디지털산업정보학회 논문지 제13권 제1호-2017년 3월
http://dx.doi.org/10.17662/ksdim.2017.13.1.103

사례로 살펴본 렌섬웨어 공격에 의한 피해를 최소화하는 연구 고찰

최 희 식* · 조 양 현**

Research on Minimizing the Damage from Ransomware Attack by Case Study

Choi Heesik · Cho Yanghyun

〈Abstract〉

Recently, new variants of Ransomware are becoming a new security issue.

Ransomware continues to evolve to avoid network of security solutions and extort users' information to demand Bitcoin using social engineering technique.

Ransomware is damaging to users not only in Korea but also in all around the world. In this thesis, it will present research solution to prevent and cope from damage by new variants Ransomware, by studying on the types and damage cases of Ransomware that cause social problems. Ransomware which introduced in this paper, is the most issued malicious code in 2016, so it will evolve to a new and more powerful Ransomware which security officers cannot predict to gain profit. In this thesis, it proposes 4 methods to prevent the damage from the new variants of Ransomware to minimize the damage and infection from Ransomware.

Most importantly, if user infected from Ransomware, it is very hard to recover. Thus, it is important that users understand the basic security rules and effort to prevent them from infection.

Key Words : Ransomware, Malidity Code, Security Issuses

Ⅰ. 서론

최근 변종된 랜섬웨어가 새로운 보안이슈로 등장하고 있다. 랜섬웨어는 계속해서 변종되어 이에 대처하는 보안 솔루션 망을 피해서 사회 공학적 기법으로 사용자들의 정보를 탈취하고 비트코인을 요구하는 방식으로 우리나라뿐만 아니라 세계 여러 곳에서 많은 이용자들에게 피해를 주고 있다. 새로운 랜섬웨어 등장은 해마다 전년대비 6배 이상 증가하고 있고 랜섬웨어에 대한 피해도 급증하고 있으며 문제는 일단 감염이 되고 나면 치료할 방법이 없다는 것이 더 큰 문제점이다. 본 논문에서는 최근 악성코드의 변종으로 인해 사회적 문제점을 야기하고 있는 랜섬웨어의 종류와 피해 사례를 중심으로 새로운 변종 랜섬웨어로부터 피해를 예방하고 위험으로 대처할 수 있는 예방 방안을 제시하고자 한다.

* 삼육대학교 컴퓨터학부 외래교수
** 삼육대학교 컴퓨터학부 교수(교신저자)

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 랜섬웨어에 대한 전반적인 동향에 대해서 살펴보고, 3장에서는 랜섬웨어 공격유형에 대해서 알아보고, 4장에서는 랜섬웨어 피해 예방을 위한 방안 제시, 5장에서 결론으로 마무리하고자 한다.

Ⅱ. 관련연구

2.1 랜섬웨어 정의

랜섬웨어는 몸값(Ransom)과 소프트웨어(Software)의 합성어로 컴퓨터에 저장 된 문서, 이미지, 음원, 동영상 등의 파일을 암호화한 뒤 이를 풀어주는 대가로 금전을 요구하는 형식의 대표적인 신종 악성코드로 분류한다. 공격자는 사용자의 컴퓨터 또는 데이터 파일을 사용자가 접근할 수 없도록 암호화하고, 암호해제를 빌미로한 대가로 일정 금액의 몸값을 요구하게 된다. 만약, 사용자가 이에 불응하거나 금액을 지불하지 않을 경우, 컴퓨터나 데이터 파일에 접근할 수 없게 하거나 또는 암호화된 파일을 복구하지 못하도록 영구히 삭제하기도 한다. 특히, 랜섬웨어의 감염 경로는 사용자 시스템의 네트워크 보안이 취약한 웹 사이트나 가짜 이메일 등에 심어져 들어와 랜섬웨어를 실행시키고 감염시키는 수법을 사용하고 있다. 그러나 대부분의 랜섬웨어는 이메일을 통해 전파되어 감염되는 경우가 많으며 여전히 파일을 암호화 시킨 후, 원상복구 시켜주는 조건으로 해독용 열쇠 프로그램을 전송해 주는 수법으로 금품을 요구하고 있다[1].

2.2 랜섬웨어 공격 특징

랜섬웨어의 공격적 기법과 특징에는 <표 1>과 같은 측면도 있지만 아래와 같은 공통적인 특성도 가지고 있다.

