커넥티드 의료기기 해킹 및 랜섬웨어 대응기술 동향

Security Technology Trends to Prevent Medical Device Hacking and Ransomware

권혁찬 (H.C. Kwon, hckwon@etri.re.kr) 네트워크·시스템보안연구실 책임연구원
정병호 (B.H. Chung, cbh@etri.re.kr) 네트워크·시스템보안연구실 책임연구원
문대성 (D.S. Moon, daesung@etri.re.kr) 네트워크·시스템보안연구실 책임연구원/실장
김익균 (I.K. Kim, ikkim21@etri.re.kr) 정보보호연구본부 책임연구원/본부장

ABSTRACT

Ransomware attacks, such as Conti, Ryuk, Petya, and Sodinokibi, that target medical institutions are increasing rapidly. In 2020, in the United States., ransomware attacks affected over 600 separate clinics, hospitals, and organizations, and more than 18 million patient records. The cost of these attacks is estimated to be almost $21 billion USD. The first death associated with a ransomware attack was reported in 2020 by the University Hospital of Düesseldorf in Germany. In the case of medical institutions, as introduced in the Medjack report issued by TrapX Labs, in many cases, attackers target medical devices that are relatively insecure and then penetrate deep into more critical network infrastructure, such as EMR servers. This paper introduces security vulnerabilities of hospital medical devices, considerations for ransomware response by medical institutions, and related technology trends.

KEYWORDS 비침습적 보안, 의료기관 랜섬웨어, 의료기기 보안, 커넥티드 의료기기 해킹

Ⅰ. 서론

최근 의료기기를 공격하기 위한 Ripple20, Urgent/11, NAT slipstreaming2.0 등 다양한 보안 취약점들이 지속적으로 보고되고, Conti, Sodinokibi, Ryuk, Petya 등 의료기관 대상의 랜섬웨어가 전 세계적으로 기승을 부리고 있다. Comparitech사에 의하면 미국의 경우 2020년 한 해 동안 랜섬웨어로 인해 600개 이상의 의료기관이 피해를 보았고, 1,800만 명 이상의 환자 기록이 영향을 받았으며, 그로 인한 피해액은 210억 달러에 이른다고 한다[1]. 작년(2020년) 7월에는 독일의 뒤셀드로프 병원에서 랜섬웨어로 인한 최초의 환자 사망사고가 발생하기도 했다.

* DOI: https://doi.org/10.22648/ETRI.2021.J.360503
* 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임[No.2020-0-00447, "안전한 의료·헬스케어 서비스를 위한 커넥티드 의료기기 해킹대응 핵심기술 개발"].

현재 전 세계적으로 랜섬웨어에 대응하기 위한 다양한 연구 및 솔루션들이 연구·개발되고 있으나, 가용성이 최우선되는 등의 의료기관의 특수성으로 기존 기술의 적용 및 대응에는 한계가 있다. 또한 의료전용 프로토콜(HL7, DICOM 등), 특수한 목적의 전용 네트워크(뉴매틱 튜브 시스템(PTS) 등) 등이 혼재되어 운용되는 특수한 환경도 고려가 필요하다.

현재, 국내 상급병원의 경우 평균 약 8천~3만여 개의 의료기기가 운영 중이다. 의료기관의 보안 관점에서 의료기기가 특히 중요한 이유는 의료기기 자체의 데이터 유출, 오작동의 위협뿐만 아니라 장악한 의료기기를 통해 병원 내부 깊은 서버군까지 침투가 가능하기 때문이다. 실제로 의료기관의 경우 많은 공격이 상대적으로 보안에 취약한 의료기기를 공격한 후, EMR 서버 등 병원 깊숙한 곳까지 침투하는 공격을 하여 성공을 거두고 있다.

본고에서는 의료기관의 커넥티드 의료기기 해킹 및 랜섬웨어 대응 기술 동향에 대해 살펴본다. Ⅱ장에서는 보안 관점에서의 의료기기의 특수성, 보안 취약성 및 의료기관 대상의 랜섬웨어 특성 등을 살펴보고, Ⅲ장에서 이에 대응하기 위한 국내외 기술 동향을 소개한다.

Ⅱ. 의료기기 해킹 및 랜섬웨어 현황

1. 의료기기 보안 취약성

현재 상급종합병원의 경우 기관별 차이가 있지만 보통 8천~3만여 개의 의료기기가 설치 및 운용 중이고, 그 기기 대다수는 네트워크에 연결되어 서비스되고 있다. 그림 1은 병원의 커넥티드 의료기기가 보안에 취약할 수밖에 없는 요인들을 보여준다.

