Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.1, Feb. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.1.155

의료산업에서의 랜섬웨어 대응 방법*

전 인 석,[1†] 김 동 원,[2] 한 근 희[3‡]
[1]고려대학교 정보보호대학원, [2]건양대학교 PRIME창의융합대학, [3]건국대학교

How to Cope with Ransomware in the Healthcare Industry*

In-seok Jeon[1†], Dong-won Kim[2], Keun-hee Han[3‡]
[1]Graduate School of Information Security, Korea University
[2]PRIME College of interdisciplinary & Creative studies, konyang University
[3]Kunkouk University

요 약

의료산업은 세계적으로 빠르게 변화하고 의료서비스가 네트워크와 연결 되면서 다양한 형태의 서비스 제공이 검토되고 있다. 의료정보의 가치는 금융정보의 가치보다 높게 평가되고 있으며, 이로 인해 의료정보의 보호가 매우 중요해지고 있다. 랜섬웨어는 지속적으로 고도화 되고 있으며 정보의 가치가 높은 산업군을 대상으로 하고 있다. 특히, 2017의 랜섬웨어는 성장기를 지나 성숙기로 진입하면서 매우 다양하게 발전하고 고도화 되었다. 의료산업은 대부분 폐쇄망으로 구성되어 있었기 때문에, 악성코드의 위협에 대비가 부족하며, 이로 인해 랜섬웨어의 공격에 매우 취약하다. 단순히 의료산업의 보안표준에 명시되어 있는 기준을 충족하기 위한 보안이 아닌 실제 랜섬웨어의 유입을 효과적으로 막거나, 공격이 성공 했다 하더라도 그 피해를 최소화 하고 복구를 할 수 있는 방안이 추가 되어야 한다. 랜섬웨어는 매우 빠르게 진화하고 고도화 되고 있기 때문에 이에 대한 대비도 매우 빠르게 진행되어야 하고 실무적인 관점에서 접근을 해야 한다. ISO 27799, 27002 표준을 기준으로 진화된 랜섬웨어에 대응할 수 있는 요소를 도출하여 기존의 의료정보보호 시스템을 유지/관리 하면서도 랜섬웨어에 보다 효율적으로 대응할 수 있도록 하였다.

ABSTRACT

As medical healthcare industry is growing up rapidly these days, providing various new healthcare service is considered carefully. Health information is considered to be more important than financial information; therefore, protecting health information becomes a very significant task. Ransomware is now targeting industry groups that have high information value. Especially, ransomware has grown in various ways since entering maturity in 2017. Healthcare industry is highly vulnerable to ransomeware since most healthcare organizations are configured in closed network with lack of malware protection. Only meeting the security criteria is not the solution. In the case of a successful attack, restoration process must be prepared to minimize damages as soon as possible. Ransomware is growing rapidly and becoming more complex that protection must be improved much faster. Based on ISO 27799 and 27002 standard, we extract and present security measures against advanced ransomware to maintain and manage healthcare system more effectively.

Keywords: healthcare industry, ransomware, malware, telemedicine, medical services

Received(10. 20. 2017), Modified(1st: 12. 06. 2017, 2nd: 12. 21. 2017), Accepted(12. 27. 2017)

* 본 연구는 보건복지부의 재원으로 한국보건산업진흥원의 첨단의료기술개발사업 지원에 의하여 이루어진 것임(과제고유번호 : HI14C2756).

† 주저자, wilcois@ahnlab.com
‡ 교신저자, khhan@konkuk.ac.kr(Corresponding author)

I. 서 론

1.1 연구배경 및 목적

2016년 보안동향 자료를 보면 랜섬웨어로 시작해서 랜섬웨어로 끝났다고 볼 수 있을 정도로 랜섬웨어에 대한 이슈가 지속적으로 발생하였다. 각종 보안업체 및 정부기관에서는 랜섬웨어를 예방하기 위한 수많은 가이드가 나왔고 그 피해가 매우 빈번했기 때문에 많은 사용자 및 관리자들도 심각성을 인지하고 대응하고 있다. 하지만 랜섬웨어의 피해사례는 전혀 감소하지 않고 증가하고 있다. 특히 랜섬웨어는 정보의 가치를 인질로 삼아 비용을 요구하기 때문에 정보의 가치의 클수록 그 공격의 대상이 될 수 있다. 의료정보는 그 정보의 가치가 매우 크고 최근 스마트병원 및 스마트의료기기의 증가로 인하여 그 정보가 빠르게 교환되고 있다. 의료서비스가 랜섬웨어의 공격을 받을 경우 환자의 생명과 안전에 영향을 줄 수 있기 때문에 의료산업의 특수성을 고려해서 대응 방안을 고려해야 한다. 2016년이 랜섬웨어의 성장기라면 2017년은 성숙기라고 볼 수 있다. 단순히 단발성으로 랜섬웨어 공격을 하는 것이 아니라 다른 공격기법들과 결합 되어 많은 피해사례를 남기고 있다. 따라서 랜섬웨어가 어떤 형태로 진화하고 있는지를 분석하여 의료산업에서의 랜섬웨어에 대한 피해를 최소화 할 수 있도록 대응방안을 마련하고자 한다.

1.2 연구방법 및 구성

전통적인 랜섬웨어에 대한 대응방법은 악성코드 대응방법과 동일하다. 하지만 최근의 랜섬웨어는 일반적인 악성코드 대응방법으로는 효과적으로 대응할 수 없다. 따라서 2017년 상반기에 진화된 랜섬웨어 유형을 수집하고 분석하여 공격자가 진화하는 방향을 파악하고자 한다. 추가된 기능이나 기존의 대응 방법을 우회한 요소들을 식별하여 추가적인 대응 방안을 수립함으로서 현재까지 알려진 랜섬웨어에 대하여 대응조치를 진행할 수 있도록 하였다. 의료산업은 스마트병원, 스마트의료기기, 웨어러블 의료기기, 등 빠르게 발전하고 있으며, 더 많은 정보가 연결되고 있다. 의료정보의 가치와 랜섬웨어의 대상 산업군을 추가 분석하여 의료산업에 대한 랜섬웨어 위협을 도출하였다. 마지막으로 진화방향을 분석하여 앞으로 랜섬웨어의 고도화 방향을 예측하고 이를 대비할 수 있도록 ISMS 및 ISO 27799의 통제항목에서 랜섬웨어 대응을 위한 대응방안을 도출 하였다.

