The Journal of the Convergence on Culture Technology (JCCT)
Vol. 2, No. 1, pp.79-85, February 29, 2016. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2016.2.1.79
JCCT 2016-2-7

랜섬웨어 분석과 피해 최소화 방안

Ransomware Analysis and Method for Minimize the Damage

문재연*, 장영현**

Moon Jaeyeon, Chang Younghyun

요 약 랜섬웨어는 미국을 중심으로 활동하는 악성코드였으나 기하급수적인 컴퓨터 보급과 사용자의 증가를 매개체로 하여 전 세계적으로 급속하게 유포되었으며 최근에는 국내에서도 출현하였다. 초기 랜섬웨어는 E-Mail을 공격매개체로 사용하였으며 스팸메일을 통해 파일을 클릭하도록 유도하는 방식이 가장 일반적이나 SNS나 스마트폰 메시지를 통해서도 유포되고 있다. 현재는 한글 버전으로 국내 대형 커뮤니티 사이트들을 공격하는 등 국내에서도 많은 피해가 증가하는 추세이다. 랜섬웨어는 파일을 암호화하여 사용자에게 경고 메시지를 출력하며, 추적상태를 유추하기 어려운 비트코인 가상 화폐를 통한 결제를 요구하면서 금전적인 피해를 유도한다. 본 논문에서는 랜섬웨어로 인한 피해 사례 분석과 해결방안을 제시한다.

주요어 : 랜섬웨어, 악성코드, 스팸메일, 암호화, 추적상태

Abstract Ransomware was a malicious code that active around the US, but now it spreads rapidly all over the world and emerges in korea recently because of exponential computer supply and increase in users. Initially ransomware uses e-mail as an attack medium in such a way that induces to click a file through the spam mail Pam, but it is now circulated through the smart phone message. The current trend is an increase in the number of damage, including attacks such as the domestic large community site by ransomware hangul version. Ransomware outputs a warning message to the user to encrypt the file and leads to monetary damages and demands for payment via bitcoin as virtual currency is difficult to infer the tracking status. This paper presents an analysis and solutions to damage cases caused by ransomware.

Key Words : Ransomware, Malicious Code, Spam Mail, Encryption, Tracking Status

Ⅰ. 서 론

2014년 기준으로 대한민국 인터넷 보급률은 81.6%를 보여주고 있다. 인터넷의 보급률이 높아짐과 동시에 인터넷의 필요충분조건에서 실행되는 기능들로 SNS나 E-Mail 등과 같이 사람과 사람이 소통하는 기능 또는 Naver와 Google같은 대형 웹사이트부터 소형 웹사이트에 이어 HTML5 웹 플랫폼 기술, 웨어러블 디바이스 및 NFC 기술, 클라우드 컴퓨팅 기술, 사물인터넷/만물인터넷(Internet of Things/Everything) 기술, 빅 데이터(Big data) 기술, 3D 입체영상 기술 및 인지(recognition) 기술[1]까지 등장하는 등, 가파른 발전

*준회원, 배화여자대학교 스마트IT학과
**정회원, 배화여자대학교 스마트IT학과
접수일자: 2015년 12월 11일, 수정완료일자: 2015년 12월 20일
게재확정일자: 2016년 1월 18일

Received: 11 December 2015 / Revised: 20 December 2015
Accepted: 18 January 2016
*Corresponding Author: cyh@baewha.ac.kr
Dept. of Smart IT, Baewha Women's University, Korea

과 성장세를 이어가고 있다. 인터넷이 일반화되고 세계적으로 많은 사람들에 의해 사용되어짐에 따른 부정적 측면에서 보안의 위험성도 동시에 부각되기 시작했다. SNS나 E-Mail의 첨부파일을 클릭하면 컴퓨터가 바이러스 등, 심각한 악성코드에 감염되는 경우가 발생하기 시작했고, 방문자가 거의 없는 웹사이트에 들어가기만 해도 악성코드에 감염되는 사례도 빈번하게 발생하고 있다.

