2016. 06. 24

랜섬웨어의 표적형 공격, 의료기관 겨냥하나

표적화로 진화 중인 랜섬웨어

AhnLab

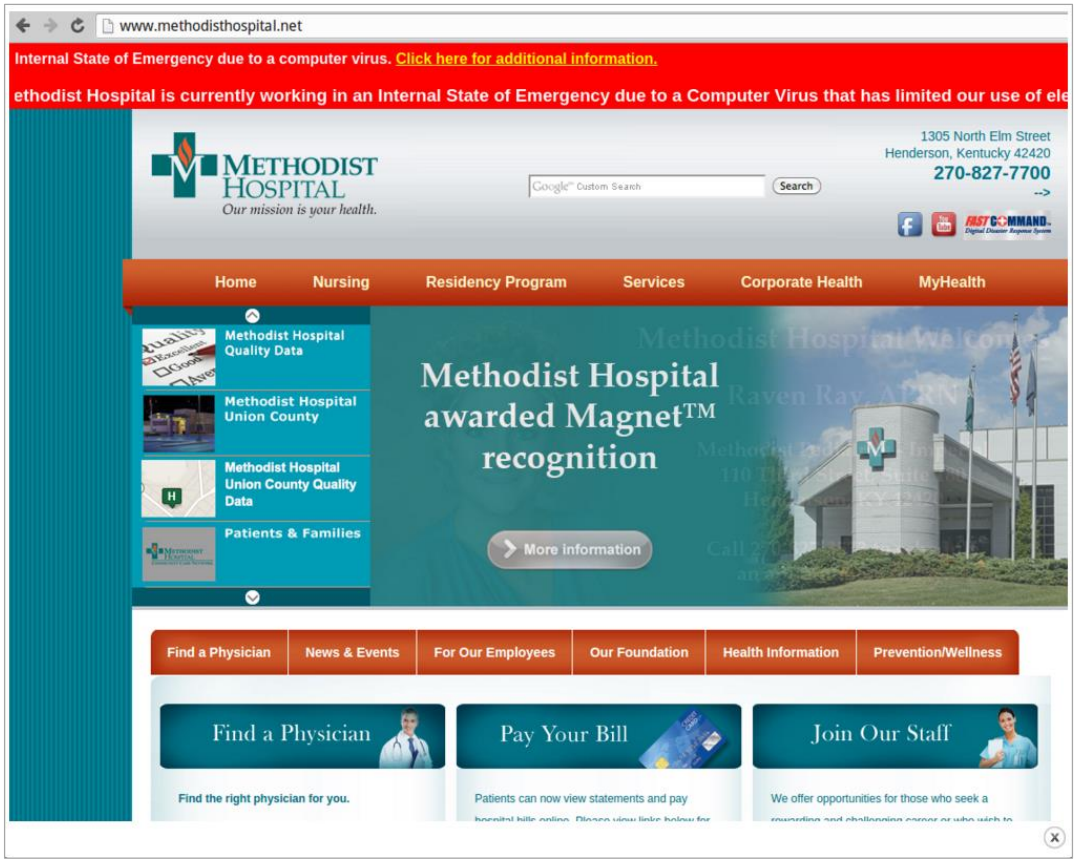
경기도 성남시 분당구 판교역로 220 (우) 13493 | 대표전화 : 031-722-8000 | 팩스 : 031-722-8901 | www.ahnlab.com
© AhnLab, Inc. All rights reserved.

불특정 다수를 대상으로 하던 랜섬웨어가 최근 들어 타깃 공격 형태로 진화하고, 그 방식 또한 고도화 되어가고 있다. 특히, 올해 초부터 의료기관을 중심으로 국내·외에서 발생하고 있는 랜섬웨어의 피해 사례가 많이 보고되고 있다. 공격자는 환자의 생명과 직결되어 있는 중요 정보와 시급성 때문에 의료기관의 랜섬웨어 협박에 대한 반응률이 여타 산업에 비해 상대적으로 높다는 점을 간파해 주요 표적으로 삼고 있는 것으로 보인다.