병원에 설치된 의료기기 중 상당수는 제작된 지 10년이 넘은 고가의 장비로 구형 운영체제가 탑재

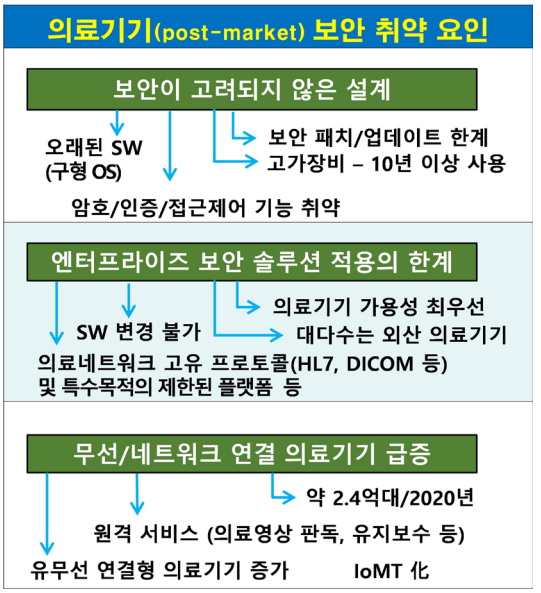


그림 1 의료기기 보안 취약 요인

된 경우가 많다. 또한 사람의 생명, 건강이 직결된 의료기기의 특성상 고가용성이 요구되기 때문에 운영체제/소프트웨어의 패치/업데이트, 백신 등 보안 모듈의 추가 설치 등이 자유롭지 않은 것도 문제이다. 상급병원의 경우 제조사, 모델, 제조일이 모두 다른 1만여 개 이상의 의료기기/장비에서 취약점을 찾기도 매우 어려운 일이다. 또한 유무선 네트워크에 연결된 의료기기가 증가하면서 그 위협도 계속 확대되는 추세이다[2].

그림 2는 의료기기의 보안 취약성을 보여준다. PC, 모바일 단말, IoT 기기 등에 존재하는 보안 위

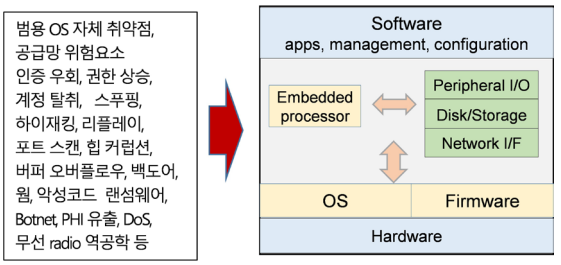


그림 2 의료기기 보안 취약성

표 1 의료기관 랜섬웨어에 활용되는 주요 exploit

exploit, vulnerability	주요 특징
RDP exploit (Bluekeep)	• MS windows의 원격데스크톱 프로토콜(RDP: Remote Desktop protocol) 취약점 • 원격에서 memory corruption bug, UAF 등 발생, 상승 권한으로 원격코드 실행 • 현재 다수의 랜섬웨어에서 활용 • 관련 CVE: CVE–2019–0708 (지속적으로 취약점 업데이트, 수십 년간 지속된 공격)
SMB exploit (EternalBlue)	• MS SMB(Server Messaging Block) 취약점 • 조작된 패킷으로 memory corruption 발생, 인증 우회하여 원격코드 실행 가능, SMB 서버의 직접 공격도 가능 (RCE 취약점 악용) • 2017년 wannacry 랜섬웨어에서 백도어 설치도구인 doublepulsar와 함께 활용, 현재 다수의 랜섬웨어에서 활용 • 관련 CVE: CVE–2020–1206, 1301, CVE–2021–0796
Ripple20 vulnerability	• Trek사의 TCP/IP 소프트 라이브러리 보안 취약점 • 의료장비(약물주입펌프 등), 산업제어시스템 등 다양한 IoT 장비 대상의 공격 가능 • DNS 캐시 포이즈닝, 네트워크 경계 패킷 응답 등을 통한 공격으로, 악성코드 은닉, 원격 하이재킹, 원격 코드실행, NAT 우회, 중간자 공격 등이 가능 • 관련된 9개의 CVE: CVE–2020–11901, 11896, 11897 등
Urgent/11 vulnerability	• VxWorks RTOS의 TCP/IP(IPnet) 관련 취약점 • VxWorks는 의료장비(MRI, PMS 등), 기계제어, 항공 우주 등 20억 개 이상의 장치에서 사용되는 실시간 운영체제 • NAT/방화벽 우회, 원격 장치제어, 멀웨어 전파 등 가능하며, 방화벽 등의 보안장비도 VxWorks를 사용하는 경우 공격 가능 • 관련된 11개의 CVE: CVE–2019–12256, 12257, 12260~3 등
NAT slipstreaming2.0	• 방화벽이나 NAT를 우회하여 내부의 장치를 노출 및 원격 접속 가능 • NAT의 ALG(Application level gateway)를 속여 내부 접속을 위한 pinhole을 만듦 • 관련 CVE: CVE–2020–16043, CVE–2021–23961, 1799
PwndPiper vulnerability	• 병원의 의약품, 혈액 샘플 등을 전송하는 뉴매틱 튜브 네트워크(PTS)의 제어판에 대한 취약점(정확히는 Swisslog healthcare의 translogic PTS 시스템에서 발견) • 인증우회, 메모리 변형을 통한 원격코드 실행, 권한 상승 등을 통한 PTS 통제력 획득 • 관련 CVE: CVE–2021–37163, 37160~4, 37166~7
기타	• CVE–2019–19781: Citrix Application Delivery Controller • CVE–2019–11510 Pulse Connect Secure • CVE–2018–8453: Windows Win32k components • CVE 2012–0158: Microsoft Office Common Controls 등 다수

협이 의료기기에도 동일하게 적용되며, 그림 1의 의료기기 보안 취약 요인까지 가미되면서 보안 위협은 더욱 확대되는 상황이다[3].

