https://doi.org/10.7840/kics.2022.47.11.1932

랜섬웨어 피해 확산에 따른 국가 사이버안보정책 개선방안

김 진 민•, 권 대 현*, 주 승 현*, 신 용 태°

A Study on the Improvement of the National Cyber Security Policy Against the Spread of Ransomware Damage

Jinmin Kim•, Daehyun Kwon*, Seunghyun Joo*, Yongtae Shin°

요 약

4차 산업혁명 시대가 도래하며 경제·사회의 모든 영역이 사이버공간과 연결되고 있다. 이런 가운데 2017 '워너크라이' 랜섬웨가 등장하였고 2021년에는 미 '콜로니얼파이프' 사가 랜섬웨어에 감염되어 미 동부지역 에너지 공급이 중단된 사건도 있었다. 이렇게 전 세계적으로 확산되고 있는 랜섬웨어의 피해는 단순히 기술적 보안의 문제를 넘어서 국가 사이버안보에 심각한 영향을 주고 있다. 또한, 최근에는 개인이나 해킹 그룹이 주도하던 사이버공격이 국가 배후 해킹조직으로 확산되며 점차 조직화·지능화되고 있어 대규모 사회적 피해가 우려되는 실정이다. 그러나 기존의 연구는 랜섬웨어라는 악성코드의 기술적 분석에만 치중하여 '랜섬웨어가 국가안보에 어떤 영향을 주고 있는가?' 라는 물음에서 시작되는 거시적인 차원의 정책연구가 부족하였다. 이에 본 논문에서는 최근 국내·외 주요 랜섬웨어 피해사례 및 현황을 살펴보고 가상화폐, 다크앱시장 등이 랜섬웨어 확산에 어떤 영향을 주었는지 분석한 후 주요 선진국 및 우리의 랜섬웨어 대응 정책을 비교함으로써 우리나라 사이버안보 수준을 높이기 위한 정책 개선방안을 제시하였다.

Key Words : Ransomware, Cybersecurity, Security policy, Hacking, Cryptocurrency, Dark web

ABSTRACT

With the advent of the 4th Industrial Revolution, all areas of economy and society are being connected to cyberspace. In the meantime, 2017 "WannaCry" ransomware appeared1, the U.S. "Colonial Pipe" was infected with ransomware in 2021. and energy supply to the eastern U.S. was suspended. The damage to ransomware, which is spreading around the world, is having a serious impact on national cybersecurity beyond just a technical security problem. In addition, cyberattacks led by hacking organizations behind the state and are gradually being organized and intelligent, which is feared to cause massive social damage. However, the existing research focused only on the technical analysis of malicious code, and there was a lack of macro-level policy research starting with with the question, "How is ransomware affecting national security?" In this paper, we presented a policy improvement plan to increase the level of cybersecurity in Korea by comparing the ransomware response policies of major developed countries and Korea after examining the recent major ransomware damage cases, in-depth analysis of how cryptocurrency and dark app markets affected the spread of ransomware.

• First Author : Graduate School of IT Policy and Management, Soongsil University, cyberkim@soongsil.ac.kr, 정회원
° Corresponding Author : Professor, Soongsil University, shin@ssu.ac.kr, 정회원
* Graduate School of IT Policy and Management, Soongsil University, daehyunka@ls-electric.com; shjoo@ncsoft.com
논문번호 : 202208-157-0-SE, Received July 25, 2022; Revised August 22, 2022; Accepted September 1, 2022

Ⅰ. 서 론

4차 산업혁명 시대가 도래하며 IT 기술의 유례 없는 빠른 발전으로 인해 경제·사회 전 분야에서 스마트화가 진행되고 있다. 사람과 기기들이 네트워크에 연결되며 사회의 전 영역이 사이버공간과 연결되어 사이버세계와 현실세계가 하나로 결합하고 있다. 그러나 사이버공간이 이렇게 확대됨에 따라 사이버공격에 노출되는 기기 또한 증가하고 있으며 전통적인 산업기술과 IT기술이 융합됨에 따라 국가의 모든 영역이 사이버 위협의 대상이 되었다. 특히 랜섬웨어 공격과 같은 경제적인 이득을 목적으로 하는 해킹이 급부상함에 따라 개인과 기업, 국가·공공기관의 피해가 큰 폭으로 증가하고 있다.

이런 환경에서 국내에서는 2021년 한국원자력연구원이 북한으로 추정되는 국가 배후 해킹조직에 의해 공격받아 연구 기밀자료를 절취당했을 뿐만 아니라 우리나라를 대표하는 대표 방산기업인 한국항공우주산업(KAI)·대우조선해양·핵융합에너지연구원 등이 추가로 해킹에 노출되어 사회적으로 큰 문제가 되었다[1]. 해외에서도 2017년 나타나 전 세계로 순식간에 확산된 '워너크라이' 랜섬웨어를 필두로 2021년 미국 동남부의 에너지 기반시설을 운영하는 '콜로니얼 파이프'사가 랜섬웨어 공격을 받아 에너지 공급이 멈추는 등 랜섬웨어에 의한 피해가 하나의 국가를 넘어 전 세계에 그 영향을 주고 있다.

이렇게 전 세계적으로 급격히 확산되고 있는 랜섬웨어의 피해가 이제는 단순히 기술적인 IT보안의 문제를 넘어서 국가안보, 국가 사이버안보에 심각한 영향을 주고 있다. 예전에는 개인이나 일부 해킹 그룹이 주도하던 사이버공격이 국가가 배후가 된 해킹조직이나 범죄단체로까지 확산되며 점차 조직화·대규모화되고 있으며 이로 인해 대규모 사회적 피해와 함께 국가 주요 기반시설의 마비·파괴까지 우려가 되는데 현실이다.

그러나 기존의 랜섬웨어에 관한 연구는 '2019 국내외 주요 및 신규 랜섬웨어 동향 분석'[2], '2021년 랜섬웨어 현황 및 대응 예방정책 동향'[3], '커넥티드 의료기기 해킹 및 랜섬웨어 대응동향'[4] 등과 같이 랜섬웨어 감염사례와 함께 데이터를 암호화한 암호화 알고리즘이 무엇이고 어떤 차이가 있는지를 비교하는 사례 연구가 한 주류를 이루고 있었고, '하이브리드 분석을 통한 머신러닝 기반의 랜섬웨어 탐지모델'[5], '정적 분석 정보와 동적 분석 정보를 이용한 랜섬웨어 탐지모델 제안'[6], '랜섬웨어 분석 및 탐지패턴 자동화 모델에 관한 연구'[7]와 같이 악성코드 단위의 리버스 엔지니어링 또는 레지스트리 변경내용 모니터링 등과 같은 랜섬웨어 특성을 기술적으로 분석함으로써 랜섬웨어를 어떻게 효과적으로 탐지하고 방어할 것인지에 대한 연구가 한 주류를 이루고 있었다. 하지만 랜섬웨어 공격기법의 기술적인 분석에만 치중하여 '랜섬웨어가 현실 국가안보에 어떤 영향을 주는가?' 라는 물음에서 시작되는 거시적인 차원의 정책연구는 부족하였다. 이러한 연구 경향은 국가안보 그중에서도 IT기술에 기반한 사이버안보정책에 관한 연구가 아직 초기 단계로 향후 더 많은 연구가 필요한 시점이라는 것을 말해 준다.

이에 본 논문에서는 최근 국내외 주요 랜섬웨어 피해사례 및 현황을 살펴보고 전 세계적인 랜섬웨어 확산 요인이 무엇인지에 대한 심층적인 분석과 함께 미국, 유럽 등 주요 선진국과 우리 정부의 랜섬웨어 정책을 시의적절하게 비교 분석함으로써 우리의 사이버안보 수준을 제고 하기 위한 정책적 개선방안을 제시하고자 한다.

Ⅱ. 관련 연구

2.1 국내·외 주요 랜섬웨어 피해사례

랜섬웨어란 '몸값(ransome)'과 '소프트웨어(ware)'의 합성어로 컴퓨터 시스템의 문서를 암호화하여 이를 인질로 잡고 돈을 요구하는 악성 해킹프로그램의 일종을 말한다[8]. 최근의 랜섬웨어는 기존의 다양한 해킹공격 기법들과 결합하면서 점점 고도화·지능화되고 있다. 특히 하나의 랜섬웨어 악성코드가 등장하면 변종 랜섬웨어가 빠르게 등장하면서 짧은 시간 안에 전세계로 확산되는 특성으로 인해 큰 피해를 주었다. 국내·외에서 발생했던 대표적인 랜섬웨어들의 사례별 주요 피해 내용은 <표 1>과 같다.

표 1. 대표적인 랜섬웨어 피해 사례
Table 1. Representative Ramsomware Damage Cases

	A case in point	Major Damage
Oversea	"Wanna Cry" ransomware	In 2017, 300,000 infections in 150 countries became an international security issue
	"NotPetya." Ransomware	The damage started in Ukraine in 2017 and spread to 60 countries around the world
	German Düsseldorf University Hospital	In 2020, 30 servers in hospital were paralyzed, emergency patients died

	A case in point	Major Damage
	American Colonial Pipeline	In 2021, suspension of oil shipments to eastern United States for six days (paying 5.6 billion to hackers)
Domestic	Web hosting "NAYANA" Infection	In 2017, 153 servers are infected and 5,500 customer sites paralyzed
	Ransom DDoS attack	In 2020, 10 places including Woori Bank, Kakao Bank, K-Bank, CJ, Hanwha, and POSCO will be affected by Ransom DDoS
	"ELand Group." Infection	In 2020, some offline stores of the Eland group's affiliates were shut down and 1 million customer information was leaked

2.1.1 (해 외)'워너크라이' 랜섬웨어

2017년 5월 등장해 150여 개국 20만 대 이상의 컴퓨터를 감염시킨 '워너크라이'를 가장 대표적인 랜섬웨어 피해사례로 들 수 있다. '워너크라이(WannaCry)'는 패치되지 않은 마이크로소프트 윈도우 취약점을 통해 확산되었으며 4차 산업혁명으로 인한 전 세계적인 네트워크의 연결성과 세계 경제의 인터넷 의존성이 랜섬웨어라는 악성코드에 의해 얼마나 큰 피해를 줄 수 있는지를 여실히 보여주었다. 영국에서는 국가의료보건 서비스(NHS)에 연결된 병·의원들의 예약, 약 2만건이 갑자기 모두 취소되면서 9,200만 파운드(약 1,400억)의 손실을 보는 등 전 세계적으로 최대 40억 달러(약 5조) 상당의 경제적 손실을 초래한 것으로 분석되었다[9]. 이와 관련 미 법무부 및 사이버인프라보안국(CISA)은 '워너크라이' 랜섬웨어의 배후로 북한 해킹조직을 지목하였다[10].