이 글에서는 의료기관에서 발생한 랜섬웨어의 피해 사례를 소개하고, 이에 대한 대응 방안에 대해 살펴본다

의료기관을 타깃으로 하는 랜섬웨어 등장

지난 3월, 미국의 대형 병원 세 곳이 랜섬웨어로 피해를 입은 사실이 보도되었다. 피해 병원은 헨더슨의 감리 병원(Methodist Hospital), 캘리포니아의 치노밸리 의료센터(Chino Valley Medical Center), 데저트밸리 병원(Desert Valley Hospital) 등이다. 이 세 곳의 병원이 피해를 입기 전에 할리우드 장로 병원(Hollywood Presbyterian Medical Center)이 랜섬웨어에 감염된 사실이 밝혀지기도 했다. 할리우드 장로 병원은 랜섬웨어로 인해 열흘간 시스템 접근이 불가능했으며, 결국 공격자에게 몸값(1만 7천 달러)을 지불해 시스템을 복구시킨 것으로 알려졌다.



[그림 1] 핸더슨 감리 병원은 홈페이지 상단 배너를 통해 악성코드 감염에 의한 서비스 사용 제한을 알렸다.

 © AhnLab, Inc. All rights reserved.

앞서 언급한 것과 같이 기존의 랜섬웨어들이 불특정 다수를 겨냥한 무작위 공격의 형태를 지니고 있었다고 하면, 최근에 발견되는 랜섬웨어는 타깃을 정해서 공격하는 표적형 랜섬웨어로 점차 진화하고 있다. 2015년말 특정 그룹, 특히 민감한 정보와 환자 정보가 많은 의료기관을 타깃으로 한 랜섬웨어 '삼삼(SamSam)'이 등장했다. 일반적인 랜섬웨어는 스팸 메일이나 보안이 취약한 웹사이트를 통해 불특정 다수에게 대량으로 악성코드를 유포하고 사용자 파일을 암호화한 후 USD 혹은 비트코인(Bitcoin)을 요구한다. 반면, 랜섬웨어 삼삼은 특정 그룹 내부에서 사용하는 인프라의 취약점이 있는지를 조사하고 이것을 활용하여 내부 인프라 및 네트워크에 연결된 사용자 컴퓨터에 대한 파일 암호화 후 돈을 요구하는 공격 형태를 보이고 있다. 그리고 랜섬웨어 삼삼은 공격자가 업로드한 RSA 키를 인자로 실행하여 시스템을 감염시키고 중요 문서 및 사진 파일을 RSA-2048 방식으로 암호화하여 사용자에게 암호화가 되었음을 알리는 HTML을 생성한다.

