정 보 보 호 학 회 지
제 32 권 제3호, 2022. 6

2021년 및 2022년 상반기 주요 랜섬웨어 대응 정책

강 수 진*, 김 종 성**

요 약

COVID-19로 인해 증가된 사이버 활동과 함께 랜섬웨어 공격으로 인한 피해사례도 증가하였다. 랜섬웨어 공격자들은 2021년 새로 발견된 취약점을 악용하고, 기업을 대상으로 공격하여 2차 피해를 야기하였다. 세계 각국에서는 이러한 피해를 줄이기 위해 랜섬웨어 대응을 위한 정책을 발표하였다. 본 논문에서는 2021년 큰 피해를 유발한 주요 랜섬웨어 공격을 정리한다. 관련된 2021년과 2022년 상반기까지 발표된 랜섬웨어 대응 정책을 조사하고 공통된 특징점을 찾아 4가지 유형으로 분류한다. 각 유형별로 최근 세계 정부 및 기관에서 제시하는 랜섬웨어 대응 동향에 대해 살펴본다.

Ⅰ. 서 론

악성 소프트웨어인 랜섬웨어(Ransomware)는 사용자의 시스템을 잠그거나 주요 파일을 암호화하여 접근을 제한하고 이를 인질로 몸값을 요구한다. 특히 COVID-19 이후 사이버 활동의 증가와 더불어 랜섬웨어의 공격도 증가하였다[1]. 랜섬웨어 공격자들은 새로 발견된 취약점을 악용하여 2차 피해가 연쇄적으로 발생할 수 있는 기업 및 소프트웨어 제공업체를 대상으로 공격을 수행하였다[2]. 또한, 주요한 사용자 및 기업의 데이터를 수집한 뒤, 다크웹 사이트에서 판매 및 유포하는 방법으로 기업의 피해를 증가하고 있다[3]. 이에 따라 세계 각국에서는 증가하는 랜섬웨어 공격에 대응하여 피해를 줄이기 위한 여러 랜섬웨어 대응 정책을 펼치고 있다. 본 논문에서는 2021년 동안 발생한 주요 랜섬웨어의 피해사례를 정리하고, 이에 대응하기 위해 제안된 랜섬웨어 대응 정책을 함께 정리한다. 랜섬웨어 대응 정책별 포함하는 내용을 기준으로 나누어 분류하고기 제안된 정책의 특징과 동향을 살펴본다.

논문의 구성은 다음과 같다. 2장에서는 2021년 발생한 주요 랜섬웨어 피해사례를 정리하며, 3장에서는 피해사례와 관련된 여러 랜섬웨어 정책을 소개한다. 끝으로 4장에서 결론으로 마무리한다.

Ⅱ. 2021년 주요 랜섬웨어 피해사례

본 장에서는 2021년 다수의 피해를 유발하여 추후 관련된 정책 및 대응 방안이 제시된 랜섬웨어의 피해사례를 다룬다.

2.1. Conti 랜섬웨어

3월 경, Conti 랜섬웨어는 미국의 241개의 학교, 센터 및 기술 대학이 속한 BCPS (Broward County Public Schools)의 서버를 암호화하는 공격을 수행하였다. 이로 인해 BCPS는 서버를 강제 종료해야 했으며, 서비스가 마비되었다[4]. 공격자들은 학생과 직원의 개인 정보, 계약 및 재무 문서가 포함된 1TB 이상의 데이터를 훔쳐 4천만 달러를 요구하였다. 9월에는 유럽의 글로벌 콜센터 서비스 제공업체인 GSS를 공격하였다[5]. 이 공격으로 IT 시스템 대부분이 마비되었으며, 스페인어 사용 고객 대상 콜센터의 운영이 중지되었다. 나아가 GSS 서비스를 사용하는 방송국, 상수도 회사와 이동통신업체의 업무에도 피해가 발생하였다. 9월 말, Conti 랜섬웨어는 일본의 다국적 전자 회사인 JVCKenwood의 일부 서버를 공격하였다[6]. 공격자들은 JVCKenwood 고객과 공급업체 정보, 재무 등에 관한 데이터를 포함한 1.7TB의 데이터를 훔쳤다고 주장