실제로 의료기관의 경우 많은 공격이 상대적으로 보안에 취약한 의료기기를 공격한 후, EMR 서버 등 병원 깊숙한 곳까지 침투하는 공격이 성공하고 있다. TrapX사의 Medjack 보고서에서도 최초 MRI 장비의 감염을 시작으로 점차 내부 클라이언트 단말 그리고 결국 PACS 서버까지 침투한 탐지 사례가 소개되기도 하였다[4].

2. 의료기관 랜섬웨어 개요

의료기관을 공격하는 랜섬웨어는 일반 랜섬웨어와 동작 과정은 유사하다. 단, 의료기관의 특성에 따른 일부 차별화된 공격 특성을 갖기도 한다. 이를테면 상대적으로 보안이 취약한 의료기기를 점유해 병원 내부 침투, 구형 OS/SW 탑재 의료기기 공격을 위한 오래된 취약점 · exploit 활용, 구형 OS 탑재 저사양 의료기기 선별 공격, 병원 전용 네트워크 프로토콜(HL7, DICOM 등) 및 PTS 등의 특수 네트워크의 특성/취약점을 이용한 공격[5] 등이

있다.

랜섬웨어 동작을 위한 주요 단계는 크게 다음의 세 단계로 구분할 수 있다.

1) 단말에 침투하여 권한을 획득하는 단계(exploit)
2) 랜섬웨어 동작 단계(ransomware)
3) 랜섬웨어 확산 단계(spreading)

가. 단말침투 및 권한상승 단계(Exploit)

랜섬웨어 공격을 위한 첫 번째 단계는 exploit 단계이다. exploit 공격은 단말의 보안 취약점 또는 소프트웨어/하드웨어 버그 등을 이용한 공격을 말하며, 이를 통해 단말에 침투하여 권한을 획득하는 과정을 말한다. 의료기관 랜섬웨어 공격을 위해 주로 사용되는 보안 취약점 및 exploit들은 표 1에 소개되어 있다.

현재 랜섬웨어 공격에서 가장 많이 사용하는 exploit은 MS windows 시스템 대상의 RDP와 SMB 취약점을 이용하는 방식이다. RDP 프로토콜의 경우 특정 virtual channel을 생성하여 바인딩하는 과정에서 heap corruption을 발생하여 공격자의 코드가 타겟 기기에서 시스템 레벨에서 실행이 가능하게 되는 취약점이 존재한다.

Urgent/11 취약점이 존재하는 VxWorks 같은 경우, 의료기관의 일부 MRI 장치, 환자 감시장치 등에 사용되고 있어 실제적인 위협이 되고 있다. 최근 Armis사는 Urgent/11 취약점을 이용하여 Spacelabs사의 Xpression 환자 감시장치를 해킹한 시연 영상을 공개하기도 하였다[6].

NAT slipstreaming2.0의 경우 방화벽이나 NAT로 보호되고 있는 의료기기의 정보(IP 등)를 노출하고, 해당 의료기기로의 임의 접근을 가능하게 ALG를 속이는 방식으로 역시 의료기관에 위협이 된다[7].

표 1 외에도 다양한 취약점, exploit들이 공개되고 있으며, 특히 알려지지 않은 제로데이 exploit 공격들도 지속적으로 등장하고 있어 대응이 쉽지 않은 상황이다.

나. 랜섬웨어 동작 단계(Ransomware)

기기에 침투하여 권한을 획득한 이후의 랜섬웨어의 동작 과정은 그 종류에 따라 매우 다양하다. 일반적인 동작과정을 하나의 사례로 소개하면 다음과 같다.

먼저 침투한 기기에 dropper가 설치되고, 기기의 시스템과 네트워크 환경을 분석하여 이 기기를 랜섬웨어 공격 대상으로 할 것인지 단순히 경로로만 활용할 것인지를 결정한다. 랜섬웨어 공격 대상이라면, C&C 서버로 접속하여 랜섬웨어 소프트웨어 도구를 다운로드한다. 암호화를 위한 키를 생성하고 파일을 암호화한다. 추후 파일 복구를 위한 정보 또는 복구를 위한 키를 C&C 서버로 전달한다. 또는 복구를 위한 키 생성을 위한 일부 정보를 시스템에 은닉하기도 한다. 백도어를 설치하고, 공격의 흔적들을(log, cache, shadow 파일 등) 모두 삭제하고, 랜섬노트를 생성하여 남긴 후 사라진다.

랜섬웨어 공격자에게 가장 중요한 부분은 흔적을 남기지 않고 추적이 불가능하게 하는 점일 것이다. 따라서 C&C 서버와의 통신, 몸값을 받고, 복구 도구를 전송하는 등의 과정에서 추적이 불가능한 토르(Tor) 네트워크를 사용하기도 한다. 또한 암호화 과정에서의 탐지를 피하기 위해 파일은 비교적 속도가 빠른 대칭키로 암호화하고, 파일 암호화에 사용된 키는 공개키로 암호화하기도 한다. 또한 암호과정의 속도를 빠르게 하기 위해 최근에는 라운드가 적은 경량의 암호화를 사용하기도 한다.

다. 랜섬웨어 확산 단계(Spreading)

목적 기기까지 도달하기 위해서나 랜섬웨어의

확산을 위한 단계로 보통 Emotet, Trickbot, Powerghost 등의 다양한 멀웨어가 사용된다.