II. 관련 연구

전통적인 랜섬웨어의 경우 대부분 이메일을 통해 유입이 발생하고 있었으나, 최근의 랜섬웨어의 유입경로는 매우 다양해 지고 있다, 특히 보안업체 이노티움의 랜섬웨어침해대응센터에 접수된 피해 사례를 분석해 보면 인터넷을 통한 랜섬웨어 유입이 70%를 차지하고 있다. 지난 2년간 센터에 신고 접수된 7494건을 전수조사한 결과에 의하면 특정 홈페이지 접속만으로 랜섬웨어 감염 피해가 발생하고 있다. 이는 위장 이메일이 랜섬웨어 감염 루트인 미국, 영국 사례와 완전히 다른 결과다. 랜섬웨어의 유입양상이 변화하고 있다는 것을 의미한다.

2.1 2017년 랜섬웨어 동향

2017년 6월까지 이노티움 랜섬웨어침해사고대응센터에 접수된 피해 신고는 총 2561건으로 이미 2015년 연간 피해 건수(2678건)와 비슷한 수준으로 증가하고 있다. 랜섬웨어의 위협은 이미 2016년에 크게 증가하였으며, 증가추세도 문제지만 가장 큰 문제점은 2017년에는 양적인 증가 보다는 질적인 진화가 큰 위협으로 작용하고 있다.

전통적인 랜섬웨어는 2016년에 성장기를 거치면서 2017년에는 성숙기에 접어든다고 볼 수 있다. 공격기법들이 이미 높은 수준에서 정교화 되었고 방어기법에 대한 분석을 진행한 것으로 보인다. 특히 서비스형 랜섬웨어(RaaS)를 통해 신종 랜섬웨어가 유포되고 있기 때문에 전문가가 아니더라도 누구라도 랜섬웨어 공격을 할 수 있으며, RaaS도 여러 가지 편의기능을 추가하여 발전하고 있기 때문에 매우 큰 위협이다. Table 1은 2017년 상반기에 국내에 유포된 랜섬웨어 리스트이다.

지난 2017년 4월, 해킹 그룹 쉐도우 브로커스(Shadow Brokers)가 '이터널블루(Eternal Blue)'라는 윈도우 운영체제 취약점을 공개했다[1]. 해당 취약점을 악용한 워너크립터(WannaCryptor) 랜섬웨어는 5월 12일 전 세계적으로 확산됨과 동시에 약 120여개국에 있는 25만대 이상의 PC에 감염 피해를 입혔다. 이는 과거의 랜섬웨어의 유포방식과는 많은 부분에서 차이점이 있다. 가장 큰 차이점은 랜섬웨어

Table 1. Ransomware trends in the first half of 2017

Month	type
1	Venus Locker Satan
2	Mac OS Ransomware CryptoShield Sage Erebus Lockdroid
3	Revenge Locky Variants
4	Wanna Cryptor Conficker
5	Matrix Fatboy
6	Erebus Variants Petya Variants

가 OS취약점을 이용하여 사용자가 어떠한 행위(WEB, 이메일, 등)를 하지 않아도 패치가 되지 않은 OS사용자는 인터넷에 연결만 했다는 이유로 감염이 가능함을 의미한다. 결과적으로 랜섬웨어가 OS취약점을 이용했을 경우 엄청난 파급효과를 발생시킬 수 있었다.

2017년 6월 10일에 국내 웹호스팅 업체인 '인터넷나야나'의 웹 서버와 백업 서버가 에레버스(Erebus) 랜섬웨어에 감염되는 사태가 발생했다. 153대의 서버가 감염되어 암호화되었고, 이로 인해 해당 웹호스팅 업체의 서비스를 받고 있던 약 3천여 업체의 홈페이지가 마비되는 피해를 입었다. 이 침해사고는 랜섬웨어가 APT를 이용했을 경우에 어떤 영향을 줄 수 있는지를 보여주고 있다. 대상업체가 보안에 미흡한 부분은 있었으나, 랜섬웨어의 가장 중요한 대비책으로 알려진 백업에 대해서는 3중으로 백업을 진행하고 있었다. 하지만 공격자는 대상업체의 백업시스템을 분석하여 백업시스템을 우회하여 침해사고를 발생시켰다. 과거에는 사용자가 많은 시스템을 대상으로 광범위하게 랜섬웨어를 유포하였으나 최근 동향은 특수목적시스템을 포함하여, 정보의 가치가 중요한 시스템은 APT공격과 결합하여 랜섬웨어를 유포하고 있다.

스포라(Spora) 랜섬웨어는 다른 랜섬웨어와 크게 다르지 않지만, 랜섬웨어에 감염된 피해자에게 다양한 지불 옵션을 제공한다는 점이 특징이다[3]. 스포라는 CnC 서버 없이도, 또 마스터 키 배포 없이도 모든 피해자를 유효하게 공략할 수 있다. 랜섬웨어를 대응하는 보안관리자는 RSA키를 전달하는 CnC서버를 차단함으로서 랜섬웨어가 정상적으로 동작할 수 없도록 만들고 있다. 공격자는 이를 우회하기 위하여 로컬에서 암호화키를 생성하기도 하지만 이 경우 한 피해자를 복화하하거나 코드분석을 통하여 복호화키가 공개되는 경우가 발생할 수 있다. 스포라는 RSA공개키를 포함하고 있는 부분은 오프라인 암호화방식의 랜섬웨어와 동일하지만 이후 해당 키를 이용하여 개별적으로 AES키를 이용하여 암호화를 진행하는 방법으로 진화하였다.