① 마이크로소프트 매크로 형태로 첨부되거나, 최근에는 주로 자바스크립트 파일이 첨부되어 배포되고 있다.

② 기본적으로 비트코인을 몸값으로 지불하고 있으나, 악성코드 유포자 설정에 따라 최대 3비트 코인까지 요구하는 경우도 있다.

③ 연결되어 있지 않은 네트워크 UNC 경로를 식별하여 암호화한다.

④ 피해자 컴퓨터 바탕화면을 복구 서비스 안내 이미지로 변경한다.

<표 1> 랜섬웨어 특징

항목	내 용
악성코드	금전적인 이익을 목적으로 만들어진 악성코드의 일종이다.
암호화	문서파일, 이미지, 음원, 동영상 파일을 암호화하여 접근하지 못하도록 한다.
금전요구	사용자 파일을 암호화한 뒤, 금품을 요구하는 형식의 공격적 특성을 가진다.
파일복구	암호화키 복구는 대가를 지불해도 사실상 불가능하다는 게 현실이다.

<표 1>에서 살펴본 바와 같이 랜섬웨어가 일반적인 악성코드와 가장 큰 차이는 사용자의 파일을 암호화하여 <그림 1>과 같이 암호를 해독해 준다는 조건으로 금품을 요구하며, RSA 공개키 암호화 알고리즘을 사용한다는 것이다[5].

<그림 1> 랜섬웨어 공격 방법[7]

2.3 랜섬웨어 동향

2013년 크립토락커가 등장한 이후, <그림 2>와 같이 랜섬웨어의 공격적 기법과 랜섬웨어 유포 방식이 <표 2>와 같이 다양하게 변화되면서 큰 피해를 주고 있다.

<표 2> 랜섬웨어 변천[13]

년도	설 명
2013	CryptoLocker WIN 랜섬웨어 트로이목마 CryptoWall 최초로 비트코인을 요구
2014	CTB Locker C&C에 토렌트 사용 TorrentLocker CryptoWall 2.0
2015	CrytoWall 3.0 TeslaCrypt 1.0~2.2 온라인 게임 저장파일을 통해 잠입 CryptoWall 4.0 CryptoLocker Service 서비스 형태로 제공
2016	Locky MS워드 파일을 통해 유포 소셜엔지니어링 기법 활용 KERANGER 첫 OS X 타킷 랜섬웨어 Cerber 음성지원 랜섬웨어 Cryptxxx 1.0~3.0

① 2013년 크립토락커(CryptoLocker)

RSA 공개키 암호화 알고리즘 기법을 이용하여 파일들을 암호화하여 피해자로 하여금 복구할 수 없다는 강력한 메시지 전달과 함께 암호화 해제를 위해서는 금액을 지급하라는 형식의 금전적 이익을 취하는 최초의 랜섬웨어이다. 크립토락커 랜섬웨어는 Drive-By-Download 방식으로 사이트에 접속만 해도 감염이 되는 공격적 형태를 취하고 있다[2].

② 2014년 크립토월(Cryptowall)

크립토월 랜섬웨어는 크립토락커와 유사한 형태의 특성을 가지고 있으며 사용자 PC 파일을 RSA 공개키 암호화 알고리즘 기법을 사용하여 파일을 암호화시킨 뒤, 파일 복구비용을 요구한다. 크립토월이 실행되면 즉시 "C:\Documents and Settings_사용자명_\Application Data" 경로에 폴더를 생성하고 불특정한 형식의 이름으로 자가 복제한 파일을 생성하고, 원본 악성 파일은 삭제한다[9].

③ 한글판 2015년 크립토락커

랜섬웨어 중 메시지가 한글로 나오는 최초 한글 버전으로 국내 사용자들이 웹 서핑 도중 Drive-By-Download 방식에 의해 감염되게 된다.

한글판 크립토락커는 영문판과 거의 유사한 공격 기법으로 악성코드에 감염된 파일은 RSA-2048로 암호화되어 있기 때문에, 해당 파일은 암호키 없이 복구가 불가능하다. 또한, 해커가 요구한 금액을 지불하더라도 파일을 복구해주는 해독키를 보내주지 않기 때문에 위험도가 높은 악성 프로그램이라 할 수 있다. 암호화하는 파일의 종류로는 xls, xlsx, docx, pdf, jpg, cd, jpeg, icd, rar, mdb, zip 등으로 대부분 일상에서 널리 사용하는 파일 등을 포함하고 있다[10].