인터넷과 함께 진화해온 악성코드는 감염된 파일, 혹은 파일 안의 문서들을 열람 할 수 없는 단계부터 시작하여 PC사용자의 정보를 해커에게 전송하는 단계까지 지속적으로 진화해오고 있다. 최근에는 파일을 암호화시켜 해커가 사용자에게 금품을 요구하는 수준의 '랜섬웨어'라는 악랄한 악성코드도 나타나게 되었다.

랜섬웨어란, 몸값(ransom)과 제품(ware)의 합성어로 컴퓨터의 정보를 '인질'로 잡고 돈을 요구한다고 해서 붙여진 명칭이다. 랜섬웨어는 사용자의 컴퓨터 내부에서 중요한 정보를 암호화시키고 사용자에게 돈을 요구한다. 지정된 계좌로 돈을 보내면 암호화된 정보를 원래상태로 복구할 수 있다는 협박을 하는데, 시간이 지날수록 금액이 증가되어지고 협박강도도 올라간다. 사용자는 불가피하게 돈을 지불하지만, 돈을 받고나서도 암호를 풀어주지 않는 경우가 많다. 따라서 중요한 정보를 컴퓨터나 스마트폰에 보관하는 현대인들에게 치명적인 암적 존재이다.[2]

컴퓨터 사용자의 파일이나 문서를 볼모로 하여 금품을 요구하고 금품을 지불하지 않으면 그 대가가 점점 높아지는데, 이로 인하여 기업이나 개인의 PC가 '랜섬웨어'에 감염되었을 경우 심각한 사회문제로 확대되는 문제점이 부각되고 있다. 파일이나 문서만이 아닌, Dropbox, N드라이브, Google Drive와 같은 국내외 유명 클라우드 서비스도 '랜섬웨어'에 감염될 수 있다는 것이 확인되었다. 따라서 중요한 문서 파일과 디지털 카메라 또는 스마트폰으로 찍은 jpg 사진 파일, zip, rar 압축 파일 등을 대상으로 한 범죄가 증가추세에 있으며 불안감을 호소하는 ICT 분야의 개발자와 사용자들이 증가하고 있다. '랜섬웨어'의 피해가 늘어나고 있는 반면에 '랜섬웨어'를 제거 및 복구 할 수 있는 프로그램과 예방방법이 제기되고 있지만 완전한 해결책은 제자리걸음을 하고 있다. 따라서 본 논문은 '랜섬웨어'에 대한 정의와 사례분석, 피해 해결방안 및 예방에 관해 연구한다.

II. 랜섬웨어의 출현과 진화과정

2.1 랜섬웨어 동향 분석

원래 랜섬웨어는 미국을 중심으로 활동하는 악성코드였으나 기하급수적인 컴퓨터 보급과 사용자의 증가를 매개체로 하여 전 세계적으로 급속하게 유포되었으며 2015년 4월에는 국내에서도 출현하게 되었다. 2013년, 신종 랜섬웨어 '크립토락커'는 미국을 중심으로 유행하기 시작했으며, 현재까지 전 세계에서 가장 악명 높고 영향력 있는 랜섬웨어로 알려져 있다. 크립토락커는 한글버전이 없었으나 최근에는 한글버전도 발견되었다.[3] 한글버전이 유포되었다는 단계는 본격적으로 한국 인터넷 사용자들을 공격하겠다는 의미이며 금전요구도 비트코인으로 받아 해커들을 용이하게 추적할 수도 없는 방법론까지 부가되어졌다. 크립토락커 랜섬웨어는 Drive-By-Download 방식, 즉 사이트에 접속만 해도 감염이 되는 형식을 취하고 있어 피해가 대규모로 확산될 수 있다. 그러나 원하는 액수의 돈을 지불하여도 복호화에 대한 확정상태는 미지수라 할 수 있다. 현재까지 적절한 대응방법과 대책이 수립되지 않고 있으며 절실한 근본적 방법론이 다양한 연구논문을 통하여 제시되어야 할 단계이다.

