[2021년 3분기]

의료기관 대상 랜섬웨어 위협 대응을 위한 보안설정 가이드

본 보고서는 최근 의료분야를 대상으로 발생하는 랜섬웨어 위협을 대응하기 위해 의료기관에서 참고할 수 있는 보안설정 방법을 제공합니다.

진료정보침해대응센터
Korea Healthcare Computer Emergency Response Team

보건복지부

SSiS 한국사회보장정보원
KOREA SOCIAL SECURITY INFORMATION SERVICE

CONTENTS

01 개 요

1 국내 · 외 랜섬웨어 공격 사례

코로나19 확산에 따라 의료기관에 대한 사회적 관심이 집중되면서 의료기관에 대한 사이버 위협이 전 세계적으로 증가하고 있다. 2021년 8월 발표한 Philips와 CyberMDX의 연구 보고서 "Perspective in Healthcare Security"에 따르면 **미국 의료기관의 48%가 지난 6개월 동안 랜섬웨어로 인해 네트워크 연결이 중단**되었다고 응답했다. 의료기관의 규모에 따라서 중형병원이 이러한 공격의 영향을 가장 많이 받은 것으로 확인된다. 대형병원의 경우 랜섬웨어 공격으로 인한 네트워크 중단으로 시간당 21,000달러의 비용으로 평균 6.2시간의 가동 중단을 겪었다. 이에 비해 중형병원은 **시간당 45,700달러의 비용이 발생하는 업무 중단이 평균 10시간 가까이 발생**했다고 응답했다.

[그림 Ⅰ-1] 미국 병원 절반이 랜섬웨어로 인해 네트워크 폐쇄(출처 : 인포시큐리티 매거진)

또한, 미국의 사이버 보안 및 기반시설 보안국(CISA)은 **랜섬웨어 공격으로 인한 병원의 치료 지연으로 사망률이 상승하는지에 대한 연구를 진행**중이다. 최종 결과가 나오진 않았으나 환자의 사망까지 이르는데는 이견이 있을 수 있으나 **응급환자의 치료 지연으로 건강의 악영향 및 영구적인 손상을 초래**할 수 있다고 밝혔다. 미국 Northwell Health 병원 관계자 Jarrett은 **랜섬웨어 공격에 직면한 모든 병원은 이러한 사이버 위협을 정보기술 문제가 아닌 환자의 안전 문제로 인식해야 한다**고 말했다.

[그림 Ⅰ-2] 팬더믹으로 인해 병원의 랜섬웨어 공격 위험이 드러났다(출처 : 더버지)

국내의 경우도 랜섬웨어 공격을 위주로 의료기관의 피해 사례가 보고되고 있다. 보안 수준이 미흡한 병·의원급 의료기관 뿐만 아니라 기본적인 보안장비를 갖춘 종합병원 및 상급종합병원에서도 랜섬웨어를 통한 진료정보의 멸실과 정보 유출 사고가 발생하고 있다. 의학신문의 2021년 6월 25일 "코로나19 관련 의료기관 랜섬웨어 공격 비상", 쿠키뉴스의 2021년 6월 29일 "의료기관 랜섬웨어 공격 심각… 정부 주의 촉구" 등의 기사에서 국내 의료기관 대상 랜섬웨어 공격이 지속적으로 보고되고 있다고 보도했다. 또한 데일리 메디의 2021년 7월 8일 "무차별 랜섬웨어 공격…서울대병원도 뚫렸다"라는 보도를 통해 상급종합병원의 랜섬웨어 공격으로 인한 환자 개인정보 유출 사례가 알려졌다.


무차별 랜섬웨어 공격…서울대병원도 뚫렸다

지난 6월 악성코드 감염 해킹…환자 개인정보 파일 유출 우려

[2021년 07월 08일 06시 17분]

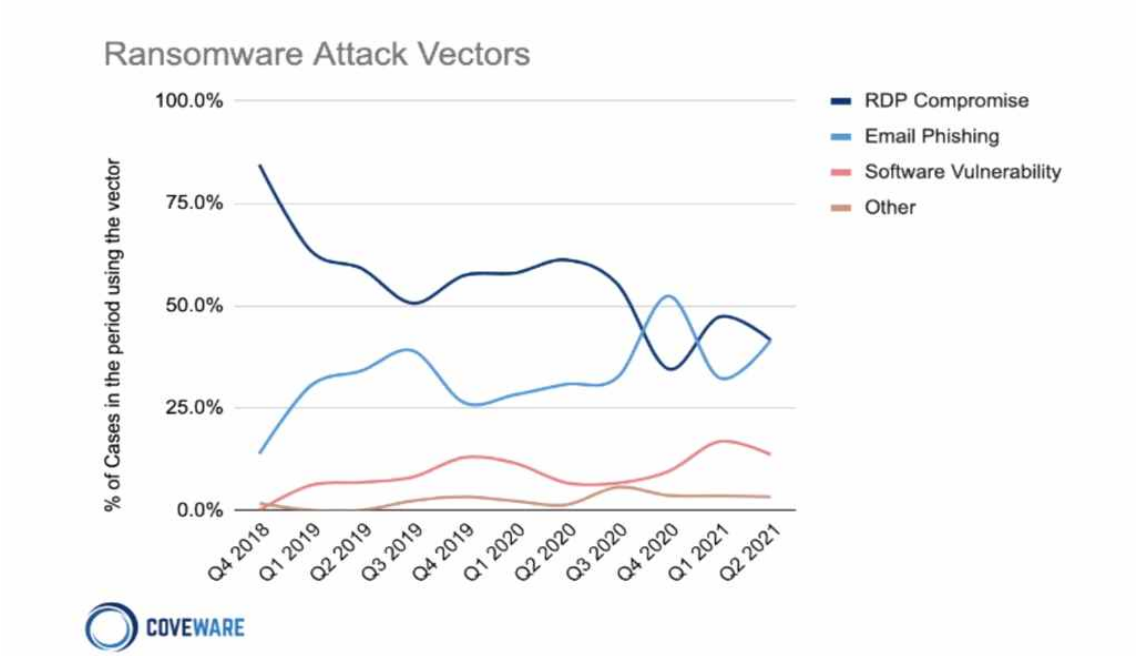
[그림 Ⅰ-3] 무차별 랜섬웨어 공격…서울대병원도 뚫렸다(출처 : 데일리메디)

진료정보침해대응센터의 집계에 따르면 의료기관 대상 사이버 공격이 2021년 10건이 넘었다. 2020년 총 13건에 비해 올해 7월까지 11건이 발생하여 **침해사고 건수는 더욱 늘어날 전망**이다. 병원 규모에 따라 병원급이 4건으로 가장 많았고, 상급종합병원급에서도 2건이 신고됐다. 사고 유형별로 랜섬웨어가 9건으로 대부분을 차지했다. 이처럼 의료기관 대상의 랜섬웨어 공격이 지속적으로 발생함에 따라 국내·외에서 발생하는 랜섬웨어의 공격 유형을 분석하여 이에 맞는 대응방법을 제공하고자 한다.

다양한 규모의 의료기관에서 본 보고서를 활용할 수 있도록 **OS, 네트워크, 보안장비에서의 보안설정 방법을 제시**한다. 각 의료기관은 상황에 맞는 방법을 선택하여 적용할 수 있다. 또한 본 보고서에서 제공하는 **보안조치를 겹겹이 적용**하여 사이버 위협에 대한 위험을 최대한 경감시킬 수 있는 **심층방어(Defense in Depth) 모델**을 병원 IT 환경 및 보안장비 전반에 적용할 것을 권고한다.

2 랜섬웨어 공격 유형

2021년 4월 미국의 랜섬웨어 전문 보안업체 Coveware가 발표한 보고서에 따르면 공격자들이 시스템을 랜섬웨어에 감염시키기 위해 사용한 공격 방식은 ① RDP 공격, ② 이메일 공격, ③ 소프트웨어 취약점 공격이 가장 많이 사용된 것으로 확인된다. RDP는 잘 알려진 공격 방법이며, 안전한 원격 접속을 위한 다른 방법이 있음에도 여전히 랜섬웨어 공격자가 가장 많이 사용한 공격으로 집계 되었다. 이메일 공격은 인증 정보를 탈취하는 악성코드 또는 원격 접근 트로이 목마를 설치하는 것이 주요 공격 방법으로 남아있다. 2021년 1분기 가장 많이 사용된 소프트웨어 취약점은 포티넷, 펄스시큐어와 같은 VPN 장비와 연관되어 있다.

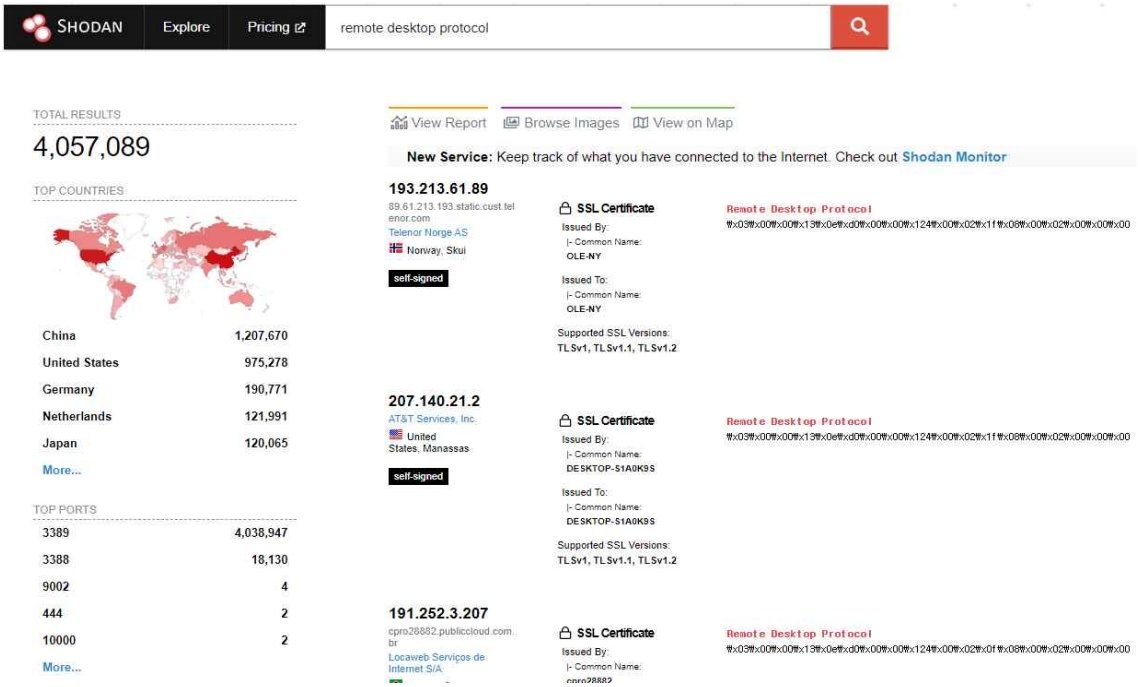


[그림 Ⅰ-4] 랜섬웨어 공격 벡터 현황(출처 : Coveware)

(1) RDP(Remote Desktop Protocol) 공격

RDP 공격은 Shodan*과 같은 사이트를 이용해 외부에 공개된 RDP 서비스를 목표로 공격한다. 원격 접속으로 외부에 노출된 서버에 연결한 후, 내부의 Active Directory 서버 등을 통해 내부 전체 시스템을 대상으로 대규모 악성코드 전파를 수행하는 사례가 발생한다. 외부로 노출된 RDP 및 SSH 서비스는 Shodan과 같은 사이트를 통해 확인할 수 있으므로 공격자의 손쉬운 공격 대상이 될 가능성이 크다. 또한 초기 침투 이후 내부 시스템 침투를 위한 악성코드 전파 통로로도 활용되고 있다.

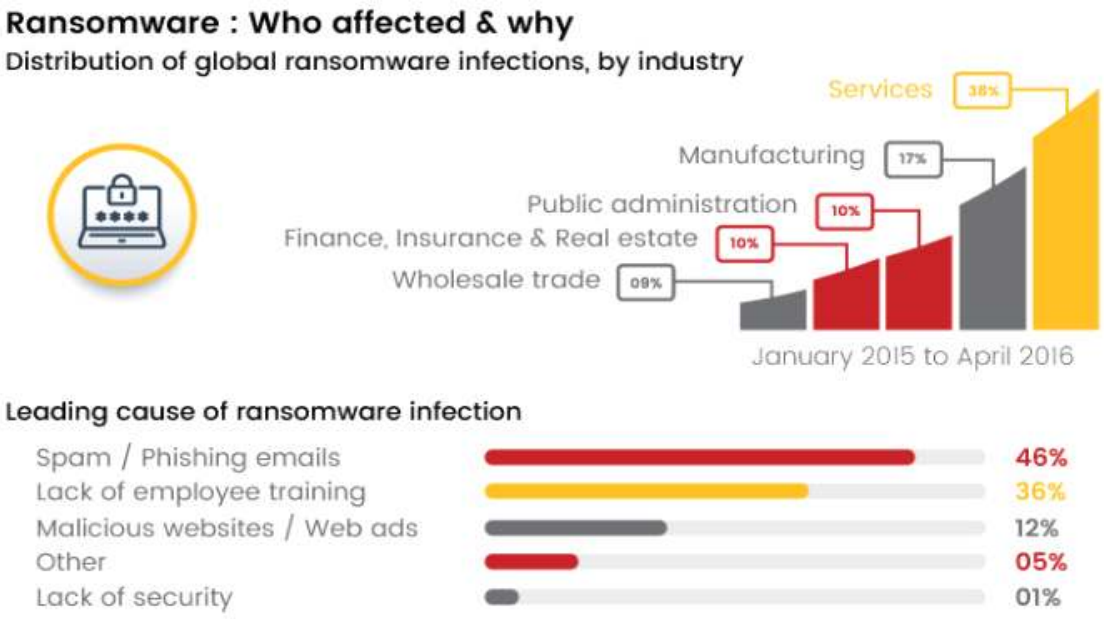
* Shodan : 인터넷에 연결된 모든 시스템을 찾아주는 검색엔진으로 검색 대상 시스템의 취약점 및 개방된 포트 등의 현황까지 확인 가능



[그림 Ⅰ-5] 외부로 공개된 원격 데스크톱 서비스 현황(출처 : Shodan.io)