④ 2016년 Locky

Locky 램섬웨어는 Microsoft Word 문서에 악성 매크로 코드를 심어 이메일을 통해 무작위로 전파시

키게 된다. 사용자는 첨부된 Word 문서를 여는 순간 문서 파일이 암호화하여 Locky 랜섬웨어에 감염되게 된다. 또한, Locky는 네트워크 공유를 통해 연결된 PC를 감염시킬 뿐만 아니라 원본 파일명도 변경하는 변칙성을 가지고 있으며 PC 디렉토리와 PC에 연결된 이동식 스토리지에 저장된 파일까지도 암호화시키고 있다[11].

⑤ 직소(JigSaw)

직소 랜섬웨어는 파일을 암호화 한 뒤 단계적으로 삭제해 나가며 피해자가 몸값을 지불할 수밖에 없도록 공포감과 압박을 심어준다. 직소 랜섬웨어는 1fichier[.]com 이라는 무료 클라우드 저장 서비스에서 다운로드 되며, 일부 성인 사이트를 통해서도 다운되며 사용자가 클릭하는 순간 감염되게 된다[12].

<표 3> 랜섬웨어 유포 방식[14]

유포 방식	특 징
스팸 메일	• 전통적인 악성코드 유포 기법 • 이메일 제목 및 내용, 첨부 파일 등으로 사용자를 속여서 메일의 첨부 파일을 열도록 유도하여 감염
익스플로잇킷(EK)	• 웹 취약점(Drive-by-download) 이용 • 불특정 다수의 감염에 효과적
멀버타이징	• EK와 광고 모듈이 결합된 방식 • 불특정 다수를 대상으로 악성코드를 감염시킬 수 있음

Ⅲ. 랜섬웨어 공격

실생활에 있어서 PC가 랜섬웨어에 감염되게 되면 컴퓨터가 부팅되더라도 레지스트리와 같은 시작 프로그램에 계속 잔재하기 때문에 금품을 요구하는 알림 메시지가 지속적으로 오게 된다. 백신을 사용하여 감염된 시스템을 치료할 수 있지만 감염된 파일들은 이미 암호화되어 치료에 대한 복구가 불가능하므로 사용할 수가 없다. 즉, 백신으로 랜섬웨어를 제거하더라도 암호화된 파일을 해독할 수 없는 키가 없다면 파일을 사용할 수 없다[4]. 해커들은 가상화폐인 비트코인 확산으로 랜섬웨어 유포를 통해 돈을 벌수 있다는 잘못된 생각으로 새로운 변종 랜섬웨어 개발에 열을 올리고 있어서 랜섬웨어 피해는 더욱더 가중될 것으로 전망된다.

3.1 와이파이 랜섬웨어

요즘은 각종 공공기관이나 편의시설 어디에 가더라도 무료로 와이파이에 접속하여 편리하게 인터넷을 이용할 수 있다. 국내 사용자들 중에서도 많은 사람들이 와이파이에 접속하여 단순한 메신저 사용, 메일, 웹서핑 뿐 아니라 인터넷에 접속하여 VOD 방송보기 등을 지하철과 도서관, 공항, 커피숍과 같은 공공기반의 주변에서 많이 찾아볼 수 있다. 하지만 이 무료 와이파이 접속이 공짜라해서 무심코 사용하다간 사용자 스마트폰이 랜섬웨어 공격에 감염되어 큰 피해를 볼 수 있다. 공격자는 무선랜 보안의 취약성에 대한 인지를 못하는 도서지역 및 랜섬웨어와 같은 악성코드에 대한 사전 정보가 없는 열악한 환경의 실태를 미리 파악하여 공격적 대상으로 삼기 때문에 피해가 발생하게 된다[15].

사례 : 많은 사용자가 무료 와이파이에 접속하여 유명한 게임 애플리케이션을 다운받아 랜섬웨어에 감염되었다. 공격자는 사람들이 많이 모이는 휴게소나 카페 등에 무료 와이파이를 개설하여 사람들이 무선 와이파이에 접속하길 기다렸다가 접속하게 되면, 무선 공유기를 해킹하여, 해당 와이파이에 접속하는 사용자 스마트폰에서 이메일과 같은 개인정보

를 유출해 간다.