2.2 랜섬웨어의 진화

초기 랜섬웨어는 미국을 중심으로 확산되었으며 E-Mail을 사용하여 공격했다. 스팸 메일을 통해 파일을 클릭하도록 유도하는 방식이 가장 일반적이며 SNS나 스마트폰 메시지를 통해서도 유포시키고 있다. 현재는 한국을 목표로 하여 한글 버전을 만들어 국내 대형 커뮤니티 사이트들을 공격하는 등 많은 피해가 증가하는 추세이다. 랜섬웨어는 계속적인 진화를 하고 있다. 2015년의 클리앙 사태와 같이 IE와 플래시 플레이어의 취약점을 중심으로 공격하거나 DDoS를 조합한 형태로 진화되었다. 랜섬웨어 기본적 기능에 DDoS 공격 기능이 추가된 것으로, 악성코드가 활성화되면 특정 C&C 서버에 접속해 사용자의 PC 정보를 유출할 뿐만 아니라, 공격자의 명령에 따라 DDoS 공격을 수행한다.[4] 사용자들의 랜섬웨어에 대한 지식이 증가하면서, 기대

했던 만큼 금전적인 이익을 갈취하기 어려워졌기 때문이다. 랜섬웨어는 다양한 기능을 복합적으로 포함시키면서 진화함에 따라 피해는 심각한 수준을 초과하면서 진행되고 있다. 만약 랜섬웨어가 커뮤니티 사이트가 아닌 국가 기관이나 은행 등의 보안 시스템을 해킹당한다면 사태는 무한책임의 범주를 넘어 피해를 측정할 수 없을 정도의 어려운 상태까지 예견할 수 있다. 결론적으로 랜섬웨어의 진화에 맞춰 백신기술이 국가와 전문기업의 집중적인 투자를 통하여 발전시켜야 한다.

2.3 랜섬웨어 감염 방식

랜섬웨어는 Drive-By-Download 방식으로 감염되는 악성코드로, OS 및 SW의 보안 취약점을 통해 변조된 웹사이트를 방문하면 악성코드가 유포되는 방식이다. 즉, 보안 취약점이 있는 OS나 SW를 사용하고 있는 사용자는 악성코드에 감염된 인터넷 홈페이지를 접속하면 감염된다. [5]

랜섬웨어가 다른 바이러스들과 다르게 홈페이지 접속만으로도 감염될 수 있는 이유는 코드삽입방식이기 때문이다. 랜섬웨어는 Windows 보안센터를 강제종료 시키고 중요 파일을 RSA-2048 암호화 알고리즘을 통해 “(파일명).(암호화 대상 파일 확장자).encrypted” 파일 패턴으로 저장한다. 감염된 환경에서는 Windows 운영 체제 자체는 문제없이 사용할 수 있지만, 특정 폴더(%Windir%, %Temp% 추정)를 제외한 위치에 암호화 대상 파일을 저장할 경우 암호화 처리되어 열어볼 수 없게 된다. 이후 DECRYPT_INSTRUCTIONS.html, DECRYPT_INSTRUCTIONS.txt 파일을 생성하여 웹 브라우저 또는 메모장을 통해 “본인의 모든 파일을 Crypt0L0cker 바이러스로 코딩했습니다.” 라는 경고 메시지를 출력하여 안내에 따라 추적상태를 유추하기 어려운 비트코인(BitCoin) 가상 화폐를 통한 결제를 유도한다. [6] [7]

Ⅲ. 랜섬웨어 종류와 사례분석

랜섬웨어는 새롭게 등장한 신종 악성코드가 아니라 2010년 12월에 출현한 악성코드다. 컴퓨터 화면을 잠그거나 사용자 인터페이스를 변경하여 사용을 어렵게 한 후 원상복구를 전제로 돈을 요구했다. 당시에는 보안 프로그램으로 치료하거나 하드디스크를 분리해 다른 컴퓨터에 연결하여 필요한 자료만 복사하면 해결할 수 있었다. [8] 그러나 현재의 랜섬웨어는 진화를 거듭하여 ‘치명적인 악성코드’로 재탄생했다. 랜섬웨어에 공격당한 사례는 국내에서도 계속 증가하고 있는 추세이다.