Ⅲ. 대응 기술 동향

1. 주요 기술 동향 및 솔루션

이 절에서는 디바이스 레벨 및 네트워크 레벨에서의 랜섬웨어 탐지 및 대응 기술을 소개하고 각각에 대한 의료기기 및 의료기관 적용 가능성 등을 살펴본다.

가. 디바이스 단에서의 대응 기술

디바이스 레벨에서 랜섬웨어 탐지를 위한 시그니처, 행위 기반의 기술이 많이 연구되고 있다. 그림 3은 디바이스 단에서 시그니처 및 행위 기반 랜섬웨어 탐지를 위해 고려되는 주요 피처들을 소개한다. 주로 Ⅱ장에서 소개된 랜섬웨어 동작 단계에서의 탐지를 위해 활용되는 피처들이다.

기기에서 암호화를 위한 준비과정, 암호화 과정에서 발생하는 프로세스 호출, 파일 I/O, Import/export 패턴, code crc 등을 분석하여 랜섬웨어의 동작을 탐지한다. 일반적으로 랜섬웨어의 동작 특성을 시그니처화할 수도 있고, 디바이스의 정상 동작을 학습 후 정상에서 벗어나는 패턴을 탐지하여 분석하는 방법도 가능하다.

랜섬웨어 탐지를 위한 주요 feature (단말)	
Process, File I/O file difference magic bytes file removed file extension canary files	Entropy Directory Frequency functions cryptographic primitives decoy 등

그림 3 시그니처/행위 기반 랜섬웨어 탐지를 위해 고려되는 주요 feature들(디바이스)

랜섬웨어 자체가 단말에서 동작하기 때문에 디바이스 레벨에서의 대응 방식이 효과적이기는 하지만 알려지지 않은 공격, 수많은 랜섬웨어 및 변종, 다양한 우회/회피 공격 탐지에 한계도 존재한다. 예를 들어 magic bytes를 피해서 암호화하는 랜섬웨어도 있으며, MBR 자체를 암호화하는 petya 같은 경우는 표 1의 상당수의 피처로 탐지가 어렵다.

무엇보다 디바이스 단에서의 대응은 의료기기에 적용이 매우 어렵다는 문제가 있다. Ⅱ장 1절에서 언급한 것처럼 고가용성이 요구되는 의료기기 자체에 anti-virus 등 보안 모듈 설치가 매우 제한적이기 때문이다.

나. 네트워크 단에서의 대응 기술

Ⅱ장 2절에 소개된 랜섬웨어 동작을 위한 3가지 단계를 기준으로 할 때 단말에서의 대응은 두 번째 단계(랜섬웨어 동작단계)에서, 네트워크 단에서의 대응은 첫 번째(exploit)와 세 번째(확산) 단계에서의 대응으로 볼 수 있다.

그림 4는 네트워크 단에서 랜섬웨어 탐지를 위해 고려되는 주요 피처들을 소개한다. 주로 네트워크 패킷에 대한 파일 해시를 검사하거나, C&C 서버 등 악성 IP/DNS 정보, exploit을 위한 포트 정보 등을 모니터링하여 위협을 탐지한다. 일반적으로 Snort나 Suricata 같은 open IDS 도구들과 다양한 랜

랜섬웨어 탐지를 위한 주요 feature (네트워크)	
DNS C&C Packet hash Port DGA	IP/URL/Domain ASN GeoIP SMB traffic RDP traffic 등

그림 4 랜섬웨어 탐지를 위해 고려되는 주요 feature들(네트워크)

섬웨어에 탐지를 위한 룰셋(시그니처) 등을 활용하여 탐지를 수행하게 된다.

알려진 랜섬웨어라면 시그니처 기반의 방식이 효과적으로 탐지가 가능하지만, 시그니처 방식의 탐지는 디바이스단 대응과 마찬가지로 알려지지 않은 공격, 수많은 랜섬웨어 변종, 우회/회피 공격에 매우 취약하다. 1년에 신규로 등장하는 랜섬웨어만 해도 거의 수백만 종에 달한다. Wannacry 랜섬웨어의 변종만도 400여 개이다.

예를 들어 C&C 서버의 경우 어떤 랜섬웨어는 C&C 서버에 접속 자체를 안 하는 경우가 있고, 또한 DGA를 사용하는 경우 서버의 도메인 네임이 계속 바뀌기도 하며, 토르 네트워크를 이용하는 경우는 아예 탐지·추적이 불가능하다.

따라서 최근에는 시그니처 기반 탐지를 보완하기 위해 AI 기반의 네트워크 행위를 분석하여 이상행위 및 위협을 탐지하는 연구가 매우 활발하게 진행되고 있다.

또한 네트워크 침입을 차단하고 랜섬웨어의 확산을 방지하기 위해 망분리, 망연계, 네트워크 세그멘테이션·가상화 등의 다양한 솔루션도 적용되고 있다.

다. 해외 솔루션 현황

의료기관 랜섬웨어 대응을 위한 대표적인 해외 솔루션으로 Zingbox(Paloalto networks), Armis, Medigate 등의 솔루션이 있다. Zingbox는 2019년 Paloalto Networks에 인수되어 현재는 Paloalto Networks의 자회사로 존재한다.