(2) 이메일 공격

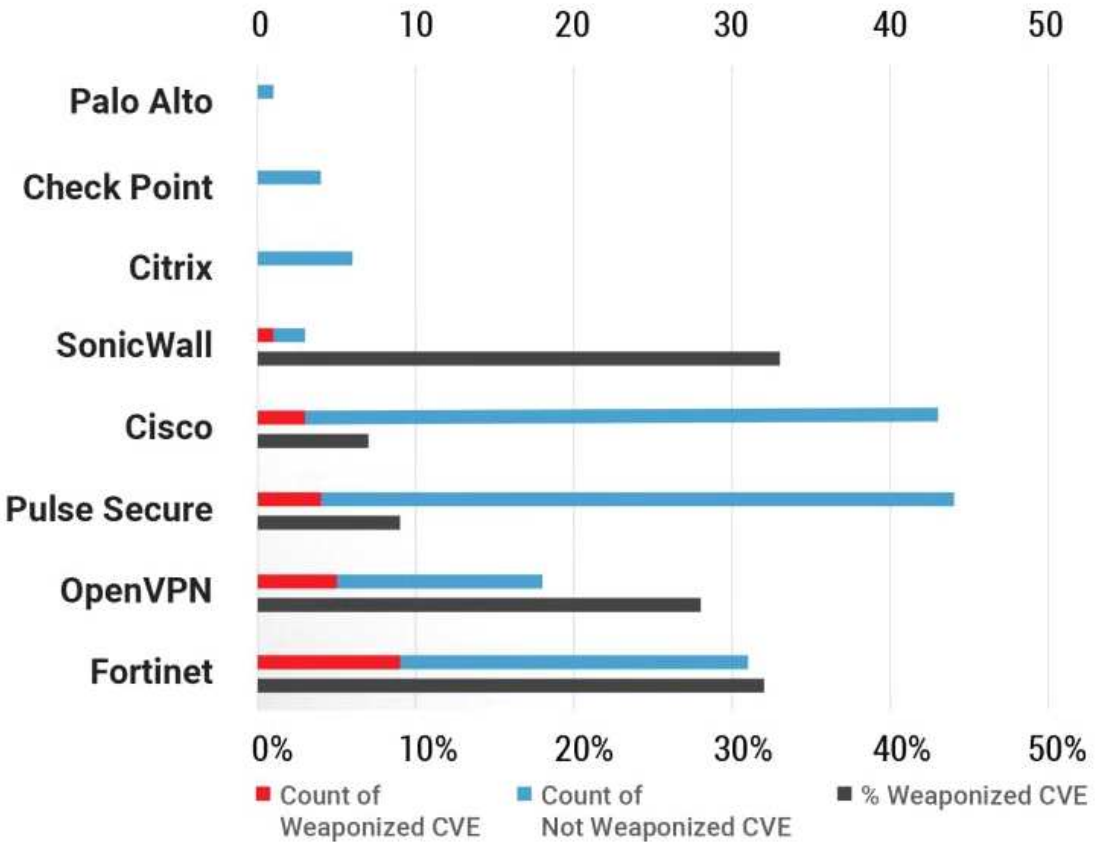
이메일 내 첨부문서 또는 악성 링크를 통한 랜섬웨어 감염 또한 주요 공격벡터로 알려져 있다. 해외 보안기업의 설문조사를 보면 랜섬웨어 감염의 가장 주요한 원인으로 이메일 공격을 지목하고 있다. 클롭(clop), 이그레거(egregor) 등의 랜섬웨어 공격자가 이메일을 이용한 피싱 공격을 주요 공격기법으로 사용하고 있다.



[그림 Ⅰ-6] 랜섬웨어의 공격 벡터(출처 : briskinfosec.com)

(3) 소프트웨어 취약점 공격

COVID-19 사태로 인해 재택근무가 늘어나 VPN 장비 사용이 급격히 늘어났으며, 이로 인해 VPN 취약점을 이용한 대규모 랜섬웨어 공격도 함께 늘어나게 됐다. 2019년 여름 이후 Pulse Secure, Palo Alto Networks, Fortinet, Citrix, Secureworks, SonicWall 등을 비롯한 글로벌 VPN 장비 제조사들로부터 다양한 취약점이 공개됐다. 이러한 취약점은 재택근무를 운영하는 기업의 공격벡터로 활발히 악용되고 있다.

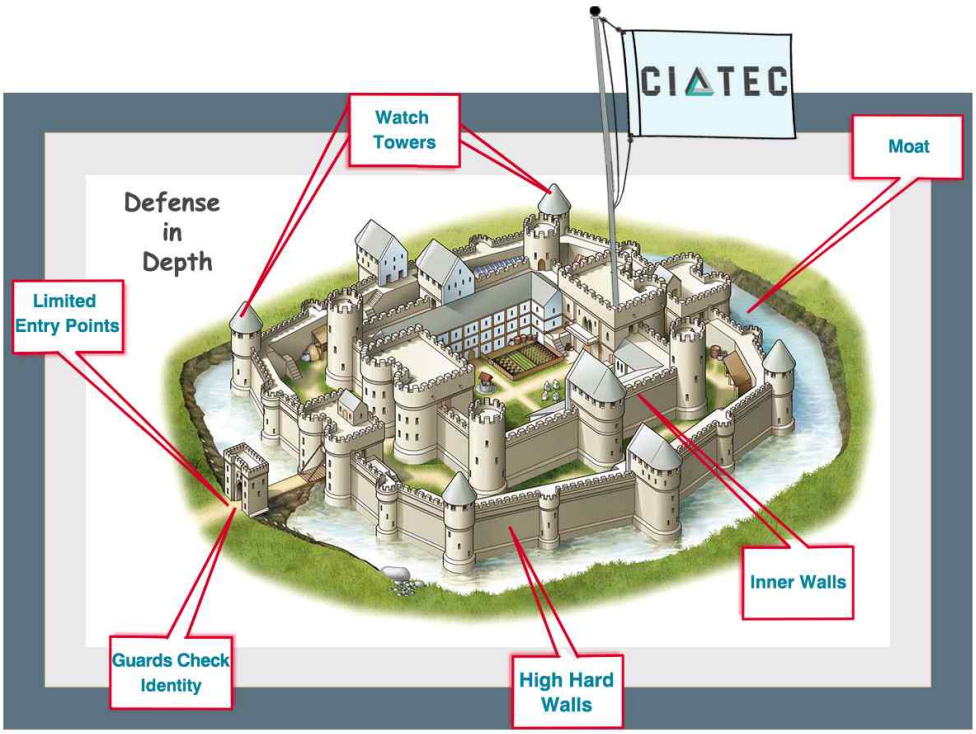


[그림 Ⅰ-7] VPN 벤더사별 취약점, 취약점을 무기화한 현황

공격자들은 취약점을 보유하고 있는 VPN 접속 정보를 다크웹 마켓을 통해 구매하고 취약한 패스워드가 설정된 RDP 접속을 통해 내부 시스템을 침입하는 방법을 사용하고 있다.

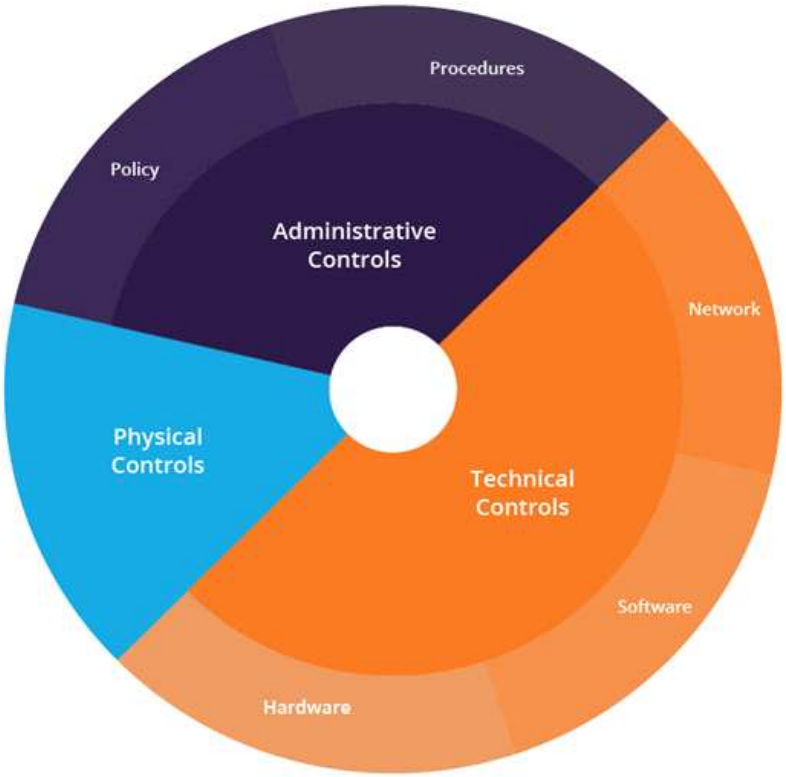
3 심층방어(Defence in Depth) 아키텍처

심층방어는 보안 조치를 여러 계층으로 구축하여 조직의 자산을 보호하는 전략이다. 한 방어선이 손상되면 다른 계층의 방어장치가 동작하여 위협을 차단할 수 있다는 개념이다. 심층방어(Defence in Depth)의 기원은 중세시대 군사전략에서 유래하였는데 침입자의 진행을 늦추기 위해 배치된 성벽(Wall), 해자(Moat), 도개교(Drawbridge), 탑(Watch Towers) 등을 구축해놓은 성(Castle)의 방어를 생각해 볼 수 있다.



[그림 Ⅰ-8] 중세시대 성(castle)의 계층화된 방어 전략(출처:CIATEC社)

미국 NIST에 따르면 심층방어는 사람, 기술 및 운영 기능을 통합하여 조직의 여러 계층과 임무에 걸쳐 다양한 장벽을 설정하는 정보보안 전략으로 정의하고 있다. 또한 보안 목적을 달성하기 위해 계층적 또는 단계적 방식으로 여러 대응책을 적용한다. 심층방어를 조직에 적용하기 위한 방법으로는 공통 공격벡터에 이기종 보안 기술을 계층화하여 한 기술에서 놓친 공격을 다른 기술이 탐지하도록 하는 것을 포함한다. 보안 제어가 실패하거나 취약점이 악용되는 경우 여러 중복 방어 조치를 제공하는 정보 보증 전략이라고 할 수 있으며 심층방어 보안 아키텍처는 네트워크의 물리적, 기술적 및 관리적 측면을 보호하도록 설계된 제어를 기반으로 한다.



[그림 Ⅰ-9] 심층방어, 계층화된 보안 아키텍처(출처:imperva)

○ 심층방어(계층화된 보안 아키텍처)

심층방어 보안 아키텍처는 네트워크의 물리적, 기술적 및 관리적 측면을 보호하도록 설계된 제어를 기반으로 한다.

- 물리적 통제 : 이러한 통제에는 경비원이나 잠긴 문과 같은 IT시스템에 대한 물리적 접근을 방지하는 보안 조치가 포함된다.
- 기술적 통제 : 기술적 통제에는 방화벽 어플라이언스나 바이러스 백신 프로그램과 같은 하드웨어나 소프트웨어를 사용하여 네트워크 시스템이나 리소스를 보호하는 보안 조치가 포함된다.
- 관리 통제 : 관리 통제는 조직의 직원을 대상으로 하는 정책 또는 절차로 구성된 보안 조치이다. 예를 들어 사용자에게 민감한 정보에 "기밀"이라는 레이블을 지정하도록 하는 것이다.

또한 다음 보안 계층은 네트워크의 개별 측면을 보호하는데 도움이 된다.

- 액세스 측정 : 액세스 측정에는 인증 제어, 생체 인식, 시간 제한 액세스 및 VPN이 포함된다.

- 워크스테이션 방어 : 워크스테이션 방어 수단에는 바이러스 백신 및 스팸 방지 소프트웨어가 포함된다.
- 데이터 보호 : 데이터 보호 방법에는 저장 데이터 암호화, 해싱, 보안 데이터 전송 및 암호화된 백업이 포함된다.
- 경계 방어 : 네트워크 경계 방어에는 방화벽, 침입탐지 시스템 및 침입방지 시스템이 포함된다.
- 모니터링 및 예방 : 네트워크 공격의 모니터링 및 예방에는 네트워크 활동, 취약성 스캐너, 샌드박싱 및 보안 인식 교육에 대한 로깅 및 감사가 포함된다.

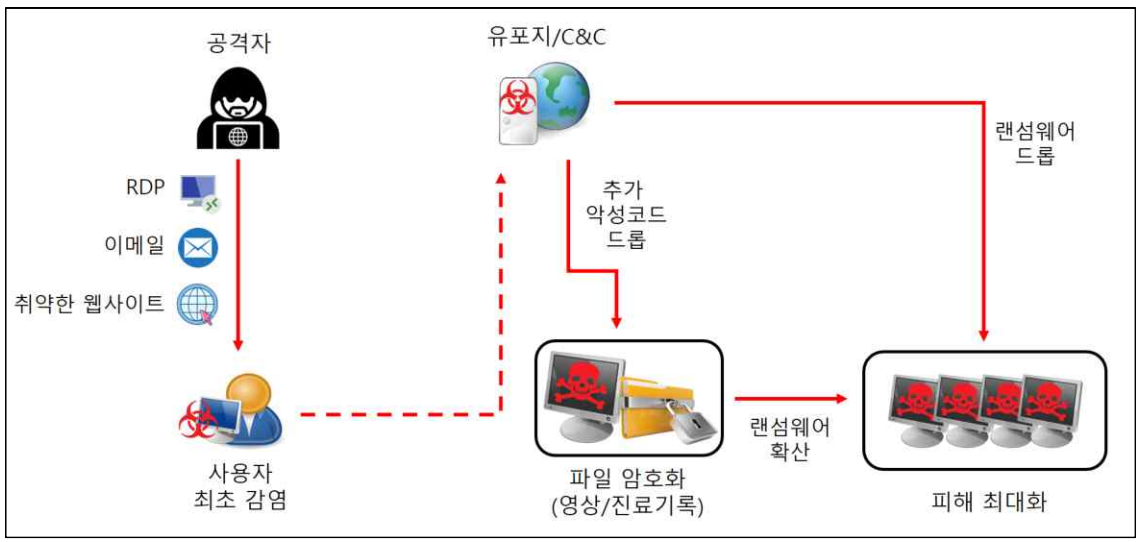
○ 심층방어 사용 사례

- 웹사이트 보호 : 심층방어 사용자 보호에는 위협을 차단하고 중요한 데이터를 보호하기 위한 보안 제품(WAF, 백신 등)과 교육의 조합이 포함된다. 사이버 공격으로부터 최종 사용자를 보호하기 위한 소프트웨어를 제공하는 공급업체는 동일한 제품에 여러 보안 제품을 번들로 제공할 수 있다. 예를 들어 바이러스 백신, 방화벽, 스팸 방지 및 개인 정보보호 기능을 함께 패키징 한다. 그 결과 사용자의 네트워크는 악성코드, 웹 공격(XSS, CSRF 등)으로부터 보호된다.
- 네트워크 보안 : 조직은 방화벽을 설정하고 네트워크를 통해 흐르는 데이터를 암호화하고 저장 데이터를 암호화한다. 공격자가 방화벽을 통과하여 데이터를 훔쳐도 데이터는 암호화된다. 조직은 방화벽을 설정하고 훈련된 보안 운영자와 함께 침입 방지 시스템을 실행하고 바이러스 백신 프로그램을 배포한다. 이것은 3개의 보안 계층을 제공한다. 공격자가 방화벽을 통과하더라도 침입방지시스템(IPS)에 의해 탐지되고 차단될 수 있다. 그리고 최종 사용자 컴퓨터에 도달하여 악성코드를 설치하려고 하면 백신 프로그램에서 탐지되어 제거할 수 있다.