본 논문은 2022년도 과학기술정보통신부(암호이용활성화)의 재원으로 한국인터넷진흥원의 지원을 받아 수행된 연구사업임
* 국민대학교 금융정보보안학과 (대학원생, szin31@kookmin.ac.kr)
** 국민대학교 금융정보보안학과/정보보안암호수학과 (교수, jskim@kookmin.ac.kr)

하였다. 이를 증거로 직원의 여권 데이터를 일부 유출하고 700만 달러의 몸값을 요구하였다.

2.2. DarkSide 랜섬웨어

2월, DarkSide 랜섬웨어는 브라질의 전력 기업인 Eletrobras (Centrais Eletricas Brasileiras)와 Copel (Companhia Paranaense de Energia)를 공격하였다[7]. 공격으로 두 기업은 일부 시스템을 종료하였으며, 공격자들은 Copel 기업의 경영진과 고객의 개인 정보가 포함된 100GB의 데이터를 훔쳤다고 주장하였다. 5월 7일, DarkSide 랜섬웨어는 미국의 가장 큰 연료 운반 시스템 기업인 Colonial Pipeline를 공격하였다[8]. 이로 인해 5,500마일의 연료 파이프라인이 폐쇄되어 미국 내 연료 공급에 차질이 발생하여 석유값이 폭등하였다. 해당 기업은 데이터 유출을 막고 시스템을 복구하기 위해 공격자들에게 비트코인으로 440만 달러를 지불하였다[9].

2.3. REvil 랜섬웨어

5월 31일, REvil 랜섬웨어는 식품 회사이자 세계 최대의 육류 생산 기업인 JBS Foods를 공격하여 해당 기업의 모든 생산이 중단되었다[10]. 해당 기업은 자체적으로 일부 시스템을 복구하였으나, 고객 데이터의 유출을 막기 위해 공격자들과의 협상을 통해 1,100만 달러를 몸값으로 지급하였다. 7월 2일, REvil 랜섬웨어는 미국 IT 관리용 솔루션 제공업체인 Kaseya를 공격하여 이와 관련된 1,000개 이상의 관리형 서비스 제공업체인 MSP (Managed Service Provider) 기업을 공격하였다[11]. REvil 랜섬웨어는 수천 명의 고객을 보유한 MSP 기업을 표적으로 삼아 MSP 업체가 고객을 관리하기 위해 사용하는 RMM (Remote Monitoring and Management) 소프트웨어인 Kaseya VSA의 제로 데이 취약점(CVE-2021-30116)을 악용하여 공격하였다. 이 공격으로 REvil 랜섬웨어는 백만 개 이상의 시스템을 암호화하는 피해를 발생시켰다.

2.4. Hive 랜섬웨어

8월 15일, Hive 랜섬웨어는 미국의 오하이오와 웨스트버지니아에 있는 3개의 병원(Marietta Memorial Hospital, Selby General Hospital, Sistersville General Hospital)이 있는 비영리 통합 의료 시스템인 Memorial Health System을 공격하였다[12]. 이로 인해 임상 및 재정 운영에 차질이 생겨 긴급 수술과 방사선 검사가 취소되었으며, 약 200,000명의 환자 정보가 유출되었다. 11월 8일에는 유럽 전역에 1,000개 이상의 매장을 보유하고 있는 최대 규모의 전자 제품 아울렛인 MediaMarkt를 공격하였다[13]. 이 공격으로 신용카드, 직불 카드 결제와 같은 모든 IT 시스템이 마비되었다.