케르베르(Cerber)는 2016년 3월에 최초 발견된 후 가장 오랜 기간 동안 활발하게 활동하고 있는 랜섬웨어로 암호화 사실을 음성으로 알려주는 최초의 랜섬웨어다. 이번 2017년 2월에 새롭게 발견된 케르베르 버전 6는 윈도우 보안 센터에 등록된 보안 제품 실행 경로를 윈도우 방화벽 차단 목록에 추가하여 정상적인 보안제품의 동작을 방해하는 것이 가장 큰 특징이다[4]. 랜섬웨어가 사회적으로 이슈가 되면서 수많은 보안업체에서 빠른 속도로 랜섬웨어의 샘플을 확보하고 분석하여 대응을 하고 있다. 케르베르의 가장 큰 특징은 보안 제품의 동작을 방해하는 기능으로 진화하고 있다.

샌드박스 기술의 발전으로 인하여 악성코드 및 랜섬웨어에 대응하는 방어기술이 빠르게 향상하고 있는 것이 사실이다. 하지만 랜섬웨어 공격자는 직접적으로 금전적인 이득을 얻고 있기 때문에 매우 빠르고 정교하게 발전하고 있다. 특히 방어기술에 대한 분석을 통하여 랜섬웨어를 발전시키고 있는 것이다. 최근 2017년에 진화된 랜섬에서 가장 중요하게 생각해야 하는 부분은 랜섬웨어가 SW취약점, WEB, 메일을 이용한 전통적인 방법에서 APT와 OS취약점과 결합하고 있다는 부분이다. 이는 사회 전반적으로 파급력이 아주 크거나(OS취약점) 특정 대상(APT)에 매우 효과적인 공격방법이 될 수 있다. 의료정보의 가치를 생각하면 의료시스템을 대상으로 특수 제작 된 랜섬웨어 공격에 대비가 필요하다.

2.2 랜섬웨어 분석

2016년 11월 샌프란시스코의 경전철 운행을 중단시킨 사고와 2017년 1월 30일 워싱턴 DC의 CCTV가 마비된 사건은 모두 MBR 영역을 암호화하는 HDD크립터 랜섬웨어에 의한 것이었다[3]. 데이터베이스를 대상으로한 랜섬웨어는 Table 2와 같이 2017년 1월부

Table 2. DB Targeting ransomware[3]

Date	Target
01.03	MongoDB
01.13	ElasticSerch
01.18	Hadoop
02.25	MySQL

터 2달에 걸쳐 발생하였다. 1월 3일에는 오픈소스 프로그램인 몽고DB(MongoDB) 서버, 13일에는 분산형 검색 및 분석 엔진인 엘라스틱서치(ElasticSearch) 서버에 대한 암호화 공격이 발견되었으며 18일에는 빅데이터를 처리할 수 있는 오픈소스 프레임워크인 하둡(Hadoop) 서버에 대한 암호화 공격이 확인됐다[3].

랜섬웨어의 공격대상이 단순히 윈도우 시스템을 암호화한 후 복구비용을 요구하는 것에서 그치지 않고 자산의 가치가 중요한 DB를 대상으로도 다양하게 진화하고 있다는 것을 의미한다. 많은 사용자를 감염시키는 것을 목적으로 대중적인 OS나 어플리케이션을 대상으로 하다가 사용자가 적고 감염시키기 어렵더라도 정보의 가치가 있는 대상으로 진화하고 있는 것이다.

Table 3과 같이 랜섬웨어의 유입경로가 매우 다양해 지고 있기 때문에 이에 대한 대비가 필요하다. 특히 Wanna Cryptor 와 Erebus Variants 에 대한 분석을 통한 대응방안을 마련해야 한다.

Wanna Cryptor 사태로 인하여 랜섬웨어가 얼마나 파급적이고 여러 산업시스템을 동시에 감염시킬 수 있음을 우리는 알게 되었다. Fig. 1과 같이 워너크라이는 특정한 행위를 하지 않고 취약점이 있는 시

Table 3. The first half of the year 2017 ransomware inlet path

Means	Ransomware type
Email	- Venus Locker - Sage - Locky Variants
WEB	- Satan - CryptoShield - Revenge - Matrix
BitTorrent	- Mac OS Ransomware
SW Vulnerability	- Erebus
Smart Phone	- Lockdroid
OS Vulnerability	- Wanna Cryptor - Conficker - Petya Variants
APT	- Erebus Variants

스템은 인터넷에 연결되어 있는 상황만으로도 감염이 발생한다. 의료정보시스템과 같은 특수목적 시스템은 특별한 일이 있지 않으면 별도 관리 없이 24시간 운영되는 경우가 많다.

Wanna Cryptor와 같은 랜섬웨어의 변종은 이와 같은 시스템을 매우 빠르게 감염시킬 것이고 이에 대한 대비가 필요하다. 특히 Wanna Cryptor의 침해사고를 분석해 보면 내부망에 유입된 이후 빠르게 퍼져나간 사례가 확인 되고 있다.

일반적으로 폐쇄망에 있는 시스템의 경우 OS에 대한 업데이트가 미흡한 경우가 많고 내부망이기 때문

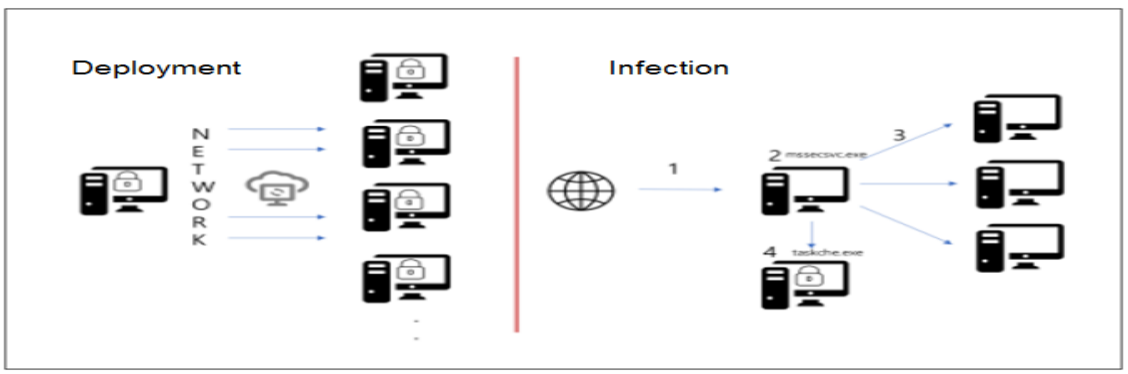

Fig. 1. Wanna cryptor infection Process[3]