의료기관에서 보유한 IT 인프라 현황에 맞춰 각 장비의 적절한 보안 설정을 통해 심층방어를 구현할 수 있다. 본 보고서에서는 기술적 통제(Technical Control) 부분에서 운영체제, 네트워크 장비, 보안장비 등의 유형에 대한 보안설정 방법을 설명하고 의료기관 보안 담당자는 자신의 상황에 맞는 방법을 선택하여 심층방어를 구현할 수 있다.

02 상세분석

1 초기 침투 유형 분석



[그림 Ⅱ-1] 랜섬웨어 침투/감염 경로 (출처:의료ISAC)

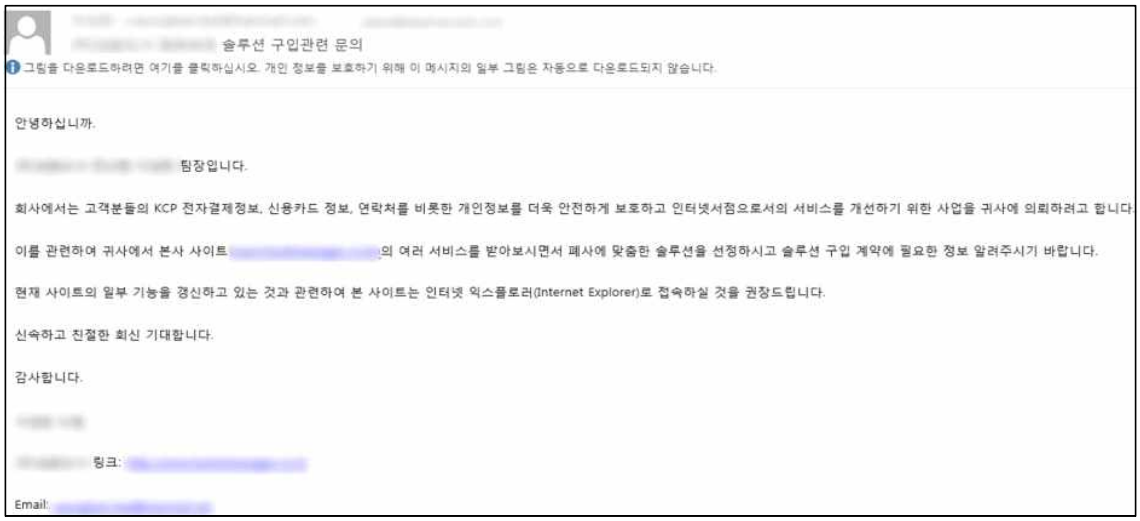
□ 원격 접속을 통한 공격

공격자는 랜섬웨어를 유포하기 위해 원격 데스크톱 프로토콜(RDP) 서버에 무차별 암호 대입 공격으로 대상 단말을 직접 공격 한다. IT관리자는 RDP를 사용하여 단말을 원격으로 접근하고 제어할 수 있다. 그러나 이러한 방식은 해당 단말을 악의적인 목적으로 공격할 수 있는 공격자의 기회가 되기도 한다. 공격자는 Shodan사이트와 Nmap 등과 같은 포트 스캐너를 사용하여 취약한 단말을 검색할 수 있다. 대상 단말기 확인이 되면 공격자는 무차별 대입 공격으로 액세스 권한을 얻은 다음 관리자 권한으로 로그인 한다. 기본 암호 또는 취약한 암호로 된 자격 증명과 암호 크랙 도구를 함께 사용한다. 신뢰할 수 있는 관리자 권한으로 로그인한 공격자는 단말을 완전히 통제하면서 랜섬웨어를 배포하고 데이터를 암호화 할 수 있다. 또한 단말에 설치된 보호 솔루션을 무력화 하거나, 백업을 삭제하여 복구 불가능하게 하여 금전 지불의 가능성을 높이는 등 심각한 피해를 입을 수 있다.

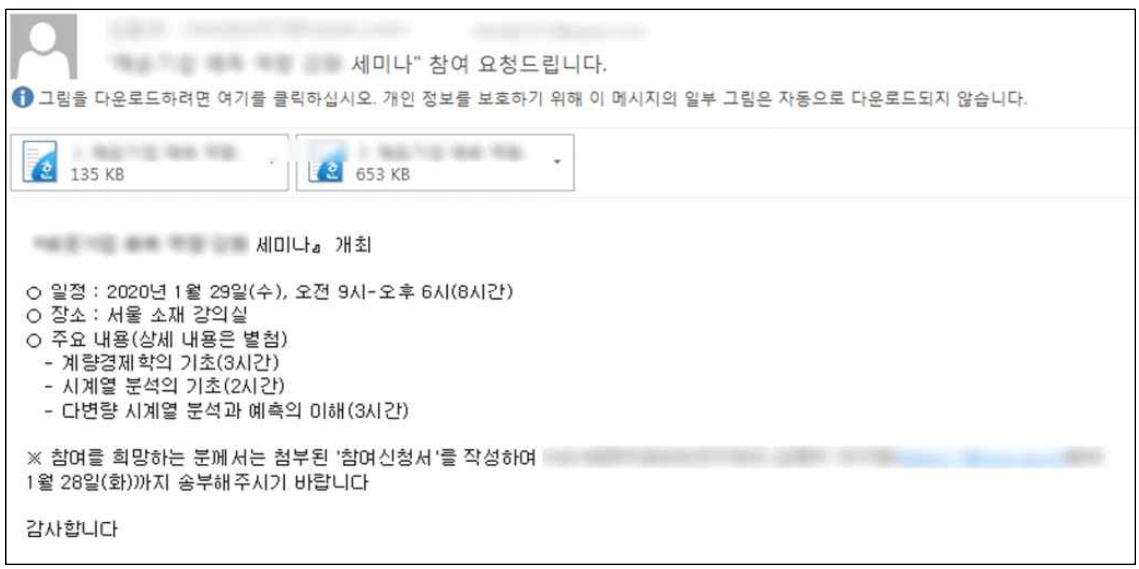
□ 이메일을 통한 공격

공격자가 랜섬웨어를 유포하기 위해 사용하는 가장 일반적인 방법으로 이메일에 악성 파일이나 링크를 삽입하여 유포한다. 이 공격 방식은 점점 진화하여 신뢰를 얻을 수 있는 발신자로 위장하거나 신뢰할 수 있는 계정을 탈취해서 사용자의 신뢰를 얻는 방법들을 사용한다. 아래는 기업을 사칭해 메일을 보낸 사례이다.

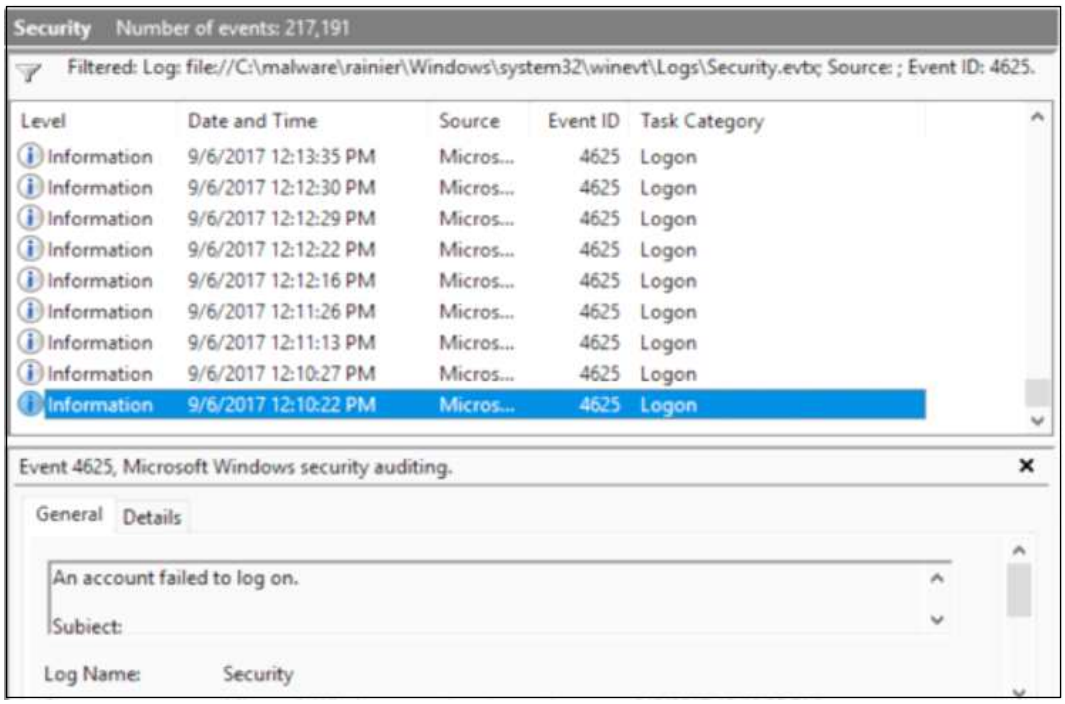
또한 이메일의 내용도 사용자가 개인적 또는 업무적으로 관심있는 내용들로 구성하여 유포한 링크나 첨부파일을 클릭하도록 유도한다. 첨부파일도 과거에는 실행파일 또는 압축파일 형태로 보내져서 육안으로 구분을 할 수 있었지만 최근에는 PDF, DOC, HWP 파일 등 문서 파일로 위장하여 문서를 열람하기 위해 클릭하면 내부의 스크립트가 동작하여 악성행위를 하는 등 외형상 구분하기 어렵다는 특징이 있다.



[그림 Ⅱ-2] 기업사칭 메일로 링크를 삽입하여 악성 사이트 접속 유도 (출처:KISA)



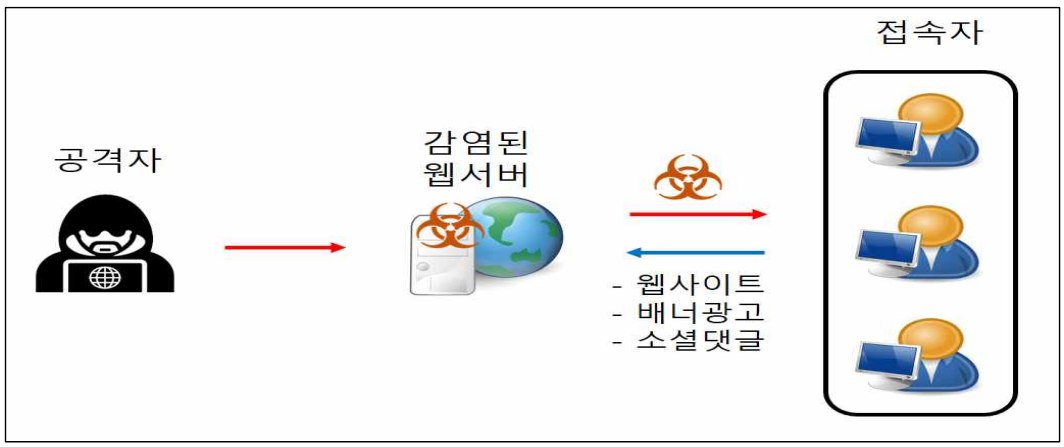
[그림 Ⅱ-3] 악성 스크립트가 포함된 한글파일을 첨부한 피싱메일 (출처:KISA)



[그림 Ⅱ-4] BruteForce 공격으로 로그온 실패 윈도우 이벤트 다수 발생 (출처:secplicity)

□ 취약한 웹사이트를 통한 공격

공격자는 손상된 웹 사이트를 이용하여 간편하게 랜섬웨어를 삽입할 수 있다. 피해자는 평소 자주 방문하던 사이트를 의심없이 방문한다. 그러면 공격자에 의해 손상된 사이트는 최신 버전의 소프트웨어(예 : 인터넷익스플로러, 자바, 플래쉬플레이어 등)를 다운로드하기 위한 페이지로 사용자를 리다이렉트 시킨다. 이는 드라이브 바이 다운로드 공격방식으로 악성코드를 유포하는 방식은 그림과 같다.



[그림 Ⅱ-5] 취약한 웹사이트를 통한 랜섬웨어 유포 (출처:의료ISAC)

□ 감염된 파일 또는 애플리케이션 다운로드를 통한 공격

다운로드용 파일이나 애플리케이션이 랜섬웨어 일 수도 있다. P2P 또는 웹하드 등과 같은 불법 파일 공유 사이트에 있는 크랙 소프트웨어는 쉽게 변조될 수 있고 대체로 악성코드를 포함하고 있다. 최근 MBRLocker 사례에서 이러한 방식을 통해 감염된 사례가 있다. 공격자가 정상적인 웹사이트를 해킹하여 감염된 실행 파일을 제공할 가능성도 있다. 피해자는 이런 파일 또는 애플리케이션을 다운로드여 실행하면 랜섬웨어에 감염될 수 있다.