2.5. BlackMatter 랜섬웨어

9월 13일, BlackMatter 랜섬웨어는 일본의 의료 기술 회사인 Olympus를 공격하였다[14]. 이로 인해 유럽, 중동 및 아프리카의 IT 시스템에 영향을 미쳤으며, Olympus는 데이터 전송과 같은 네트워크 시스템을 종료하였다. 9월 20일, BlackMatter 랜섬웨어는 미국 아이오와주를 중심으로 하는 농업 기업인 New Cooperative Inc를 공격하였다[15]. 이로 인해 기업의 데이터가 암호화되어, 가축 사료 및 곡물 공급에 차질이 발생하였다. 공격자들은 직원 정보, 재무 문서, 연구 개발 문서, 토양 매핑 기술과 관련한 소스 코드를 포함하여 1,000GB 상당의 파일을 훔쳤다고 주장하며, 590만 달러의 몸값을 요구하였다[16]. 다음 날인 9월 21일, BlackMatter 랜섬웨어는 미디어 광고 및 트래픽 관리 서비스 제공업체인 Marketron을 공격하였다[17]. Marketron은 모든 서비스를 중지하고 대부분의 주요한 서비스를 오프라인으로 운영하였다. 이로 인해 해당 서비스를 사용하는 약 6,000개의 기업의 업무에 차질이 발생하였다.

2.6. Cuba 랜섬웨어

2월 3일, Cuba 랜섬웨어는 미국 내 여러 도시와 기관의 지불 처리에 사용되는 결제 시스템인 AFTS (Automatic Funds Transfer Services)를 공격하였다[18]. 일시적으로 웹사이트가 마비되었으며, 공격자들은 데이터 유출 페이지를 통해 이용자의 이름, 주소, 신용카드 정보와 같은 개인 정보를 훔쳤다고 주장하였다. 이로 인해 AFTS를 이용하는 도시 및 기관은 데이터 침해에 관한 안내를 진행하였다.

Ⅲ. 주요 랜섬웨어 대응 정책

지속적인 랜섬웨어 공격으로 인한 피해를 줄이고자 세계 정부 및 기관은 랜섬웨어 공격에 대응하기 위한 정책을 수립하고 있다. 각 대응 정책별에 따라 포함된 내용은 각기 상이하며, 공통적인 특징에 따라 정책을 크게 크게 4가지로 나누어 볼 수 있다[표 1].

A 정책의 경우, 일반 사용자 및 기업들을 대상으로 랜섬웨어 공격을 인식하여 위협에 대응할 수 있도록 안내하는 정책이다. B 정책의 경우, 특정 랜섬웨어의 공격 기술에 대한 세부 내용과 침해 지표를 안내하는 정책이다. C 정책의 경우, 랜섬웨어 공격 특징을 바탕으로 관련 정보를 제공하고 이에 대한 대응을 안내하는 정책이다. 마지막으로 D 정책의 경우, 랜섬웨어에 대응하기 위한 국가적 차원의 계획 발표 및 대응 기관, 조직의 설립 혹은 사이트 개설 등이 포함된다. 이를 기반으로 2021년과 2022년 상반기에 제안된 주요 랜섬웨어 대응 정책을 정리한 것은 [표 2]와 같다.

〔표 1〕 랜섬웨어 정책 내용별 타입

타입	내용
A	랜섬웨어 인식 고취 및 예방법 안내
B	랜섬웨어 공격 기술 세부 사항 혹은 침해 지표
C	랜섬웨어 정보 제공 및 대응 안내
D	랜섬웨어 대응 기반 구축 및 계획 발표