2.1.2 (해 외)'낫 페트야' 랜섬웨어

2017년 6월 발생한 낫페트야 랜섬웨어 공격은 우크라이나 주요 기업들과 정부 기관들을 대상으로 최초 공격이 시작되었다. 하지만 그 후 유럽 각국을 거쳐 전세계로 퍼져 나가 피해가 급증하게 되었다. 낫페트야는 2016년에 등장한 페트야(Petya) 랜섬웨어에서 나왔지만, '낫페트야'라는 이름에서 유추할 수 있다시피 '페트야가 아니다'라는 의미로 '낫페트야'로 명명되었다[11]. '낫페트야'는 '페트야' 랜섬웨어와 유사하게 보이지만 사실은 감염된 피해자의 시스템을 파괴하기 위한 목적으로 제작된 것으로 분석되었으며 전세계 60개국으로 확산되어 100억 달러 이상의 피해를 일으켰다. 머스크, 페덱스 등 잘 알려진 다국적 기업들이 큰 손해를 입었으며 '낫페트야' 공격 배후로 우크라이나에 사회적 혼란을 조장하려는 목적으로 러시아 군 첩보기관(GRU) 해커들이 개입한 것[12]으로 알려졌다.

2.1.3 (해 외)'독일 뒤셀도르프 대학 병원' 사례

2020년 독일 뒤셀도르프에 있는 대학 병원이 랜섬웨어에 감염되어 병원에서 운영 중이던 30여 개 주요 서버가 마비되는 사건이 있었다. 이로 인해 병원내 수술실 사용이 불가능해졌고 응급치료가 필요한 환자는 32km 밖 인근 병원으로 긴급 이송되었으나 응급치료가 한 시간이나 지연되며 환자가 사망하였다[13]. 이는 랜섬웨어로 인해 인명피해가 직접적으로 난 최초의 사례이다.

2.1.4 (해 외)'美 콜로니얼 파이프라인' 사례

2021년 5월 다크사이드(DarkSide)라는 대규모 랜섬웨어 조직에 의해 미 동부지역 석유 운송량의 43%를 담당하는 송유관 운영 기업 '콜로니얼 파이프라인'사의 IT시스템이 랜섬웨어에 감염되어 그 운영이 마비되었다. 이로 인해 6일간 미 동부지역의 송유가 중단되고 미국의 휘발유 가격은 7년 만에 최고로 상승하게 되었다[14]. '콜로니얼파이프라인'사는 해킹조직에 약 4,340만 달러 상당의 비트코인(한화로 약 56억)을 지불하였다. 또한, 공격자들은 데이터를 암호화 했을 뿐만 아니라 100GB 상당의 회사 내부 자료까지 훔쳐가 주요 국가 인프라 시설마저 사이버 공격에 얼마나 취약한지를 여실히 보여주었다. 러시아 해킹조직인 '다크사이드'는 주로 대기업 등을 노리고 랜섬웨어 악성코드(일명 서비스형 랜섬웨어 : RaaS)를 제작·유포하고 있는 것으로 미 국무부는 분석했다[14].

2.1.5 (국 내) '인터넷나야나' 사례

2017년 국내 인터넷 기업을 직접적으로 공격한 대표적 랜섬웨어 사례로 '인터넷나야나' 사건을 들 수 있다. 웹호스팅업체인 '인터넷나야나'는 '에레보스(Erebus)' 랜섬웨어에 의해 감염되어 153대의 서버와 최대 5,500개나 되는 내부 홈페이지 사이트가 변조되었으며 데이터 복구를 위해 '인터넷나야나'는 결국 약 13억 원에 상당하는 비트코인을 해킹조직에 지급함으로 우리 사회에 랜섬웨어가 사회와 경제에 악영향을 주는지 그 파괴력을 새롭게 각인시키는 첫 계기가 되었다[15].

2.1.6 (국 내) '랜섬디도스' 공격

코로나19로 인해 재택근무 전환이 한창이던 2020년 국내 대기업과 금융기업 여러 곳이 랜섬디도스 공격을 받았다. 8월에는 신한은행과 카카오뱅크, 케이뱅크, 한국거래소 등이 '랜섬디도스' 공격을 받았으며 10월에는 자신을 '팬시베어'라고 스스로 밝힌 해킹조직이 CJ 그룹과 한화그룹에 '랜섬디도스' 공격을 하였으며 이어 우리은행과 기업은행, 포스코, 한국전력공사 등으로 랜섬디도스 공격이 연속적으로 발생하였다[16].

2.1.7 (국 내) '이랜드 그룹' 사례

2020년 국내 대기업인 이랜드 그룹의 내부 시스템이 '크롭' 랜섬웨어에 감염, 이랜드 그룹의 계열사인 뉴코아 백화점, 2001아울렛 등의 오프라인 매장시스템이 일부 마비되어 영업의 50% 가량이 중단되었다. 랜섬웨어 공격을 한 해커 그룹 '클롭'은 약 4백만 달러(45억원)를 요구하였고 랜섬웨어 공격과 함께 내부 시스템에서 개인정보 100만 건을 빼내 다크웹에 공개하기도 하였다[17].

2.2 랜섬웨어 위협 실태 및 공격방식의 진화

2.2.1 랜섬웨어 위협 실태

한국인터넷진흥원(KISA)의 '2021년 랜섬웨어 최신 동향 분석' 리포트에 따르면 국내 기업의 랜섬피해 접수가 2018년 22회, 2019년 39회, 2020년 127회, 2021년(9월) 149회로 급증하고 있었다. 또한, 2018년~2021년간 랜섬웨어 피해접수 총 337건 중 약 90%인 306건이 중소기업 중심으로 발생한 것으로 확인되었다[18]. 또한, 과기정통부가 시행한 '2021년 정보보호 실태조사'에 따르면 국내 기업의 사이버침해사고 경험을 유형별로 구분하면 '랜섬웨어'가 47.7%로 순위가 가장 높았고, 다음 순서는 '악성코드(41.9%)', '해킹(11.4%)' 순이었다. 또한, 682개 기업에 소속된 정보보안책임자(CISO) 및 보안담당자 95%가 '랜섬웨어 위험'이 기업에서 바라보는 가장 중요한 위협 중에 하나라고 밝혔다. 그러나 그럼에도 불구하고 이들 중 44.86%의 회사는 '랜섬웨어에 대한 대응을 수립하지 못했다'고 답했다[19]. 위와 같은 현실은 해외의 경우도 마찬가지이다. 미 연방수사국(FBI) 산하 인터넷범죄신고센터(IC3)가 발표하는 인터넷범죄리포트 보고서에 의하면 랜섬웨어 피해 접수가 2018년 1,493건에서 2021년 3.729건으로 4년간 150% 가까이 폭증하였으며 그 피해규모도 2018년 360만 달러에서 2021년 4,920만 달러로 10배 이상 늘어난 것으로 분석되었다. 또한, 세계적 경영컨설팅업체 중에 하나인 프라이스워터하우스쿠퍼스(PwC)가 세계경제포럼(WEF) 기간에 스위스 다보스에서 발표한 '2022년 글로벌 CEO 설문조사'(세계 89개국 CEO 4,446명 응답)에 의하면 올해 최대 글로벌 위협 요인이 무엇이었냐는 질문에서 설문조사에 참여한 기업 중 49%가 '사이버 위협'[20]이라고 말했다.

2.2.2 랜섬웨어 공격방식의 진화

랜섬웨어 해커가 사용자들을 공격할 때 주로 사용하는 공격 방식은 '피싱' 이메일 열람, 악성코드가 숨겨진 홈페이지 접속, 시스템 취약점을 이용한 직접 해킹 등을 들 수 있다. 공격 대상은 개인PC에 저장된 개인 데이터에서 기업이 보유하고 있는 영업기밀·특허자료 등 점차 다변화되고 있다. 그러나 국가적으로 문제가 되고 있는 점은 그동안 사이버공격에서 안전하다고 여겨졌던 국가기반시설들이 운영하는 제어시스템까지 그 공격의 대상이 되고 있다는 점이다. 또한, 공격 경로도 개별적으로 운영중인 IT장비만을 대상으로 하는 것이 아니라 대규모 공급망이라 할 수 있는 클라우드 시스템 업체들을 공격하여 해당 시스템을 이용중인 사용자들을 한꺼번에 공략함으로써 공격 효과를 증가시키는 방법으로 발전하고 있다. 이런 공격방식을 선호하는 이유는 클라우드 시스템을 장악할 시 여러 기업 데이타에 대한 접근 권한을 동시에 얻을 수 있기 때문에 공격자에게는 매력적인 공격 포인트가 되기 때문이다.

랜섬웨어 기법도 점차 지능화되고 있는데 과거엔 컴퓨터 하드디스크에 저장된 파일들을 무작위로 암호화하였다면 최근에는 보다 공격 효과를 높이기 위해 사용자가 보유중인 모든 파일을 검색하여 문서파일, 엑셀 파일 등 중요 파일을 찾아 선별적으로 암호화하고 파일의 중요도에 따라 암호화하는 알고리즘을 각기 달리하여 암호 해독에 난이도를 높이는 수법을 사용하고 있다. 이렇게 공격자는 랜섬웨어 공격으로 치명적인 손해를 입을 수 있는 기업을 노리고 어느 서버를 공격해야 할지 사전에 철저히 분석하고 있다. 또한 기업이나 공공기관의 필수적인 서비스와 시스템이 무엇인지 사전 분석한 상태에서 공격하기 때문에 방어하는 입장에서는 대응이 더욱더 어려워지고 있다.

이뿐만이 아니라, 랜섬웨어의 확산은 기존의 사이버공격 수단에도 큰 변화를 가져다주었다. 온라인 기반의 서비스가 전 사회로 확대되고 인터넷 트래픽이 대규모로 증가함에 따라 이런 취약점을 노린 사이버공격으로 진화한 것이다. 기존의 서비스거부 공격은

정치·외교적인 목적이나 경쟁사의 운영을 방해할 목적으로 발생하였으나 이제는 금전적 수익성을 노려 협박 공갈과 결합해 기업에 금전을 요구하는 방식으로 변화하였다. 일명 '랜섬디도스'로 알려진 이런 공격은 공공기관이나 기업을 대상을 분산 서비스 거부 공격을 시범적으로 시도한 후 기관을 협박해 가상자산 등의 금전을 구체적으로 요구하는 방식이다. 인터넷을 기반으로 서비스를 제공하는 기업들이나 공공기관들에게는 치명적인 손해를 입힐 수 있기에 효과적인 협박 수단이 되었다.