[그림 2] 사용자에게 암호화가 되었음을 알리는 HTML

<V3 제품군의 진단명>

Trojan/Win32.Samas

<AhnLab MDS 진단명>

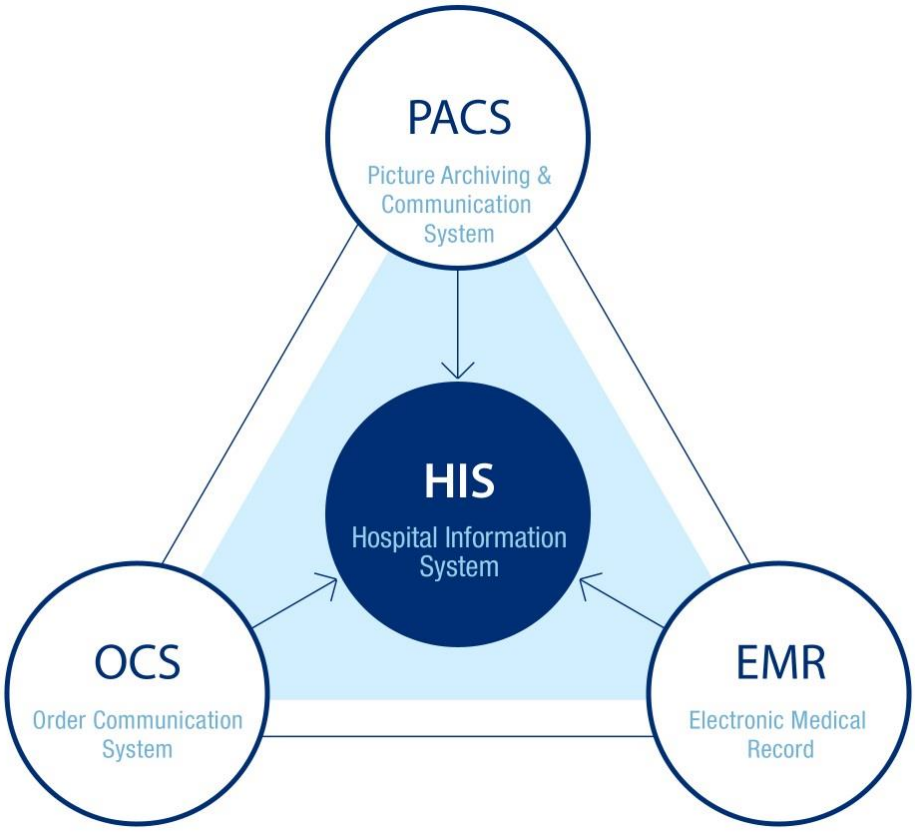
Suspicious/MDP.Create

Malware/MDP.Behavior

 © AhnLab, Inc. All rights reserved.

병원정보시스템(HIS)과 잠재적 보안 위험

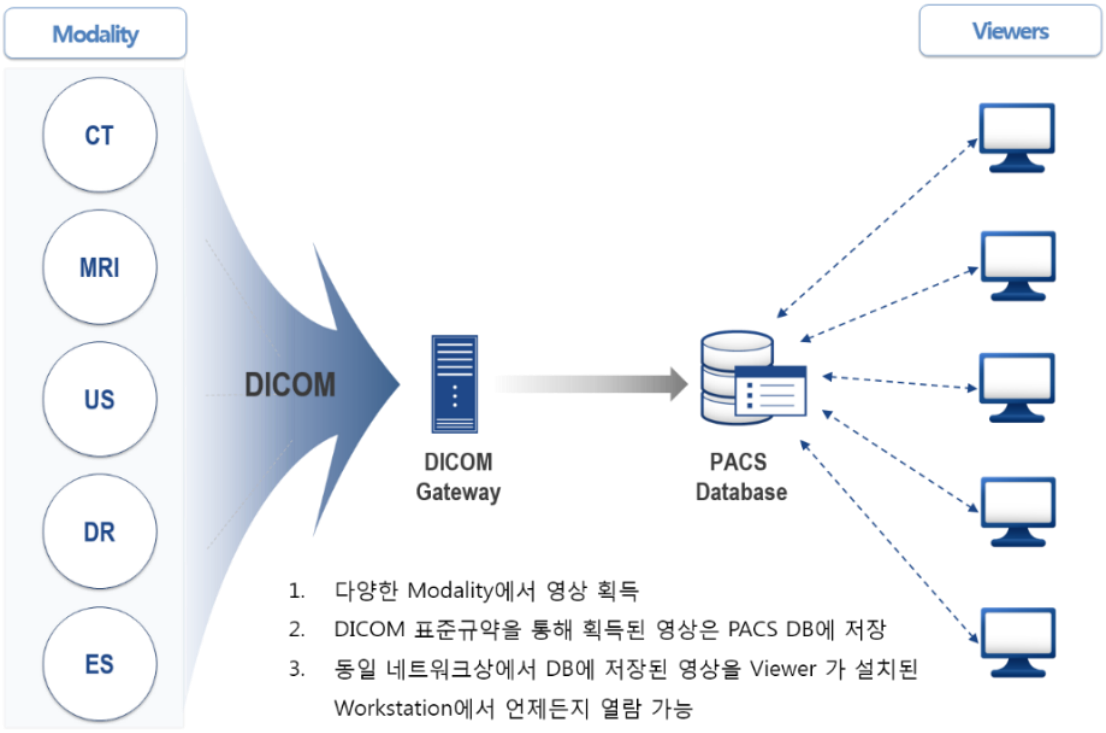
대부분 의료 기관들은 병원 내 의료 및 행정업무를 관리하기 위한 병원정보시스템(Hospital Information System, 이하 HIS)을 사용한다. 이 시스템은 진료 현황부터 의약품관리, 재무관리, 환자관리 및 각종 의료 영상 정보까지 관리하는 통합 시스템이다. 특히 HIS의 핵심이라 할 수 있는 전자의료기록(Electronic Medical Record, EMR), 처방전 전달 시스템(Order Communication System, OCS), 의료 영상 저장 및 전송 시스템(Picture Archiving & Communication System, PACS)은 민감한 환자 정보를 다루고 있고 네트워크를 통한 시스템간 유기적인 연동이 가능해야 한다.