3.1. 랜섬웨어 인식 고취 및 예방법 안내

랜섬웨어 공격의 위험성에 대한 사용자 인식을 고취하고, 예방법을 안내하는 정책은 여러 국가에서 발행하고 있다. 2021년 상반기에는 미국과 영국에서 랜섬웨어 위협에 대한 전반적인 설명과 그에 따른 예방법을 안내하였다. 미국의 사이버보안 및 인프라 보안국인 CISA (Cybersecurity and Infrastructure Security Agency)는 랜섬웨어 위협 완화 캠페인을 통해 사이버 상의 랜섬웨어 위협에 대한 인식을 높이고자 하였으며[19], 영국의 국제 안보 연구소에서는 랜섬웨어 위협을 분석하여 조직, 정책 입안자, 법 집행 기관 및 국가 사이버 보안 기관이 위협에 대응하기 위한 행동 지침을 설명하였다[20]. 미국 국립표준기술연구소인 NIST (National Institute of Standards and Technology)는 랜섬웨어 공격에 대응하고 데이터를 보호하기 위한 방안을 제공하는 프로젝트를 발표하였다[21]. 9월에는 캐나다와 뉴질랜드에서 각각 랜섬웨어 예방에 관한 보고서를 발간하였다. 캐나다의 사이버 보안 센터인 CCCS (Canadian Centre for Cyber Security)는 조직이 랜섬웨어 공격에 어떻게 대응하고 복구해야 하는지에 대한 보고서를 발표하였다[22]. 뉴질랜드의 사이버 보안 센터인 NZ NCSC (National Cyber Security Centre)는 랜섬웨어가 기업을 대상으로 수행하는 일반적인 공격 방법에 관해 설명하고 이에 따라 각 공격 과정에 대응하기 위한 가이드를 발표하였다[23].

3.2. 랜섬웨어 공격 기술 세부 사항 혹은 침해 지표

2021년에 여러 피해사례를 유발한 DarkSide, Conti, Hive, BlackMatter 및 Cuba 랜섬웨어의 경우, 보고서 발행을 통해 해당 랜섬웨어의 공격 기법을 설명하고 IP 주소, 해시값 및 파일명과 같은 침해 지표를 제공하였다[24,25,26,27,28]. 2022년 상반기에는 Ragnar Locker, AvosLocker 및 BlackCat/ALPHV 랜섬웨어에 대한 세부 공격 기술 및 침해 지표가 포함된 보고서가 발행되었다[29,30,31]. 특히 REvil 랜섬웨어가 수행한 Kaseya 공격으로 대규모의 피해가 발생하였고, 이에 미국의 CISA와 FBI는 추가 피해를 막고자 관련된 사용자들의 행동 지침을 안내하였다[32]. MSP와 그 고객들이 수행해야 할 행동 지침을 통해 REvil 랜섬웨어로 인한 피해를 줄이고자 하였다.

3.3. 랜섬웨어 정보 제공 및 대응 안내

미국의 CISA와 FBI는 2021년 다수의 랜섬웨어 공격이 주말 및 업무 휴일 기간에 발생한 것을 파악하여 일반 사용자와 기업이 이를 인지하여 대응할 수 있도록 안내문을 발행하였다[33].

2022년에는 2021년 동안 발생한 랜섬웨어 공격을 분석하여 해당 정보를 제공하는 보고서들이 발행되었다. 미국 CISA에서는 랜섬웨어 동향을 분석하여 주요 기술을 설명하고 대응 방안을 제시하였으며[34], FBI는 2021년 발생한 랜섬웨어 공격과 피해에 대한 통계 정보를 제공하였다[35]. 4월에는 미국, 호주, 캐나다, 뉴질랜