2.3 '랜섬웨어 공격'급증 요인 분석

2.3.1 '코로나19'와 '디지털 대전환 '

다보스포럼의 창립자인 클라우드 슈밥이 2016년 세계경제포럼에서 처음 제시하였던 '제4차 산업혁명' 이라는 이슈는 이제 세계에서 가장 중요한 이슈가 되었으며 4차 산업혁명으로 인해 시작된 디지털 대전환이 사회 전반에서 점차 가속화 확대되고 있으며 2020년 1월 전 세계로 확산된 코로나19 바이러스는 아이러니하게도 우리의 생활을 온라인과 비대면 방식이라는 새로운 환경으로 이끌었다. 재택근무, 원격 교육, 배달서비스 확대 등 일상 곳곳에서 비대면 방식이 확산 되었고, 대면 업무만 가능했던 공공행정 서비스 영역에서조차 대부분의 민원 서비스를 원격 서비스로 전환하는 등 사회 전 영역에서의 디지털 혁신을 촉진시켰다. 비대면을 강제화했던 코로나19 상황이 그동안 대면이 당연시되었던 일상생활의 많은 문화를 디지털로 혁신시킨 것이다. 사람 간의 직접 접촉을 막아야 했던 코로나19의 전 세계적인 보건위기 상황은 네트워크와 IT기술의 접목으로 인해 거꾸로 사람이 만날 필요가 없는 상황을 강제적으로 만들었다.

코로나19로 인해 사회가 급속도로 IT혁신의 길로 들어섰으나 우리가 간과해서는 안 될 부분이 있다. 많은 공공기관들과 기업들이 원격근무, 재택근무에 돌입한 상황에서 재택근무는 다양한 보안시스템에 의해 보호받아왔던 사무실 보안환경에 비해 랜섬웨어 등 각종 사이버 위협에 매우 취약하다는 사실이다. 재택근무를 위해 망분리 정책을 임시로 예외 적용하여 운용했던 공공기관이나 급하게 홈워크 시스템을 강제로 이용해야 했던 기업들을 대상으로 보안취약점을 이용한 악성코드 침입 시도가 대폭 증가하고 있다는 것이다. 가정에서 공용으로 사용하던 개인용 PC를 업무용도로 사용하다 보니 랜섬웨어 등의 악성코드에 감염될 경우 가정용 PC가 2차로 회사 서버를 감염시키는 통로로 활용되기 때문이다.

실제 영국 사이버보안센터(NCSC)와 미국 국토안보부(DHS)는 공동으로 최근 코로나19 사태로 인해 원격·재택근무가 전세계적으로 확대되면서 VPN 및 원격접속 소프트웨어의 취약점을 이용한 랜섬웨어 등의 사이버공격이 급증하고 있다며 긴급 경고한 바 있다[21].

2.3.2 '가상화폐'사용의 확산

암호화폐(Cryptocurrency)는 블록체인과 같은 암호화 기술을 이용하여 만든 디지털 화폐를 말한다. 암호화폐는 우리가 일상생활에서 사용하는 지폐나 동전과 같은 실물의 형태를 가지고 있지 않으며 디지털 데이터로 존재하기에 가상화폐(Virtual money)라고도 부른다[22]. 가상화폐가 초기에 얼리 어답터들의 전유물이었다면 지금의 가상화폐 시장은 새로운 자산시장의 하나로 대중화되었으며 기존의 금융시장이 제공하지 못하는 새로운 서비스를 제공하는 대체 시장이 되고 있다. 금융위원회 산하의 금융정보분석원(FIU)은 2022년 3월 '2021년도 하반기 가상화폐 사업자 실태조사' 결과를 발표하였는데 국내 가상화폐 시장 시가총액이 2021년 기준으로 55조2,000억 원에 달한다고 밝혔다[23]. 그러나, 이러한 가상화폐의 익명성과 국경을 넘나드는 금전거래의 용이성이라는 특징이 국제적 랜섬웨어의 확산을 부추기는 부작용을 낳고 있다. 랜섬웨어 협박을 통해 벌어들이는 수익금을 손쉽게 다른 계좌로 이체하거나 이를 현금자산으로 바꾸는 자금세탁 수단으로 활용하는데 있어 편하기 때문이다. 가상화폐는 현금이나 은행 계좌거래와 다르게 수사기관이 자금의 흐름을 추적하기가 어려우며 암호화폐 거래소를 통해 이종 간의 암호화폐로 바꾸기도 쉽기 때문이다.

따라서, 2021년 10월 조 바이든 대통령은 전세계 30여개국과 '반랜섬웨어 이니셔디브 다자 회의를 개최하며 가상화폐의 랜섬웨어 범죄 악용에 대한 부작용을 경고하였고[30] 2022년 미 법무부가 발간한 디지털 자산관련 법집행 보고서에서 랜섬웨어 근절을 위해 가상화폐 시장 단속에 집중하고 있다고 밝혔다[24].

2.3.3 '다크웹'범죄 시장화

다크웹(Dark web)'은 인터넷을 통해 접속 가능한 웹사이트의 일종이지만 접속을 위해서 특정한 웹브라우저 프로그램을 사용해야만 하는 특수한 웹사이트이다. 또한, 일반적인 검색 엔진으로는 찾을 수 없으며 접속 서버를 사용자가 바로 확인할 수 없어 사이버공

간의 범죄시장이 되고 있다[25]. 보통은 '토르(TOR)'와 같은 특수한 전용 웹브라우저 프로그램을 사용해야만 접속할 수 있으며 정확한 주소를 모르면 검색으로 찾기도 어렵다.

이런 은닉성으로 인해 초창기에는 인터넷 검열이 심한 권위주의 국가들에서 사용자가 자유롭게 인터넷을 사용하기 위한 방법으로 고안되었다. 그러나, 다크넷은 이제 대표적인 사이버 범죄시장이 되어 해킹도구, 자금세탁 마약·총기류 거래 등 암시장의 주경로로 활용되고 있다. 다크넷이라는 사이버공간이 공급자와 수요자의 욕구를 일치시키고 있다. 누군가가 랜섬웨어 등의 해킹 프로그램을 만들고(공급자) 누군가는 그 프로그램을 구매한 후 손쉽게 공격을 실행(수요자)한다. 수요자와 공격자가 서로 이득을 공유하는 비대면의 지하경제 환경이 구축된 것이다. 사이버공간의 특성상 비대면으로 손쉽게 다크넷이라는 시장에 접근할 수 있게 되었다.

이 같은 다크넷의 불법적 사용으로 인해 각국 정부들의 대응도 더욱 강경화되고 있는데 구체적인 사례가 2020년 미 재무부가 미 연방수사국(FBI) 등과 함께 공조하여 매출 기준으로 세계 최대인 다크넷 '히드라' 서버를 폐쇄시키고 불법이 의심되는 비트코인(2,500만 달러 상당. 약 304억원)을 압류한 사건이다[26].

2.3.4 서비스형 랜섬웨어(RaaS)의 등장

범죄 암시장이 되어버린 다크웹 공간에서 주요한 수익상품이 새롭게 등장하였는데 바로 '서비스형 랜섬웨어(Ransomware as a Service)'이다. 서비스형 랜섬웨어는 사용하는 사람이 별도의 프로그래밍에 관한 전문적인 지식이 없어도 일정 비용만 지급하면 누구라도 손쉽게 랜섬웨어를 유포해 협박을 할 수 있게끔 서비스 형태로 제공된다[27]. 전문적인 IT 지식을 가진 해킹조직의 전유물로만 여겨졌던 랜섬웨어가 다크웹이라고 알려진 사이버 암시장과 만나 시장에서 이미 만들어진 상품을 구매하는 것처럼 손쉽게 구매할 수 있게 되었으며 필요에 따라서는 협박 대상, 금전 요구 방식까지 구매자가 옵션으로 선택해 맞춤형으로 랜섬웨어를 제작해주는 대행 서비스까지 등장했다. 구매자들은 단일 상품처럼 랜섬웨어 악성코드만 구매하기도 하고 대규모 공격을 서로 공모하여 랜섬웨어 수익금을 서로 분배하기도 한다. 서비스형 랜섬웨어의 가장 큰 문제점은 랜섬웨어라는 해킹도구를 비트코인 등의 암호화폐를 이용하여 저렴한 가격에 누구나 손쉽게 구할 수 있다는 사실이며 이로 인해 랜섬웨어에 의한 사회적 피해를 광범위하게 양산하게 될 가능성이 커졌다는 것이다.

Ⅲ. 랜섬웨어 대응 최근 동향 및 문제점

3.1 해외의 랜섬웨어 대응 동향

3.1.1 미국 정부의 정책 동향

2020년 미국은 네트워크 관리 프로그램인 솔라윈즈(SoladWinds)의 취약점으로 인해 다수의 연방정부가 러시아 해커들에게 공격 받았으며 곧 이어 중국 국가안전부와 연계된 해커조직들이 MS 이메일 익스체인지 S/W의 취약점을 이용하여 연방정부와 기업들을 대상으로 대규모 해킹한 사실이 밝혀져 사회적으로 큰 파장이 일었다[28]. 그런 가운데 그 이듬해인 2021년 미 최대 송유관 운영사인 '콜로니얼 파이프라인'과 글로벌 식품업체인 'JBS푸드'가 잇따라 랜섬웨어에 감염되는 등 지속적으로 사이버공격으로 인한 피해를 입게 되었다.

연달아 발생한 위 사건들은 미국이 랜섬웨어를 포함한 사이버위협에 보다 적극적으로 대응하는 방향으로 정책을 변화시키게 되는 주요한 계기가 되었다. 단순히 개인정보의 유출이나 웹사이트 마비 정도가 아닌 사회 주요 인프라가 공격받아 국가 공급망 자체가 흔들렸던 일련의 사건들은 랜섬웨어 감염만으로도 국가안보에 위기 상황을 초래할 수 있다는 정책적 판단을 하게 만든 것이다.