3.2 스마트폰 랜섬웨어

랜섬웨어 중 위험도 높은 것은 스마트폰 관련 앱을 설치했다가 악성 랜섬웨어에 감염되어 스마트폰이 잠겨서 사용할 수 없는 경우이다. 스마트폰이 랜섬웨어에 감염되게 되면 사용자 동의 없이 강제로 특정 앱을 실행시키는 것은 물론 스마트폰에 저장된 모든 정보를 빼갈 수 있다. 특히, 안드로이드 관련 스마트폰에 있는 특정 폴더에 데이터 파일을 일반 파일인 것처럼 'form.html'와 같은 형태로 숨겨서 'classes.dex' 코드가 실행되면 악성코드가 실행되어 감염되게 한다[8].

사례 : 포켓몬 고(Pokemon GO)의 인기에 힘입어 랜섬웨어가 포켓몬 고 게임으로 위장한 랜섬웨어 제작에도 악용되었다. 사용자가 포켓몬 고 게임 애플리케이션 앱을 설치하면 이와 관련된 정상적인 앱인 것처럼 위장하여 설치된 후, 스마트폰 화면을 강제로 잠가버린 뒤, 사용을 못하도록 한다.

3.3 사물 인터넷(Internet of Things) 랜섬웨어

모바일 환경의 증가에 따라 IoT 디바이스는 인터넷에 연결되어 다양한 조작을 가능하게 하여 활용되고 있다. 대표적인 제품들에는 스마트워치, 스마트 TV, 스마트 홈, 스마트냉장고, 스마트 잠금 및 스마트 차량 등에 응용되고 있다. 특히, IoT 디바이스는 유·무선 통신을 통하여 센서 정보와 같은 데이터들을 활발하게 주고받으며 상호작용하기 때문에 안전하지 못하다. 게다가 IoT 디바이스들은 센서 정보뿐만 아니라 개인정보와 기업정보 등 민감한 정보를 가지고 있고, 스마트 자동차, 원격진료 시스템 등의 IoT 이용분야가 확산되어진다면 더욱더 보안 위협 증가에 따른 개인정보의 유출이나 랜섬웨어에 감염되어 금전적 피해에 쉽게 노출될 수 있다[6].

사례 : 스마트냉장고 구글 계정의 로그인 정보가 유출되어 IoT 보안 강화에 대한 취약점이 드러났다.

3.4 제로데이 공격

제로데이 공격은 누구에게나 영향을 미칠 수 있는 공격일 수 있다. 한 때 인터넷 익스플로러 구 버전 지원 종료로 인해서 제로데이 보안 위협에 처한 경우가 있었다. 뿐만 아니라 제로데이 공격은 바이러스, 이메일 첨부 파일, 웹페이지, 팝업 창, 인스턴트 메시지와 소셜 미디어 서비스 등 공격 경로와 방법이 무궁무진하다. 랜섬웨어 신종 바이러스 출현 이후, 치료에 대한 패치가 나오기 전까지 제로데이 공격 위험으로부터 벗어날 수가 없다. 제로데이 공격은 수많은 시스템들이 공격의 대상이 되므로 막대한 피해가 예상될 뿐만 아니라 해당 공격을 탐지하기 위한 징후도 쉽지 않아 위험한 공격이라 할 수 있다[3].

사례 : 윈도우 바로가기 파일(.lnk) 형태의 랜섬웨어가 발견되어 악성 자바스크립트 파일을 생성 및 실행하는 코드가 삽입돼 있어 사용자 모르게 랜섬웨어에 감염된다. 해당 랜섬웨어는 사용자 PC의 사진 및 그림 파일, 각종 오피스 문서 등을 암호화하여 몸값을 요구한다.

Ⅵ. 방안 제시

2016년도 보안업계에서는 새로운 형태의 신종 악

성코드에 사전 정보 및 탐지가 어려워 많은 피해를 보게 되었다. 뿐만 아니라 유명 앱을 사칭하는 가짜 랜섬웨어 및 유명 사이트 바로가기를 빙자한 유도성 랜섬웨어도 등장하였다. 4장에서는 3장 랜섬웨어 공격에 의한 피해사례를 가지고 사용자가 사용하는 IT 디바이스에 의한 랜섬웨어 피해를 최소화하기 위한 방안을 제시한다.