해외 솔루션들의 주요 특징은 거의 유사하다. 모두 의료기기가 아닌 네트워크 레벨에서의 탐지방식을 적용한다. 기본적으로 의료기기가 연결된 네트워크의 메타 데이터를 클라우드로 전송하고, 클라우드에서 딥러닝 분석 등을 통해 의료기기의 이상행위를 탐지한 후 이상행위의 원인을 보안분석가의 2차 분석을 통해 찾아내는 방식이다. 해외 솔루션들의 위협 탐지 구조는 그림 5와 같다. Paloalto Networks나 Armis의 경우는 스위치 장비를 미러링하여 데이터를 추출하며(그림 5의 (1))[8], Medigate는 인라인 형태의 패킷 수집 장치를 사용하여 병원 서버군 앞단에서 수집하는 엔터프라이즈 레벨, 각각의 의료기기 앞단에서 수집하는 의료기기 레벨 등으로 적용이 가능하다(그림 5의 (2-4))[9].

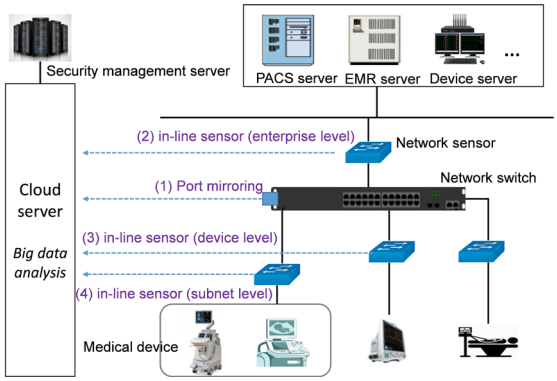


그림 5 해외 솔루션들의 일반적인 구조

현재 상기의 해외 솔루션들이 국내 병원에 적용된 사례는 아직 없는 것으로 파악된다. 국내 상황상 의료기관의 민감한 정보를 외부 클라우드로 보내 분석하는 방식에 대한 이슈와 현재까지 솔루션 자체가 충분히 검증되지 않았다는 점도 그 요인이 될 것으로 예상된다. 최근까지도 미국 등 선진국에서도 의료기관 랜섬웨어 피해가 급증하는 등 아직까지는 충분한 기술적 대책이 마련되었다고 보기는 어려울 것 같다.

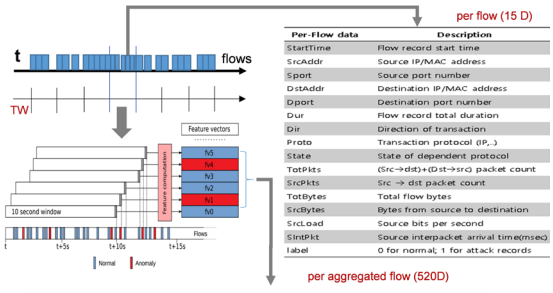
2. 국내외 연구 사례

본고에서 반복적으로 언급되었듯이 의료기기 해킹 및 랜섬웨어 대응은 단말이 아닌 네트워크 단

에서 exploit, spreading 단계에서 의료기기의 이상행위를 비침습적으로 분석·탐지하는 것이 현실적이다. 관련 연구가 국내외로 일부 진행되고 있다. 본 절에서는 그 중 몇 가지 연구 사례를 소개한다.

가. OpenICE 기반 랜섬웨어 탐지 기술 (Murcia, Pennsylvania 대학)

Murcia 대학, Pennsylvania 대학, Waterford Institute of Technology에서는 의료기기 네트워크 환경에서 정상 및 4종의 랜섬웨어(petya, wannacry, badrabbit, powerghost)에 대한 랜섬웨어 탐지 기술을 제안하였다[10]. 본 기술에서 의료기기 네트워크 데이터셋은 OpenICE[11] 및 의료기기 시뮬레이터 기반의 시험 환경을 구축하여 기기에 랜섬웨어를 임의로



Per-Flow data	Description
StartTime	Flow record start time
SrcAddr	Source IP/MAC address
Sport	Source port number
DstAddr	Destination IP/MAC address
Dport	Destination port number
Dur	Flow record total duration
Dir	Direction of transaction
Proto	Transaction protocol (IP,)
State	State of dependent protocol
TotPkts	(Src→dst)+(Dst→src) packet count
SrcPkts	Src → dst packet count
TotBytes	Total flow bytes
SrcBytes	Bytes from source to destination
SrcLoad	Source bits per second
SIntPkt	Source interpacket arrival time(msec)
label	0 for normal, 1 for attack records

Feature Attributes	Aggregated Flow Features
TCP/UDP(416) (internal/incoming, internal/outgoing, external/incoming, external/outgoing)	Number of flows(8), % of flows (8)
	Mean and stddev of flow duration (16) mean and stddev of time two consecutive flows(16)
	Number of different destination IPs(8) Entropy of Destination IPs(8)
	Sum, min, max, mean, stddev, median of total packets(48), * of source packets(48)
	* of total bytes (48), * of source bytes (48), * of total loads (48)* of source loads (48)
	% of source/destination ports>1024 (16) % of source/destination ports<1025 (16)
	Number of different source and destination ports(16) Entropy of source and destination ports(16)
TCP/UDP(74) (directions)	Number of flows(2)
	Sum, min, max, mean, stddev, median of total packets(12), * of source packets(12)
	* of total bytes (12), * of source bytes (12), * of total loads (12)* of source loads (12)
ARP(8)	Number of flows(1)
	Mean and stddev of flow duration (2) mean and stddev of time two consecutive flows(2)
	Number of different destination IPs(1) Entropy of destination IP(1) Median of the duration(1)
Last flow(22)	Protocol used(TCP, UDP, ARP)(3) State(INT, RST, FIN, CON)(4)
	Source/destination port<1024(2) Destination port(1)
	Direction(incoming, outgoing, internal, external)(4)
	Total pkts, source pkts, total bytes, load, source load, source mean interpkt arrival time, destination mean interpkt arrival time(8)

출처 Reproduced with permission from [9], CC-BY.