[표 Ⅱ-1] 랜섬웨어 초기 공격유형 및 유형별 조치사항 (출처:의료ISAC)

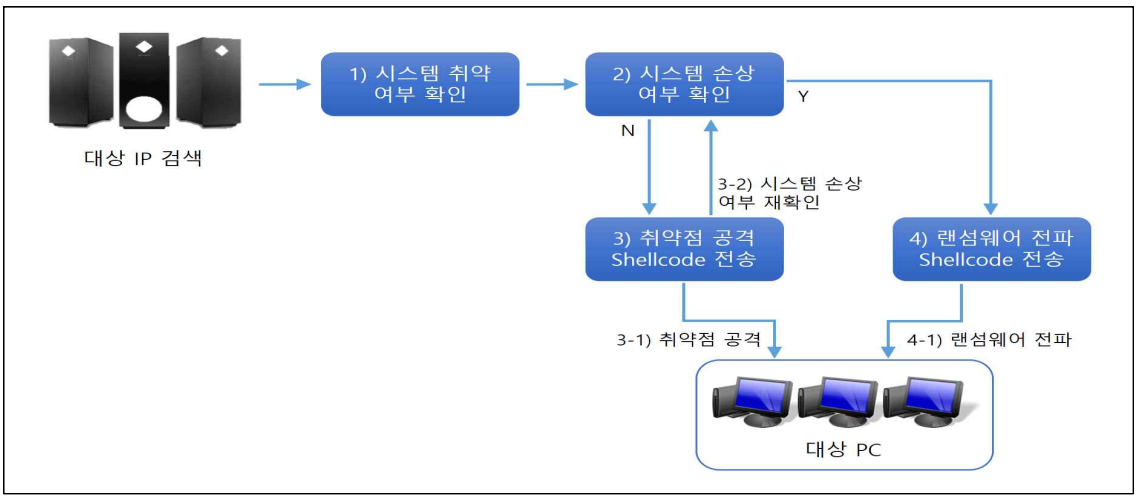
공격 형태	조치사항	관련 페이지
이메일을 통한 공격	사용자 보안 교육/훈련(의심 메일 열람 금지)	해당없음
	(기타) 스팸메일 신고 기능 활용	Ⅲ-4(P.30)
원격접속을 통한 공격	(OS) RDP 서비스 비활성화	Ⅲ-1(P.16)
	(OS) RDP 디폴트 포트 변경	Ⅲ-1(P.17)
	(OS) 파일공유(SMB) 서비스 기능 해제	Ⅲ-1(P.17)
	(OS) Windows 방화벽에서 RDP, SMB 서비스 접근 차단	Ⅲ-1(P.18)
	(네트워크) RDP, SMB 관련 포트 차단	Ⅲ-2(P.25)
	(보안장비) 방화벽 원격접속 관련 포트 차단	Ⅲ-3(P.28)
취약한 웹사이트를 통한 공격	사용자 보안 교육(불필요 사이트 접속 금지)	해당없음
	(OS) Windows 보안패치	Ⅲ-1(P.15)
	(기타) 인터넷 브라우저 최신버전 업데이트	Ⅲ-4(P.30)
감염된 파일 또는 애플리케이션 다운로드를 통한 공격	사용자 보안 교육(토렌트 등 불법 자료공유 사이트에서 SW 다운로드 금지)	해당없음
	백신 설치 및 정기적인 업데이트	해당없음
	(OS) Windows 보안패치	Ⅲ-1(P.15)
	(기타) 인터넷 브라우저 최신버전 업데이트	Ⅲ-4(P.30)

2 내부 확산 유형 분석

□ SMB(Server Message Block) 취약점 이용 전파

SMB(Server Message Block)는 도스나 윈도우에서 파일이나 디렉토리 및 주변 장치들을 공유하는데 사용되는 메시지 형식이다. 랜섬웨어는 SMB 메시지를 대상 PC에 전송하여 취약점을 공격하고, 랜섬웨어를 전파한다. 의료ISAC 보안관제 현황을 보면 SMB를 이용하여 전파를 시도하는 악성코드가 가장 많이 탐지되고 있다.

WannaCry 랜섬웨어의 취약점 공격 흐름은 대상 PC의 취약 여부를 확인 후 취약하다고 판단되면 shell code를 전송하여 취약점 공격 및 악성코드 감염을 시도한다.



[그림 Ⅱ-6] WannaCry 랜섬웨어 SMB 취약점 공격 흐름 (출처:SOMANSA)

□ RDP(Remote Desktop Protocol) 이용한 전파

2019년에 발견된 BlueKeep취약점(CVE-2019-0708)은 WannaCry 랜섬웨어의 SMB 취약점을 이용해서 내부 단말에 랜섬웨어를 전파한 것과 동일한 기능을 하는 취약점이다. 윈도우 원격 데스크톱 서비스(RDP)를 이용해 정상적인 인증 단계를 거칠 필요 없이 원격에서 임의의 코드를 실행하는 취약점이다.

[그림 Ⅱ-7] RDP BlueKeep 취약점 작동 원리 (출처:의료ISAC)

RDP 취약점이 있을 경우 공격자가 이를 활용할 수 있지만 여러 사고사례에서 살펴보면 공격자가 RDP를 내부전파에 이용할 때는 계정탈취를 하여 정상적인 사용자로 로그인하여 랜섬웨어를 전파한다. 초기침투를 통해 내부거점을 확보한 공격자는 네트워크 탐색을 통해 내부 구성을 파악하고 외부에서 계정탈취를 위한 JexBoss(취약점 스캐너), Mimikatz(Windows 계정 탈취 도구) 등의 툴을 다운로드 받아 이를 사용한다. JexBoss는 Jboss 취약점 스캐너로 내부 내트워크 스캔을 통해 RDP포트가 열려있는 단말과 취약점을 스캔하고 얻은 정보를 바탕으로 무차별 대입 공격을 통해 계정 정보를 탈취 한다. Mimikatz는 Windows 취약점을 확인하기 위한 도구로 개발 되었으나 지금은 Windows 계정 탈취를 위한 악성코드로 많이 사용된다. 이렇게 얻은 계정정보를 통해 원격 접속하여 랜섬웨어 파일을 유포하여 실행한다.

[표 Ⅱ-2] 랜섬웨어 내부 확산유형 및 유형별 조치사항 (출처:의료ISAC)

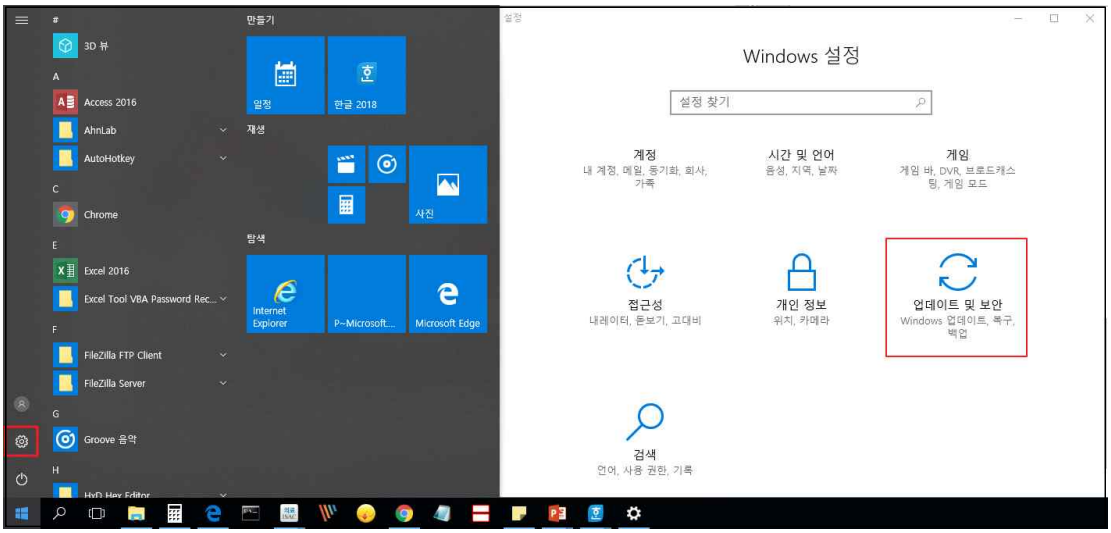
공격 형태	조치사항	관련 페이지
SMB(Server Message Block) 취약점 이용 전파	(OS) Windows 보안패치	Ⅲ-1(P.15)
	(OS) 파일공유(SMB) 서비스 기능 해제	Ⅲ-1(P.20)
	(네트워크) RDP, SMB 관련 포트 차단	Ⅲ-2(P.25)
	(보안장비) 방화벽 보안 조치	Ⅲ-3(P.28)
RDP(Remote Desktop Protocol) 이용한 전파	(OS) Windows 보안패치	Ⅲ-1(P.15)
	(OS) RDP 디폴트 포트 변경	Ⅲ-1(P.16)
	(OS) RDP 서비스 비활성화	Ⅲ-1(P.16)
	(OS) Windows 방화벽에서 RDP, SMB 서비스 접근 차단	Ⅲ-1(P.18)
	(네트워크) RDP, SMB 관련 포트 차단	Ⅲ-2(P.25)
	(보안장비) 방화벽 보안 조치	Ⅲ-3(P.28)

03 보안 대책

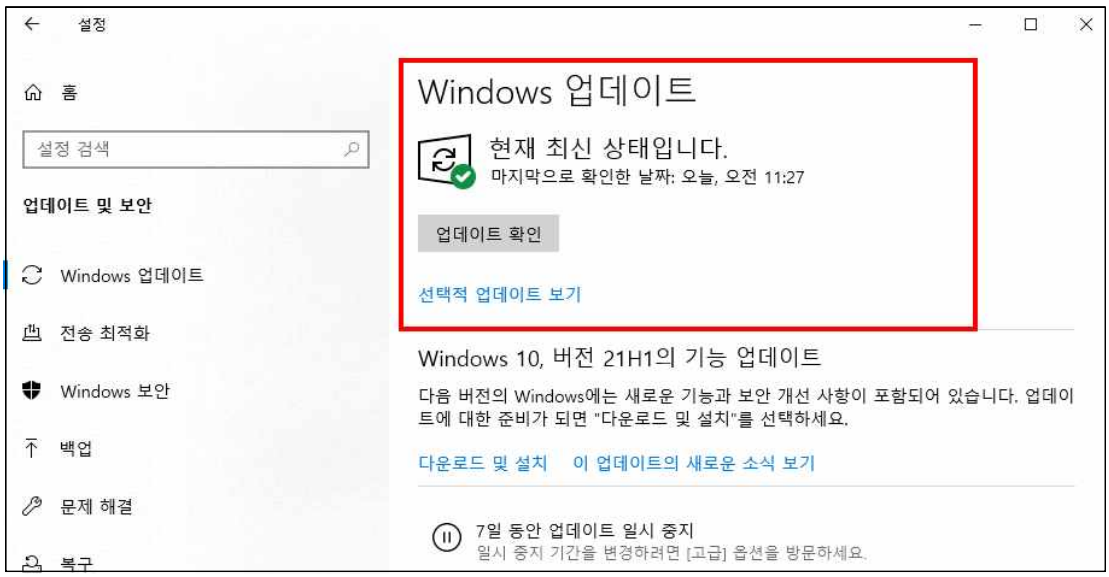
1 OS 보안설정

○ Windows 보안 최신 업데이트

▶ 시작 → 설정(⚙) → 업데이트 및 보안 → 윈도우 업데이트



[그림 Ⅲ-1] 윈도우 업데이트 화면 진입 (출처:의료ISAC)



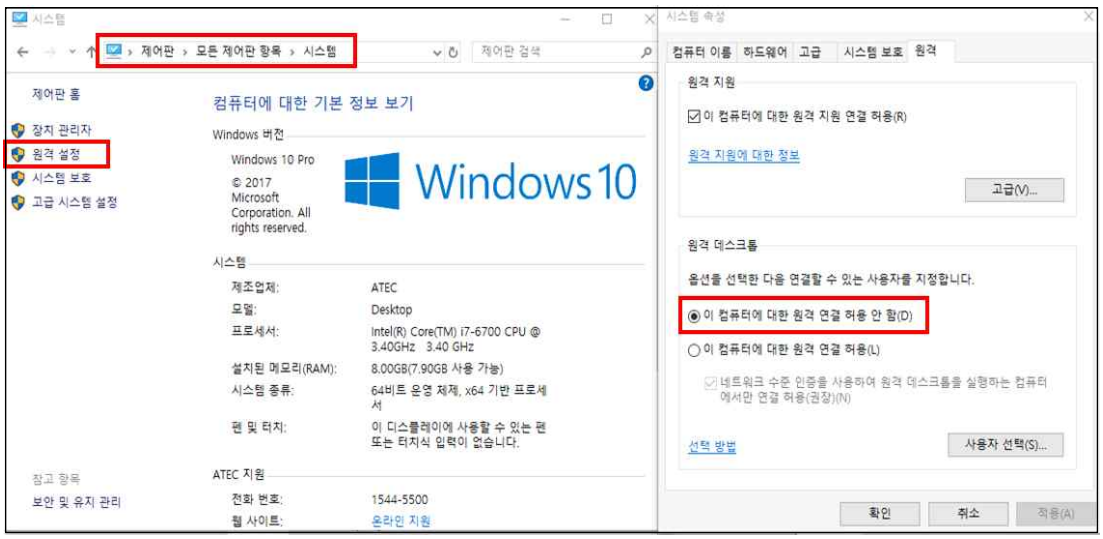
[그림 Ⅲ-2] [업데이트 확인] 후 최신버전이 아닐 경우 업데이트 진행 (출처:의료ISAC)

○ 원격 서비스 : 원격 데스크톱 프로토콜(RDP)

원격 데스크톱 프로토콜(RDP)을 사용하지 않는 일반 사용자는 비활성화하는 방법이 가장 효과적이지만 불가피하게 사용이 필요할 경우 보안대책을 강구한 후에 사용하여야 한다.

