].

현재 랜섬웨어를 방어하기 위한 다양한 백신들이 출시되고 있지만 사용자 관점에서 충분하게 고려를 하지 못한 구조적인 문제로 인해 랜섬웨어의 피해는 시간이 흐를수록 지속적으로 증가하고 있다[2,3]. 기존의 랜섬웨어의 공격을 방어하기 위한 대부분의 방법은 시그니처 방식을 기반으로 한 사전 차단이며, 이러한 백신을 이용한 사전 차단 방식을 이용하는 이유는 랜섬웨어에 감염된 후에는 감염된 데이터를 복원하기 위해 암호화키가 반드시 있어야하기 때문이다[4]. Fig. 1은 랜섬웨어의 공격 방식을 나타낸 프로세스이다.

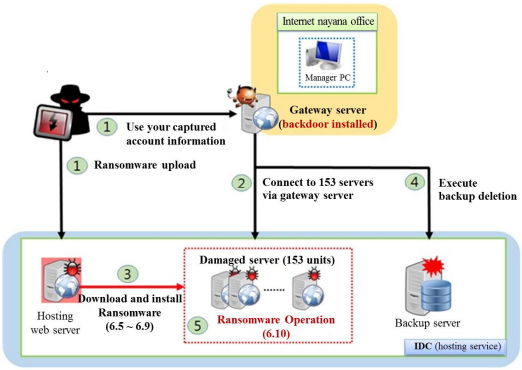

Fig. 1. Structure diagram for disk access[8]

랜섬웨어에 감염되는 대부분의 사용자는 백신 사각지대에 놓인 사용자이며, 시그니처 방식에 의존하는 대부분의 백신은 기존에 알려진 랜섬웨어가 아닌 신종 랜섬웨어에 대해서는 대응이 매우 어렵다. 최근에는 이러한 시그니처기반의 사전 차단 방식에 대한 단점을 해결하기 위해 최근 랜섬웨어를 행위기반으로 탐지하는 방법들이 연구되고 있나, 랜섬웨어 행위를 탐지하기 위해 운영체제에 설치되는 형태의 백신은 바이러스에 의해 쉽게 탐지 동작의 차단될 수 있다는 단점이 있다[5]. 그리고 특정 운영체제의 정보에 종속되어 랜섬웨어를 탐지하기 때문에, 최근 다양한 플랫폼에 공격을 가하는 신종 랜섬웨어를 모두 대응하는 것은 사실상 불가능하다. 이와 같이 랜섬웨어를 탐지하여 차단하는 기존의 설치형 백신은 많은 한계점을 가지고 있다.

따라서 다양한 랜섬웨어를 탐지하여 차단하기 위해서는 랜섬웨어 탐지를 위한 기술적 접근 방법에 변화가 있어야 히며, 감염 이후에 복원이 불가능한 설치형 백신의 문제를 해결하기 위한 방안도 필요하다. 또한 특정 OS에 종속적이지 않고 다양한 시스템에 적용이 가능한 형태의 기술이 필요하며, 백신의 권한 탈취에 의해 무력화되기 쉬운 운영체제에 설치되는 형태보다는 외부 공격으로부터 안전한 백신의 보호 기술이 필요하다.

이를 위해 본 연구에서는 최신의 IT환경의 사용자 측면에서 최상의 보안을 유지 할 수 있는 보안 시스템의 구성 방법 및 대응 방안을 제시하고자 한다. 첫 째, 랜섬웨어의 동작 행위의 탐지를 위해 기존의 방식인 시그니처 방식이나 특정 운영체제에 종속적인 정보를 사용하지 않고 모든 OS에 광범위하게 적용되는 방법을 사용하고, 둘째, 모든 OS에 설치가 가능하기 위해 설치형 SW가 아니라, 탑재형 모듈 형태로 개발하며, 셋째, 랜섬웨어에 감염된 데이터의 복원이 가능하도록 디스크의 입출력 데이터를 통제할 수 있는 방안을 제시하고자 한다.

따라서, 본 연구에서는 랜섬웨어의 위협에 대응하기 위한 기존 문헌들의 연구 결과를 토대로 보다 광범위하고 최신의 IT 환경에 맞는 랜섬웨어 대응 방법을 도출한 후, 이 제안 방법에 대한 설문조사 및 분석을 통해 기존의 랜섬웨어 백신이 접근하는 방식에 비해 사용자 요구사항에 대한 적합성이 얼마나 더 높은지를 통계적으로 검증하고자 한다.