그림 6 OpenICE 기반 랜섬웨어 탐지를 위한 피처 추출 방법 및 구성

감염시켜 데이터를 확보하였다. 네트워크 플로우 데이터 추출은 OpenArgus를 활용하였다.

본 기술에서는 단일 플로우 기반으로 16개의 피처를 추출하고, Time window상에서 취합된 플로우의 집합에서 다시 520차원의 피처를 생성하여 학습데이터로 활용하였다. 그림 6은 AI 분석을 위한 네트워크 플로우 피처 정보 및 추출 방법을 보여준다.

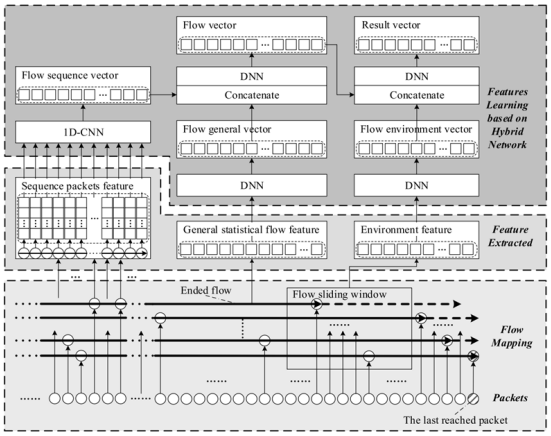
520차원의 피처를 기반으로 이상행위 탐지는 OC-SVM(1-class SVM), 랜섬웨어 분류는 naive bayes를 이용하여 학습하였다. 본고에서 OC-SVM의 이상행위 탐지 성능은 F1-Score 0.9596이 나왔다(precision 0.93232, Recall 0.9997, FPR 0.046). Naive bayes를 이용한 랜섬웨어 분류 성공률은 Time window를 20초, threshold를 0.0005로 한 경우 petya 0.9872, badrabbit 0.9622, wannacry 1.0, powerghost 0.9875로 좋은 성능을 보였으나, time window 사이즈, threshold 값에 따라 각각의 랜섬웨어에 대한 탐지율 변동폭이 크다는 단점이 있다.

나. Multi-type flow feature 기반 네트워크 이상행위 탐지

Zhengzhou Science and Technology Institute에서는 multi-type flow feature 분석 기반 네트워크 이상징후 탐지 기술을 제안하였다[12]. 본 연구는 의료기기 네트워크를 대상으로 한 것은 아니지만, 네트워크의 다양한 이상행위를 분석하는 기술로 의료기관 랜섬웨어 대응에도 적용이 가능한 기술이다.

본 연구에서 고려한 multi-type flow feature는 각각 다음과 같다. 다중 피처의 생성 및 분석 과정은 그림 7과 같다.

- SPF(Sequence packet feature)
- GSF(General statistical feature)
- ENF(Environmental feature)



출처 Reprinted with permission from [11], CC-BY 4.0.

그림 7 multi-type flow feature 생성 및 분석과정

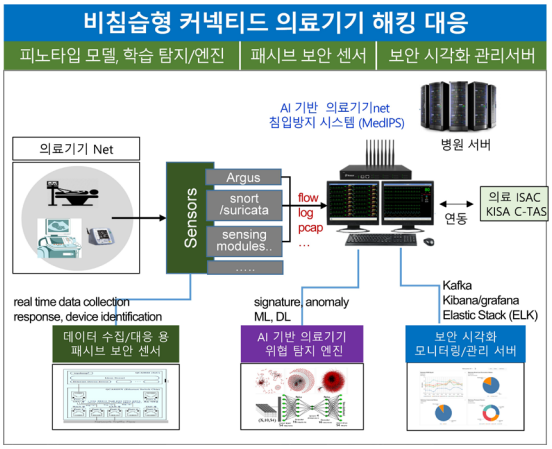


그림 8 비침습형 커넥티드 의료기기 해킹 대응 서비스 개념도 (ETRI)

그림 7 아래쪽에 있는 동그라미는 패킷, 굵은 화살표는 플로우를 표현한 것이다. 각 패킷은 모아져서 sequence packet feature(SPF)를 구성한다. Sequence packet feature는 2차원 텐서로 구성이 되는데, 예를 들어 SPFi.Sm(n)의 경우, Flow i에 대한 SPF이며 n번째 packet의 m번째 feature가 된다.

특정 flow가 종료되는 경우, 그 flow의 통계적 특성 피처를 계산하여 General statistical flow feature(GSF)를 생성한다. 또한 Sliding window 단위로 윈도우에 속하는 flow들에 대한 환경적 피처를 계산하여 Environmental feature(ENF)를 생성한다. Sliding window는 각 flow 종료 시점 전후 +/− a 시간으로 설정된다. 이렇게 생성한 multi-type 피처셋의 분석은 1D-CNN과 DNN으로 구성된 하이브리드 뉴럴 네트워크를 통해 학습/분석 및 퓨전되어 활용된다. 본 연구에서 활용한 실험 데이터셋은 ISCX-IDS-2012와 CIC-IDS-2017을 활용하였다.