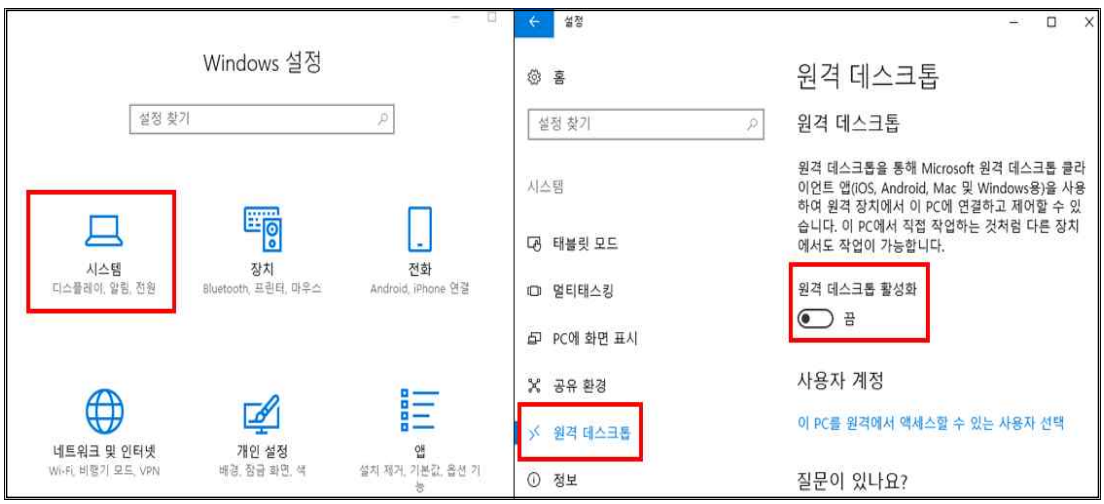
(1) RDP 서비스 비활성화 방법(2가지)

▶ 제어판 → 시스템 → 원격 설정 → 시스템 속성창의 원격 탭 → 원격 연결 허용 안 함



[그림 Ⅲ-3] RDP 서비스 비활성화 첫 번째 방법 (출처:의료ISAC)

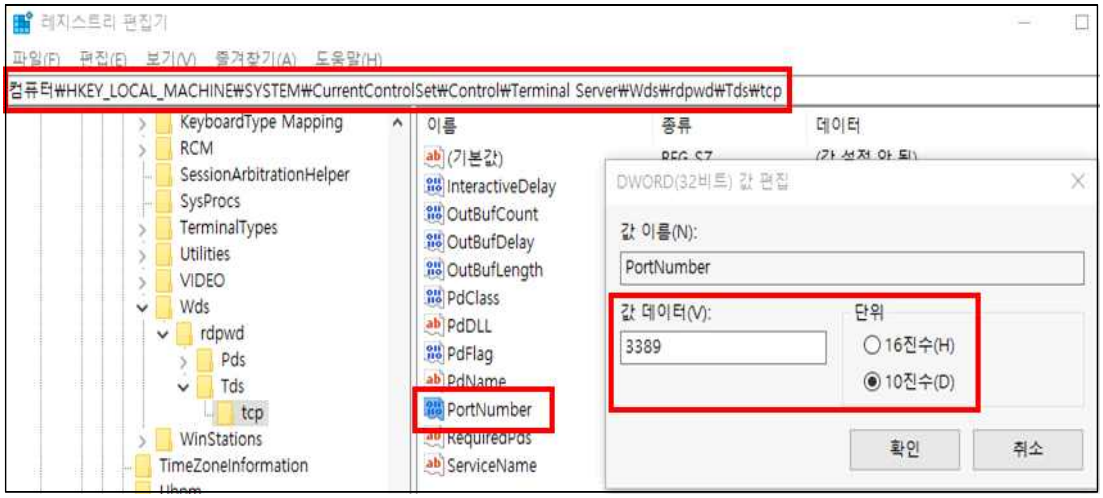
▶ 시작 → 설정(⚙) → 시스템 → 원격 데스크톱 → 원격 데스크톱 활성화 끔



[그림 Ⅲ-4] RDP 서비스 비활성화 두 번째 방법 (출처:의료ISAC)

(2) RDP 디폴트 포트 변경

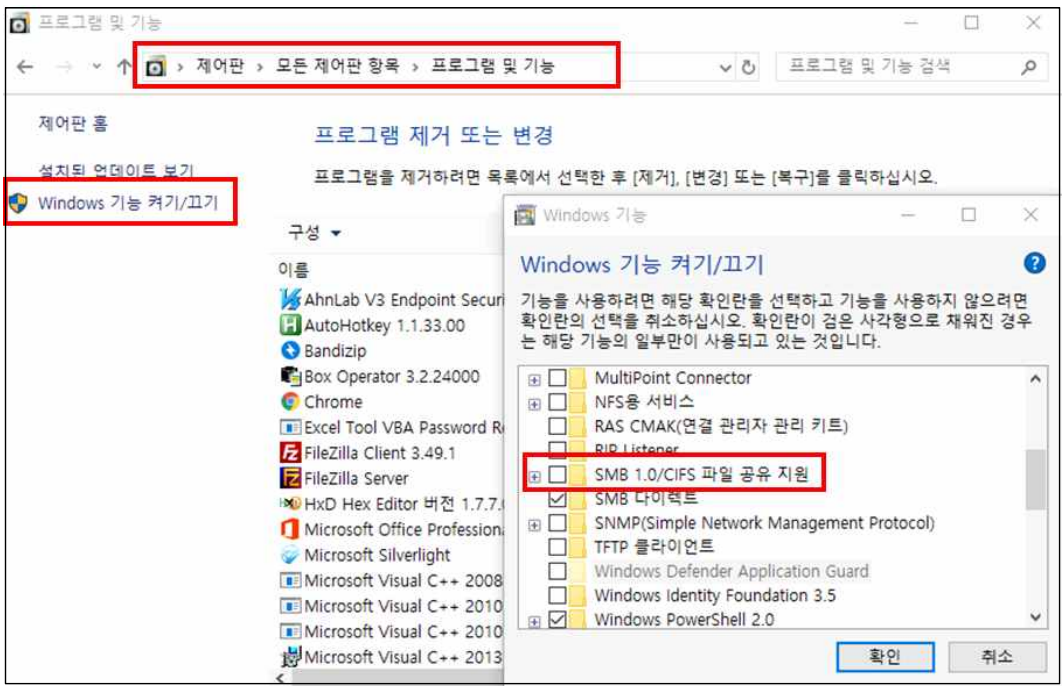
▶ 윈도우 키(⊞) + R → 실행 창에서 "regedit" 입력 → "HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩Terminal Server₩Wds₩rdpwd₩Tds₩tcp" 경로에서 [PortNumber]를 클릭 → 10진수 '3389'에서 다른 숫자로 변경



[그림 Ⅲ-5] 레지스트리에서 RDP 디폴트 포트 변경 설정 (출처:의료ISAC)

○ 파일공유(SMB) 서비스 기능 해제

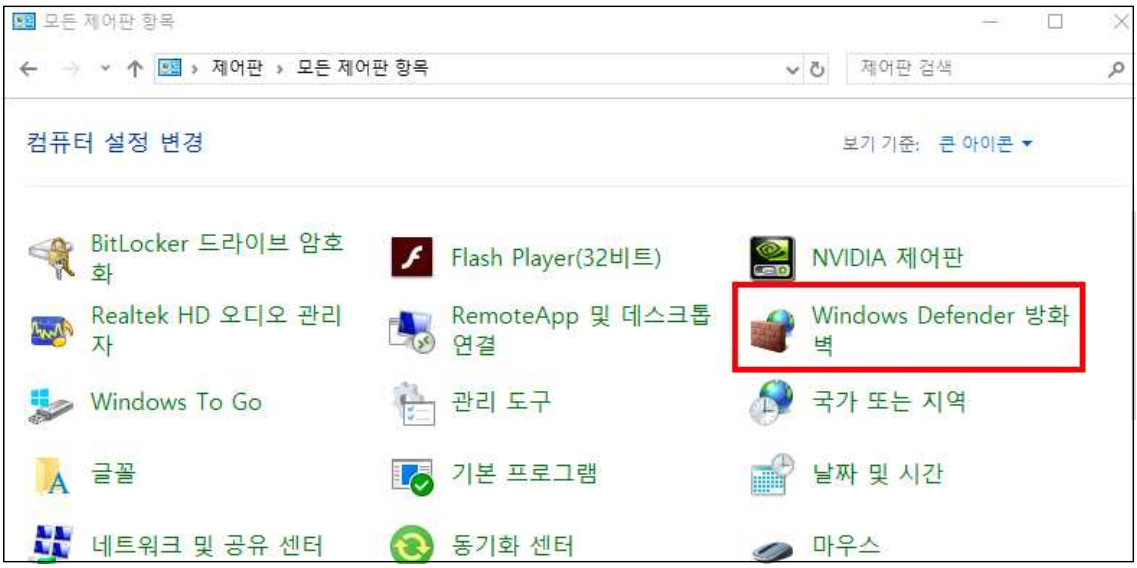
▶ 제어판 → 프로그램 및 기능 → Windows 기능 켜기/끄기 → "SMB 1.0/CIFS 파일 공유 지원" 기능 해제 → 확인 후 재부팅



[그림 Ⅲ-6] SMB관련 기능 해제 설정 (출처:의료ISAC)

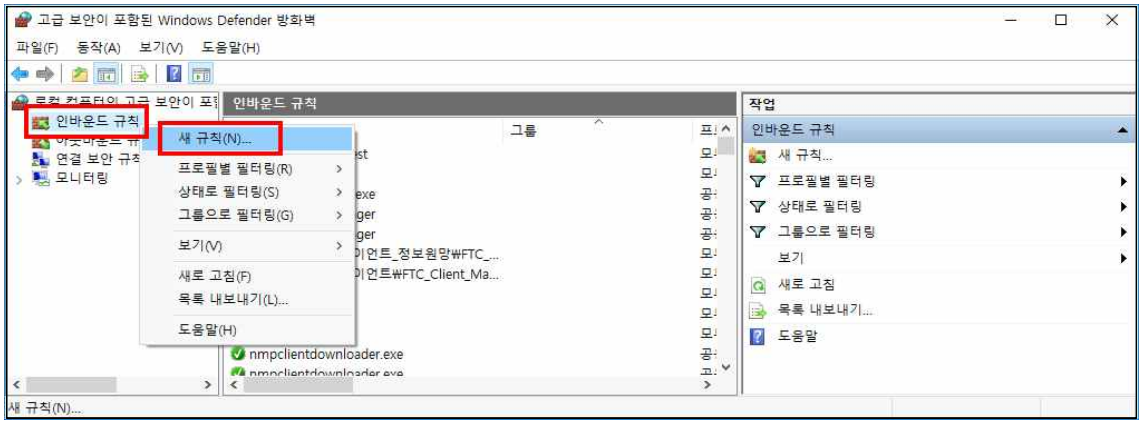
○ Windows 방화벽에서 RDP, SMB 서비스 접근 차단

▶ 제어판 → Windows Defender 방화벽 → 고급 설정 → '인바운드 규칙' 우클릭 후 '새규칙' 클릭 → 새 인바운드 규칙 마법사에서 '포트' 체크 → 'TCP, 특정 포털 포트' 체크 후 '139, 445, 3389' 입력 → '연결차단' 선택 → '도메인', '개인', '공용' 체크 → 이름을 'SMB, RDP 포트 차단' 입력

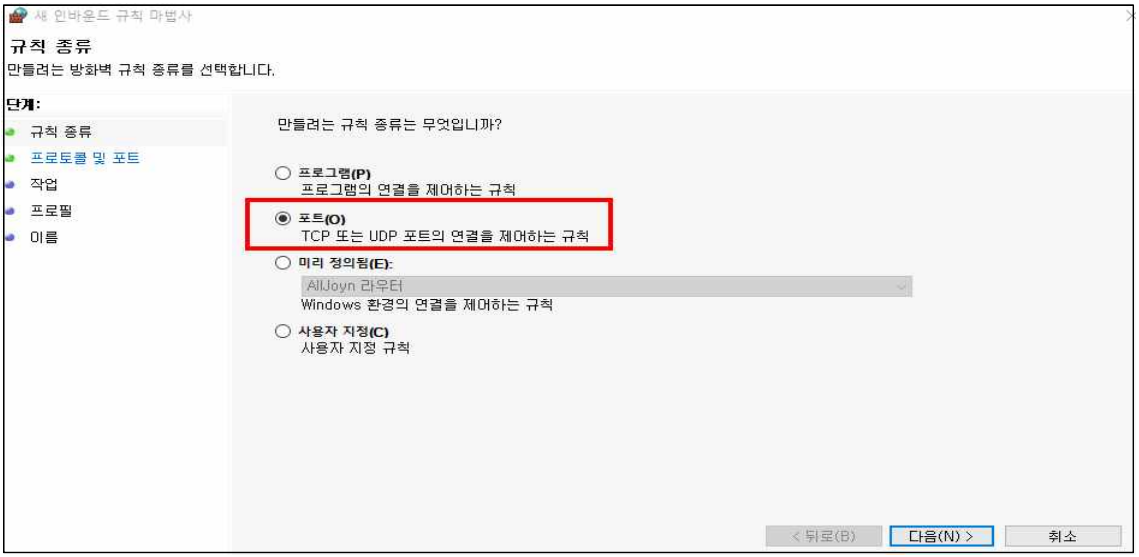


[그림 Ⅲ-7] Windows방화벽 설정 진입 (출처:의료ISAC)

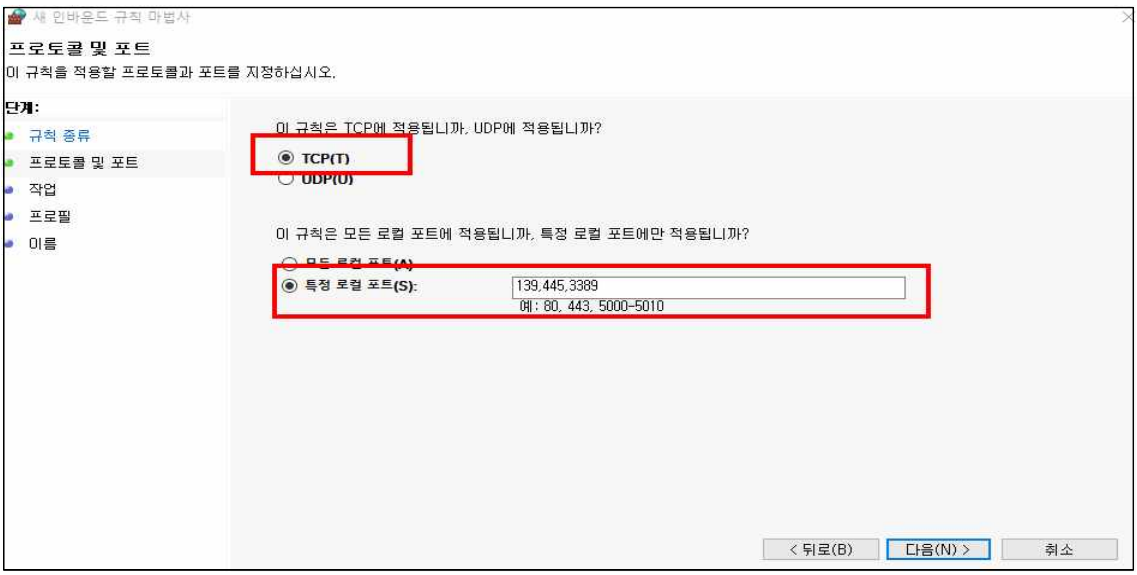
[그림 Ⅲ-8] Windows방화벽 고급 설정 진입 (출처:의료ISAC)