랜섬웨어 악성코드 공격의 특성은 그들이 원하는 다양한 공격 유형으로 사용자의 시스템, 디바이스, 문서 파일 등을 암호화로 감염시킨 후, 암호 해독을 이유로 금전적 이득을 취하기 위한 입금을 요구해 온다. 사용자는 감염된 중요한 파일을 복구하기 위해서 우선적으로 신고보다는 복구 대가를 지급하려고 노력한다. 하지만 컴퓨터 지식이 부족한 사람에게는 비트코인이 무엇인지도 모르고 또한 그것을 어디서 사서 어떤 방식으로 보내는지 조차 모른다. 그러나 더 큰 문제는 대부분 사용자가 어려운 상황에서 금전적 대가를 지불한다 해도 암호화된 파일은 복구는커녕 응답도 없는 것이 대부분이다. 즉, 공격자는 돈만 챙기고 암호 복구는 관여하지 않고 잠적하는 것이 그들의 수법이다. 사용자는 복구가 거의 힘들다는 점을 명시하고 무엇보다 랜섬웨어 악성코드에 감염되지 않도록 예방하는 것이 무엇보다 중요하다.

4.1 사물 인터넷 보안 제안

인터넷의 발전으로 인터넷 사용자가 늘고 인터넷 네트워크를 기반으로 사물인터넷과 빅데이터의 중요성이 대두대기 시작하였다. 많은 사람들은 사물인터넷을 활용한 가전기기와 차량 등에서 그 편리성을 기대하면서 활용하기 시작하였다. 그러나 사물인터넷 사용이 대부분 무선 네트워크를 이용한 인터넷 기반으로 이용되고 있는 취약성을 이용하여 안전이 위협되고 있다. 앞으로도 사물인터넷 기기를 이용한 사용자가 늘어나면서 랜섬웨어 공격도 증가할 것으로 예상하고 있다. 그러나 아직까지는 사물인터넷 기기에 대한 데이터가 한정적이고 기기에 중요한 데이터가 들어있다 하더라도 기기의 정보를 초기화함으로써 피해에 대한 수습은 아직까지는 그나마 안전하다고는 할 수 있다. 하지만 기기를 감염시키고 원격으로 조정하여 오작동 유발과 새로운 공격으로 이어질 경우 큰 피해를 예고하기 때문에 제품을 개발하는 관계자 및 기관에서는 사물인터넷 기기에 강화된 보안 제품 출시에 좀 더 신경을 써야할 것으로 사료된다.

4.2 무선 와이파이 보안 제안

많은 사용자가 카페에서 무선 와이파이를 찾아서 접속하는 방법은 어렵지 않게 잘 이용하고 있다. 그런데 무선 와이파이 접속 시 자세히 살펴보면 보안사항에 대해서는 안전이 보장되지 못하기 때문에 안전성을 고려하여 보안을 설정함을 추천한다는 경고성 메시지를 표시하고 있다. 그런데도 불구하고 대부분의 사람들은 안전성 확보에 대한 경고를 무시하고 있다. 이로 인해 공격자가 설치해 놓은 랜섬웨어에 무방비로 당할 수밖에 없는 실정이다. 무선 근거리 무선망 영역에서 피해를 보지 않도록 사용자는 무선 공유기에 접속할 때는 반드시 개인 접속비밀번호를 설정해 놓는 것이 좋다.

① 무선 공유기 비밀번호 : 개인 접속 비밀번호 외에 무선 공유기 비밀번호도 함께 바꾼다.

② 관리자용 비밀번호 : 접속 비밀번호 외에도 관리자 비밀번호까지 바꾸어 함께 바꾸어 안전성을 확보한다.

③ 공유 지역 내 무선 기기 사용시간을 제어하는

방안을 제시한다. 공유 와이파이는 여러 사람이 공동으로 이용하는 만큼 피해 확산에 대한 예방 조치 방안과 여러 사람들의 사용 편의를 고려하여 사용시간을 설정하여 서비스를 제공한다. 만약, 고객이 무선 와이파이 영역에 접속하여 지정된 시간이 초과할 시에는 자동으로 접속이 차단되도록 하게 하여 공격자의 공격 유발을 피할 수 있도록 한다.