2. 관련연구

2.1 랜섬웨어 탐지 기술

바이러스를 탐지하는 가장 전통적인 방법은 바이러스의 고유 핵사 정보인 시그니처를 이용한 탐지 방법이다. 이 방법은 정확도가 높고, 오탐지율이 0%에 가깝다는 장점이 있지만, 신종 랜섬웨어를 탐지하기 어렵기 때문에 최근에는 많이 사용되지 않는 방식이다[6]. 최근에는 딥러닝을 이용한 정적분석 방법을 사용하기도 하는데, 이는 통계적인 정보를 바탕으로 탐지하기 때문에, 신종 랜섬웨어에 대해서 정확한 탐지가 어렵고, 특정 운영체제에 종속적인 단점이 있다. 또한 다른 방식으로는 미끼

를 이용한 탐지 방법이 있는데, 미끼로 지정한 특정 파일들이 랜섬웨어의 공격에 의해 변조가 되는지를 모니터링하여 변조 시 해당 랜섬웨어 공격을 판단하는 방식이다[7]. 이 방식은 랜섬웨어가 미끼를 회피하여 탐지를 쉽게 우회해서 공격할 수 있어 효용성이 많이 떨어진다. 그 밖에 랜섬웨어의 행위를 분석하여 탐지하는 방법도 많이 소개되었다. 하지만 이 방법 역시 특정 운영체제에 종속적인 정보를 활용하여 탐지 알고리즘을 구동하기 때문에, 플랫폼을 구분하지 않고 공격하는 랜섬웨어에 대응하는 것에는 한계가 있다. 이와 같이 기존 기술은 사용자 관점에서 다양한 문제를 가지고 있지만, 가장 치명적인 문제는 모든 탐지 기술들이 랜섬웨어를 100% 차단하기에 불가능 하다는 문제가 있다[8,9].

2.2 랜섬웨어 복원 기술

랜섬웨어는 감염 이후에는 데이터 복원이 불가능하고, 감염 전 사전 탐지에 의한 100% 차단이 불가능하기 때문에 이를 위한 선 대응적인 복원 기술들이 제안되었다. 가장 많이 사용되는 방법은 데이터를 미리 백업 하는 방법이다. 백업 영역에 대한 접근 권한을 지정하고, 해당 영역에 데이터를 백업하여 임의 접근을 차단하는 방법이다. 하지만 이 방법은 매번 많은 양의 데이터를 모두 백업해야 하므로 시스템 성능에 좋지않은 영향을 미치고, 해킹으로 인해 접근 권한을 빼앗기는 경우에는 언제라도 데이터를 손실할 위험이 있다. 이에 따라, 최근에는 랜섬웨어에 의해 파괴된 데이터를 복원하는 방법에 대해 다룬 논문이 발표되고 있다[2,9,10]. SSD(Solid State Drive)는 하드웨어의 특성에 따라, 사용자 영역에서 삭제된 데이터를 실제로는 삭제하지 않고, 가비지 컬렉션이라 정의된 동작이 발생할 때 삭제된다. 즉, 사용자영역에서 이미 지워진 데이터가 실제로는 아직 남아 있는 것이다. 이것를 SSD의 지연삭제(Delayed Deletion)라 하고, 이를 이용하여 복원이 가능하다는 주장이 있다. 본 연구에서는 이와 같은 내용을 기반으로 복원이 가능한 구조에 대해 제안한다.

3. 제안하는 랜섬웨어 탐지 시스템

본 연구에서는 랜섬웨어의 위협에 대응하기 위한 기존 문헌들의 연구 결과를 기반으로 보다 광범위하고 최신의 IT 환경에 맞는 대응 방법을 도출하여, 이 제안방법에 대한 설문조사를 실시하고, 기존의 백신에 의한 방식 보다 사용자 요구사항에 대한 적합성을 통계적으로 검증하고자 한다. 앞에서 언급한 랜섬웨어 탐지에 대한 접근 방법에서 많은 단점과 한계점을 가지고 있는 기존 기법들의 단점과 한계점을 해결하기 위해 다음과 같이 사전 설치 없이 다양한 OS를 지원하고 감염 이후에도 데이터 복원이 가능한 탑재형 모듈 기반의 랜섬웨어 탐지 시스템을 제안한다.