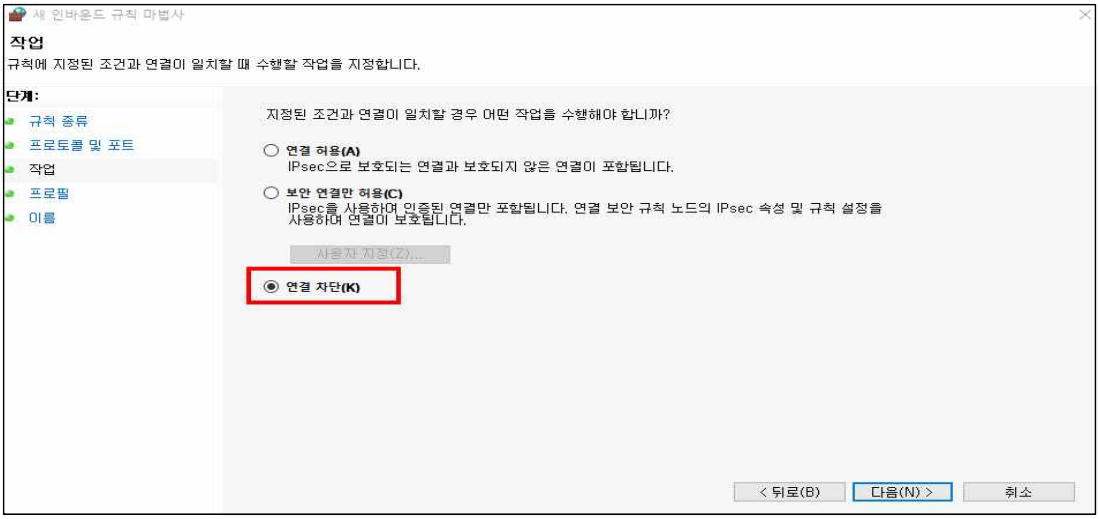
[그림 Ⅲ-9] Windows방화벽 인바운드 규칙에서 새 규칙 설정 (출처:의료ISAC)



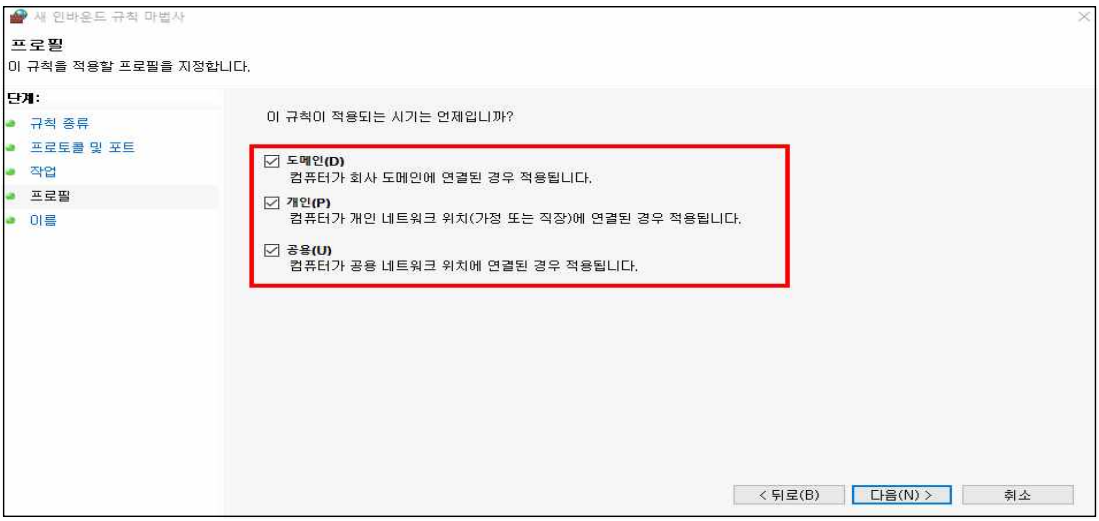
[그림 Ⅲ-10] 규칙 종류에서 포트 선택 (출처:의료ISAC)



[그림 Ⅲ-11] 프로토콜 및 포트에서 TCP선택, 차단할 포트 기입 (출처:의료ISAC)



[그림 Ⅲ-12] 작업에서 '연결 차단' 선택 (출처:의료ISAC)

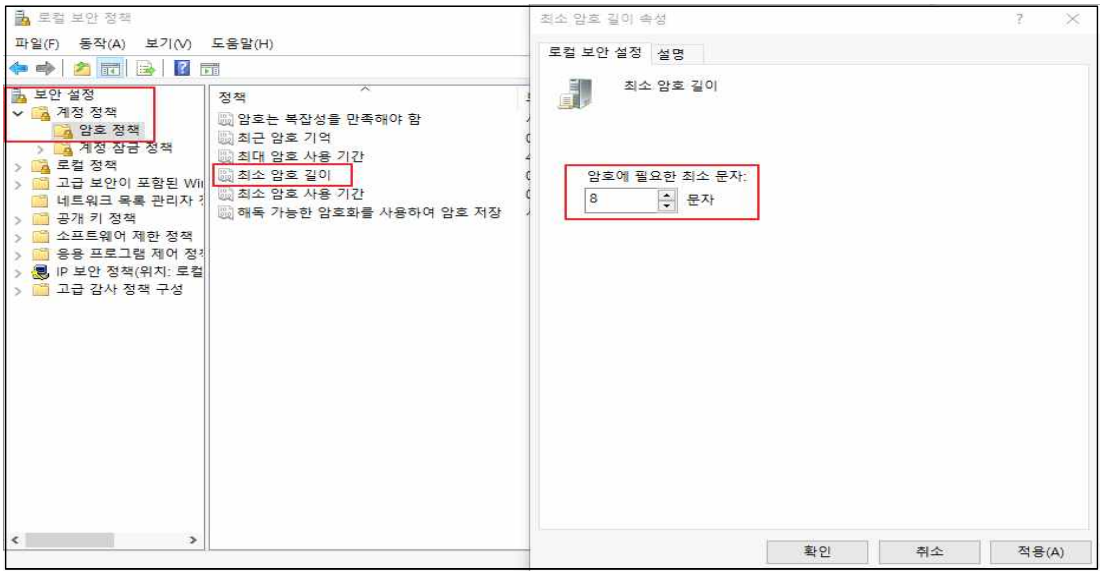


[그림 Ⅲ-13] 프로필에서 전부 선택 (출처:의료ISAC)

[그림 Ⅲ-14] 규칙 이름 기입 (출처:의료ISAC)

○ 패스워드 복잡성 설정

▶ 윈도우 키(⊞) + R → 실행 창에서 'SECPOL.MSC' 입력 → 계정 정책 → 암호 정책 → 최소 암호 길이 8문자로 설정

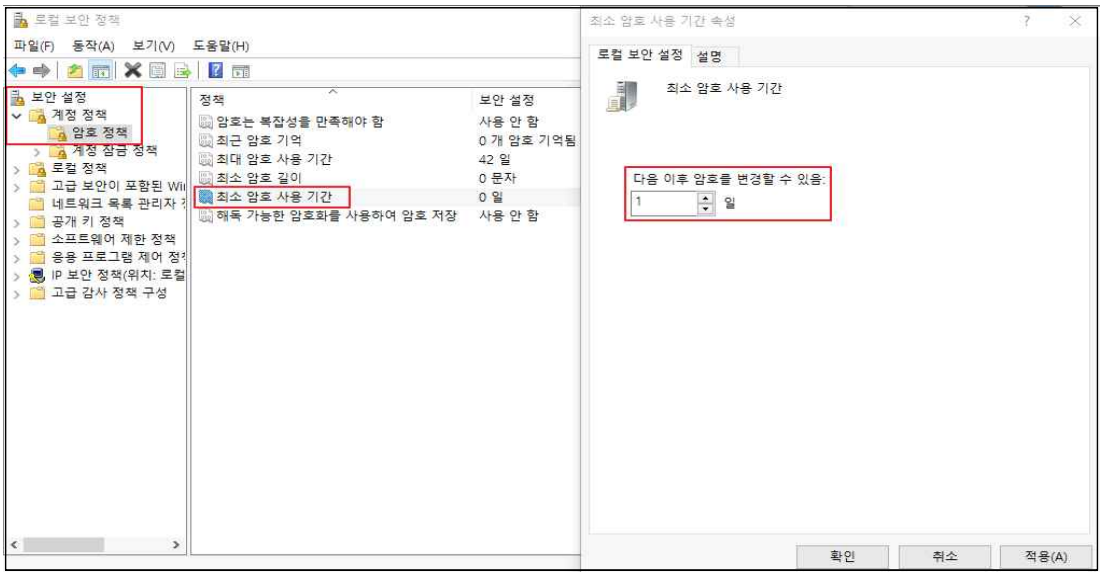


[그림 Ⅲ-15] 패스워드 복잡성 설정 (출처:의료ISAC)

○ 패스워드 최소, 최대 사용 기간 설정

(1) 패스워드 최소 사용기간 설정

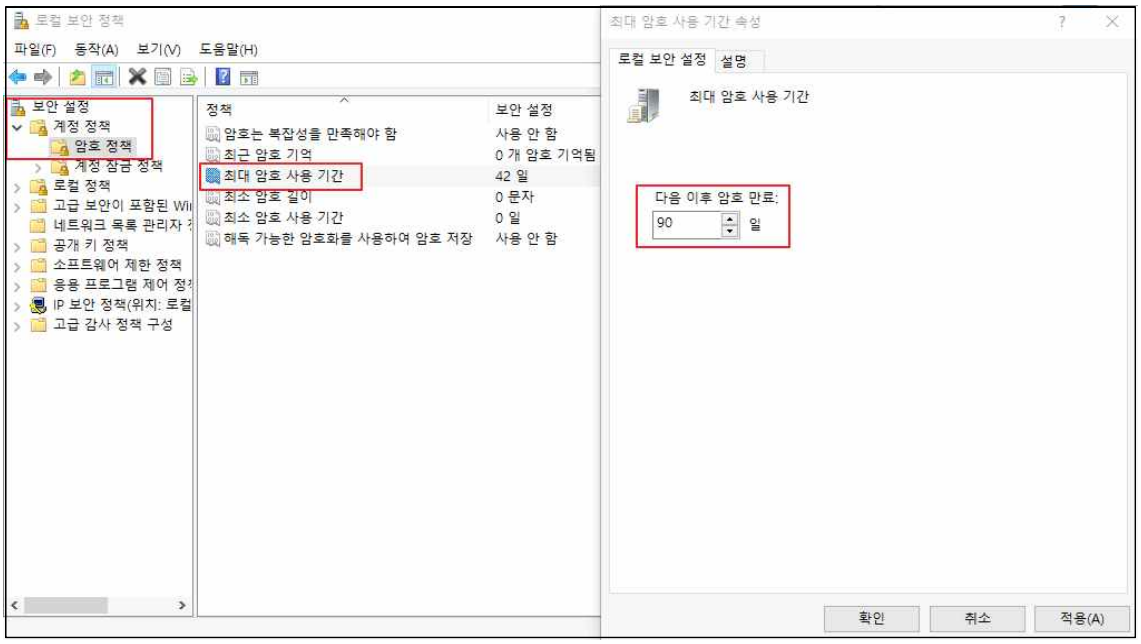
▶ 윈도우 키(⊞) + R → 실행 창에서 'SECPOL.MSC' 입력 → 계정 정책 → 암호 정책 → 최소 암호 사용기간 → 1일로 설정 변경



[그림 Ⅲ-16] 패스워드 최소 사용 기간 설정 (출처:의료ISAC)

(2) 패스워드 최대 사용 기간 설정

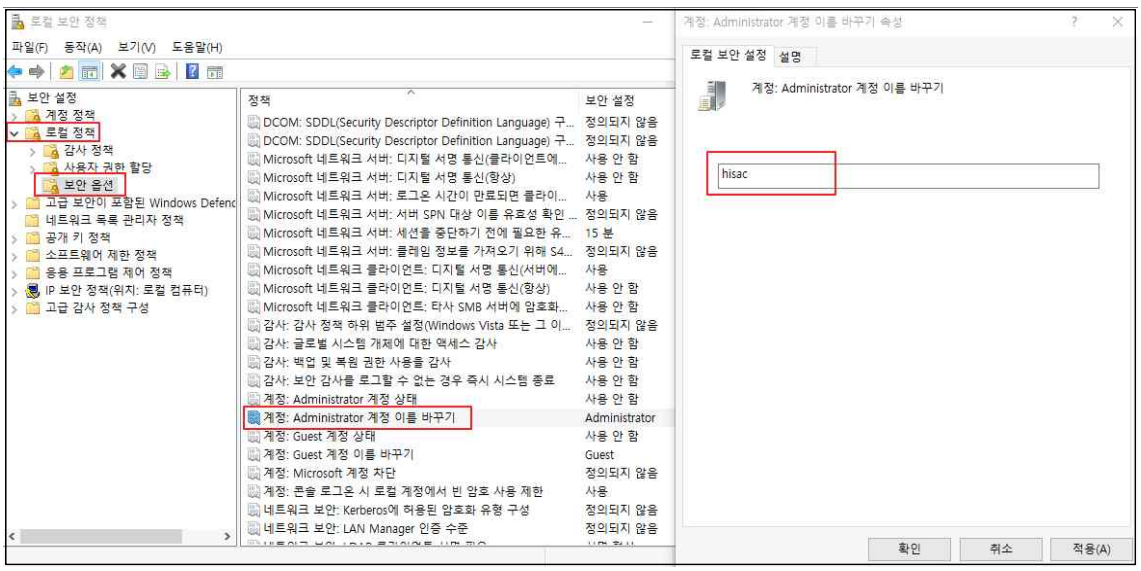
▶ 윈도우 키(⊞) + R → 실행 창에서 'SECPOL.MSC' 입력 → 계정 정책 → 암호 정책 → 최대 암호 사용 기간 → 90일로 설정 변경