본 논문에서는 기업과 개인을 위협하는 랜섬웨어의 종류와 피해를 입은 사례에 대해 기술한다.

3.1 크립토락커(CrypToLocker)

크립토락커는 랜섬웨어의 한 종류로 한글 버전이 유포되고 있다. 감염된 PC의 시스템 파일을 제외한 MS 오피스 및 한글 문서 파일, 압축 파일, 동영상, 사진 등을 대상으로 암호화한다. 해당 국가 언어로 작성된 txt, html 파일을 생성해 사용자에게 PC가 감염된 사실을 알리는 것으로 확인 되었다.[9]

그림 1. 크립토락커 랜섬웨어에 감염된 PC화면(1)
Fig 1. Infected PC screen by CryptoLocker Ransomware(1)

암호화된 문서를 복호화하기 위해 [그림 1]과 같은 ‘파일 복원 지불하려면 여기를 클릭하십시오.’를 선택하면 [그림 2]와 같은 화면이 출력되고 금전을 요구한다. 따라서 사용자는 자신의 컴퓨터에 내장된 정보접속이 불가능해진다. 그러나 금전을 지불하게 되어도 암호는 복호화 되지 않고, 클립토락커 랜섬웨어를 유포한 해커는 더 높은 금전을 요구하며 사용자의 개인정보를 해킹하거나 최종에는 제거되지 않는 경우도 발생한다. [6] [10]

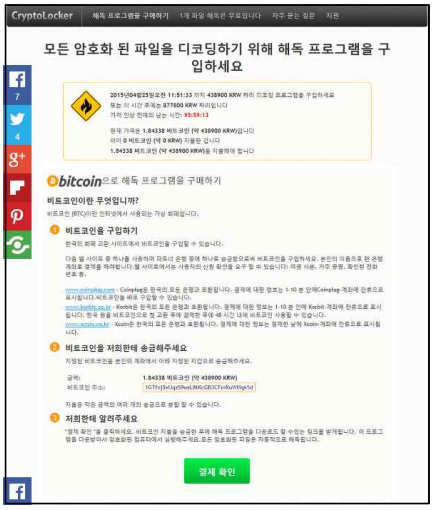

그림 2. 크립토락커 랜섬웨어에 감염된 PC화면(2)

Fig 2. Infected PC screen by cryptoLocker ransomware(2)

3.1.1 클리앙 공격 사례

최초로 한국에서 랜섬웨어에 공격을 당한 곳은 '클리앙' 이라는 IT커뮤니티사이트였다. 클리앙 운영자는 [그림 3]과 같이 사이트가 독립적으로 운영되는 광고 서버를 통해 감염되어 악성코드가 유포되었다. 사용자들이 2015년 4월 21일 새벽부터 11시경까지 클리앙에 익스플로러를 사용하여 접속했을 경우 랜섬웨어에 감염됐을 가능성이 매우 높은 것으로 확인되었다. [11]

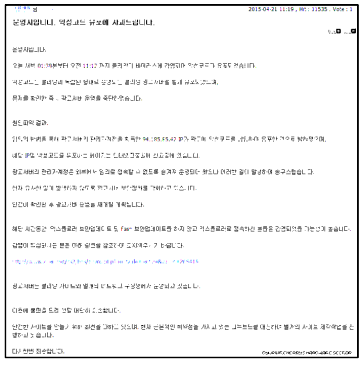

그림 3. 클리앙 랜섬웨어 공격에 의한 악성코드 유포 관련 공지

Fig 3. Malware spreading announcements by clien ransomware attack

현재 랜섬웨어는 익스플로러를 경유할 경우 가장 많이 유포 · 감염되고 있는 것으로 밝혀졌다. 특히 익스플로러9 이하와 플래시 플레이어 구 버전을 사용하는 컴퓨터가 주요 공격대상이다. 즉, 업데이트 하지 않은 사용자일수록 랜섬웨어에 감염될 확률이 매우 높다.