2021년 5월 12일 미국은 '민간기업 및 연방 정부 네트워크에 대한 사이버안보 강화'에 관한 대통령 행정명령에 서명함으로써 미 연방정부의 내부적 보안을 강화하는 방안을 먼저 마련하였다. 이 행정명령에는 연방정부 정보시스템 운영에 관계되는 IT서비스 제공자는 사이버공격과 관련된 정보를 입수할 경우 즉각 연방정부와 의무적으로 공유하는 체계를 만들었고 연방 정부와 민간부문간의 정보공유를 확대하는 한편 미국내 소프트웨어 공급망을 강화하는 활동을 포함하고 있다[29]. 이어 2021년 10월 미국은 랜섬웨어 공격과 같은 국제적인 사이버문제에 대응하기 위하여 국무부에 사이버·디지털 정책국이라는 조직을 신설·운영하기로 결정하였다. 미 국무부는 신설된 사이버·디지털 정책국을 통해 랜섬웨어를 포함한 미국 주요 인프라시설 대상 사이버공격에 대비하여 효과적인 사이버안보 정책을 개발하고 동맹국과의 협력 등 사이버안보 문제에 적극 대응할 것이라고 밝혔다[30].

또한, 미국은 랜섬웨어 공격을 단지 미국 자국만의 문제로 인식하지 않고 사이버공격에 의한 피해가 본

질적으로 복잡하고 글로벌하기 때문에 국제 공동 대응이 필요한 문제라고 인식했다. 따라서 2021년 6월 영국에서 열린 세계 주요 7개국(G7) 정상회의에서 랜섬웨어를 주요 의제로 다뤘으며[31] 랜섬웨어를 포함한 불법적인 사이버 활동과 이와 연결된 가상화폐 문제점에 대해 국제사회가 공동으로 협력하기로 합의했다. 같은 달 열린 북대서양조약기구(NATO) 정상회의에서도 랜섬웨어의 피해가 급증하는데 대해 나토 차원에서 적극적으로 대응한다는 정책결정을 이끌어 내었다[32]. 연달아. 2021년 10월 미 백악관 국가안보보장회의(NSC)를 중심으로 영국, 프랑스, 독일 등 G7 국가를 포함하여 EU(유럽연합), 일본, 한국 등 30 여 개국이 참여하는 '반랜섬웨어 이니셔디브 다자 회의'를 개최하였는데 이 회의는 랜섬웨어 대응을 주제로 열린 최초의 다자간 회의로 러시아, 중국 등의 국가가 암시적으로 지원하는 사이버범죄에 맞서 전세계가 공동 대응하기로 하였다[33].

미국은 다자간 협력뿐만 아니라 양자간 협력도 동시 추진하였다. 특히 한·미 양국은 2021년 한·미 정상회담을 계기로 국제제재를 받고 있는 북한이 랜섬웨어를 적극 활용하고 있어 제재 사각지대가 되고 있다고 판단함에 따라 한국과 미국의 사이버안보 협력을 보다 강화하기로 합의하고 '한·미 사이버워킹그룹' 회의를 개최하였다[34].

미국의 사이버안보정책 중 특히 주목해야 할 부분은 사법기관을 통한 해킹조직 기소·공개 수배 및 체포, 자금동결, 가상화폐 회수, 거래소 활동 차단 등 실효적이고 직접적인 정책을 실행하고 있는 부분이다. 국가안보에 위협을 주는 해킹활동에 대해서 단호하게 외교적인 공개 경고를 하는 한편 해커 개개인을 대상으로는 사법 기소· 고액의 현상금 수배 등의 직접적인 대응을 병행함으로써 전방위적인 강한 압박에 나서고 있다. 미국 연방 정부의 법집행 기관중에 하나인 비밀경호국(United States Secret Service)은 지난 2015년부터 현재까지 총 1억 2백만 달러(한화 약 1천 263억원) 상당의 불법 가상화폐 자금을 압수했다[35]. 이 자금에는 국제적으로 랜섬웨어 공격을 한 러시아와 북한의 해킹조직이 협박으로 벌어들인 수익금도 포함되었다. 다음의 <표 2>는 미국에 의해 진행된 주요 사이버위협 대상 국가 대응조치 현황이다.

특히 미국은 국가안보국(NSA)과 중앙정보국(CIA) 등의 정보기관들이 전면에 나서 파이브아이(Five Eyes) 국가들인 영국, 뉴질랜드, 호주, 캐나다 등 5개국 정보 공동체와 함께 정보기관간 협력을 통해 사이버안보를 위협하는 해킹조직 및 해커들의 공격 동향

표 2. 사이버위협에 대한 미국의 주요 대응조치 사례
Table 2. Major U.S. Response cases to Cyber Threats

Date	Major countermeasure (USA)
2022.4.26	State Department wanted six Russian GRU members on charges of attacking ransomware "NotPetya" ($10 million)
2022.4.14	U.S. Court Arrests U.S. People Who transfer Cryptographic Technology to North Korea, Fines $100,000 and Sentences 63 Months
2022.4.05	Russian-based darknet "Hydra" and cryptocurrency exchange "Garantex" on suspicion of money laundering blocked trading activities
2022.3.14	Kaseya Ransomware attack hacker group Leville arrested in Poland, extradited to the U.S. in 115 years
2021.9.21	Russia's cryptocurrency exchange 'Suex' sanctions, alleged money laundering in connection with at least eight ransomware activities
2021.8.24	Two people involved in ransomware hacker groups(Sodinokibi and Revil) have been charged and $6.12 million seized
2021.2.17	Three hackers from the North Korea were indicted, and they were suspected of producing and distributing WannaCry ransomware from Lazarus Group
2021.11.8	Casheya ransomware distribution hacker group Leville has been set aside for $10 million, and two hackers have been charged
2020.9.16	11 people, including China (5), Russia (2), and Iran (2), have been charged with hacking on research institutes and think tanks in the U.S

정보를 다각도로 수집·감시하고 있으며 연방수사국(FBI), 국토안보부(DHS), 사이버인프라보안국(CISA)과 함께 해커들의 공격 수법을 분석하여 범증을 확보함으로써 미 법무부와 재무부가 랜섬웨어 해커들을 기소·체포하거나 자산동결 등 직접적인 제재를 단행하는 데 결정적인 역할을 하고 있다.

3.1.2 유럽연합(EU)의 정책 동향

국제적 안보 쟁점이 되고 있는 랜섬웨어 공격 대응에 있어서 유럽연합(EU)은 유사입장국(Like-minded)인 미국 및 나토 가입국을 중심으로 긴밀한 조율을 통해 대응하고 있다. 유럽 또한 한 국가만의 대응이 아닌 유럽연합 명의 또는 유사 피해를 본 국가들이 모여

서 공동선언을 하는 방법을 이용하고 있다. 또한, 유럽을 공격한 해킹조직을 미국과 공동 추적, 비난 성명을 대외적으로 공개 발표하는 등 해킹 공격에 대한 외교적 책임을 적극적으로 묻는 행보를 강화하고 있다. 이는 복잡한 국제관계 속에서 동맹간의 협력을 통한 연대 외교를 중시하고 있다는 것을 보여준다.

유럽은 유럽연합 소속 정상들의 모임인 유럽이사회, 유럽의회, 유럽연합내 정책 입안·집행을 담당하는 EU 집행위원회를 중심으로 대응이 이뤄지고 있는데 그중에서도 유럽네트워크정보보안기구(ENISA)가 그 실행의 중심에 있다. ENISA는 'ENISA Threat Landscape' 보고서를 통해 2020년 랜섬웨어 공격이 2019년에 비해 150% 증가하였는데 특히 '가상통화로 몸값 지불을 요구하고 있는 랜섬웨어의 피해가 급증하고 있어 국가안전보장의 최우선 사항이 되고 있으며 밝혀지지 않은 랜섬웨어 공격이 훨씬 많은 상황으로 유럽 각국은 랜섬웨어와의 싸움을 강화할 필요성 높다'라며[36] 유럽 각 국에 적극적인 대응을 권고했다.

유럽의 정책 중 눈여겨 볼 것은 2020년 7월 유럽연합 이사회가 EU 회원국을 대상으로 지속해서 사이버

표 3. 사이버위협에 대한 유럽의 주요 대응조치 사례
Table 3. Major EU Response cases to Cyber Threats

Date	Major countermeasure (EU and U.K.)
2021.9.6	Germany has publicly warned Russian hacker group 'Ghost Writer' on charges of massive hacking attacks against a German mmber of Parliament and political parties
2021.7.19	EU, NATO and UK jointly identify hackers behind China's national security as MS Exchange attackers
2021.6.29.	The EU seized and searched the servers of Double VPN, a VPN company suspected of being linked to Russia, for hacking into EU agencies
2021.4.15	The U.K. and U.S. jointly warn of Russian intelligence hackers being responsible for the Solarwinds hacking
2020.12.31	The U.K. Foreign Ministry has sanctioned the Russian hacker group GTsSS for hacking into European government agencies such as the German Federal Assembly
2020.10.22	The EU Commission has sanctioned two Russians and an agency for hacking into the German parliamentary intelligence system
2020.10.19	The U.K. has blamed a Russian intelligence agent for hacking into the 2018 PyeongChang Olympics and the 2020 Tokyo Olympics organizing committee
2020.7.31	The EU has frozen assets of three hackers and institutions in North Korea, China and Russia for hacking major European institutions

공격을 한 북한, 러시아, 중국 등 3개국 해커나 기관 3곳에 대하여 자산동결, 입국금지 조치 등의 실효적인 제재를 최초로 결정한 사례이다[37]. 다음의 <표 3>은 유럽에서 발생한 주요 사이버위협에 대해 유럽이 대응한 주요 조치내용이다.

2021년 7월 유럽위원회는 자금세탁방지 및 테러자금조달방지 규제를 강화할 새로운 입법안을 발의했다. 유럽위원회가 새로 발의한 법안의 핵심은 가상화폐 송금을 추적 가능하게 만드는 것으로 가상화폐 거래소가 가상화폐를 보내고 받을 때 양쪽 사용자 모두에게 세부적인 정보를 수집하도록 하고 익명 가상화폐 지갑을 사용하는 것은 금지하는 것이다. 이를 통해 비트코인 같이 랜섬웨어 범죄에 악용되고 있는 가상화폐의 불법적인 계좌이동을 추적하고 범죄자금 세탁이나 테러자금 조달에 사용되지 못하도록 하는 것이 목적이다[38].