다. ETRI

ETRI는 공동연구기관인 건국대학교병원, (주)휴네시온, 스마트의료보안포럼과 함께 의료기기 피노타입 기반 비침습적 해킹 대응을 위한 기술을 개발하고 있다(2020.4~2023.12, 과학기술정보통신부).

기술의 서비스 개념도는 그림 8과 같다. 본 기술은 (1) 의료기기 자동식별 및 의료네트워크 실시간 데이터 수집·대응을 위한 패시브 보안 센서, (2) AI 기반 의료기기 이상징후 학습·분석·탐지 및 원인분석을 수행하는 위협 탐지 엔진, (3) 의료기기·네트워크 보안 시각화 및 관리 기능을 제공하는 보안관리 서버로 구성되며, 연구용 데이터는 건국대학교병원의 실데이터셋을 활용한다.

본 기술은 시그니처 및 행위분석 기반의 탐지 기술을 혼합 적용하며, 의료기기 이상행위 탐지를 위해 다음의 관점에서 의료기기 네트워크의 행위를 특성화·피처화하여 학습·분석한다.

- Periodicity(주기성): flow에 대한 duration, periodicity, size, time difference 등의 특성
- Familarity(친숙성): IP, port, protocol, src/dst 등의 조합을 벡터화하여 학습·분석된 현 네트워크에서의 행위 친숙도

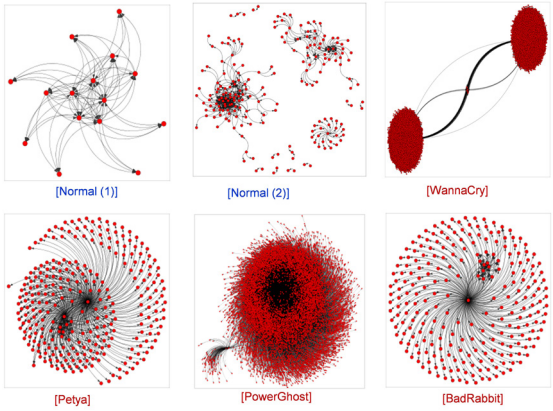


그림 9 의료기기 랜섬웨어 감염에 따른 의료 네트워크 행위 시각화

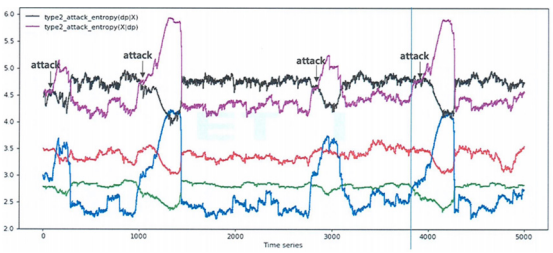


그림 10 공격발생에 따른 엔트로피 변화 추이

- Entropy(엔트로피): src(dst) address(port), flow duration, packets/bytes, in(out) degree, conditional entropy 등 다양한 네트워크 엔트로피 변화량
- 기타 network flow의 통계적·환경적 특성

그림 9는 앞서 살펴본 특성화된 피처를 기반으로 분석한 일부 랜섬웨어 공격 시의 네트워크 행위적 특성을 보여주며, 그림 10은 랜섬웨어 공격(exploit, spreading) 발생에 따른 네트워크 엔트로피의 변화를 보여준다. 공격이 발생한 시점에서 entropy의 이상변화를 관찰할 수 있다.

본 기술은 전체 탐지된 네트워크와 의료기기의 이상행위 원인을 분석하여 시각적으로 보여주는 ELK(Elasticsearch, Logstash, Kibana) 기반의 시각화 대시보드도 함께 제공되며, 데이터베이스는 Redis in-memory DB를 활용한다.

본 기술개발의 결과물은 상급병원 대상의 실증까지 진행할 예정이며, 의료 ISAC(의료기관 공동보안관제센터) 및 KISA의 C-TAS(사이버 위협정보 분석·공유 시스템)와 연동되는 형태의 상용수준의 솔루션이 될 것이다.

라. 기타

의료기관에 특화된 기술은 아니지만, IoT 등 기기 대상으로 비침습적 해킹 대응을 위한 연구도 활발히 진행되고 있다. 참고문헌 [13]에서는 네트워크 엔트로피 기반의 이상징후를 탐지하는 기법을 제안하였고, 참고문헌 [14]에서는 네트워크의 통신 패턴을 2차원 행렬로 이미지화하고, GLCM texture의 피처를 분석하여 이상징후를 탐지하는 기법을 제안하였다. 참고문헌 [15]에서는 디바이스의 CPU 전력 소비 패턴을 분석하여 크립토 랜섬웨어를 탐지하는 기술을 소개하였다. 참고문헌 [16]에서는 네트워크 플로우 기반이 아닌 패킷 레벨에서의 악성 트래픽을 탐지하는 기법을 제안하였다. Word embedding을 통해 패킷의 의미를 추출하고 패킷 헤더의 필드 간의 시간적 관계를 학습하기 위해 LSTM을 사용하였다.