3.1.2 시코 공격 사례

클리앙 사건 이후 다른 국내 사이트에서도 랜섬웨어가 유포됐다. 시디플레이어 커뮤니티 사이트인 '시코(Seeko)' 는 광고 서버를 통해 랜섬웨어가 유포되었다. 시코 측은 유포 관련 사과와 함께 문제가 된 광고 서버를 차단했다.[12] 시코에 접속할 경우 광고 서버 쪽에서 medbps.filmwedding.ro 주소를 가진 사이트로 접속을 유도하는데, 현재도 차단된 상태이다. [13] 클리앙과 마찬가지로 시코 또한 Drive-By-Download 방식으로 유포되었으며, 사이트에 접속하는 것만으로도 감염된다.

3.1.3 대형 커뮤니티 사이트 공격 사례

크립토락커 랜섬웨어가 이벤트 응모관련 사이트와 토렌트 관련 사이트 등 대형 커뮤니티 사이트에 유포되었으며, Drive-By-Download 방식으로 사용자들에게 피해를 입힐 수 있다. 한국형 크립토락커는 커뮤니티 사이트의 광고 서버나 첨부파일을 통해 확산되며, 여러 커뮤니티 사이트를 경유지로 악용하고 있다.[14] 심지어 대형 커뮤니티 사이트인 '디시인사이드' 까지 감염되는 등, 차례로 국내의 많은 커뮤니티 사이트들이 감염되는 사례가 급증하고 있는 추세이다.[12]

3.2 레베톤(Reveton)

랜섬웨어 가운데 변종 형태로 발전된 랜섬웨어로 레베톤 랜섬웨어가 있다. 레베톤 랜섬웨어는 거짓으로 법 집행기구의 경고 문구를 표시하고, 사용자가 법령을 어겨 PC 내 파일이나 소프트웨어의 사용이 제한된다고 경고하며 돈을 요구하는 악성코드이다. 랜섬웨어가 레베톤 랜섬웨어로 변종되면서 이전의 랜섬웨어에는 없는 새로이 추가된 기능이 있다. 즉, 레베톤 랜섬웨어만의 고유한 기능이 나타난 것이다. 최근 발견된 레베톤 랜섬웨어 일부는 '포니' 라는 모듈이 결합되어 있다.

'포니' 는 '트로이 목마' 등에 자주 사용되는 보편적인 비밀번호 도용 모듈 중 하나로, '포니' 와 결합된 레베톤 랜섬웨어는 정보도난기능을 갖춘 소프트웨어로 진화하고 있음이 발견되었다. 연구에 따르면

'포니' 는 암호화된 다양한 형태의 비밀번호를 평문으로 복호화 시킬 수 있다. 레베톤 랜섬웨어는 '포니' 를 통해 사용자의 FTP 패스워드, VPN이나 이메일 클라이언트 등에 접근, 암호문들을 복호화 시킨다. 해킹한 개인정보들을 통해 레베톤 랜섬웨어 개발자는 사용자의 개인정보나 비트코인과 같은 가상화폐를 입수한 후 지하시장 거래를 통해 금전적인 이득을 취한다.[15]

3.3 심플로커(SimpleLocker)

'심플로커' 는 모바일 랜섬웨어로, 2014년 5월부터 꾸준히 출현하고 있다. 스마트폰의 파일을 암호화하고 금전을 요구한다는 점에서 Windows 기반의 랜섬웨어와 유사하다. 설치하는 과정에서 안드로이드, 플래시 플레이어, iGO의 아이콘을 사용하여 일반 앱으로 위장한다.