3.2 우리나라의 대응 현황 및 문제점

최근 해킹, 랜섬웨어 등 사이버공간에서 벌어지고 있는 위협이 국민생활 및 사회·경제 전반에 걸쳐 큰 영향을 미치고 있다. 2021년 8월 3일 국가정보원은 국내에서의 랜섬웨어 공격 피해가 확산되는 정황을 포착하고 국가공공기관을 대상으로 사이버위기 경보를 3년여 만에 '정상'에서 '관심'으로 상향 조정하였다[39]. 경보 조치 발령에 이어 8월에 개최된 '제42차 비상경제 중앙대책본부 회의'에서 과기정통부와 관계부처 명의로 '랜섬웨어 대응 강화방안'을 발표하였다. 정부 방안의 주요 내용을 살펴보면 랜섬웨어 공격에 대비해 국가 중요 기반시설 확대 지정, 중소기업 보안역량 강화사업 확대, 랜섬웨어 대응·복구를 위한 핵심기술 개발사업 등이 포함되어 있다[40].

우리나라도 랜섬웨어의 피해에 대해 그 심각성을 인식하고 다양한 정책을 실행하고 있다. 그러나 다음과 같은 이유로 이런 정책들이 랜섬웨어를 효과적으로 근절할 수 있는지 의문이 든다.

3.2.1 랜섬웨어에 대한 사회적 위험 인식 부족

먼저, 우리 사회는 랜섬웨어를 바라보는 사회적 위험 인식이 아직 많이 부족하다. 이에 따라 정부의 대응 방식이 단기적으로 피해를 최소화 하는데에만 급급, 총체적인 대응이 이루어지지 못하고 있다. 랜섬웨어를 국가안보를 위협하는 주요한 위협요소로 바라보지 않고 단순하게 새롭게 등장한 사이버범죄 유형 중 하나로 바라보기에 랜섬웨어 대응을 위한 대처가 소극적이며 즉흥적이다. '국가사이버안보센터'가 발표한

'2021년 연례보고서'에 따르면 우리나라의 방위산업·조선 관련 기업과 양자기술·인공지능 등의 첨단 산업 기술을 노린 해킹이 현재 빈번하게 일어나고 있으며 랜섬웨어로 인한 사회적인 피해가 주요한 안보 위협이 되고 있다고 한다[41]. 이러한 상황에서 에너지·통신 등 국가의 주요 인프라 시설 운영기업, 방산기업들은 랜섬웨어 감염, 랜섬디도스 공격 등으로 인해 실제적인 피해를 입어도 기업 이미지 보호를 위해 이를 공개하지 않고 숨기려고만 한다. 이에 따라 관련 정부기관들이 정보를 확보하지 못해 조기에 피해를 막지 못하고 다른 기업이나 국책연구소 등으로 2차 3차 피해가 확산되는 악순환을 겪고 있다. 공격자들의 최근 협박 패턴을 살펴보면 경제적 이득을 극대화하기 위하여 중요 데이터를 암호화하여 협박에 활용할 뿐만 아니라 중요한 데이터는 암호화하기 전에 외부로 몰래 전송한 후 이를 인터넷 등에 공개하겠다고 협박함으로써 2중 3중으로 압박을 가중시킨다. 이 같은 경우, 대다수 기업이나 공공기관들은 기업 이미지 하락이나 서비스 중단으로 인한 외부 비난을 우려해 협박에 응하게 되는 경우가 많다.

우리나라뿐만 아니라 전세계적으로도 이 같이 피해를 은닉하려는 기업들의 경향은 비슷하며 그렇기에 피해를 입은 기업들은 사회적인 비난을 감수하더라도 협박범에게 비용을 몰래 지불하는 경우가 많다. 사이버보안 컨설팅사인 'Cyberedge Group'에서 전세계 17개국을 대상으로 조사한 결과를 보면 랜섬웨어로 인한 피해복구를 위해 비용을 지불하는 경우가 2018년 38.7%에서 2019년 45.1%, 2020년 57.5%으로 계속해서 증가하고 있는 것을 확인할 수 있다[42].

3.2.2 진화하는 공격방식에 비해 뒤처지는 정책

랜섬웨어 조직들이 주로 다크웹을 기반으로 활동하며 공격 수법도 점차 조직화, 분업화, 대형화 추세인데 반해 이를 막기 위한 정책 수단이 부족하다. 랜섬웨어 공격을 예방하기 위한 정부의 여러 정책적 노력들은 일정부분 효과가 있겠지만 피해 대상만 바뀌게 될 뿐 완벽히 근절하기 위한 수단으로서는 미흡한 게 현실이다.

랜섬웨어 조직들은 해킹프로그램 개발, 유포, 협박 및 협상, 자금세탁 등 그 역할을 나눠 점조직 또는 분업화된 구조로 운영되고 있어 이를 일망타진하기가 쉽지 않다. 랜섬웨어 조직들은 다크웹 시장에서 필요 인력을 수시로 모집하기도 하며 벌어들인 수익금을 총괄 책임자, 악성코드 제작자, 중간역할 담당 등에게 성과금처럼 지급하는 등 기업화된 운영을 하고 있다.

이뿐만이 아니다. 북한, 중국, 러시아 등의 권위주의 국가들은 정보기관 해커들이 직접적으로 해킹을 하거나 또는 해킹 조직을 배후에서 조정하며 랜섬웨어 시장에 뛰어들고 있어 날로 심각해지고 있다. 따라서 효율적으로 대응하기 위해서는 주요 피해에 대해서는 신고를 의무화하고 정보·수사 기관들이 해커 추적을 효과적으로 실행할 수 있도록 필요한 법안을 새로 입법화하는 등 제도적 뒷받침이 필수적이다.

3.2.3 가상화폐 시장 발전에 따른 부작용

랜섬웨어 조직들은 가상화폐의 은밀성이라는 특성을 적극 이용하여 피해자들에게 협박자금을 받거나 해외에서 자금세탁을 하고 있으나 정부의 통제나 규제는 이를 따라가지 못하고 있다. 2017년부터 법무부, 기재부, 금융위를 포함한 정부기관들이 '가상화폐 합동 TF'를 최초 구성하였고 2020년 '특정금융정보법 시행령' 개정을 통하여 그동안 가상화폐 거래소가 실명 확인 입출금 계좌를 보유하도록 규제하였다. 이어 2022년에는 일명 '트래블룰'을 시행하여 거래소에서 비트코인 같은 가상자산을 거래할 시에 누가 보냈는지 누가 받았는지에 대한 전자기록을 남기도록 하였다, 이는 일반 은행에서 송금할 때 송금인과 수신인 계좌거래 정보를 남기는 것과 동일한 원칙을 제시한 것이다[43]. 이 제도를 통하여 랜섬웨어 공격조직들이 금전을 요구하여 국내 거래소를 이용할 경우에는 그 거래정보를 확인할 수 있게 되었으며 정부나 수사기관이 요청하면 거래 정보를 확인할 수 있기에 범죄예방 효과를 노릴 수 있게 되었다.

그러나, 이렇게 정부도 가상화폐의 폐단을 인식하여 시장에 대한 통제와 규제방안을 속속 마련하고 있지만 시장과 기술의 발전을 따라가기에는 역부족이다. 이용자들간 금융거래의 자유를 제공하겠다는 암호화폐의 기본 철학이 존재하는 한 근본적인 해결이 힘든 상황이다. 그 단적인 예가 '다크코인'의 새로운 등장이다. '다크코인'의 등장은 정부의 추적을 더욱 까다롭게 만들었다. 다크코인은 거래의 익명성을 보장하고 프라이버시 강화를 목적으로 나타난 암호화폐로 기존의 암호화폐와 다른 점은 거래내역을 블록체인 네트워크에 공개하지 않아 거래정보가 드러나지 않는다[44]. 따라서 마약거래, 자금 세탁 등 불법적인 수단에 다크코인이 사용되는 경우가 점점 많아지고 있다. 모네로, 제트캐시 등이 이에 속한다.

3.2.4 랜섬웨어 대응 국제 협력 미비

마지막으로, 사이버라는 공간적 특성으로 인해 랜

섬웨어 공격이 한 나라에 국한되지 않고 여러 나라를 거쳐 발생한다는 점을 심각하게 고려해야 한다. 사이버공간에서 이루어지는 공격은 이제 하나의 기업이나 한 국가만의 힘만으로는 대응하기 어려운 게 현실이다. UN 등 국제사회 차원에서의 글로벌 거버넌스를 구축하여 대응하는 방안과 안보동맹 관계에 있는 국가들의 공동대응 또는 민주적 가치를 공유하는(like-minded) 국가 간에 긴밀히 정보를 공유하고 협력하는 정밀한 외교·안보 정책이 필요하다, 현실적으로 국제사회는 사이버안보에 대한 국민적 인식이 다다르고 형사사법제도도 제각기 다름에 따라 랜섬웨어 조직을 추적·수사하는데 있어 많은 어려움이 있다. 랜섬웨어에 의해 발생되는 피해를 효과적으로 차단하기 위해서는 국제적인 공조와 정보협력 방안이 필요하다.

Ⅳ. 국가사이버안보를 위한 정책 개선방안

4.1 국가안보의 핵심영역이 된'사이버안보'

전세계적으로 민간 및 공공분야를 가리지 않고 사이버공간의 안전이 위협받고 있다. 최근 국가경제·사회의 안전을 마비시킬 목적의 조직적인 해킹이 빈번히 발생하고 있다. 국제안보 환경에 큰 변화가 생긴 것이다. 단순히 기술적인 측면에서 바라보는 'IT 보안·정보보안'에서 더 나아가 '사이버안보'의 시각으로 바라봐야 한다. 이제 '사이버안보'라는 개념은 '국가안보'와 직결되는 매우 핵심적인 안보요소가 되었다. 이미 주요국들은 국가의 안전과 경제를 지키기 위해 사이버안보를 최우선적으로 강화해야 할 안보영역으로 바라보고 있다. 사이버공간의 중요성이 증가하는 가운데 국제정치적 안보갈등 상황에서 국가 배후 해커조직들에 의한 랜섬웨어 사이버 위협은 국가의 주요 기능을 마비시킬 수 있는 주요한 공격수단이 되었으며 정부 입장에서는 매우 심각한 안보리스크가 아닐 수 없다.

우리나라도 2022년 5월 새 정부가 들어서며 한·미 정상회담을 갖고 공동성명을 발표했다. 해당 성명에서 우리 정부는 사이버·우주 등 첨단기술 분야에서 한·미 간 협력을 강화해 다양한 위협에 공동으로 대응할 것을 공표했다[45]. 이는 사이버안보가 국가안보와 직결되며 글로벌한 협력체계 구축이 사이버안보 확보에 가장 중요한 요소라는 것을 인식하였다는 점을 보여준다.