[그림 3] 주요 병원정보시스템

특히 PACS는 여러 가지 의료 영상 장비(MRI, CT, X-ray 등)로부터 획득한 의료 영상 정보를 저장 및 전송하는 시스템으로, 환자의 치료 및 생명과도 직결되는 만큼 안전하게 관리되어야 하는 중요 시스템이다. 또한 의료 영상 및 그 소견서의 법적 의무 보관 기간이 5년이므로 혹시 발생할 수 있는 사고에 대비하여 자료에 대한 백업 관리도 중요하다. 만약 NAS(Network Attached Storage) 영역을 활용하여 저장된 PACS의 의료 영상 정보가 영상판독 뷰어가 설치된 클라이언트 시스템을 통해 유입된 랜섬웨어에 의해 암호화가 되고, 백업 데이터까지도 동일 네트워크상에 위치한 저장 장소에 관리되어 암호화가 된다면 병원 보안 담당자로서는 상상하기도 싫은 사태가 발생하게 될 것이다.

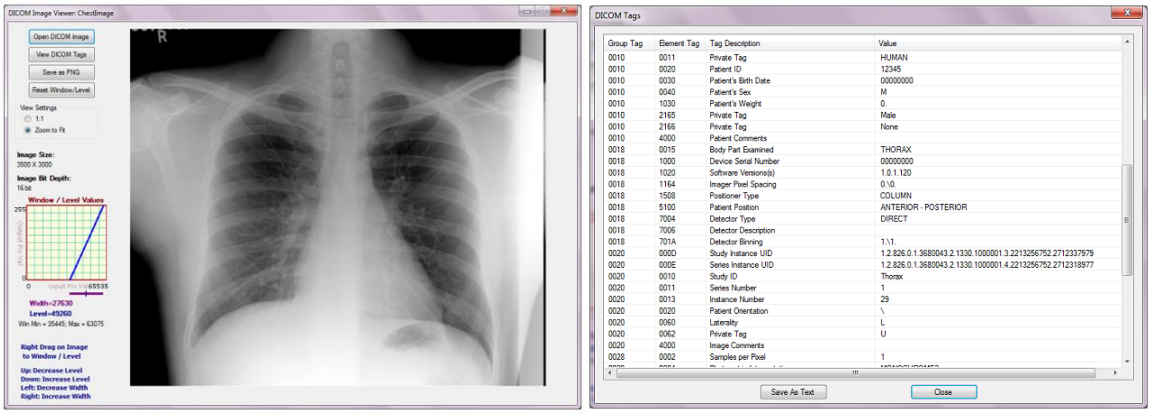
 © AhnLab, Inc. All rights reserved.



[그림 4] PACS 시스템 개념도

* CT(Computed Tomography), MRI(Magnetic Resonance Imaging), US(Ultrasound), DR(Digital Radiography), ES(Endoscopy)

PACS 서버에 저장되는 의료 영상 정보는 미국방사선의학회(ACR)와 미국전기공업회(NEMA)에서 구성한 연합위원회에 의해 정해진 의료 영상 표준 규격, 즉 DICOM(Digital Imaging & Communications in Medicine) 파일 형태로 저장되어 관리된다. 이는 단순한 이미지와 파일에 대한 형식이 아닌 데이터 전송(Transfer), 저장(Storage) 및 출력(Display)에 대한 전반적인 표준 규격이다. 표준 규격에 따라 해당 영상에는 DICOM 태그(Tag) 정보들이 포함되어 있는데 여기에는 환자의 성별, 나이, 이름 등의 개인정보도 포함되어 있기 때문에 랜섬웨어에 의해 암호화되어 유출된 후 복호화 키와 함께 블랙마켓에서 판매가 된다면 자칫 더 큰 보안 사고로 확대될 수 있다. 최근 인기리에 방영된 드라마 '태양의 후예'에서도 국가 고위급 인사의 의료정보가 기밀사항으로 취급되고 있는 것을 볼 수 있었다. 이러한 정보들이 악의적인 목적에 의해 유출된다면, 어떻게 활용하느냐에 따라 그 피해의 정도는 상상을 초월할 것이다.



[그림 5] DICOM Viewer를 통해 본 의료 영상(좌) 및 DICOM Tag에 있는 각종 민감 정보(우)

출처: http://www.codeproject.com/Articles/36014/DICOM-Image-Viewer

 © AhnLab, Inc. All rights reserved.