그림 4. 랜섬웨어의 아이콘
Fig 4. Icon for ransomware

설치 과정에서 프로그램 설치 권한과 휴대전화 관리자 권한을 요구한다. 앱을 설치하면 4PDA(iGO) 러시아 페이지를 출력하고, 스마트폰의 디바이스 정보(IMEI)를 전송한다. 이후 [그림 4]와 같이 스마트폰에 저장된 문서, 이미지, 동영상 파일을 jddlasssadxc322323sfo74hr 이라는 키 값으로 암호화한 뒤, '.enc'라는 확장자를 추가하여 저장하고 원본 파일은 제거한다.

다른 사례로 플래시 아이콘으로 위장한 악성 앱을 실행하면 [그림 5]와 같이 스마트폰의 기기모델명, 디바이스 정보(IMEI), 전화번호, 국가 정보를 가져와 초기화면에 출력하고 불법 저작권과 관리법을 위반하여 벌금을 내야 한다는 메시지가 생성된다.

벌금을 내지 않을 경우 2~8년 동안 자유를 박탈하겠다고 협박하는 내용이 출력된다. 잠긴 스마트폰을 풀고 복호화하려면 $500 달러를 입금해야하며 입금 확인이 되면 미국 재무부에서 24시간 안에 차단을 해제해 주겠다는 메시지가 출력된다.[16]

그림 5. FBI를 사칭한 협박과 금전 요구
Fig 5. Threat and cash requirements by Impersonating government

랜섬웨어에 감염된 스마트폰은 제어가 불가능하다. 다른 앱의 실행과 더불어 악성 앱을 제거할 수 없게 수많은 방법과 수단을 적용하고 있다.

Ⅳ. 랜섬웨어(Ransomware)의 해결방안

랜섬웨어에 의한 피해가 지속적으로 증가하고 있으며, 기업들의 중요문서가 랜섬웨어에 감염되면 사회적으로 심각한 문제로 확대될 수 있다. 따라서 본 논문에서는 랜섬웨어의 피해를 최소화 할 수 있는 방법을 제안한다.

▶중요한 파일들은 보안 암호화하여 백업하기

현재, 랜섬웨어를 제거할 수 있는 보안 프로그램들이 대부분 마련되어 있지만 랜섬웨어에 의해 암호화된 파일들을 완벽하게 복호화하는 방법은 없다. 따라서 랜섬웨어에 감염되었다면 미리 백업해둔 파일을 이용해 복원하는 것이 가장 기본적인 방법이고 인지하고 있는 방법임에도 최대로 좋은 조치 방법이다. 또는 암호화 프로그램을 이용하여 백업 파일에 대한 랜섬웨어의 해킹을 미리 방지한다.

▶자동으로 SW 업데이트하기

Drive-By-Download 방식으로 유포되는 랜섬웨어

는 사용자 PC에 설치되어 있는 SW의 취약점을 이용한 공격이다. 그렇기 때문에 취약한 버전의 SW를 패치하지 않으면 랜섬웨어에 감염될 확률이 높아진다. 따라서 자주 사용하는 SW(Abode Flash Player, IE, java 등)를 자동으로 업데이트 해주는 것이 가장 중요하다.

▶윈도우OS와 브라우저 최신으로 업데이트하기

윈도우의 개발사인 MS는 매월 둘째 주 화요일에 보안 업데이트를 진행하고 있다. 또한 PC 내에 고위험의 취약점이 발견되었을 경우, 비정기적으로 임시 보안업데이트를 진행하고 있다. 이 업데이트들은 이미 알려진 취약점에 대해 패치를 진행하는 것으로, 사용자들은 윈도우 보안업데이트 및 브라우저를 항상 최신 버전으로 유지하는 것이 중요하다.

▶중요파일 권한 리버스 옵션으로 변경하기

랜섬웨어에 감염되어 암호화 된 파일은 대개 읽기/쓰기 권한이 부여되어 있는 파일들이다. 기본으로 설정되어 있는 쓰기 권한을 제거한 후 중요 파일에 대한 읽기 권한을 기본으로 부여하여 랜섬웨어에 감염되어도 파일들을 안전하게 보호한다.