에 악성코드의 유입에 대해서 안전하다고 생각하는 경우가 많다. 하지만 Wanna Cryptor의 경우에 어떠한 접점에 의해 내부망과 연결되는 순간에 내부에서 빠른속도로 확산이 되었으며, 내부망에서 외부로의 통신이 불가능하기에 추후에 비용을 지불[1]하거나 CnC서버를 해킹하여 복호화키를 확보한다 하더라도 복구가 불가능한 상황이 발생하게 된다.

Erebus Variants은 전통적인 랜섬웨어의 대응 방안으로 더 이상 진화된 랜섬웨어에 대응할 수 없음을 명확하게 보여주는 침해사고이다. 가장 큰 특징은 랜섬웨어가 더 이상 단독적으로 공격하지 않고 APT와 결합된 사례이다. 피해시스템은 모두 리눅스 시스템이었으며, OS취약점을 포함한 어떠한 SW취약점이 이용되지 않았다. 공격자는 일반적인 APT공격처럼 근무자의 PC에서 서버계정을 탈취하여 리눅스시스템을 암호화 진행 하였다. 단일 목표를 대상으로 한 랜섬웨어는 의미하는 바가 매우 크다. 의료정보시스템은 별도로 운영되는 시스템이 많기 때문에 그 수가 많지가 않다. 따라서 지금까지 의료기관이 피해를 입은 사례는 대부분 윈도우OS시스템이 랜섬웨어에 감염되면서 의료서비스에 문제가 발생한 케이스가 대부분이다. 하지만 이번 침해사고와 같이 의료정보시스템을 대상으로 한 APT 공격이 준비 될 수 있으며, 이 경우 의료정보시스템 자체에 대한 공격이 이루어지기 때문에 취약점 패치를 하는 수준에서 예방 할 수 없다.

또한, APT와 결합되었다는 의미는 대상 시스템에 대하여 많은 정보를 획득하고 분석을 했다는 것을 의미한다. 지금까지 랜섬웨어를 예방하는 방법에서 최후의 보루는 백업이다. 모든 위협에 대해서 예방을 할 수 없기 때문에 예방을 준비하면서 실제 침해사고가 발생했을 경우 빠른 복구를 위해서 사실상 유일한 수단은 백업이 유일하다고 볼 수 있다. 따라서 중요 시스템을 운영하는 경우는 2중 3중으로 백업을 진행하고 있다. 문제는 이번 Erebus Variants의 피해업체의 백업시스템을 분석해 보면, 단순히 백업만으로는 랜섬웨어를 효과적으로 막을 수 없음을 판단할 수 있다. Erebus Variants 피해업체의 백업시스템은 Fig. 2와 같이 총 3중으로 구성하였다.

1) 랜섬웨어 감염이 발생했을 경우 공격자에게 비용을 지불하지 않는 것이 원칙이지만 암호화 된 정보가 환자의 생명에 매우 직접적으로 영향을 주는 정보이거나 복호화 비용을 지불함으로 서 추가 발생할 수 있는 피해가 해당 정보의 가치보다 낮을 경우에 한해서 복구비를 지불하고 복구하는 경우가 있음.

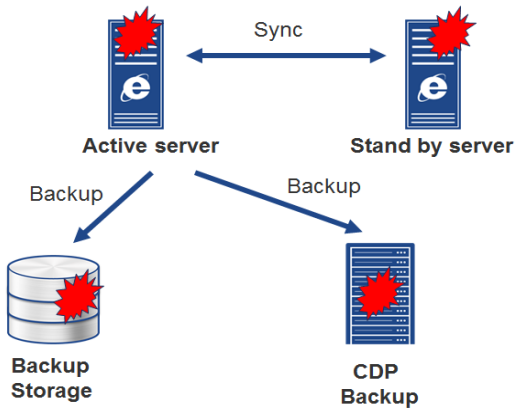

Fig. 2. Erebus variants configure Backup to target vendors

먼저 Active Server의 데이터는 Stand by server와 실시간으로 동기화를 진행하고 있었으며, 별도 백업스토리지를 이용하여 데이터에 대한 백업을 진행하고 있었다. 또한 별도 솔루션을 이용하여 서버에 대한 이미지를 스냅샷으로로 남기고 있었다. 이는 일반적인 기업수준 보다 높은 수준의 백업프로세스이며, 병위원급에 대한 실태조사 결과를 기반에서도 더 높은 수준이었다. 현재 의료정보시스템의 백업수준은 대체적으로 이보다 낮은 수준이 유지되고 있다. 이와 같은 백업시스템을 운영하고 있었으나 각각의 백업시스템은 APT공격에 의해서 무력화 되었다.

첫 번째 백업시스템인 Active Server와 Stand by server서버의 실시간 동기화는 Active Server가 암호화 진행되면서 함께 모든 파일이 암호화가 되어 데이터를 복구할 수 없었다. Active-Stand의 경우 고가용성을 유지하기 위한 백업체계이기 때문에 랜섬웨어를 예방할 수 있는 수단은 아니다.

두 번째 백업시스템인 백업스토리지의 경우에는 파일의 변경을 기록하기 때문에 랜섬웨어에 대한 복구 방법이 될 수 있고, 가장 많이 사용하는 방법이다. 랜섬웨어에 의해 원본파일이 암호화되면 암호화 이전에 백업한 파일로 복구할 경우 별도의 비용지불이나 복구절차 없이 백업파일로 복원이 가능하다. 하지만 이번 피해사례의 경우에는 공격자가 백업시스템의 권한을 획득하여 모든 백업파일을 삭제함으로 서, 백업스토리지에 의한 백업을 무력화 하였다.