3.1 다양한 OS 지원 방안

랜섬웨어 대응솔루션은 대부분 운영체제(OS)에 종속적인 정보 (프로세스, 암호화 라이브러리의 호출 등)를 활용하여 탐지하고 있다. 이러한 종속적인 정보로 인해 OS 위에서만 동작이 가능하다. 랜섬웨어의 공격은 다양한 OS 및 플랫폼을 구분하지 않기 때문에, 범용적인 탐지 기술을 구현하기 위해서는 시스템에 종속적이지 않은 정보를 활용해야 한다.

Fig. 2는 데이터를 디스크에 기록하기 위해 거치는 과정에 대한 구조이다.

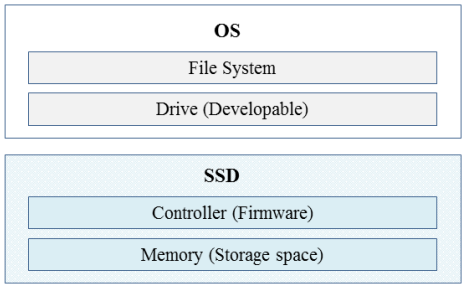

Fig. 2. Structure diagram for disk access

3.2 탑재형 모듈로의 개발 방안

랜섬웨어는 운영체제 위에서 동작하지만, 최종적으로는 디스크에 입출력 행위를 통하여 감염을 진행한다. 따라서, 랜섬웨어 탐지를 위한 알고리즘이 입출력 정보만을 활용한다면, 해당 모듈을 드라이브 내에도 설치가 가능하고, SSD 컨트롤러 내부의 펌웨어에도 탑재가 가능하다. 따라서 랜섬웨어 입출력 정보의 분포만을 활용해 랜섬웨어 행위를 분류할 수 있다면 플랫폼에 독립적인 탐지 기술의 개발이 가능하다. 이와 같은 연구가 가능함을 보여주는 선행 연구[2]가 있었고, 향후 랜섬웨어 탐지 도구가 범용성을 가지려면 이와 같은 기술이 반드시 필

요하다.

현재까지의 랜섬웨어 탐지 기술은 시스템의 종속적인 정보를 활용할 뿐 아니라, 백업 공간 확보나 침입에 의한 백신 프로세스의 강제 종료를 차단하기 위해 운영체제의 슈퍼유저, 관리자 권한 등과 같은 상위 레벨 권한을 획득하여 동작한다. 이는 탐지 백신이 운영체제에 종속되도록 하는 단점이 있다. 이러한 단점을 해결하기 위해는 기존 백신과 같이 운영체제의 종속적인 설치형 백신이 아닌 탑재형 라이브러리가 더욱 적합하다 할 수 있다. 네이티브 언어인 커널 수준의 라이브러리만 활용하여 C언어로 개발을 하게 되면 드라이브부터 펌웨어 까지 모두 이식이 가능하다. 특히 드라이브나 SSD의 컨트롤 내부는 랜섬웨어의 공격으로부터 위변조가 불가능하기 때문에 탑재형 라이브러리 방식은 보안 레벨을 더욱 높이는 장점이 있으며, 이를 위해서는 ANSI 표준의 C보다 더욱 저 레벨의 라이브러리와 문법을 사용해야 한다.

3.3 감염 후 데이터 복구 복원 기법

관련 연구에서 언급했듯이, 기존 랜섬웨어 대응솔루션의 가장 큰 문제점은, 감염이전에 반드시 설치가 되어야 하는데, 일반 사용자는 랜섬웨어의 대응을 위해 사전에 랜섬웨어 백신 소프트웨어를 적극적으로 설치하지 않는다는 것이다.

Fig. 3은 SSD의 특징은 지연 삭제 동작을 나타낸 것이다. 일반적으로 사용 중인 블록은 데이터가 기록되어 있으며, 사용자가 이를 삭제하거나 다른 데이터로 덮어쓰게 되면 이 데이터는 변경되어야 한다. 하지만 10,11,12번 블록을 보면 가비지 컬렉션 전에는 삭제된 데이터이지만 아직 데이터가 유지되고 있음을 알 수 있다.