지속적으로 진화하는 랜섬웨어 대응 방안

악성코드 제작자를 비롯한 사이버 범죄자들은 보안 솔루션을 우회하는 다양한 방법과 기능으로 중무장한 랜섬웨어 변종을 지속적으로 유포하고 있다. 더 나아가 단순히 유포에 그치지 않고 금전적 이득을 극대화하기 위해 특정 업체를 표적화하여 공격하는 양상을 띠고 있다.

안랩은 지속적으로 진화하는 랜섬웨어에 대응하기 위해 다양한 랜섬웨어 변종과 관련된 악성파일 진단을 지속적으로 추가하고 있다. 또한 지능형 위협 대응 솔루션인 '안랩 MDS'의 실행보류 기능(Execution Holding)으로 기존의 랜섬웨어 뿐만 아니라 다양한 변종에 대한 대응이 가능하다. 특히, 사용자가 아무런 인지가 없는 상태에서 '악성코드가 자동으로 설치되는 다운로드 실행(Drive-by-Download)' 형태의 공격에 대한 피해를 방지할 수 있다.

[그림 6] 안랩 MDS 실행 보류(Execution Holding) 기능

랜섬웨어 대응에 핵심적인 역할을 하는 것은 바로 안랩 MDS의 '실행보류' 기능이다. 이 기능은 네트워크에서 발견된 의심파일에 대한 분석이 끝나기 전에 PC에서 해당 파일이 실행되는 것을 우선 보류하고, 분석 후 정상 파일로 판정된 파일에 대해서만 실행을 허용한다.

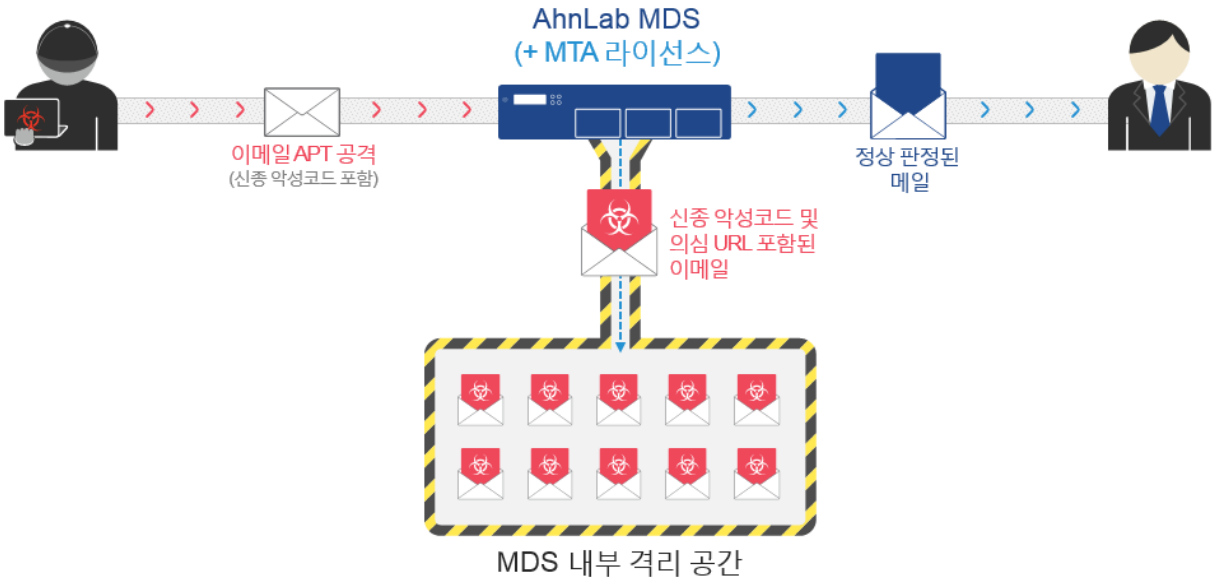
랜섬웨어 삼삼의 경우에도 특정 서버의 취약점을 악용해 서버에 침투하고 트리거(Trigger) 형태인 각종 악성 파일을 로컬 네트워크 단말에서 실행시킨다. 하지만 안랩 MDS의 실행보류(Execution Holding) 기능으로 네트워크를 통해 침입한 랜섬웨어가 PC에 있는 파일을 암호화하는 행위를 방지할 수 있다.