[그림 Ⅲ-17] 패스워드 최대 사용 기간 설정 (출처:의료ISAC)

○ 유추하기 쉬운 계정명 변경 : Administrator Default 계정 이름 변경 설정

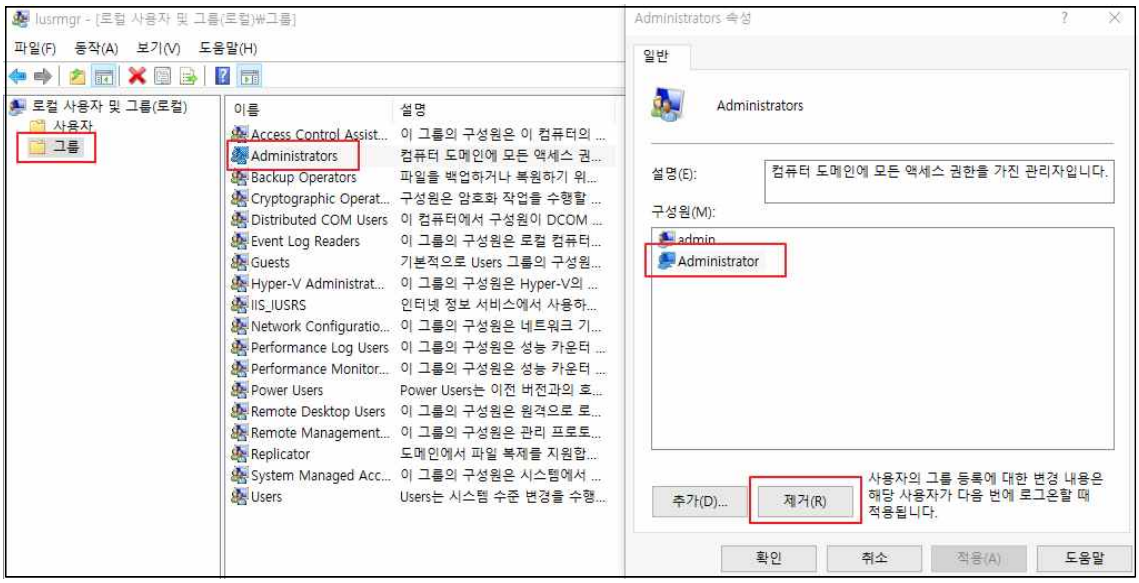
▶ 시작 → Windows시스템 → 제어판 → 관리 도구 → 로컬 보안 정책 → 로컬 정책 → 보안 옵션 → Administrator 계정 이름 바꾸기



[그림 Ⅲ-18] Administrator Default 계정명 변경 (출처:의료ISAC)

○ 관리자 그룹에 최소한의 사용자만 포함

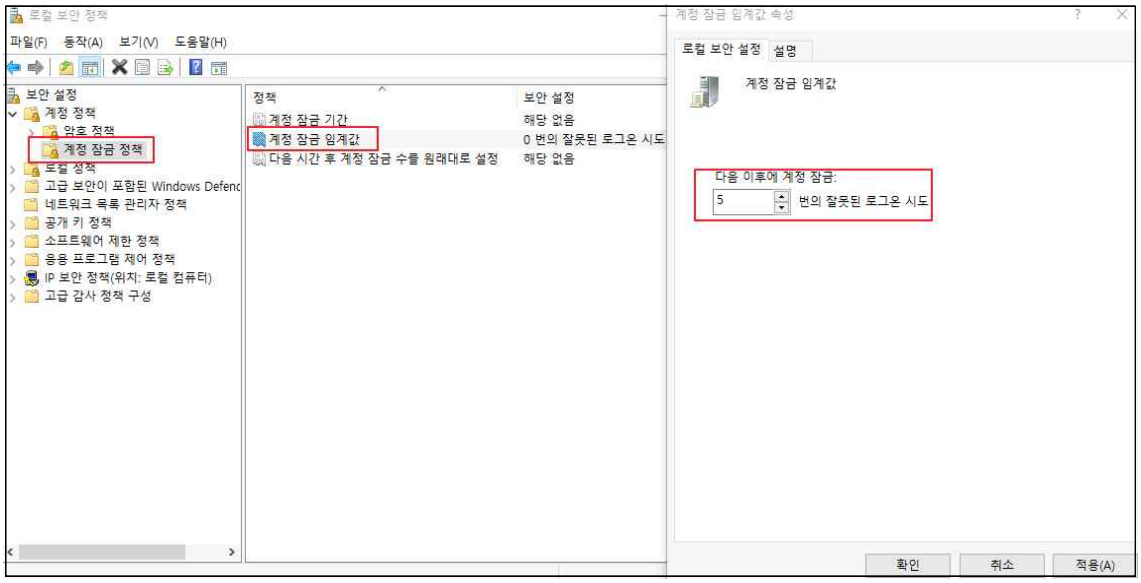
▶ 시작 → 실행 → LUSRMGR.MSC → 그룹 → Administrators 속성 → Administrators 그룹에서 불필요한 계정 제거 후 그룹 변경



[그림 Ⅲ-19] 관리자 그룹에 불필요 계정 제거 (출처:의료ISAC)

○ 로그인 시도 임계값 설정

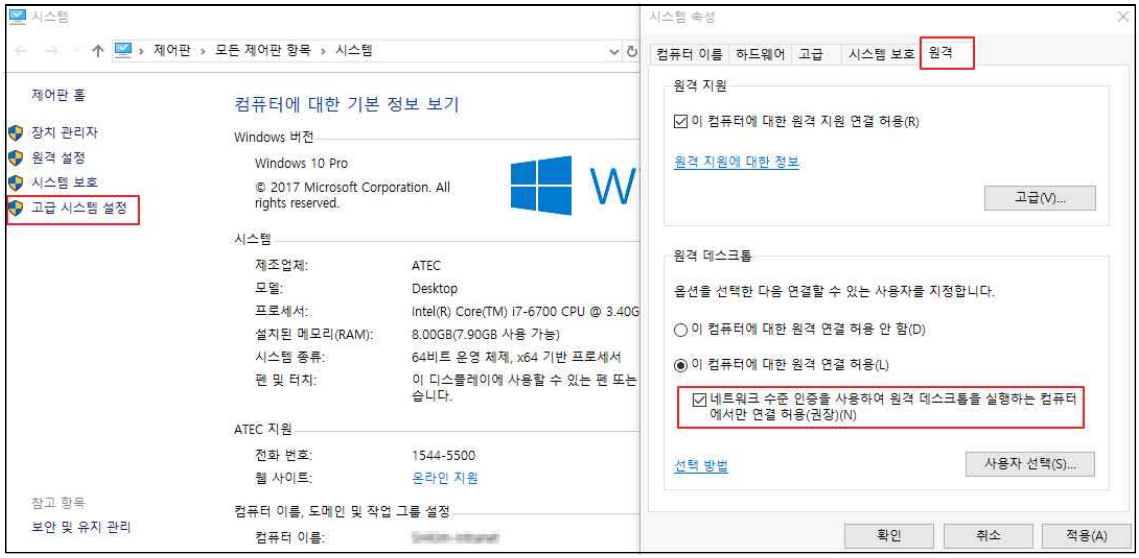
▶ 윈도우 키(⊞) + R → 실행 창에서 'SECPOL.MSC' 입력 → 계정 정책 → 계정 잠금 정책 → 계정 잠금 임계값 → 5번 이하 값으로 설정



[그림 Ⅲ-20] 로그인 시도 임계값 설정 (출처:의료ISAC)

○ NLA(Network level authentication) 사용

▶ 윈도우 키(⊞) + X → 시스템 → 정보 → 시스템 정보 → 고급 시스템 설정 → "네트워크 수준 인증을 사용하여 원격 데스크톱을 실행하는 컴퓨터에서만 연결 허용" 체크



[그림 Ⅲ-21] 네트워크 수준 인증(NLA) 사용 설정 (출처:의료ISAC)

2 네트워크 장비 보안설정

○ 공유기 보안정책 설정

소규모 의료기관이나 기업에서는 별도의 방화벽(Firewall)과 같은 보안장비를 운영하지 않고 공유기만으로 인터넷을 사용할 수 있다. 그러면 보안관리가 미흡하여 랜섬웨어에 쉽게 감염될 수 있으므로 최상단에 설치된 공유기에서 랜섬웨어 공격과 관련된 서비스를 차단하는 등의 보안설정을 통해 랜섬웨어를 예방할 수 있다.

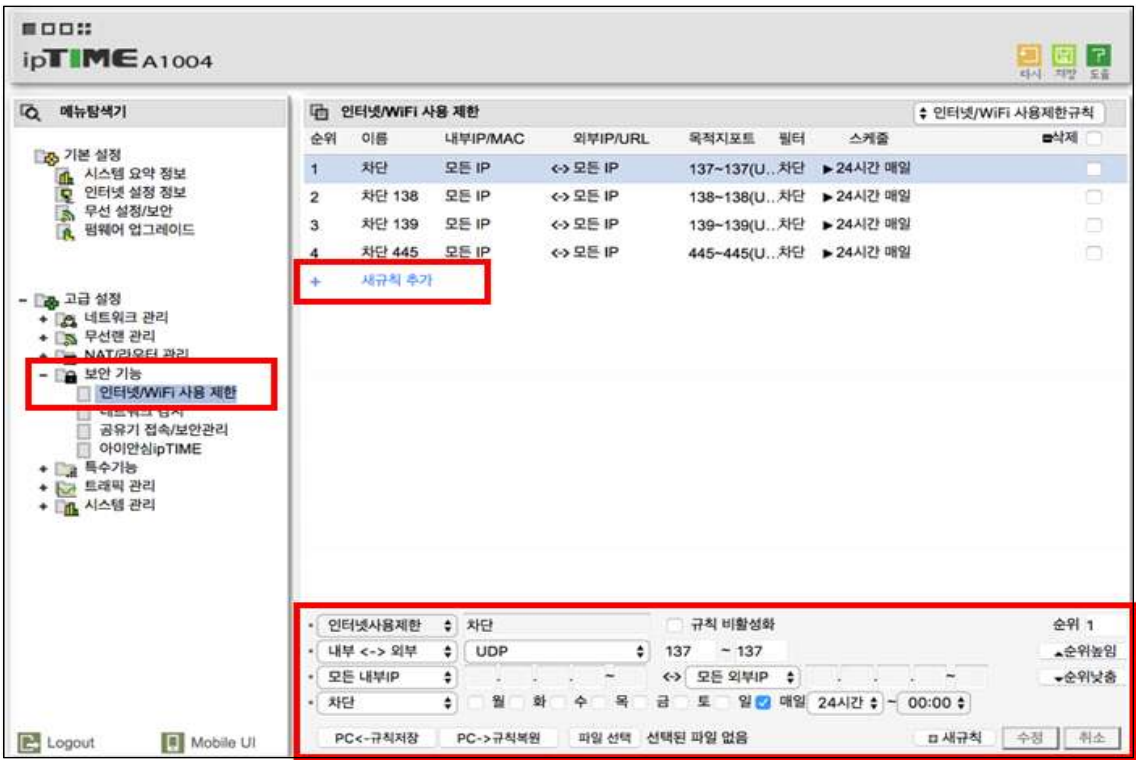
(1) 공유기에서 RDP, SMB관련 포트 차단하기(iptime 기준)

▶ 웹브라우저 → 공유기 IP 입력 → 관리자 계정으로 로그인

※ 관리자 IP 주소와 관리자 계정은 공유기에 따라 상이하기 때문에 설명서를 참고

[그림 Ⅲ-22] 공유기(iptime) 로그인 화면 (출처:KISA)

▶ 보안 기능 → 인터넷/WIFI 사용 제한 → 새규칙 추가 → 정책 설정 후 적용



[그림 Ⅲ-23] 공유기 새규칙 추가 설정 화면 (출처:milkissboy.tistory.com)

▶ 정책설정시 규칙 이름, 방향성, TCP/UDP 프로토콜, 포트넘버, IP주소, 차단/허용 등 세부 정책 설정 후 적용

[그림 Ⅲ-24] 공유기 특정 포트 차단 규칙 설정 (출처:milkissboy.tistory.com)

○ 공유기 네트워크 감시 분석기능 설정

네트워크 감시는 내부 네트워크에 연결되어 있는 모든 단말기 중 트래픽을 유발하거나 웜 바이러스 통신을 할 때, 해당 단말기를 차단하고 관리자에게 내역을 통보하는 기능이다.

▶ 관리자 페이지 접속 → 고급 설정 → 보안 기능 → 네트워크 감시 → *네트워크 감시 설정 → 적용 → 네트워크 감시 내역 확인

※ 네트워크 감시 설정

- 동작 설정 : 실행
- 감시 대상 : 알려진 웜 바이러스 통신
- 감시 수준 : 보통
- 감지된 통신차단 : 예

[그림 Ⅲ-25] iptime 공유기 네트워크 감시 설정 화면 (출처:dazemonkey.tisory.com)

3 보안장비 정책설정

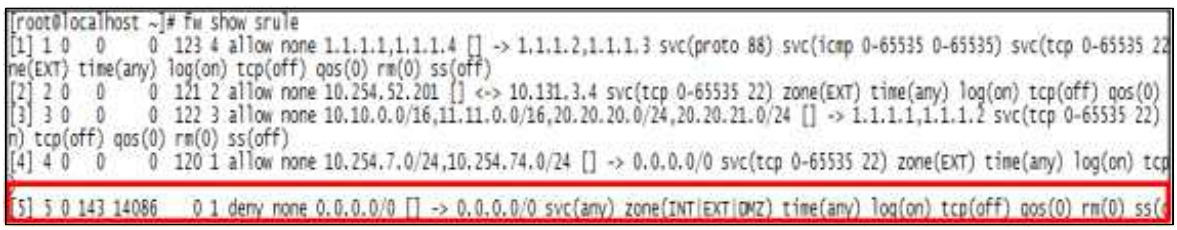
○ 방화벽(Firewall) 장비 보안 정책 설정

방화벽 정책은 우선순위가 존재하며 'Top-Down' 방식으로 정책 리스트에서 위쪽에 있을수록 정책의 우선순위가 있다. 대부분의 방화벽 정책의 마지막에는 외부에서 모든 접근을 차단하는 정책으로(Any → Any, 거부) 설정 화면에 보이지 않더라도 해당 정책을 기본탑재하고 있는 경우가 있으니 확인해야 하며 없을 경우 해당 규칙을 마지막 부분에 추가하여 내부 네트워크로 불필요한 접근을 차단하여야 한다.