4.2 사이버안보 정책 개선방안

4.2.1 국가중요시설 보호를 위한 제도 기반 확대

랜섬웨어 공격자들은 대상이 되는 시스템을 사용하지 못하도록 공격할 뿐만 아니라 시스템 내에 저장된 자료를 훔쳐 인터넷 공개를 2차 협박하는 등 그 공격수단과 기법이 점차 심각해지고 있다. 그러나, 현행법상 사이버공격으로 인해 개인정보가 직접적으로 유출되지 않는 이상 아무리 큰 피해를 입었다. 하더라도 해당 피해사실 공개가 의무화되고 있지 않기에 대다수 사례가 거의 밝혀지지 않고 있다[46].

따라서, 랜섬웨어를 포함하여 사이버공격으로 인한 피해 확인시 피해 정도에 상관없이 관계기관에 신고하는 것을 의무화하는 제도를 서둘러 도입해야 한다. 특히나 대상 기관이 에너지·전력·교통·통신 등 국가 주요 기반시설 운영과 관련되었거나 국가안보에 직접적인 영향을 주는 방산기업·정부출연 연구소 등인 경우에는 예외가 없어야 할 것이다. 국가의 기반시설이나 핵심기술을 대상으로 하는 사이버공격은 국가안보에 있어 치명적인 결과를 초래하기 때문에 신속한 정보공유와 대응을 통해 2차, 3차 피해를 예방하고 국가 주요 기능의 회복력을 확보하기 위한 포괄적인 국가 지원체계를 가동해야 하기 때문이다.

이를 위해서 우선적으로 고려하고 추진해야 할 것이 '국가사이버안보법'의 제정이다. 우리나라는 국가안보, 국민 안전과 직결된 국가의 중요한 시설조차 위험에 대비한 예방업무에 소홀하거나 중대한 보안 권고조치 사항을 이행하지 않아 반복적으로 침해사고를 받아왔다. 이에 따라 범정부적인 사이버거버너스 확립 차원에서 '국가사이버안보법' 제정이 무엇보다도 필수적이다. 우리나라는 지난 16년 동안 사이버안보법 제정과 관련된 무수한 논의가 지속되어 왔다[52]. 그동안 수많은 학계·전문가들이 법 제정 필요성에 많은 공감대를 형성해 왔음에도 불구하고 여러 정치적인 이유 등으로 인해 제정 논의가 미뤄지고 있다. 그러나 날로 심각해진 국제안보 환경 하에서 사이버위협 정보 수집과 효과적 대응, 피해신고 의무화 및 관련기관 간 정보공유 확대 등이 포함된 '사이버안보법' 제정을 이제는 더 이상 미뤄서는 안 된다.

미국이 2022년 3월 중요 인프라를 운영하는 기업들이 사이버 피해를 입었을 경우 이를 반드시 신고해야 하는 법적인 의무를 가지게 되는 '미국 사이버보안 강화법' (Strengthening American Cybersecurity Act of 2022)이 통과된 사실은 특히 우리가 주목할 부분이다[50]. 미 기업이 랜섬웨어 공격을 받았으면 공격자에

게 랜섬을 지급한 때로부터 24시간 이내에 보고해야 한다. 만약 중요 인프라 기업이 사이버공격을 받고 보고 기한인 72시간이 채 지나기도 전에 협박금을 지불하였다면 피해 기업은 미 사이버인프라보안국(CISA)에 보고하도록 하였다[46]. 이에 반해 우리나라의 주요 기반시설을 보호하는 기반보호법은 제13조에 침해사고를 통지하도록 요구하고 있지만 이행하지 않았을 때의 과태료를 규정하고 있지 않으며 강제 규정이 없다. 따라서, 기반시설 운영기관의 법적 의무를 강화하기 위한 관계 법령 정비도 조속히 이루어져야 한다.

4.2.2 가상화폐 규제 및 모니터링 강화

2015년 '워너크라이'라는 전 세계적인 랜섬웨어 해킹공격이 있었다. 해커는 데이터 복구를 조건으로 당시 수사당국의 추적이 어려웠던 비트코인을 요구했다[10]. 위 사례와 같이 가상화폐의 익명성과 정부의 통제 방안 미비가 결합하여 사용자들에게 불법적인 행위를 유혹하는 유발요인이 되고 있다. 따라서 가상화폐의 경제적 유용성과 불법 사용의 통제라는 두 가지 목적을 절충하기 위해서는 정부의 규제 및 모니터링 강화가 필수적이다.

우리 정부도 거래자간 투명성 확보를 위하여 거래소의 실명거래를 강제하는 등 가상화폐 시장에 대한 통제를 강화하고 있지만 모든 국가가 동일한 시장규제 방안을 적용하고 있지 않으며 가상화폐 거래를 국내 거래소에서만 거래할 수 있는 게 아니라는 사실을 주시해야 한다. 또한, 사용자 개인이 보유하는 비수탁형 지갑을 이용한 거래도 여전히 자금거래 기록이 남지 않기 때문에 랜섬웨어 공격조직이 정부의 추적에서 빠져나갈 수 있는 '구멍'이 될 수 있다. 랜섬웨어 공격자는 자신이 받은 가상화폐를 규제는 약하고 유동성은 높은 다른 국가의 관할권으로 쉽게 옮길 수 있기 때문이다.

한 가지 더 고려해야 할 사항은 가상화폐 기술은 계속 발전하고 있다는 사실을 인지하고 기술 발전 속도에 맞게 정책적 대응도 발맞춰 나가야 한다는 사실이다. 앞장에서 설명한 '다크코인'의 등장과 함께 해커들 사이에서는 자금 추적을 회피하기 위한 수단으로 새롭게 '믹서'라는 서비스가 등장하였다. '믹서' 서비스는 가상화폐를 쪼개고 섞어서 재분배하는 기술로 기술 자체는 불법이 아니지만, 이 과정을 반복함으로써 자금 추적, 현금화 여부 등 가상화폐 거래 추적을 어렵게 만든다. 서비스형 랜섬웨어 공격자들의 자금을 섞어서 세탁을 해주고 일정 금액의 수수료를 나누는 방식이다. 따라서, 정부는 가상화폐 시장에서 사용자가 가상화폐를 쪼개고 이동하는 행위를 반복하거나 다수의 사용자가 하나의 계좌로 빈번하게 자금을 이체하는 등의 의심되는 이상거래를 모니터링하는 제도를 추가로 마련하고 국제 금융거래 공조를 통해 범죄자가 현금을 손에 넣거나 코인을 세탁하기 어렵게 만드는 것이 중요하다. 일예로 2022년 8월 미국 재무부는 북한과 연계된 해킹그룹 '라자루스'의 가상화폐를 세탁해준 혐의로 믹서(Mixer)업체인 '토네이도 캐시'를 제재한 바 있다[53].

4.2.3 국제 협력 및 정보공유 확대

오늘날 IT 인프라는 거대한 글로벌한 하나의 생태계로 통합되고 있다. 사이버공격으로 인한 피해는 일단 발생하면 국경을 넘나들며 그 피해가 주변으로 급속히 확산되는 특성이 있어 국가간 협력 및 정보공유가 무엇보다 중요한 이유이다. 실제로 러시아의 우크라이나 침공 등 국제안보 환경이 급격히 변화하고 있으며 실제로 국가 배후 해커들은 지금도 사이버공간에서 빈번히 충돌하고 있다.

사이버안보 이슈는 더 이상 한 국가만의 문제가 아니라 국가간 협력해야 하는 최우선 안보 의제이다. 이에 따라, 미국은 빈번히 발생하는 랜섬웨어 공격과 사이버안보 문제를 해결하기 위해 2021년 국무부 산하에 사이버·디지털 정책국을 만들었고 국제 해킹조직 대상의 제재시행 등 다양한 사이버안보 정책을 만들어 나가고 있다[51]. 다행스럽게도 우리 외교부도 2022년 6월 과학기술과 사이버안보 분야를 전담하는 '과학기술·사이버국'을 외교부 내에 신설하는 방안을 검토하고 있다[47]. 외교부는 과학기술·사이버국 신설을 계기로 IT기술·산업경제·안보를 융합하는 외교적 접근을 확대해야 한다. 특히, 랜섬웨어를 비롯한 전 세계적인 사이버위협에 대응하기 위해서 국제 공조가 필수적이라는 인식하에 동맹국 중심으로 안보협력을 보다 강력하게 추진해 나가야 한다.

또한, 민간기업과 정부 간 정보공유도 중요하다. 사이버안보에 대한 시민의식 향상이 우선되어야 랜섬웨어 등 사이버공격에 의한 국가·사회적 피해를 최소화할 수 있다. 더불어, 공격에 사용된 악성코드, 협박이메일·공격 IP주소·계좌정보 등을 관계기관과 피해기업간 실시간 공유하는 체계를 마련해야 하며 정부는 상황정보를 주기적으로 민간기업에 제공, 추가 확산을 막아야 한다. 물론, 이때에 피해기관에 관련된 구체정보는 노출하지 않음으로써 정보공유에 대한 민간의 불신을 최소화해야 한다. 더불어, 정보공유 방법·절차에 관한 구체적 사항을 정부 입법체계에 포함함으로

써 정보공유 과정에서 혹시 있을 수 있는 민·형사상 법적 책임을 면제해 주기 위한 면책권 부여 방안도 함께 고려해야 할 것이다.

4.2.4 해커 추적 및 국제 제재 동참

국경이 없는 사이버공간의 익명성과 초국경성을 이용하여 발생하는 랜섬웨어 공격은 시공간의 제약 없이 언제 어디에서나 일어날 수 있다. 랜섬웨어는 대표적인 사이버범죄 유형이지만 범죄의 증거가 되는 서버가 자국 영토 내에 있지 못하면 수사관할권이 없어 직접적인 수사가 불가능하다. 이에 따라 2001년 유럽평의회는 헝가리 부다페스트에서 사이버범죄에 대응하여 신속하게 디지털 증거를 확보하고 외국과의 수사 공조를 위하여 '부다페스트 협약'을 만들었다. 현재 유럽 대부분 국가들과 미국, 영국, 일본 등을 포함하여 전세계 66여 개 국가가 가입되어 있다[48]. 하지만 우리나라는 아직 미가입국으로 가입 검토만 수년째 하고 있다. 그동안은 협약 가입에 따른 국내법 개정 문제 등을 이유로 가입에 소극적이었다. 그러나 이제는 적극적으로 국제범죄자들에 대한 수사·추적 역량을 강화하고 우리 위상에 걸맞게 국제사회의 책임있는 국가로써의 역할 기여를 해야 할 것이다.