점점 표적화 되어가는 랜섬웨어들은 주로 스피어 피싱(Spear Phishing) 기법을 이용한다. 스피어 피싱은 스팸 메일 등과는 달리 특정 기관 및 기업을 노리는 표적성, 정상적인 파일로 보이거나 의심하기 어려울 정도로 실제 메일처럼 보이게 하는 정교함을 활용하기 때문이다. 안랩 MDS는 스피어 피싱 기법을 이용하여 유포되는 악성 메일에 첨부되는 랜섬웨어에 대응하기 위해 이메일 격리(MTA) 기능을 제공한다. 이메일 격리(MTA) 기능은 악성코드가 첨부되거나 의심 URL이 포함된 메일을 MDS 내부 공간으로 격리시키는 기능이다.

 © AhnLab, Inc. All rights reserved.

점점 고도화되는 최신 보안 위협에 대응하고 예방하기 위해서는 보안의 3요소인 사람, 기술, 프로세스가 조화를 이루어야 한다. 우선 당장 발생하고 있는 보안 위협으로부터 보호받기 위해 기술 관점에서 관련 솔루션의 도입이 필요하다. 특히 안랩 MDS가 제공하는 이메일 격리(MTA) 기능을 통해 악성 메일(악성 첨부파일 및 메일 본문 악성 URL 링크가 포함된 메일)을 격리하여, 발생될 수 있는 스피어 피싱 공격에 대한 사전 대응이 가능하다. 또한 실행보류(Execution Holding) 기능을 통해 '실행이 보류된 의심 파일'이 최종적으로 악성이라는 결과를 전달받고 해당 파일을 삭제•격리 조치함으로써 사용자의 시스템을 '신종•변종 랜섬웨어'로부터 안전하게 보호할 수 있다. 특히 문서형 악성코드 분석에 최적화된 동적 콘텐츠 분석 기술(DICA, Dynamic Intelligent Content Analysis)을 통해서 '의심 행위 여부'와 상관없이 문서 애플리케이션의 제로데이 취약점까지도 정확하게 탐지할 수 있다.

이메일 격리(MTA) 기능

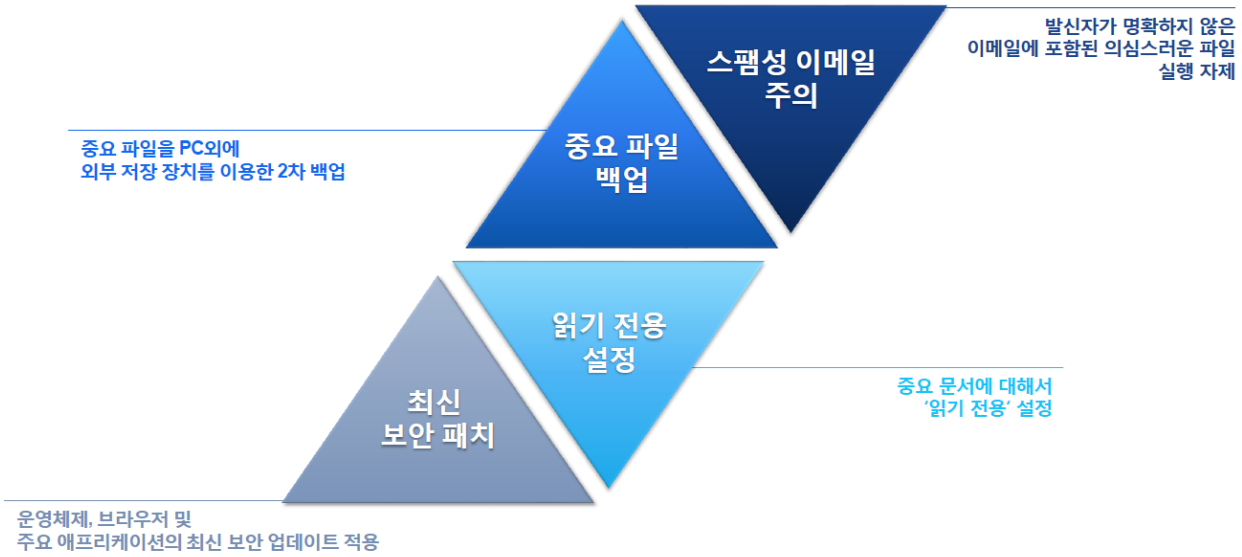


[그림 7] AhnLab MDS 이메일 격리(MTA) 기능

 © AhnLab, Inc. All rights reserved.