세 번째 백업시스템인 CDP백업은 Contionuous Data Protection의 약자로 끊임 없이 변경되는 데이터를 연속적으로 백업하는 것을 의미한다. 변경에

대한 부분을 지속적으로 백업하고 언제든지 원하는 시점으로 복원을 할 수 있는 백업으로 랜섬웨어에 대한 피해가 발생해도 빠르게 복구가 가능하다. 하지만 공격자는 CDP백업을 사전에 인지하고 암호화 시점에 비정상적인 파일변경을 반복적으로 발생시켜 CDP백업에 다수의 백업파일을 생성시키고 결과적으로 CDP백업에 정상적인 파일은 하나도 남아있지 않도록 하여 해당 백업을 무력화 하였다.

사실 현실적으로 백업서버의 관리자 권한이 탈취당한 상태에서는 모든 복구시스템을 우회할 수 있다. 하지만 우리가 관심있게 봐야하는 것은 랜섬웨어가 APT와 결합되었을 경우 충분한 시간을 가지고 백업에 대한 구조 및 방법을 사전에 분석한 다는 것을 의미한다. 그 대상이 돈이 될 수 있는 시스템이라면 그 하나의 대상만을 위해서 공격자는 충분한 시간을 가지고 분석을 한다는 것이다.

과거의 랜섬웨어는 불특정 다수를 대상으로 했고 특정한 대상으로 한정했을 경우도 특정한 어플리케이션을 사용하거나 특정한 산업군으로 한정하여 공격을 하였다. 하지만 최근에는 APT와 결합되어 하나의 대상에 대하여 분석하고 공격을 실행함으로 서 해당 기업이 가진 모든 랜섬웨어에 대한 대비책을 무력화 하고 있다.

III. 의료산업에서의 대응 방안

전통적인 랜섬웨어에 대한 대응 방안은 크게 3가지 전략으로 나눌 수 있다. 첫째는 SW의 패치를 통해서 취약점을 제거하는 것이고, 두 번째는 백업을 통해 랜섬웨어에 감염되었다 하더라도, 빠른 복구를 통해 서비스를 정상화 하는 것이다. 마지막으로 세 번째는 안티바이러스 프로그램을 통해서 악성코드의 유입을 막는 방법이 일반적으로 사용되고 있었다. 하지만 앞서 2017년 상반기에 진화된 랜섬웨어의 유형을 보면 전통적인 방법으로는 더 이상 랜섬웨어를 효율적으로 차단할 수 없음을 알 수 있다. 특히 Wanna Cryptor와 Erebus Variants과 같은 유형은 의료시스템이라는 환경적 특성에 의해 매우 큰 피해가 발생할 수 있기 때문에 이에 대한 대비가 필요하다.

3.1 의료정보의 가치

미국에서 2017년 1~2월 사이에 Table 4와 같이 공공, 서비스, 교육, 의료 등 여러 영역에 걸쳐 다수의 랜섬웨어 피해 사례가 확인되었다. 가장 먼저 1월 10일에는 미국 LA 지역 대학에서 랜섬웨어에 대량 감염되는 사고가 발생했고, 20일에는 미국 세인트루이스

Field	Korea - Malcious Attack			Korea - System Glitch			Korea - Humman Factor		
	Labor	IR Cost	Loss	Labor	IR Cost	Loss	Labor	IR Cost	Loss
Healthcare	$46.58	$38.62	$73.85	$36.19	$30.01	$57.38	$34.71	$28.78	$55.03
Financial	$42.98	$35.64	$68.14	$33.40	$27.69	$52.95	$32.03	$26.56	$50.78
Constraints	$41.38	$34.31	$65.61	$32.16	$26.66	$50.98	$30.84	$25.57	$48.89
Transportation	$33.78	$28.01	$53.56	$26.25	$21.77	$41.62	$25.18	$20.87	$39.92
Communication	$29.99	$24.86	$47.54	$23.30	$19.32	$36.94	$22.35	$18.53	$35.43
Service	$26.79	$22.21	$42.47	$20.82	$17.26	$33.00	$19.96	$16.55	$31.65
Article	$25.79	$21.38	$40.88	$20.04	$16.61	$31.77	$19.22	$15.93	$30.47
Research	$24.99	$20.72	$39.62	$19.42	$16.10	$30.79	$18.62	$15.44	$29.52
Energy	$24.99	$20.72	$39.62	$19.42	$16.10	$30.79	$18.62	$15.44	$29.52
Tourism	$22.79	$18.89	$36.13	$17.71	$14.68	$28.08	$16.98	$14.08	$26.93
Consumer	$22.59	$18.73	$35.81	$17.55	$14.55	$27.83	$16.83	$13.96	$26.69
Education	$22.19	$18.40	$35.18	$17.24	$14.30	$27.34	$16.54	$13.71	$26.22
Media	$20.59	$17.07	$32.64	$16.00	$13.27	$25.37	$15.34	$12.72	$24.33
Industry	$20.59	$17.07	$32.64	$16.00	$13.27	$25.37	$15.34	$12.72	$24.33
Public service	$16.19	$13.43	$25.67	$12.58	$10.43	$19.95	$12.07	$10.00	$19.13
Retail	$15.59	$12.93	$24.72	$12.12	$10.05	$19.21	$11.62	$9.63	$18.42

Fig. 3. Labor and IR response costs for Korea's industrial sector and personal information leakage type, loss of company (5)

Table 4. List of attacks targeted for the first half of 2017

Date	Target
01.10	La Area University
01.18	Cancer-related Charities Foundation
01.20	SL Public Library
01.26	Texas Police Department
01.28	Austria hotels
01.30	Washington DC CCTV