현실적으로 사이버범죄는 범인 추적과 검거실적 내기가 어렵다 그렇지만 조기에 성과를 내기가 어렵다는 이유로 사이버범죄 수사에 소극적이었던 기존의 관행에서도 탈피해야 한다. 대형화·집단화되며 국가안보를 위협하고 있는 랜섬웨어 해킹조직들을 추적하고 필요시 범죄자금도 압수할 수 있는 능력을 배양해야 한다. 실제 러시아·중국·북한 등 권위주의 국가에 거주하고 있어 검거를 못 할지라도 미 수사당국의 사례처럼 증거를 공개하고 전세계에 공개 수배하여 경고하는 전략을 펼쳐야 한다.국제사회에서 정보·수사기관 간 긴밀한 협력을 통해 우리 정부도 우리나라 기관·기업들을 공격하고 있는 국가 배후 해커들을 공개 지목, 경고함으로써 국제적으로 망신을 주는(Naming and Shaming) 전략도 유효하다. 동맹국간 국제제재 동참 효과를 노려볼 수도 있다.

지금까지는 랜섬웨어 공격을 예방하고 피해를 줄이는 것이 우리의 전략이었다면 이제는 적극적으로 해커를 추적·수사·기소·공개 경고함으로써 랜섬웨어 조직과 그 배후에 있는 국가를 대상으로 국제적인 압박을 가하는 적극적인 안보 정책을 구사해야 할 것이다.

4.2.5 '사이버보험제도'의 활성화

사이버보험제도는 1997년 미국 보험회사 AIG가 Y2K 문제를 계기로 세계 최초의 사이버보험을 판매함에 따라 시작되었다. 사이버보험의 주요 보상 내용으로는 데이터 유출과 관련된 피해 비용, 데이터 파괴 시 복구비, 개인정보 등 민감한 데이터가 누출되었을 경우 소송 진행과 관련된 비용, 랜섬웨어 감염에 의한 협박 비용 등이 포함된다[49].

정부가 실시하고 있는 국민의료보험제도와 마찬가지로 주요 기반시설과 같이 사회적으로 주요한 공적 서비스를 제공하거나 대량의 중요 데이터를 보유하고 있는 기업들을 사이버보험에 의무 가입하는 방안을 검토해 봐야 할 시점이다. 이를 통해 얻을 수 있는 장점은 해킹 등으로 인해 큰 피해를 입었을 때 피해보상을 받음으로써 사회적 위험을 분담할 수 있다는 점도 있지만 보험사 또는 보험사와 업무를 제휴한 보안 전문기업의 컨설팅 서비스를 통해 기업 스스로가 자사에 대한 사이버위협 발생 가능성, 보안취약성을 평가함으로써 자체 사이버 보안역량을 강화할 수 있다는 점을 추가로 고려해 볼 수 있다. 보험사는 개인이 의료보험에 가입할시 건강상태 및 질병 유무를 미리 체크하듯이 기업의 사이버 건강상태를 미리 체크해야 적정 요율의 보험료와 위험률을 산정할 수 있기 때문이다. 이런 접근방식은 자체 위험평가 능력이 부족한 중소기업에 특히 도움이 될 것이다. 물론 사이버보험이 투자 대비 효과가 불분명할 수 있다. 그러나 사이버보험제도 활성화는 사이버공격으로 인한 직접적인 손해 배상과 함께 사회 전반의 사이버보안 인식을 획기적으로 향상시킬 수 있는 좋은 대안이 될 것이다. 랜섬웨어 감염피해에 의한 사회적 비용을 낮추고 사회에 중요한 공적서비스를 제공하는 기업들에게 예방활동을 강제화하기 위해서도 적극 검토할 필요가 있다.

V. 결 론

4차 산업혁명 시대가 초래한 IT기반의 사이버공간은 정치·사회·경제·문화를 아우르는 국가의 주요한 인프라 환경이 되었으나 이는 생활의 편리함을 주는 동시에 우리에게 새로운 안보 위협 요소로 다가왔다. 북한, 중국, 러시아 등 한반도 주변국들 또한 이러한 사이버공간을 이용하여 실제로 우리의 안보를 위협하고 있다.

최근 랜섬웨어의 피해가 전세계적으로 급속히 확산됨에 따라 단순히 기술적인 보안의 문제, 범죄의 수준을 넘어 국가의 사이버안보에 심각한 영향을 주고 있음을 인식해야 한다. 본 논문에서는 최근 발생한 주요 랜섬웨어 피해사례와 함께 랜섬웨어 공격진화 양상을

살펴보고 코로나19로 인한 발생한 사회 전반의 디지털 대혁신, 가상화폐 시장과 다크웹의 확산, 서비스형 랜섬웨어(RaaS)의 등장을 랜섬웨어가 전세계적으로 급증하게 된 주요한 요인으로 분석하였다. 또한, 미국, 유럽 등 국제사회에서는 랜섬웨어의 급증 상황을 어떻게 국가 위협으로 바라보고 정책적 대응을 하고 있는지를 살펴보고 우리 정부의 대응 상황을 비교해 봄으로써 정부정책의 미흡한 점을 살펴보았다.

그 동안의 정부 대책은 피해를 수습하기 위한 단기 대책 위주로 그 장기적인 효과와 실효성에 의문이 든다. 사이버위협은 지속적으로 신기술이 적용되며 지능적으로 발전하고 있어 정책 또한 지속적인 개선이 필요하다. 또한, 정부의 규제성 정책으로 인해 IT산업의 발달을 저해하지 않으면서도 새롭게 국가 안보위협이 된 랜섬웨어를 효과적으로 차단하기 위해서 기존 정책의 틀을 지속 수정·보완해야 한다. 랜섬웨어의 사회적 피해는 점차 심각해져 국가의 주요 기본 기능을 마비시킬 수 있는 안보적 위협요인이 되었다. 따라서, 사이버공간이 국가안보에 있어 핵심영역이라는 사실을 인식하고 국가 주요 인프라를 보호할 수 있는 법적 제도적 기반을 마련하는 한편 가상화폐 시장이 불법의 온상이 되지 않도록 적절한 수준의 통제와 함께 해커조직들을 끈질기게 추적하고 국제제재에 적극적으로 동참하여야 한다. 이런 활동들을 통해 전세계 IT기술을 선도하는 디지털 강국으로써의 역할과 책임을 이행할 수 있으며 더 나아가 국제사회에 기여할 수 있게 된다.

우리 정부도 향후 보다 적극적인 사이버안보정책 실행을 통해 전 세계적으로 확산하고 있는 대규모 랜섬웨어에 의한 피해를 조기에 예방, 사회·경제적인 국가 손실에 대비할 수 있다. 사회 전반이 점점 더 사이버공간에 의존하게 됨에 따라 국가가 지속적으로 사이버공간을 안전하게 유지하는 것만이 국가 경쟁력을 유지하고, 국가안보를 확고히 할 수 있는 토대가 될 것이다.

References

[1] M. Kim, "*NIS 650 hacking cases in the first half of the year*," The Digital Times(2021. 7. 8), Retrieved Jul. 2, 2022. from: http://www.dt.co.krd/contents.html?articleno=2021070802109958044005.

[2] E. Park, S. Kim, S. Lee, and J. Kim, "Analysis of major and new ransomware trends in Korea and abroad 2019," *Rev. Korea Inst. Inf. Secur. and Cyrptol.*, vol. 29, no. 6, pp. 39-48, 2019.

[3] S. Kim, S. Kang, Y. Choi, G. Park, M. Lee, and J. Kim, "2021 Ransomware status and response/prevention policy trends," *Rev. Korea Inst. Inf. Secur. and Cyrptol.*, vol. 31, no. 6, pp. 5-11, 2021.

[4] H. Kwon, B. Jung, D. Moon, and I. Kim, "Technology trends for hacking and ransomware of connected medical devices," *Electr. and Telecommun. Trends*, vol. 36, no. 5, pp. 21-31, 2021. (https://doi.org/10.22648/ETRI.2021.J.360503)

[5] J. Kim, S. Ji, S. Kim, et al., "Machine learning-based ransomware detection model," *J. Secur. Eng.*, vol. 14, no. 4, pp. 263-80, 2017.

[6] J. Ok and E. Lim, "Proposal of a ransomware detection model using static and dynamic analysis information," in *Proc. KIISE 2018 Conf.*, vol. 6, pp. 1180-1182, 2018. (https://doi.org/10.5626/KTCP.2018.24.2.99)

[7] H.-K. Lee, J.-H. Seong, Y.-C. Kim, J.-B. Kim, et al., "The automation model of ransomware analysis and detection pattern," *J. KIICE*, vol. 21, no. 8, pp. 1581-1588, Aug. 2017. (https://doi.org/10.6109/jkiice.2017.21.8.1581)

[8] Naver website, "*Ransomware* (2017.3.2), Retrieved Jul. 1, 2022. from: https://ko.dict.nave.com/#/userEntry/koko/b95786bc372161252 fecaf8145c265fb.

[9] U.S. Department of Justice, "*North Korean Regime Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions,*" Sep. 6, 2018. Retrieved Jul. 5, 2022. from: https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

[10] U.S. CISA(Cybersecurity and Infrastructure Security Agency), "*Alert (TA17-132A) Indicators Associated With WannaCry Ransomware*," May 12, 2017. Retrieved Jul. 5, 2022. from: https://www.cisa.gov/uscert/ncas/

alerts/TA17-132A

[11] J. Freshlinger, "*Petya and Natpet, how are they different?*," CIOkorea, 2017.10.1, Retrieved Jul. 8, 2022. from: https://www.ciokorea.com/news/35938.

[12] U.S. Department of Justice, "*Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*," Oct. 19, 2020. Retrieved Jul. 5, 2022. from: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

[13] S. Ahn, *Coronavirus 'ransomware' in the digital world… The pandemic has begun*, Chosun ilbo, 2021.7.16, Retrieved Jul. 9, 2022. from: https://www.chosun.com/economy/mint/2021/07/16/6QU3IJSBLVCG5ML6GQKDT6RM24

[14] U.S. Department of State, "*DarkSide Ransomware as a Service (RaaS)*," Nov. 4, 2021. Retrieved Jul. 5, 2022. from: https://www.state.gov/darkside-ransomware‐as-a-service-raas/

[15] Yonhap News, *"Recovering ransomware damage" Controversy over 1.3 billion negotiations with hackers*, Yonhap News, 2017.6.5, Retrieved Jul. 4, 2022. from: https://www.yna.co.kr/view/AKR20170615125151017

[16] D. Oh, *"Ransom DDoS" wins during the holidays. "Threatening" to large domestic companies etnews*, 2020.10.05, Retrieved Jul. 15, 2022. from: https://www.etnews.com/20201005000122#.