〔표 2〕 2021년 및 2022 상반기 주요 랜섬웨어 대응 정책

날짜	국가 (기관)	주요 내용	관련 랜섬웨어	타입				참고 문헌
				A	B	C	D	
2022년 1월 21일	미국 (CISA)	랜섬웨어 인식 고취 및 위협 완화 캠페인	-	●				〔19〕
3월 29일	영국 (RUSI)	랜섬웨어의 위협을 분석하여 대응을 위한 접근 방식 제시	-	●				〔20〕
5월 4일	미국 (NIST)	랜섬웨어 위협 관리를 위한 사이버 보안 프레임 워크	-	●				〔21〕
5월 11일	미국 (CISA, FBI)	DarkSide 랜섬웨어 기술 세부 사항 및 경고문	DarkSide		●			〔24〕
5월 20일	미국 (FBI)	Conti 랜섬웨어 기술 세부 사항 및 경고문	Conti		●			〔25〕
7월 4일	미국 (CISA, FBI)	Kaseya 공격 피해자를 대상으로 한 행동 지침 발표	REvil		●			〔32〕
7월 14일	미국	랜섬웨어 정보 제공 사이트인 StopRansomware 사이트 개설	-				●	〔37〕
8월 5일	한국 (KISA)	한국형 StopRansomware 사이트 개설	-				●	〔38〕
8월 25일	미국 (FBI)	Hive 랜섬웨어 기술 세부 사항 및 경고문	Hive		●			〔26〕
8월 31일	미국 (CISA, FBI)	주말 및 휴일의 랜섬웨어 공격 대응 권고문	-			●		〔33〕
9월 13일	캐나다 (CCCS)	랜섬웨어 예방 및 대응 방안 방법 안내	-	●				〔22〕
9월 14일	뉴질랜드 (NZ CERT)	랜섬웨어로부터 보호 가이드 출시	-	●				〔23〕
10월 13일	호주	국가 차원의 랜섬웨어 대응 계획인 Ransomware Action Plan 발표	-				●	〔41〕
10월 18일	미국 (CISA, FBI, NSA)	BlackMatter 랜섬웨어 기술 세부 사항 및 경고문	BlackMatter		●			〔27〕
12월 3일	미국 (FBI)	Cuba 랜섬웨어 기술 세부 사항 및 경고문	Cuba		●			〔28〕
2022년 2월 7일	영국	국가 차원의 사이버 보안 향상 계획	-				●	〔42〕
2월 9일	미국 (CISA)	2021년 랜섬웨어 동향 기반으로 주요 기술과 이에 대한 대응 방안	-			●		〔34〕
3월 1일	미국 (CISA)	SHIELDS UP 페이지 개설	-				●	〔40〕
3월 7일	미국 (FBI)	Ragnar Locker 랜섬웨어 기술 세부 사항 및 경고문	Ragnar Locker		●			〔29〕
3월 22일	미국 (FBI)	2021년 3,700건 이상의 랜섬웨어 공격 및 피해 통계 정보 제공	-			●		〔35〕
3월 22일	미국 (FBI, FinCEN)	AvosLocker 랜섬웨어 기술 세부 사항 및 경고문	AvosLocker		●			〔30〕
4월 4일	미국	사이버 정책국 출범	-				●	〔39〕
4월 20일	미국 (FBI)	BlackCat/ALPHV 랜섬웨어 기술 세부 사항 및 경고문	BlackCat /ALPHV		●			〔31〕
4월 27일	미국, 호주, 캐나다, 뉴질랜드 및 영국	2021년 악용된 상위 취약점 상세 설명 및 대응 방안	-			●		〔36〕

드 및 영국의 보안 기관들이 협력하여 2021년 랜섬웨어 공격자들이 공격에 악용한 여러 취약점을 상세 설명하고 이에 대한 대응 방안을 제공하였다[36]. 이를 통해 사용자들이 취약점을 인지하고 업데이트와 같은 방식으로 보완하여 랜섬웨어 공격에 대응할 수 있도록 하였다.