지역 공공 도서관이 랜섬웨어에 감염[2]되어 도서 대여 및 출납 업무가 마비된 사례도 있었다. 이어서 26일에는 미국 텍사스주 콕렐힐시(市)에서 록키 랜섬웨어에 감염 피해가 발생하여 8년간의 수사 증거물들이 훼손되는 사고가 발생했다. 1월 30일에는 미국 워싱턴 DC에서의 HDD크립터(HDDCryptor) 감염으로 CCTV 시스템들이 작동하지 않은 사고가 있었는데, 미국 트럼프 대통령의 취임식이 있었던 시기와 겹쳐 큰 주목을 받았다. [3]

이들은 모두 랜섬웨어가 개인 PC의 데이터 손상을 넘어 공공 및 서비스 등의 마비를 초래한 대표적 사례로, 공공 영역으로 랜섬웨어 피해가 확대되었다는 점에 주목할 필요가 있다. [3]

사이버범죄 시장에서 의료 데이터의 가치는 Fig. 3과 같이 매우 높다. 신용카드는 신속하게 해지하거나 교체할 수 있지만 개인 의료 정보에는 이름, 연령, 성별, 주소, 주민등록번호, 진단 코드, 보험 정보, 개인 의료 내역 등이 포함되어 있는데 이 정보는 바꿀 수 없다. 도난 신용카드 가치의 10배에 달한다.

Fatboy 랜섬웨어는 고정 된 비용을 요구하지 않고 빅맥지수와 연동하여 감염지역의 생활수준에 따라 서로 다른 비트코인을 요구하고 있다. 이는 동일한 랜섬웨어에 감염 되었어도 암호화된 정보의 가치에 따라 다른 가격을 요구할 수 있으며, 이 경우 의료정보의 복호화 비용이 증가할 수 있음을 의미한다.

과거에 비해 의료산업에 대한 랜섬웨어 공격은 증가하고 있다. 의료정보의 가치가 고평가 되고 실제 랜섬웨어에 감염되었을 경우 비용을 지불해서 복구하는 사례가 증가함에 따라 공격자는 Table 5와 같이 의료산업을 대상으로 지속적으로 공격을 할 것이다.

Table 5. Hospital-targeted attacks

Date	Target
14.08	Korea University Hospital
16.02	Presbyterian Medical Center
17.05	England Hospitals 16EA
17.05	Korea Hospital
17.05	Taiwan Hospital

3.2 의료산업의 위험 분석

랜섬웨어에 대한 의료산업 위험이란 진화된 랜섬웨어가 의료시스템이 가지고 있는 취약점을 이용하여 의료서비스에 피해를 줄 수 있는 가능성을 의미한다. 랜섬웨어에 대한 위험을 분석하기 위해서는 대상이 될 수 있는 의료시스템을 식별하고 의료시스템이 가지고 있는 위협을 식별하여야 한다. 이를 기반으로 랜섬웨어의 유입경로를 사전에 예방하여야 한다.

3.2.1 자산과 위협

병의원은 처치에 필수적인 광범위한 자산을 보유하고 있고 따라서 이것들은 보호될 필요가 있다. 의료서비스에 필수적인 자산들은 Table 6. 과 같다.

전통적인 병원시스템은 스마트병원시스템으로 발전하고 있다. 스마트병원은 모든 의료시스템과 의료기기가 IoT기술과 결합하여 상호 통신을 진행한다. 더 정확하고 신속하게 의료정보를 교환할 수 있지만 과거에 비해 연결점이 많아지기 때문에 위협요소는 증가하게 된다. 특히 스마트의료기기의 경우 취약점이 발견되었을 경우 패치가 쉽지 않고 안티바이러스 프로그램을 사용할 수 없는 경우가 많기 때문에 특히 주의해야 한다. 따라서 기존과 같이 병원의 내/외부 경계단에서 보안을 해서는 효과적으로 악성코드 및 랜섬웨어의 유입을 효과적으로 차단할 수 없다. 의료시스템과 의료기기의 연결이 의료서비스의 품질을 향상시키고 있지만 공격자에게는 공격 가능한 포인트의 증가를 의미한다.

또한 수집되고 있는 의료정보가 방대해짐에 따라 데이터(연구 데이터, 데이터 로그 등), 모바일 클라이언트 서비스와 인식 시스템에 대한 정보의 가치가 중요해지고 있다. 모바일을 통한 의료정보제공이 늘어나면서 환자의 스마트기기를 통한 악성코드 유입의 가능성이 커지고 있고 이런 위협에 대한 추가적인 대응이 필요하다.

Table 6. Hospital medical system [6]

Category	medical system
Remote care system	• medical equipment for tele-monitoring and tele-diagnosis (e.g. measurements of blood pressure, heart rate, glucose measurements, ECG and other remote physiological measurements, threshold-triggered alarm generators etc.), such equipment may take the form of wearable or implantable devices etc.; • medical equipment for distribution of drugs (automated dosing equipment) or to administer treatment; • telehealth equipment, such as cameras, sensors and telephone/internet connections; telehealth computer system for patients to register their physiological measurements themselves (including patient-side application/software if applicable)
Identification systems	• system used to track and authenticate patients, staff or hospital equipment. • In smart hospitals, the biometric scanners do not only read the identification systems but are also intelligently networked with devices and information systems. • RFID systems with location services (software components) to assess and monitor relative movement of assets/patients/staff etc.; • CCTV (video surveillance) with recognition/authentication capabilities
Mobile Client devices	• devices intelligently integrated in smart hospitals to make the right information available at the right place at the right time and to facilitate mobility of staff and patients • Alarm and emergency communication applications for mobile devices.
Interconnected clinical information systems	• Laboratory information systems (LIS); • Radiology information systems (RIS); • Pharmacy information system (PIS); • Pathology information system; • Blood bank system; • Picture archiving and communication systems (PACS); • Research information system

의료시스템이 발전하기 전에는 대부분 해킹이 불가능하도록 문서화 되어 있거나 전산시스템으로 개발되어도 사실상 폐쇄망으로 구성되어 있었다. 현재는 Fig. 4와 같이 의료시스템이 인터넷망과 연결되어 있고 그