Ⅳ. 결론

점점 정교화·고도화되어가는 랜섬웨어 공격으로 의료기관의 피해가 급증하고 있다. 본고에서는 의료기관의 커넥티드 의료기기 보안 취약성, 의료기관 랜섬웨어 현황 및 대응기술 동향에 대해 살펴보았다. 현재 관련 솔루션은 Armis, Medigate, CyberMDX, Paloalto networks(Zingbox) 등의 해외기

관이 선도하고 있으며, 국내에서 관련 핵심기술 및 솔루션 확보가 시급한 상황이다. 기존 해외 솔루션은 의료기관의 민감한 정보를 외부 클라우드로 보내 분석하는 방식으로, 국내 현실에 맞게 의료기관 적용성을 높이기 위해서는 의료기관 내부에서 분석·탐지·대응이 가능한 보다 경량화된 솔루션이 필요할 것으로 예상된다.

의료기기 보안은 개발 단계에서 보안을 내재화하는 전략과, 기존에 설치되어 운용되고 있는 보안에 취약한 의료기기로 인한 위협 대응 등 전사적인 접근이 필요하다[17,18]. 다행히, 미국 FDA의 사이버보안 규제강화, 강화된 유럽의 MDR 등 의료기기 인허가를 위한 보안 요구사항 및 규제가 강화되면서 신규 개발되는 의료기기의 보안 기능은 점차 강화되는 추세이다.

원격의료, 개인 맞춤형 건강관리 등 의료·헬스케어 서비스가 확대되면서 의료기기가 IoT화되는 IoMT 환경이 도래하면, 좀 더 다양한 보안 이슈가 등장할 것으로 예상된다. 의료보안은 국민의 건강·생명에 직결되는 분야로 신기술 조기 확보를 위한 선제적인 접근이 필요할 것으로 사료된다.

용어해설

Exploit 기기의 소프트웨어나 하드웨어의 보안 취약점, 버그 등 설계상 결함을 찾아내어 공격자의 의도된 동작을 수행하도록 하는 취약점 공격

약어 정리

ALG	Application Level Gateway
ASN	Autonomous System Number
CNN	Convolutional Neural Network
CVE	Common Vulnerabilities and Exposures
DGA	Domain Generation Algorithm
DICOM	Digital Imaging and Communications in Medicine
DNN	Deep Neural Network
ELK	Elasticsearch, Logstash, Kibana
EMR	Electronical Medical Records
FDA	(US) Food and Drug Administration
GLCM	Gray-Level Co-occurrence Matrix
HL7	Health Level Seven
IoMT	Internet of Medical Thing
LSTM	Long Short-Term Memory
MBR	Master Boot Record
MDR	Medical Device Regulation
MRI	Magnetic Resonance Imaging
NAT	Network Address Translation
PACS	Picture Archiving and Communication System
PTS	Pneumatic Tube System
RCE	Remote Code Execution
RDP	Remote Desktop Protocol
SMB	Server Message Block
SVM	Support Vector Machine
UAF	Use After Free

참고문헌

[1] Comparitech, "Ransomware attacks on US healthcare organizations cost $20.8bn in 2020," Mar. 2021, https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

[2] 권혁찬, "의료사물인터넷(IoMT) 보안 기술 및 동향," ICT Convergence Korea 2021, 2021. 3.

[3] 권혁찬 외, "커넥티드 의료기기 보안 동향 및 이슈," 주간기술동향, 제1911호, 2019. 8.

[4] A. James and M.B. Simon, "MEDJACK.3—Medical device hijack cyber attack evolve," in Proc. RSA Conf. (San Francisco, CA, USA), Feb. 2017.

[5] Armis, "URGENT/11—Takeover of a Spacelabs Xprezzon patient monitor," 2019, https://www.youtube.com/watch?v=tpSXr4XhQwM

[6] Armis, “NAT slipstreaming v2.0,” https://www.armis.com/research/nat-slipstreaming-v20/

[7] Paloalto Networks(zingbox), “IoT guardian for the healthcare industry,” White paper, 2016.

[8] Medigate, “Dedicated medical device-security platform,” White paper, 2017.

[9] L. Fernandez Maimo et al., “Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments,” Sensors, vol. 19, no. 5, 2019.

[10] OpenICE, https://www.openice.info/

[11] C. Ma et al., “Analysis of multi-types of flow features based on hybrid neural network for improving network anomaly detection,” IEEE Access, vol. 7, 2019, pp. 148363-148380.

[12] P. Berezinski et al., “An entropy-based network anomaly detection method,” J. Entropy. vol. 17, 2015, pp. 2367-2408.

[13] FDA, “Premarket submissions for management of cybersecurity in medical devices,” 2014.

[14] FDA, “Postmarket management of cybersecurity in medical devices,” 2016.

[15] M. Zou et al., “Network phenotyping for network traffic classification and anomaly detection,” in Proc. IEEE Int. Symp. Technol. Homeland Secur. (Woburn, MA, USA), oct. 2018, pp. 23-24.

[16] A. Azmoodeh et. al., “Detecting crypto-ransomware in IoT networks based on energy consumption footprint,” J. Ambient Intell. Humanized Comput. vol. 9, 2018, pp. 1141-1152.

[17] R.H. Hwang et al., “An LSTM-based deep learning approach for classifying malicious traffic at the packet level,” Appl. Sci. vol. 9, 2019.

[18] B. Seri et al., “Pwned piper,” White paper, Armis, 2021, https://www.armis.com/research/pwnedpiper