랜섬웨어와 끊임없는 싸움의 끝은?

이미 의료기관과 헬스케어 분야에 대한 공격은 지난 수년간 지속적으로 발생하고 있으며, 이에 대한 대응방안으로 여러 가이드라인이 정부기관이나 유관 부처를 통해 배포되고 있다. 앞서 살펴본 여러 사례들을 보면 암호화를 풀기 위해 랜섬을 지불한 것에 대한 피해 규모만 산정되어 언론을 통해 보도되고 있다. 하지만 기회 비용의 관점에서 병원 시스템들이 랜섬웨어에 점령당한 기간 동안 의료기관들이 피해를 본 정량적인 매출 감소와 인명 피해, 그리고 정성적 관점에서 손상된 병원의 이미지에 대한 실질적인 피해 규모도 간과하지 말아야 한다.



[그림 8] 랜섬웨어 피해 예방을 위한 보안 수칙

랜섬웨어 대응을 위해서 기술적인 보안과 더불어 중요한 것이 사람과 프로세스에 대한 재정비이다. 조직 내에서 편의성을 위해 보안이 배제되고 있는 프로세스는 없는지 점검하고, 보안을 기반으로 한 업무 프로세스 재정립이 반드시 필요하다. 그리고 보안에 대한 조직 구성원들의 인식 개선을 위한 교육과 기본적인 랜섬웨어 예방 가이드에 대한 지속적인 교육도 함께 병행되어야 할 것이다.

참고 문헌

CYBERATTACKERS DEMAND $3.6M RANSOM FROM HOLLYWOOD HOSPITAL
http://www.hipaajournal.com/cyberattackers-demand-3-6m-ransom-from-hollywood-hospital-8313/

As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin
http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#1dff2c6b75b0

Hollywood Hospital Victimized by Ransomware Locky Spreading Fast
http://www.ktvn.com/story/31274059/hollywood-hospital-victimized-by-ransomware-locky-spreading-fast

 © AhnLab, Inc. All rights reserved.

A Hospital Paralyzed by Hackers
http://www.theatlantic.com/technology/archive/2016/02/hackers-are-holding-a-hospitals-patient-data-ransom/463008/

이 랜섬웨어...의료기관만 노린다
http://techholic.co.kr/archives/51555

한 주 만에 병원 세 곳이 랜섬웨어에! 의료계 위기
http://www.boannews.com/media/view.asp?idx=50052&kind=4

국내 주요 의료기관 랜섬웨어 대응현황 긴급진단
http://www.boannews.com/media/view.asp?idx=50174

랜섬웨어 피해 입은 미국 병원, 끝내 1만 7,000달러 비용 지불
http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=1&seq=24661

SAMSAM: THE DOCTOR WILL SEE YOU, AFTER HE PAYS THE RANSOM
http://blog.talosintel.com/2016/03/samsam-ransomware.html?m=1

Check Point Threat Alert: SamSam and Maktub Ransomware Evolution
http://blog.checkpoint.com/2016/03/28/check-point-threat-alert-samsam-and-maktub-ransomware-evolution/

의료기관 서버 취약점 노리는 '삼삼'과 감염 확산 위해 파일 압축하는 '마크텁' 발견
http://www.boannews.com/media/view.asp?idx=50117&skind=O

삼삼 랜섬웨어, 특정 기업 노리는 표적형으로 진화
http://www.boannews.com/media/view.asp?idx=50198

Samsam may signal a new trend of targeted ransomware
http://www.symantec.com/connect/blogs/samsam-may-signal-new-trend-targeted-ransomware

No mas, Samas: What's in this ransomware's modus operandi?
https://blogs.technet.microsoft.com/mmpc/2016/03/17/no-mas-samas-whats-in-this-ransomwares-modus-operandi/

Evolution of SamSa Malware Suggests New Ransomware Tactics In Play
http://researchcenter.paloaltonetworks.com/2016/03/evolution-of-samsa-malware-suggests-new-ransomware-tactics-in-play/

DICOM Standard
http://dicom.nema.org/standard.html

AhnLab © AhnLab, Inc. All rights reserved.