4.3 기본 보안수칙 제안

현대 사람들은 최근에 들어와서 인터넷을 통해 정보를 얻고 정보를 활용하는 정보의 범람 시대에 살아가고 있다. 또한, 각종 무료 앱을 얻기 위해 안전에 대한 검증을 미처 확인하지 못하고 앱을 설치하여 랜섬웨어와 같은 약성코드에 감염되기도 하고 인터넷 검색을 통해서 방문한 웹 사이트에 접속만 함으로써 악성코드가 감염되는 경우도 많다. 가장 기본적이면서도 조금만 관심을 가지고 주의를 기울인다면 일반적인 부주의로 인한 무방비 상태의 위험으로 일단은 1차 피해예방을 줄일 수 있다.

첫째, 랜섬웨어 악성코드 감염경로로 이메일이 널리 사용되고 있다. 수신된 이메일에서 내용을 확인하기 전에 발신처를 확인하고 혹시 거래가 없는 지인의 메일을 받았을 경우나 발신처가 불분명한 메일은 의심할 필요가 있고 무조건 스팸메일로 분류 처리를 하는 것이 좋다.

둘째, 웹사이트 방문 시에는 웹에서 검색된 사이트를 클릭하여 방문하는 것 보다는 URL 주소창에 직접 방문하고자 하는 웹사이트를 입력하여 접속하는 것이 좋다. 또한, 웹사이트 방문 시 검증되지 않은 웹 사이트로 부터의 다운로드는 무조건 지양하고, 개발사와 같은 공식적인 홈페이지를 직접 이용하는 것이 좋다.

4.4 제로데이 공격 피해 예방 제안

제로데이는 공격은 누구에게나 영향을 미칠 수 있는 공격으로 이메일 첨부파일에 포함된 문서파일이나 자바스크립트 파일 실행 시 감염되고 있다. 자바스크립트(Java script) 프로그래밍언어로 제작된 Javascript 랜섬웨어는 코드를 숨기거나 암호화시켜서 스팸 메일에 첨부되어 보안 솔루션으로 탐지하기가 어렵다. 제로데이와 같은 랜섬웨어의 피해와 위험적 노출은 잘 알려진 소프트웨어와 같은 프로그램에 버그와 같은 오류로 인한 취약점이 발견된 경우, 공격자는 개발 소프트웨어 회사에서 패치를 작성하여 수정 버전이 출시되기도 전에 발 빠르게 악성코드를 개발하여 유포하게 된다.

피해적 사례를 분석한 결과, 사람들이 많이 쓰는 인기 소프트웨어일수록 제로데이 공격에 감염 피해가 많았으며 개발 업체 측의 결함에 대한 버그가 공식적으로 공개되기 이전보다 취약점을 이용한 악성코드가 먼저 개발·유포되어 피해를 유발했다는 것이다. 제로데이 공격에 대한 경각심과 피해를 최소화하기 위한 제안된 방안을 살펴보자. 우선적으로 이메일로 들어오는 링크를 클릭하여 패치버전을 다운받는 것 대신 공식적인 소프트웨어 웹페이지에 접속하여 패치버전을 다운받는 것을 권고한다. 특히, 윈도우 운영체제, 익스플로러, 크롬, 파이어폭스, 오페라와 같은 인터넷 브라우저 및 오피스 관련 패치프로그램 이용 시에는 피해를 최소화하기 위해 다음과 같은 세심한 주의를 갖는 것이 절대 필요하다.

<표 4> 제로데이 피해 예방 권고

항목	내 용
이메일 링크	이메일에 첨부된 출처를 알 수 없는 업그레이드 및 오류 관련 패치버전 다운로드 유도 시에는 즉시 삭제 조치 할 것

항목	내 용
백업 저장	평소 오피스 관련 중요한 문서 파일은 저장과 백업을 동시에 해두는 습관적인 노력이 절대 필요 함
속도 의심	사용하는 컴퓨터 시스템이 평소 사용하는 속도와 다르게 느려지거나 인터넷 트래픽이 심한 경우 악성코드 감염에 대한 의구심을 갖는 것도 예방 차원에서 중요 함
익스플로잇보호	완벽한 익스플로잇 보호를 위해 잘 알려지지 않은 외부로 들어오는 메모리 호출, 샌드박스 등과 같은 보호영역에 부정적으로 사용하는 익스플로잇에 공격을 완전 차단하는 보안 솔루션 사용을 강력히 권고 함

Ⅴ. 결론

본 논문을 통해 소개된 랜섬웨어는 2016년 가장 이슈화된 악성코드인 만큼 앞으로도 금전 이득을 취하기 위해, 보안 관계자가 예측하지 못하는 더 세고 강한 신종 랜섬웨어가 등장할 것이 전망되고 있다.