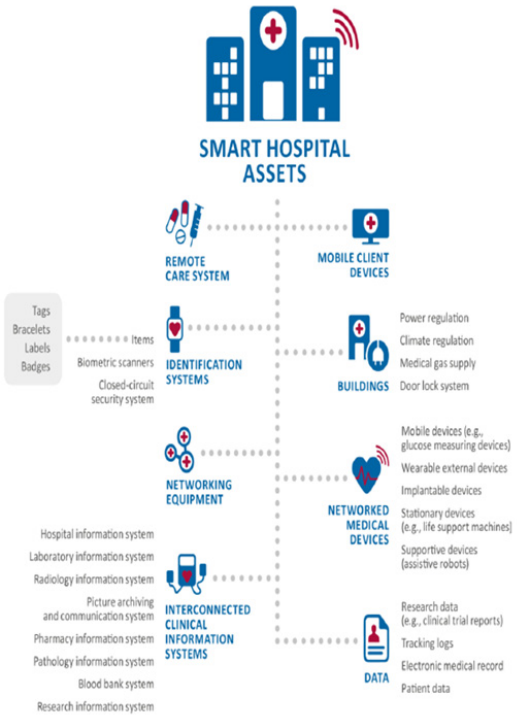

Fig. 4. Smart Hospital assets[6]

외 여러 연관시스템과도 함께 연결되고 상호작용을 하고 있다. 보안관점에서는 매우 포괄적으로 대응하여야 하고 공격자는 단순하게 가장 취약한 부분을 찾아서 공격을 시도할 것이다.

3.2.2 랜섬웨어 대응을 위한 조치

ISO27799는 의료정보분야에 특화된 ISMS 적용실무지침으로서 ISO/IEC 27002와 함께 적용을 하고 있는 국제 표준이다. 대부분 의료기관은 해당 표준을 기준으로 의료시스템을 보호하고 있다. 따라서 해당 표준을 기준으로 진화된 랜섬웨어에 대응할 수 있는 요소를 도출하여 기존의 의료정보보호 시스템을 유지/관리하면서도 랜섬웨어에 보다 효율적으로 대응할 수 있도록 하였다.

최근의 랜섬웨어의 진화하는 방향을 고려하면 Table 7과 같은 국제표준을 포함하여 아래의 내용에 대해서 깊은 고려가 필요하다.

Table 7. Responses related to controls of ISMS, ISO 27799[8][9]

control	responses
Mobile device policy	• establishing criteria for the minimum security measures in communication between mobile devices and health information system • disconnecting in case that the minimum security measures for mobile devices are not implemented
Teleworking	• establishing policies and processes for protection of health information systems in smart working environment using cloud computing and teleworking • possible of malware intrusion when security officer accessing to health information system via VPN at home
Information security awareness, education, and training	• education on latest Ransomware • information security awareness to prevent malware
Inventory of assets	• including version and type of OS and applications in asset inventory of health information system for prompt response to the newly identified vulnerability
Classification of information	• reviewing plans and processes of backup according to classification based on information value
Management of removable media	• establishing strict processes of removable media to prevent ransomware brought into the closed network
Access control policy	• establishing access control policy in communication of the closed network to prevent intruded ransomware from rapid spreading over the network
Management of privileged access rights	• managing privileged access right to prevent ransomware attacks combined with APT with administrators' IDs
Controls against malware	• establishing and reviewing controls of detection, prevention and recovery from ransomware attacks to health information systems
Backup	• implementing backup process to recover using backup data from ransomware attacks • taking account of disconnection of critical health information
Administrator and operator logs	• reviewing logs from APT viewpoint to detect ransomware combined with APT which is detectable by administrators' logs
Installation of software on operational systems	• establishing processes for patching as well as software installation
Segregation in networks	• identifying route of ransomware for health information system by checking perimeter of the segregated network between internal and public network
Response to information security incidents	• establishing specific incident response process to ransomware and implementing training in addition to general security incident training
Information security continuity	• establishing processes and measurements for providing healthcare services in case of service interruption by ransomware attack

데이터백업 : 랜섬웨어 공격자가 두려워하는 것은 방어기술이 아니라 데이터 백업기술이며, 백업을 하지 않았거나 백업을 했다 하더라도 그것을 사용할 수 없다면 공격자는 성공한 것이다. 공격자는 중요데이터를 백업했다는 것을 인지하고 있고, 해당 데이터를 파괴하기 위한 노력을 반드시 동반하고 있다. 데이터 백업은 몇 번을 강조해도 부족하지 않은 부분으로 의료시스템의 ID/PW와 백업시스템의 ID/PW를 동일하게 사용하지 말아야 한다. 또한 백업시스템은 점검 및 복구시점을 제외하고는 접근이 필요없기 때문에 별도의 접근제어를 실시하고 감사를 진행해야 한다. 현재 랜섬웨어에 대응하기 위한 백업기술들이 다양하게 나오고 있지만, 공격자 역시 백업기술을 분석하고 있기 때문에 가능하다면 백업시점을 제외하고는 네트워크 단절까지도 고려가 필요하다.

망분리, 네트워크 분리 : 중요시스템에 대한 망분리, 네트워크 분리의 필요성에 대해서는 많은 공감대가 형성되어 있다. 하지만 현실적으로 완전한 망분리를 구현할 수 없기 때문에 랜섬웨어가 유입될 수 있는 다양한 취약점이 발생할 수 있다. 크게 4가지 관점에서 관리가 필요하다. 첫째, 의료시스템망과 공용망간의 데이터 이동을 위해 불가피하게 발생하는 접점을 통해 랜섬웨어가 유입될 수 있다. 인터넷 망이 포함된 사용자 로컬 환경에서 가상화 서버로 접근하여 업무 환경을 이용할 수 있는 SBC 기반 망분리 환경에서 보안 점검을 진행한 경우, 공유폴더나 백도어를 이용해 파일 전송 제한을 우회하는 방식으로 랜섬웨어가 유입될 수 있다. 두 번째로 망간 자료 전송에 대한 예외 처리에 의해 랜섬웨어가 유입되거나 C&C통신을 발생시킬 수 있다. 세 번재로 호스트 컴퓨터에서 다수의 OS를 동시에 실행 및 관리하는 하이퍼바이저에 대한 보안 이슈도 주목해야 한다. 하이퍼바이저 기반의 서버 기반 가상화 환경 구축 시, 가상 환경의 메모리에 접근할 수 있는 수 있는 취약점을 이용할 수 있다. 마지막으로 망분리 환경을 우회하는 모든 위협에 대한 대응을 진행해야 한다. USB를 가지고 들어오거나 의료시스템망에 물리적으로 AP가 설치되거나 하는 등, 관리자가 인지하지 못하는 경로로 랜섬웨어가 유입될 수 있다.