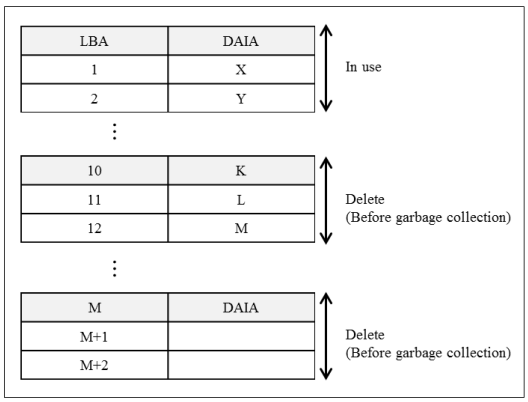

Fig. 3. Delayed deletion behavior of SSD

SSD는 삭제 동작이 매우 느리기 때문에, 성능 최적화를 고려하여 삭제 요청 시 실제 데이터는 즉시 삭제하지 않고 가비지 컬렉션이라는 동작이 발생할 때 한 번에 모두 삭제하는 특성이 있다. 이 특성을 활용하면 랜섬웨어에 감염된 데이터를 복원할 수 있다.

Fig. 4는 랜섬웨어에 의해 감염된 데이터를 복원하기 위한 방법이다.

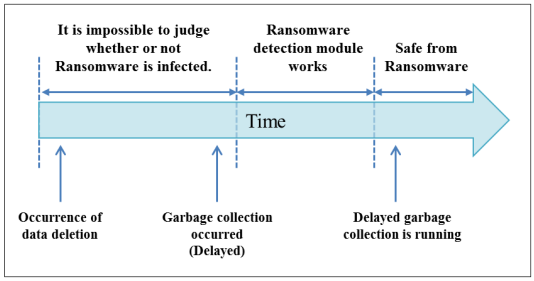

Fig. 4. Data recovery method with garbage collection delay

랜섬웨어에 감염이 되어도 가비지 컬렉션 전까지는 데이터가 남아있기 때문에 복원이 가능하므로, 랜섬웨어 탐지 모듈을 통해 감염이 되지 않았다고 확정이 될 때까지 가비지 컬렉션을 지연 시키면 시스템을 복원 가능한 상태로 보호할 수 있다. 하지만 가비지 컬렉션을 무한대로 지연시킨다면 사용할 수 있는 메모리가 급격히 감소하므로 탐지를 위한 시간과 지연 시간간의 Trade off를 적절히 고려하여 시스템을 설계해야 한다.

이와 같은 데이터 복원 기법의 가정 큰 장점은 백신의 성능 측면에서 오탐지가 큰 문제가 되지 않는다는 점이다. 백신의 구현이 어려운 이유는 오탐율 때문에 바이러스의 동작 유무에 대한 판단을 엄격히 할 수 없다는 것이다. 하지만 오탐율을 허용하면서 탐지율을 100% 만족시키는 방향으로 탐지 기술을 개발한다 하더라도 현재의 환경에서는 큰 문제가 되지 않는다. 그 이유는 이벤트로 기록을 하고 사용자의 확인까지 가비지 컬렉션을 지연하면 되기 때문이다. 따라서, 제안하는 시스템은 다른 백신에 비해 오탐지 문제가 시스템 측면에서 크게 영향을 끼치지 않는다.

사용자에 의한 별도의 백신 설치가 없이도 보안이 되는 것은 사실상 사용자 관점에서 가장 중요한 장점이다. 앞에서 제안한 세 가지 기술적 특성은 운영체제에 종속되지 않고, 탑재형 모듈이며, 복원이 가능한 기술이다. 이와 같은 형태로 개발되면 운영체제의 디바이스 드라이

브나 SSD의 펌웨어 내에 탑재가 가능하다. 이에 따라, 윈도우 보안패치나 드라이브 패치만으로도 보안이 가능하게 되고, 랜섬웨어로부터 안전한 보안 저장소의 개발이 가능하고 할 수 있다.