[17] Yonhap News, *Eland, victim of ransomware attacks. New Core Outlets and others are suspended*, 2020.11.22, Retrieved May 8, 2022. from: https://www.wowtv.co.kr/NewsCenter/News/Read?articleId=A202011220064

[18] KISA(Korea Internet and Security Agency) of R.O.K. [Insight 2021 VOL.02] *Latest trends in ransomware and implications*, Korea Internet and Security Agency; 2021.08.23. Retrieved Jul. 5, 2022. from: https://www.kisa.or.kr/20301/form?postSeq= 4&page=1

[19] MSIT(Ministry of Science and ICT) of R.O.K. "*2021 Information Protection Survey Results*," Ministry of Science and ICT; 2022.04.14. Retrieved Jul. 5, 2022. from: https://www.msit.go.kr/publicinfo/view.do?sCode=user&mPid=62&mId=63&publictSeqNo=525&publictListSeqNo=8&formMode=R&referKey=525,8

[20] PWC website, "*2021 Annual Global CEO Survey*," Jan. 17, 2022. Retrieved May 13, 2022. Retrieved Jul. 5, 2022. from: https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2022.html

[21] NCSC(National cyber security center) of U.K., *Advisory: Covid-19 Exploited by Malicious Cyber Actors*, 12.2.2021. Retrieved Jul. 5, 2022. from: https://www.ncsc.gov.uk/files/Final20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf

[22] Wikipedia, "*Cryptocurrency*," Retrieved Jul. 2, 2022, from: https://ko.wikipedia.org/wiki/Cryptocurrency

[23] K. Park, *5.58 million actual users of virtual assets in Korea...The market is worth 55.2 trillion won*(2022.3.1), Retrieved May 14, 2022. from: http://news.heraldcorp.com/view.php?ud=2022

[24] U.S. Department of Justice, *How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets*, Jul. 01, 2022 Retrieved Jul. 5, 2022. from: https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

[25] Naver IT terminology website, "*Darkweb*," Retrieved Jul. 1, 2022. from: https://terms.naver.com/entry.naver?docId=3581037&cid=59088&categoryId=59096.

[26] D. Mangan, *World's biggest darknet marketplace, Russia-linked Hydra Market, seized and shut down*, CNBC, Apr. 5, 2022. Retrieved Jul. 8, 2022. from: https://www.cnbc.com/2022/04/05/darknet-hydra-market-site-seized-and-shut-down-doj-says.html

[27] Naver IT terminology website, "*Ransomware as a Service*," Retrieved Jul. 8, 2022. from: https://terms.naver.com/entry.naver?docId=3614624&cid=59088

[28] FBI, "*Understanding and Responding to the Solar Winds Supply Chain Attack. Federal Bureau of Investigation*," Mar. 18, 2021. Retrieved Jul. 5, 2022. from: https://www.fbi.gov/news/testimony/understanding-and-responding-to-the-solar-winds-supply-chain-attack-the-federal-perspective

[29] U.S. White House, "*Executive Order on Improving the Nation's Cybersecurity*," May 12, 2021. Retrieved Jul. 5, 2022. from: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[30] U.S. Department of State, "*Establishment of the Bureau of Cyberspace and Digital Policy*," Apr. 4, 2022. Retrieved Jul. 5, 2022. from: https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/

[31] U.S. White House, "*CARBIS BAY G7 SUMMIT. White House*," Jun. 13, 2021. Retrieved Jul. 5, 2022. from: https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/carbis-bay-g7-summit-communique/

[32]. U.S. White House, "*FACT SHEET: NATO Summit: Revitalizing the Transatlantic Alliance*," Jun. 13, 2021. Retrieved Jul. 5, 2022. from: https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/fact-sheet-nato-summit-revitalizing-the-transatlantic-alliance/

[33] U.S. White House, "*Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meetin*g," Oct. 14, 2021. Retrieved Jul. 5, 2022. from: https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

[34] U.S. White House, "*FACT SHEET: United States –ROK Partnership*," May 21, 2021. Retrieved Jul. 5, 2022. from: https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/21/fact-sheet-united-states-republic-of-korea-partnership/

[35] S. Zamost and E. Javers, *Secret Service seizes more than $102 million in crypto assets*, CNBC news, Apr. 19, 2022, Retrieved May 9, 2022. Retrieved Jul. 5, 2022. from: https://www.cnbc.com/2022/04/19/secret-service-seizes-more-than-102-million-in-crypto-assets.html

[36] ENISA(European Union Agency for Network and Information Security), "*ENISA Threat Landscape 2021*," Oct. 27, 2021. Retrieved Jul. 5, 2022. from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[37] Politico website, *In a first, EU slaps sanctions on hackers in Russia, North Korea, China*; Jul. 30, 2020, Retrieved May 9, 2022. Retrieved Jul. 5, 2022. from: https://www.politico.eu/article/eu-slaps-sanctions-on-hackers-in-russia-north-korea-china/

[38] European Parliament, *Proposal for a regulation to fight money laundering and counter terrorist financing*(Jul. 26, 2021), Retrieved Jul. 8, 2022. from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698862/EPRSBRI(2021)698862

[39] J. Hong, *Public sector cyber crisis alert, … "Hacking attack,"* Yonhap News, 2021. 8. 2, Retrieved Jul. 8, 2022. from: https://www.yna.co.kr/view/AKR202108021269

[40] MSIT(Ministry of Science and ICT) of R.O.K. "*Combining Ransomware Response Capabilities, Secure Digital Transformation and New Deal Support,"* 2021. 8. 5. Retrieved Jul. 5. 2022. from: https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&bbsSeqNo=94&nttSeq

[41] NCSC(National cyber security center) of R.O.K. "*2021 Annual Report*," NCSC, 2021. 12. 2. Retrieved Jul. 5, 2022. from: https://www.ncsc.go.kr:4018/cop/bbs/selectBoardList.do#LINK

[42] K. Kim, "Status of ransomware damage and countermeasures," *The J. Korea Internet Self-*

governance Organization, vol. 2021, no. 44, pp. 26-28, 2021.

[43] K. Staff, *Implementation of 'travel rules' for virtual asset operators*, KBS news, 2022. 3. 24, Retrieved Jul. 8, 2022. from: https://news.kbs.co.kr/news/view.do?ncd=5423118&ref=A.

[44] Naver IT Terminoloty website, "*Dark coin*" 2019. 10. 22, Retrieved Jul. 8, 2022. from: https://terms.naver.com/entry.naver?docId=5843890&cid=43667&categoryId=43667.

[45] The Presidential Office of R.O.K, "*President Yoon Seok yeol spoke at a joint press conference for the Korea-U.S. summit*," May 21, 2022. Retrieved Jul. 5, 2022. from: https://www.president.go.kr/ko/contents_new_view.php?code=220&sno=&opt=&id=brief&search_item=con_subject&search_keyword=%EC%A0%95%EC%83%81%ED%9A%8C%EB%8B%B4

[46] M.-J. Jeong, "The implications and implications of President Biden's signing of the Cyber Security Enhancement Act," *The Issues and Perspectives of National Aseembly Research Service*, vol. 1937, 2022. from : https://www.nars.go.kr/report/view.do?categoryId=&cmsCode=CM0043&searchType=TITLE&searchKeyword=%EC%82%AC%EC%9D%B4%EB%B2%84&brdSeq=38714

[47] MOFA(Ministry of Foreign Affairs) of R.O.K, "*Spokesman for the Ministry of Foreign Affairs*," Ministry of Foreign Affairs; 2022. 6. 16. Retrieved Jul. 5, 2022. from: https://www.mofa.go.kr/www/brd/m_4078/view.do?seq=368443

[48] H.-S. Yoon, H. Yoon, K.-H. Ra, and K. Ra, "Preemptive task for joining the Cybercrime," *Gachon Law Rev.*, vol. 12, no. 3, pp. 201-226, 2019. (https:/dx.doi.org/10.15335/GLR.2019.12.3.005)

[49] J. Kwon and S. Kim, "Key contents and issues of cyber insurance," *BFL(Business finance law),* vol. 105, pp. 39-51, 2021.

[50] U.S. Congress, "*Strengthening American Cybersecurity Act of 2022* (S. 3600)," 3. 2. 2022. Retrieved Jul. 5, 2022. from: https://www.congress.gov/bill/117th-congress/senate-bill/3600/text

[51] U.S. Department of State, "Establishment of the bureau of cyberspace and digital policy," 4. 4. 2022. Retrieved Jul. 5, 2022. from: https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/

[52] S. Lee, "Future Direction of national cyber security legislation and good governance," *Korea Administrative Law J.*, vol. 67, pp. 239-261, 2022. (https://doi.org/10.35979/ALJ.2022.03.67.239)

[53] U.S. Department of The_Treasury, "*U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*," Aug. 8, 2022. Retrieved Jul. 5, 2022. from: https://home.treasury.gov/news/press- releases/jy0916

김 진 민 (Jinmin Kim)

2000년 2월 : 숭실대학교 컴퓨터학부 졸업
2002년 2월 : 포항공과대학교 컴퓨터공학과 석사
2022년 3월~현재 : 숭실대학교 IT정책경영학과 박사과정
<관심분야> 사이버안보, IT보안 정책, 정보보안, 보안컨설팅, 공급망보안, 전자정부
[ORCID:0000-0003-3328-5260]

권 대 현 (Daehyun Kwon)

1997년 2월 : 한양대학교 전자공학과 졸업
2000년 2월 : 한양대학교 전자공학과 석사
2022년 3월~현재 : 숭실대학교 IT정책경영학과 박사과정
현재 : LS ELECTRIC 자동화연구소 근무 중
<관심분야> 산업용 통신, 사이버보안, IEC 표준

주 승 현 (Seunghyun Joo)

2015년 2월 : 세종사이버대학교 정보보호학과 졸업
2018년 8월 : 건국대학교 정보보안학과 석사
2021년 3월~현재 : 숭실대학교 IT정책경영학과 박사과정
현재 NCSOFT(엔씨소프트) 정보보안센터 근무 중
<관심분야> 정보보호, IT정책, 네트워크 보안

신 용 태 (Yongtae Shin)

아이오와대학교 전산학 박사학위를 취득하고 1995년부터 현재 숭실대학교 컴퓨터학부 교수로 재직 중이다. 한국인터넷윤리학회 회장, 한국정보처리학회 회장, 개방형통신연구회 회장 등을 역임
<관심분야> 컴퓨터 네트워크, 정보보호