패치관리 : 악성코드이슈에 대해서 OS 및 SW 패치는 항상 거론되고 있다. 하지만 의료정보시스템과 특수 시스템의 경우 패치관리가 잘 이뤄지지 않는 경우가 있고, 특히 스마트의료기기의 경우는 더더욱 패치가 어려운 상황이다. 망분리가 되어 있는 환경에서는 인터넷 망과의 연결이 어렵기 때문에 더더욱 패치가 어렵다. 망분리 환경이라 할지라도 랜섬웨어는 유입될 수 있기 때문에 모든 망의 시스템은 패치가 되어야 한다. 최근의 사고사례를 분석해 보면 패치관리시스템(PMS)을 통한 내부망에 악성코드 유입사례가 있다. 따라서 망별로 별도의 PMS구축이 권고된다. 스마트의료기기 및 웨어러블 의료기기는 계속해서 증가하고 있고 의료시스템과의 연결이 지속적으로 발생하고 있다. 이런 취약점에 의해 랜섬웨어가 의료시스템 내부로 유입될 수 있기 때문에 추가되고 있는 스마트의료기기 및 웨어러블 의료기기에 대한 패치 관리가 필요하다.

IV. 결 론

전통적인 랜섬웨어가 사회적으로 큰 이슈가 되던 시점부터 랜섬웨어에 대한 대응방법은 패치와 백업 이었다. 하지만 정부의 백업 지침서는 10년가량 업데이트가 이루어지지 않고 있다.[7] 악성코드에 대한 위협은 계속 증가하고 있고, 그 중 랜섬웨어에 대한 위협은 매우 급증하고 있다. 악성코드 대응 가이드로는 랜섬웨어의 진화속도를 따라가지 못하고 있는 것이다. 의료산업이 랜섬웨어 대응을 위한 조치를 진행하면 서비스형 랜섬웨어(RaaS)는 해당 부분을 분석하여 진화할 것이다. 표준이나 가이드에서 말하는 수준으로 대응해서는 빠르게 진화하는 랜섬웨어에 대응할 수 없으며, 지속적으로 랜섬웨어의 고도화 과정을 모니터링 하고 분석하여야 한다. 샌드박스를 이용한 악성코드의 행위분석 기술로 인하여 악성코드에 대한 분석능력이 증가하여 많은 위협을 예방하였다. 하지만 현재의 악성코드는 샌드박스를 우회하는 기술을 개발하여 진화하였으며, 실제로 무력화 시키고 있다. 기술의 발전에 따라 계속해서 새로운 위협을 식별하고 대응방안을 업데이트 하는 것이 매우 중요하다.

References

[1] wikipedia, EternalBlue, https://ko.wikipedia.org/wiki/EternalBlue

[2] Ahnlab, “Where is the target of ransomware?”, March 6, 2017, URL : http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=

26176 (Last visited : 2017. 11)
〔3〕 Ahnlab, ASECREPORT, Vol.87, 2017
〔4〕 Ahnlab, "〔vol.87〕 The second quarter of 2017 major security issues", URL : http://www.ahnlab.com/kr/site/securityinfo/asec/asecView.do?groupCode=VNI001&seq=26596 (Last visited : 2017. 11)
〔5〕 The Personal Information Protection Association, the value of personal information and social cost analysis according to personal information infringement, 2013
〔6〕 enisa, Smart Hospitals - Security and Resilience for Smart Health Service and infrastructures, 2016
〔7〕 Korea Information and Communication Technology Association, Guideline for Backup of Information Systems, 2007
〔8〕 ISO 27799:2016, Health informatics – Information security management in health using ISO/IEC 27002
〔9〕 ISO/IEC 27002:2013, Information technology - Security techniques – Code of practice for information security controls

〈저 자 소 개〉

전 인 석 (In-Seok Jeon) 종신회원
2009년 8월: 건국대학교 정보통신대학원 정보보호학과 석사
2014년 9월: 고려대학교 정보보호대학원 정보보호학과 박사 수료
2009년 9월~현재: Ahnlab CERT팀 선임 연구원
〈관심분야〉 네트워크보안, 정보보호관리체계, 정형기법, DevOps, 소프트웨어 보안 등

김 동 원 (Dong-Won Kim) 종신회원
2009년 2월: 서울과학기술대학교 컴퓨터공학과 졸업
2012년 2월: 건국대학교 정보통신대학원 정보보호학과 석사
2014년 2월: 고려대학교 정보보호대학원 정보보호학과 박사 수료
2012년 6월: 현대오토에버 정보보안기술팀 과장
2014년 3월: 서울호서전문학교 사이버해킹보안과 전임교수
2017년 1월~현재: 건양대학교 사이버보안공학과 조교수
〈관심분야〉 시큐어코딩, 정보보호, 모바일 보안, 지능형 차량 보안, SSCA, 정형기법 등

한 근 희 (Keun-Hee Han) 종신회원
서울과학기술대학교 컴퓨터공학과 졸업
한양대학교 공학대학원 공학석사
고려대학교 대학원 이학박사
전 고려대학교 정보보호대학원 산학교수
현재 건국대학교 소프트웨어학과 전임교수 정보통신대학원 정보보안학과장
〈관심분야〉 소프트웨어 보증, 시큐어 코딩, 정보보호관리체계(ISMS), 개인정보보호(PIMS), 클라우드 보안, 의료 보안, 제조 보안 등