4. 통계검증 방법 및 분석결과

4.1 통계검증 방법

본 연구에서는 제안하는 방식이 얼마나 사용자에게 적합한지에 대한 제안 기법의 사용자 적합성 분석을 설문 및 결과 분석을 통해 수행하였다. 설문은 E-mail을 통한 온라인 방식과 오프라인 방식을 사용하였다. 설문지의 배포는 설문 대상자에게 개인별 E-mail을 보내 응답자가 메일을 확인함과, 동시에 인터넷 웹 브라우저상에서 바로 설문에 응답할 수 있는 방식으로 진행하여 설문 데이터 수집율을 최대한 높이고자 하였다. 오프라인의 경우, 설문 대상자에게 직접 설문을 배포하여 설문 응답을 받았다. 표본은 PC 사용자들을 대상으로 하였으며, 개인인지 기업인지를 분류하였다.

설문조사를 통해 보안 시스템 도입이 어려운 개인 및 중소업체를 대상으로 해당 방식이 얼마나 사용자 측면에서 적절한지를 조사하기 위해서 랜섬웨어에 대한 위험인지도, 대응 준비도, 도입 의사 측면에 대해 조사를 하였다. 본 연구에서는 각 문항에 대해 리커트 척도 7점 척도를 응답자가 인식하는 위험요인에 대한 중요 순으로 체크해줄 것을 요청하였다. 설문조사에서 수집된 자료의 통계 분석을 위해서 SPSS v12.0을 사용하였다. 각 위험요인별로 통계적 결과를 도출하기 위해 동질 영역별로 구분하였으며, 실증분석은 유의수준 5%에서 검증을 하였다. 각 영역별로 항목에 대한 척도치의 평균이 통계적 차이가 있는지 독립 표본을 통해 분석한 후 이를 통해 각 영역별 위험요인에 대한 인식의 차이를 밝히고자 하였다.

4.2 분석 결과

응답자의 일반적 특성을 알아보기 위하여 빈도분석을 실시하고, 각 랜섬웨어의 설문에 대한 문항에서 신뢰도 검사 및 문항간의 신뢰도를 측정하여 예측가능성, 정확성 등을 살펴보았으며 문항간의 신뢰도는 Cronbach's의 계수로 판단하였다.

Table 1. Statistics on PC environment and company size

Classification		Frequency	Ratio
Environment using PC	Individual	171	64.8
	Company	93	35.2
Total		264	100
Type of business	Individual business	79	29.9
	Small Business	91	34.5
	Major company	94	35.6
Total		264	100

설문 결과 데이터로 랜섬웨어에 대한 위험 인지도, 대응 준비도, 도입 의에 대해 통계적으로 분석하였으며, 본 연구에 사용된 측정도구인 신뢰성은 Cronbach's 계수를 이용하여 분석한 결과, 0.8이상으로 측정도구의 신뢰성은 양호한 것으로 나타났다.

제안 시스템 도입의사 항목은 7점 만점에서 6.3점 이상으로 매우 양호한 것으로 나타났고, 기존 솔루션에서 제안 시스템으로 변경 의사 항목은 7점 만점에서 6.0 이상으로 매우 높은 것으로 나타났다.

Table 2. Security empirical statistics of the sample

Classification		Frequency	Ratio
Whether security solutions are introduced	Companies without a security system	16	6.0
	Companies with a partial security system	72	27.3
	Companies applying security systems	176	66.7
Total		264	100
Knowledge of security solutions	Do not know	5	1.9
	Generic vaccine (ex. V3)	233	88.3
	Ransomware-only vaccine	26	9.8
Total		264	100
Experience with virus damage	Has exist	3	1.1
	None	261	98.9
Total		264	100

5. 결론

본 연구에서는 랜섬웨어의 탐지 기술에 대한 분석과 기존 랜섬웨어 탐지 기술의 단점과 한계를 정의하고, 이를 사용자 중심으로 변경하기 위한 사용자 측면에서의 요구사항을 반영한 랜섬웨어 탐지 시스템 모델에 대하여

제안하였다.

제안한 모델의 검증을 위해 설문조사를 통하여 해당 기법을 적용한 랜섬웨어 탐지 시스템에 대한 가능성 및 도입의사에 대하여 조사한 후 그 결과를 분석하였다. 향후 연구로는 앞에서 제안한 모델인 랜섬웨어의 탐지와 복원이 가능한 시스템에 대한 개발 및 성능 분석이 필요하다.