[표 Ⅲ-1] 방화벽 장비 기본 정책 예시 (출처:의료ISAC)

출발지 주소	출발지 포트	목적지 주소	목적지 포트	정책
외부	Any	메일서버	TCP_25(SMTP)	허용
외부	Any	홈페이지서버	TCP_80(HTTP)	허용
Any	Any	Any	Any	거부

[그림 Ⅲ-26] Secui社 MF2 방화벽 정책 설정 화면 (출처:Secui)



[그림 Ⅲ-27] 마지막에 모든 접근 차단 정책(Any → Any, Deny) 탑재 (출처:Secui)

(1) 외부에서 접근하는 원격 접속 포트 차단

원격 접속 포트가 방화벽 기본정책에 의해 차단되지 않을 경우 아래와 같이 규칙을 추가할 수 있다. RDP 터널링 공격처럼 내부에서 외부로(리버스 방식) 접속할 수 있기 때문에 양방향 규칙으로 설정하는 것도 검토 해봐야 한다.

[표 Ⅲ-2] 방화벽 RDP, 원격 접속 포트 차단 정책 (출처:의료ISAC)

양방향	출발지 주소	목적지 주소	목적지 포트	정책
☑	외부	내부 호스트	TCP_3389	Deny
☑			TCP_21	
☑			TCP_22	
☑			TCP_23	

(2) SMB 포트 차단

SMB포트를 통해 랜섬웨어가 전파 되는 것을 방지하기 위해 TCP 445, 139포트가 기본정책에 의해 차단되지 않을 경우 아래와 같이 규칙을 추가할 수 있다.

[표 Ⅲ-3] 방화벽 SMB관련 포트 차단 정책 (출처:의료ISAC)

양방향	출발지 주소	목적지 주소	목적지 포트	정책
☑	외부	내부 호스트	TCP_445	Deny
☑	외부	내부 호스트	TCP_139	Deny

(3) 내부에서 전파하는 원격 접속/SMB 포트 차단

내부에서 사용하는 PC가 랜섬웨어에 감염되면 감염된 PC를 거점으로 하여 피해를 확산시키기 위해 주변 단말기로 악성코드를 전파 시도를 할 경우를 대비하기 위해 내부에서 시작되는 원격접속 및 SMB관련 포트를 차단하기 위한 정책이 필요하다.

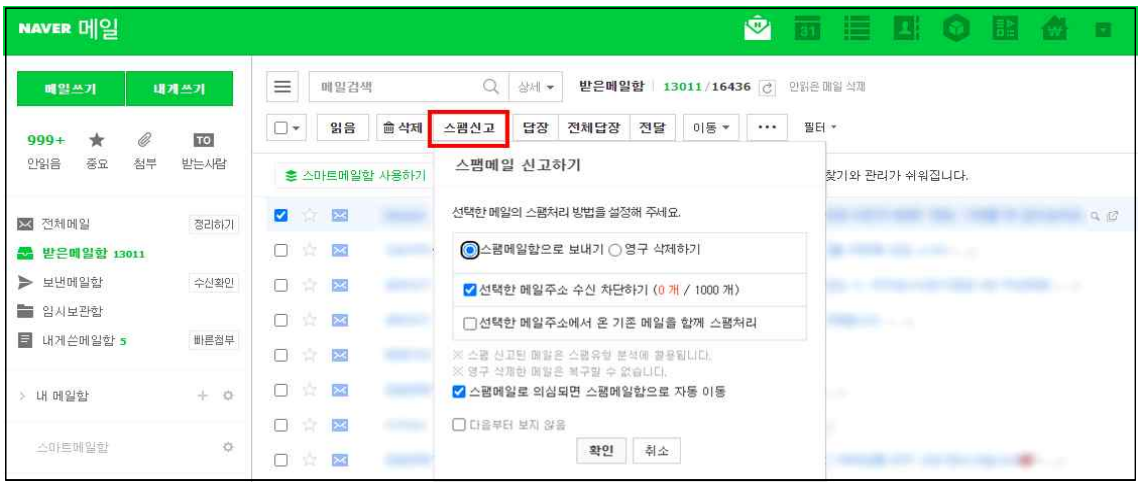
[표 Ⅲ-4] 방화벽 내부에서 전파하는 원격접속/SMB관련 포트 차단 정책 (출처:의료ISAC)

양방향	출발지 주소	목적지 주소	목적지 포트	정책
☑	내부	All	TCP_445	Deny
☑	내부	All	TCP_139	Deny
☑	내부	All	TCP_3389	Deny
☑	내부	All	TCP_21	Deny
☑	내부	All	TCP_22	Deny
☑	내부	All	TCP_23	Deny

4 기타 보안설정

○ 피싱의심 메일 수신시 스팸메일 신고 기능 사용

피싱 또는 스팸 의심메일을 수신했을 경우 신고할 메일을 선택한 뒤 스팸신고 기능을 사용하면 신고된 메일은 스팸 메일함으로 이동하고 메일을 보낸 발송인의 메일 주소는 수신차단 목록에 추가 된다. 아래 그림은 네이버 메일함의 스팸신고 기능이며 다른 웹메일 시스템에도 유사한 기능이 있으므로 이를 활용할 수 있다.

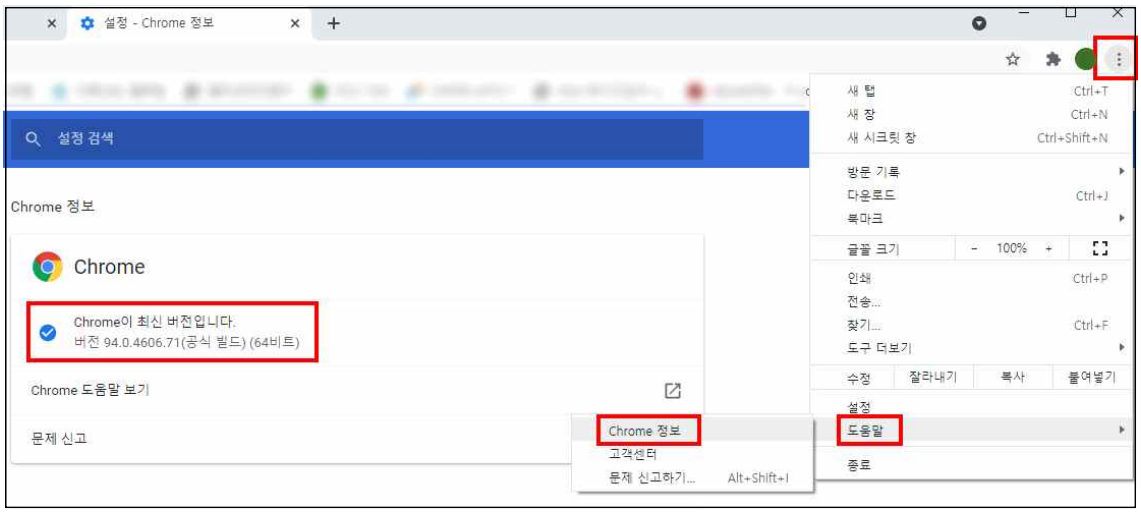


[그림 Ⅲ-28] 네이버 메일함내 스팸신고 기능 (출처:의료ISAC)

○ 웹브라우저 최신 버전 업데이트

(1) Chrome브라우저

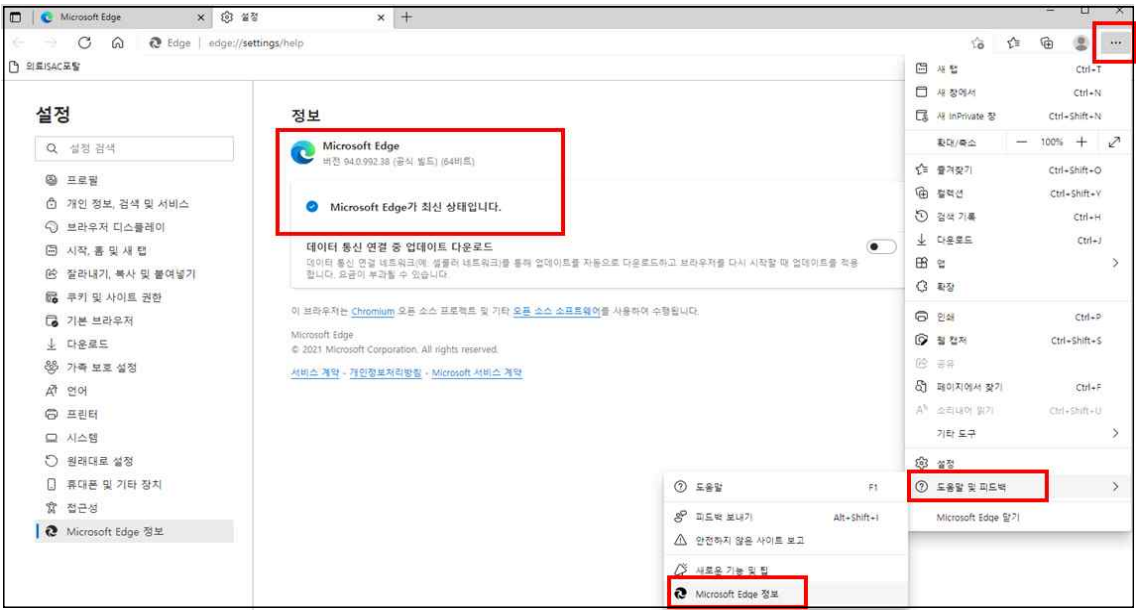
▶ Chrome 웹브라우저 실행 → 오른쪽 상단에 '더보기'(⋮) 클릭 → '도움말' > 'Chrome정보' 클릭 → 버전 확인 및 업데이트



[그림 Ⅲ-29] Chrome 브라우저 최신 버전 업데이트 화면 (출처:의료ISAC)

(2) Microsoft Edge 브라우저

▶ Edge 웹브라우저 실행 → 오른쪽 상단에 '더보기'(…) 클릭 → '도움말 및 피드백' > 'Microsoft Edge 정보' 클릭 → 버전 확인 및 업데이트

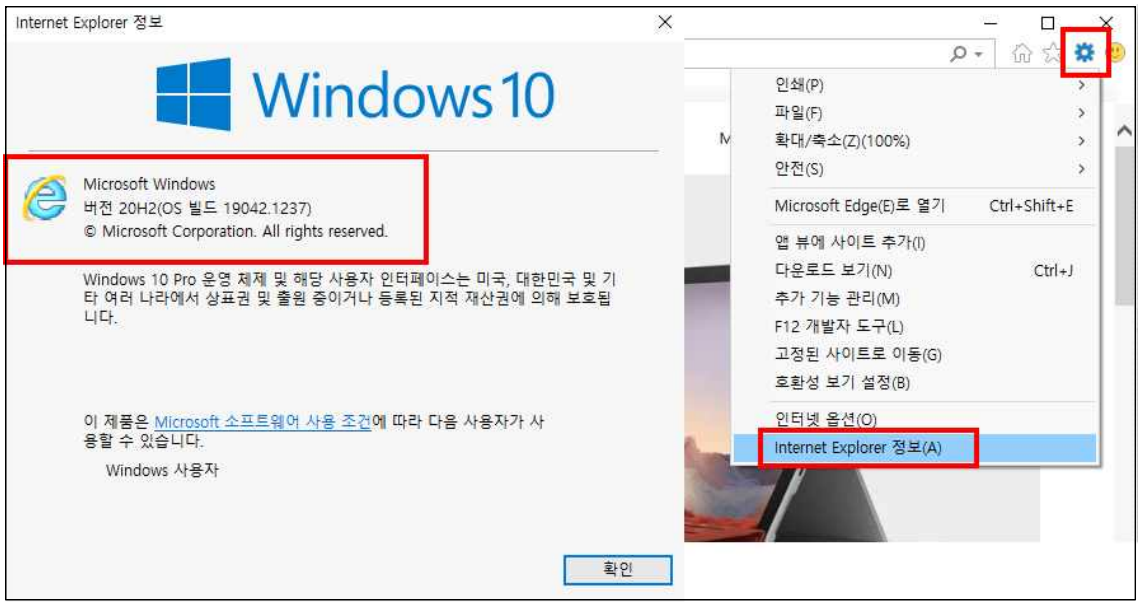


[그림 Ⅲ-30] MS Edge 브라우저 최신 버전 업데이트 확면 (출처:의료ISAC)

(3) Internet Explorer 브라우저

▶ Explorer 브라우저 실행 → 오른쪽 상단에 '설정'(⚙) 클릭 → 'Internet Explorer 정보' 클릭 → 버전 확인 및 업데이트

※ Explorer는 '22년 6월 15일부 기술지원 종료 예정으로 다른 브라우저 사용 권고



[그림 Ⅲ-31] Internet Explorer 브라우저 최신 버전 업데이트 확면 (출처:의료ISAC)

04 참고 문헌

1. https://www.infosecurity-magazine.com/news/half-us-hospitals-shut-networks/
2. https://www.theverge.com/2021/8/19/22632378/pandemic-ransomware-health-risks
3. https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority
4. https://csrc.nist.gov/glossary/term/defense_in_depth
5. https://www.ciatec.com/2018/03/defense-in-depth-a-layered-strategy-can-repel-the-hordes-of-hackers/
6. https://www.imperva.com/learn/application-security/defense-in-depth/
7. https://kr.sentinelone.com/blog/7-common-ways-ransomware-can-infect-your-organization/
8. https://nevertrustbrutus.tistory.com/212
9. https://milkissboy.tistory.com/56
10. https://cybersecurityworks.com/blog/cyber-risk/do-vpns-have-our-back.html
11. https://www.briskinfosec.com/blogs/blogsdetail/Will-your-backups-protect-you-against
12. https://www.somansa.com/wp-content/uploads/2017/06/20170608_report_2.pdf
13. https://www.krcert.or.kr/data/reportView.do?bulletin_writing_sequence=35560&queryString=cGFnZT0yJnNvcnRfY29kZT0mc29ydF9jb2RlX25hbWU9JnNlYXJjaF9zb3J0PXRpdGxlX25hbWUmc2VhcmNoX3dvcmQ9
14. https://www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=1&mode=view&p_No=259&b_No=259&d_No=115&ST=T&SV=
15. https://m.blog.naver.com/PostView.nhn?isHttpsRedirect=true&blogId=jstour78&logNo=221005798723