V. 결 론

본 논문에서는 랜섬웨어 종류와 사례를 분석하고, 해결 방안을 제시하였다. 2010년에 최초로 등장한 랜섬웨어는 현재까지는 본격적으로 한국을 공격한 사례가 없었던 만큼 대다수의 사용자들이 신속하게 대처 하지 못했으며 막대한 피해가 속출하게 되었다. 현재까지 많은 피해가 발생한 것은 아니지만, 시간이 흐를수록 진화된 랜섬웨어로 인해 일반적인 피해와 함께 국가기간산업과 공공기관등 사회적 영향력이 심각한 피해가 발생할 것으로 예측할 수 도 있다. 국가기관과 백신 소프트웨어 전문기업에서는 모든 상황을 염두에 두고 철저한 방비를 추진한 컨트롤타워를 지정하고 백신을 업그레이드를 해야 할 것이다. 개인 사용자는 스스로 정보를 보호하기 위하여 지켜야 할 내용들을 숙지하고 보안과 해킹 및 바이러스 등에 대한 공공정보망의 대처방법을 사용시스템에 적용하여야 할 것이다. 공공기관도 랜섬웨어에 대한 보안을 철저히 하고, 감염되었을 경우를 대비해 주기적 훈련과 예방책 및 대응책 등 종합적으로 마련해야할 것이다. 정부에서는 악성코드가 설치된 사이트에 대한 정보를 신속히 사용자들에게 알리고 초기에 감염되지 않도록 철저히 방어할 지침을 마련해야하며 랜섬웨어 피해를 대비하여 사고대응 매뉴얼을 제작하여 피해 발생 시 빠른 대응으로 피해를 최소화할 수 있도록 하면서, 이용자정보가 손실되지 않도록 조치를 취해야 한다. 차후 본 논문에서 제안한 피해 최소화 방안을 기반으로하는 랜섬웨어 피해예방 기술개발과 효율성 증명에 대한 연구가 필요할 것으로 판단된다.

References

[1] Sehwan Park, Yongsu Choi, "Analysis of Standardization Trend and Marketability with Tele-screen Service Platform for Smart City Foundation", JCCT, Vol.1, No.2, pp.71-75. May 31, 2015
박세환, 최용수, "스마트 시티 구축을 위한 텔레스크린 서비스플랫폼 표준화동향 및 시장성 분석",JCCT, Vol.1 No.2, , pp.71-75. May 31, 2015

[2] Naver encyclopedia of knowledg,. http://terms.naver.com/entry.nhn?docId=932418&cid=43667&categoryId=43667

[3] Security News, http://www.boannews.com/media/view.asp?idx=46006&skind=O

[4] K · BENCH, http://www.kbench.com/?q=node/149904

[5] Alyac Security Issue, http://blog.alyac.co.kr/305

[6] CryptoLocker Ransomware-Naver Blog, http://blog.naver.com/chuanstation?Redirect=Log&logNo=220368289492

[7] Korean Ransomware, http://hummingbird.tistory.com/5880

[8] Alyac Security Issue, http://alyac.altools.co.kr/SecurityCenter/Issue/ColumnView.aspx?id=52

[9] IT WORLD (http://www.itworld.co.kr/tags/63104/%ED%81%AC%EB%A6%BD%ED%86%A0%EB%9D%BD%EC%BB%A4/93112)

[10] Never Donga 동아일보(http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1

=105&oid=020&aid=0002781341)
[11] Security News (http://www.boannews.com/media/view.asp?idx=46010)
[12] Electronics Times (http://www.etnews.com/20150423000220)
[13] K · BENCH (http://www.kbench.com/?q=node/149460)
[14] Security News (http://www.boannews.com/media/view.asp?idx=46042&kind=1)
[15] Hong jiyoung, "Reveton Ransomware", 2014
[16] Removal method for Mobile ransomware 'Simplelocker', http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=23087