본 연구의 내용과 결과는 랜섬웨어 탐지 시스템의 연구자 및 개발자에게 많은 도움이 될 것으로 기대한다.

References

[1] N. Scaife, H. Carter, P. Traynor, and K. Butler, "Cryptolock(and drop it): Stopping ransomware attacks on user data", *Proceedings of IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, pp.303-312, June 2016.
DOI: https://doi.org/10.1109/ICDCS.2016.46

[2] Joon-young Paik, Keun-tae Shin, Eun-sun Cho, "Self-Defensible Storage Devices based on Flash memory against Ransomware", *IEEE Symposium on Security and Privacy*, May 2016.

[3] C. Everette, "Ransomware: to pay or not to pay?" *Journal of Computer Fraud & Security*, Vol.16, No.4, pp.8-12, April 2016.
DOI: https://doi.org/10.1016/S1361-3723(16)30036-7

[4] Y Qin, W Tong, J Liu, Z Zhu, "SmSD: A smart secure deletion scheme for SSDs", *Journal of Convergence*, Vol.4, No.4, pp.8-12, Dec. 2013.

[5] N. Hampton, Z. Baig, S. Zeadally, "Ransomware behavioural analysis on windows platforms", *Journal of Information Security and Applications*, Vol.40, pp.44-51, June 2018.
DOI: http://dx.doi.org/10.1016/j.jisa.2018.02.008

[6] J. S. Aidan, H. K. Verma, L. K. Awasthi, "Comprehensive Survey on Petya Ransomware Attack", *Proceedings of International Conference on Next Generation Computing and Information Systems (ICNGCIS)*, pp.11-12, Dec. 2017.
DOI: https://doi.org/10.1109/ICNGCIS.2017.30

[7] F. Chen, D. A. Koufaty, X. Zhang, "Understanding intrinsic characteristics and system implications of flash memory based solid state drives", *Proceedings of the International Joint Conference on Measurement and Modeling of Computer Systems*, pp.181-192, June 2009.
DOI: https://doi.org/10.1145/1555349.1555371

[8] Yu-Ji Lee, Internet Nayana, Ransomware infection by APT attack, security management, Byline Network, 2017. Available From: https://byline.network/2017/06/1-792/ (accessed Dec. 20, 2018)

[9] C. Moore, "Detecting Ransomware with Honeypot Techniques", *Proceedings of Cybersecurity and Cyberforensics Conference(CCC)*, pp.2-4, Aug. 2016.
DOI: https://doi.org/10.1109/CCC.2016.14

[10] H. Orman, "Evil offspring - Ransomware and crypto technology," *Journal of IEEE Internet Computing*, Vol.20, No.5, pp.89-94, Oct. 2016.
DOI: https://doi.org/10.1109/MIC.2016.90

[11] E. Kirda, "UNVEIL: A large-scale, automated approach to detecting ransomware," *Proceedings of tIEEE 24th International Conference on Software Analysis, Evolution and Reengineering(SANER)*, pp.20-24 Feb. 2017.
DOI: https://doi.org/10.1109/SANER.2017.7884603

고 용 선(Yong-Sun Ko) [정회원]

- 2016년 8월 : 숭실대학교 정보과학대학원 IT경영학과 (공학석사)
- 2019년 3월 : 숭실대학교 대학원 IT정책경영학과(컴퓨터공학)박사 수료
- 2006년 2월 ~ 현재 : (주)써브나라 대표이사
- 2017년 3월 ~ 현재 : 경인여자대학교 스마트IT과 겸임교수

<관심분야>
보안기술, 보안정책, 정보경영

박 재 표(Jae-Pyo Park) [정회원]

- 1998년 8월 : 숭실대학교 일반대학원 컴퓨터학과(공학석사)
- 2004년 8월 : 숭실대학교 일반대학원 컴퓨터학과 (공학박사)
- 2008년 9월 ~ 2009년 8월 : 숭실대학교 정보미디어기술연구소 전임연구원
- 2010년 3월 ~ 현재 : 숭실대학교 정보과학대학원 교수

<관심분야>
물리적 보안, 컴퓨터통신, 보안정책, 디지털포렌식