본 논문에서 살펴본 바와 같이 랜섬웨어에 일단 감염되게 되면 치료는 사실상 불가능하다. 공격자가 요구하는 금전적 이익을 취한 후, 피해자 파일 복구에는 전혀 관심이 없고 오히려 새로운 랜섬웨어 개발에만 몰두할 것이다.

본 논문에서는 랜섬웨어의 피해를 예방하고 감염에 대한 피해를 최소화하기 위한 방안을 제시하였다. 가장 중요한 것은 랜섬웨어에 일단 감염이 되면 복구가 어려운 만큼 무엇보다 사용자 개인의 기본 보안 수칙을 숙지하고 이행하는 것이 최선이다. 또한, 랜섬웨어 악성코드에 감염이 되었을 경우, 금전적 손해에 대한 피해 보상과 법적 대응에 대한 체계화된 대책 마련이 사회적인 측면에서 반드시 수립되어야할 지속적인 연구가 꾸준히 필요하다.

참고문헌

[1] 유정무, 조제경, 류재철, “파일 I/O Interval을 이용한 랜섬웨어 공격 차단 방법론,” 정보보호학회 논문지, 제 26권, 3호, 2016년, p. 646.

[2] 문재연, 장영현, “랜섬웨어 분석과 피해 최소화 방안,” The Journal of the Convergence on Culture Technology(JCCT), 제 2권, 1호, 2016년, p. 80.

[3] 김경신, 강문식, “차세대 사이버 사이버 보안 이슈와 위협 및 대처방안,” 전자공학회지, 제 41권 4호, 2014년, p. 75.

[4] 김봉준, 김운수, 이정환, 임신혁, 송상근, 이상준, “안드로이드 플랫폼 기반 프로세스 모니터링을 이용 랜섬웨어 방지 시스템의 설계 및 구현,” 정보과학회 학술발표논문집, 2015년, p. 852.

[5] 남효미, 장정숙, 전용희, “랜섬웨어의 공격 기법 분석과 대응 방안에 대한 연구,” 한국인터넷정보학회, 제 17권, 1호, 2016년, p. 284.

[6] 서규원, 김호원, “랜섬웨어의 종류와 앞으로의 동향,” 한국컴퓨터종합학술대회 논문집, 2016년, p. 1117.

[7] http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=&menu_dist=1&seq=24337

[8] http://techholic.co.kr/archives/55672

[9] http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=24288

[10] http://www.boannews.com/media/view.asp?idx=46006

[11] http://slic.tistory.com/895

[12] http://m.datanet.co.kr/news/articleView.html?idxno=98793

[13] http://mi.jiransecurity.com/589

[14] http://download.ahnlab.com/kr/site/library/Report_Ransomware_Trend_Analysis.pdf
[15] http://www.shdms.go.kr/brd/board.asp?id=type1_1&mode=view&idx=10&page=1

■ 저자소개 ■

최 희 식
(Choi Heesik)

2008년 3월 ~ 현재 삼육대학교 컴퓨터학부 외래교수
2002년 2월 숭실대학교 컴퓨터학과(공학박사)
2006년 2월 숭실대학교 컴퓨터공학과 (공학석사)

관심분야 : 정보보안, 클라우딩컴퓨터, IoT 핀테크 금융보안
E-mail : dali3054@ssu.ac.kr

조 양 현
(Cho Yanghyun)

1997년 9월 ~ 현재 삼육대학교 컴퓨터학부 교수
2011년 2월 광운대학교 전자통신학과 (공학박사)
1985년 2월 광운대학교 전자통신학과 (공학석사)
1982년 2월 광운대학교 전자통신학과(공학사)

관심분야 : 컴퓨터네트워크, 통신망(BcN), GMPLS
E-mail : yhcho@syu.ac.kr

논문접수일 : 2017년 2월 24일
수 정 일 : 2017년 3월 13일(1차), 03월 17일(2차)
게재확정일 : 2017년 3월 21일