3.4. 랜섬웨어 대응 기반 구축 및 계획 발표

랜섬웨어에 대응하기 위해 사이트 개설 및 관련 정책국 출법과 같은 대응 기반은 지속하여 마련되고 있다. 2021년 미국에서는 랜섬웨어 정보를 제공하고 공유하는 사이트인 'StopRansomware' 사이트를 개설하였다[37]. 이를 통해 다양한 기관에서 수집한 랜섬웨어와 관련된 정보를 신속하게 공유할 수 있으며, 랜섬웨어 신고와 사용자 권장 사항 등을 제공한다. 이후 한국에서도 한국형 'StopRansomware' 사이트를 개설하였다[38]. 다양한 복구 도구를 제공하고 랜섬웨어 피해를 상세히 신고할 수 있도록 하여 신속한 대응을 수행하고자 한다. 2022년 미국은 사이버 정책국의 출범을 통해 사이버 환경에서 요구되는 정책과 보안 사항을 마련하고자 한다[39]. 또한, 2022년 발생한 러시아와 우크라이나 전쟁으로 미국 CISA는 러시아의 사이버 공격에 대응하기 위해 'SHIELDS UP' 페이지 개설하였다[40]. 해당 페이지를 통해 사이버 공격에 관한 정보와 이에 대한 대응 방안을 제공한다.

국가 차원에서 랜섬웨어에 대응하기 위한 계획도 지속적으로 발표되고 있다. 2021년 호주는 국가 차원에서 사이버 보안을 강화하여 랜섬웨어에 대응하기 위한 계획을 발표하였다[41]. 2022년 영국은 랜섬웨어를 포함한 사이버 공격에 대응하기 위해 사이버 보안을 향상하기 위한 계획을 발표하였다[42]. 이러한 국가 차원의 랜섬웨어 대응은 사이버 보안에 대응하기 위한 조직을 구성하거나 협력을 통한 랜섬웨어 공격자들에 대한 수사에 관한 계획을 포함한다.

Ⅳ. 결 론

랜섬웨어는 몸값을 지불할 능력이 있는 대기업 뿐 아니라 2차 피해를 야기할 수 있는 대상에게 지속적인 공격을 수행하고 있다. 2021년에는 국가 인프라 제공 기업과 MSP 업체를 대상으로 다수의 피해사례가 발생하였으며, 이에 대응하기 위해 세계 정부와 기관들은 랜섬웨어 대응 정책을 발표하였다. 대응 정책은 크게 랜섬웨어 인식 고취 및 예방법 안내, 특정 랜섬웨어의 공격 기술 및 침해 지표 안내, 전반적인 랜섬웨어 정보 제공 및 랜섬웨어 대응 기반 구축 및 계획 발표로 나누어 볼 수 있었다. 특히 2022년 상반기에는 지난해와 비교해 2021년 동안의 랜섬웨어 공격을 분석한 정책이 다수 발표되었다. 랜섬웨어 대응 정책의 분류를 통해 랜섬웨어 대응에 관한 동향을 파악할 수 있었으며, 향후 랜섬웨어 대응과 관련된 계획을 구축하는 데 기반 자료로 활용되기를 기대한다.

참 고 문 헌

[1] "Ransomware attacks nearly doubled in 2021", Security Magazine, https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021, Feb. 2022.

[2] "2021 Top Routinely Exploited Vulnerabilities", CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-117a, Apr. 2022.

[3] "[랜섬웨어 공격 동향과 방어 기술①] 돈 되는 곳 집중하는 랜섬웨어", 데이터넷, https://www.datanet.co.kr/news/articleView.html?idxno=164660, Sep. 2021.

[4] "Conti Ransomware gang demanded $40 million ransom to Broward County Public Schools", Security Affairs, https://securityaffairs.co/wordpress/116254/cyber-crime/broward-county-public-schools-ransomware.html, Apr. 2021.

[5] "Major European call center provider goes down in ransomware attack", The Record by Recorded Future, https://therecord.media/major-european-call-center-provider-goes-down-in-ransomware-attack/, Sep. 2021.

[6] "JVCKenwood hit by Conti ransomware claiming theft of 1.5TB data", BleepingComputer, https://www.bleepingcomputer.com/news/security/jvckenwood-hit-by-conti-ransomware-claiming-theft-of-15tb-data/, Sep. 2021

[7] "Eletrobras, Copel energy companies hit by ran-

somware attacks", BleepingComputer, https://www.bleepingcomputer.com/news/security/eletrobras-copel-energy-companies-hit-by-ransomware-attacks/, Feb. 2021.

[8] "US declares state of emergency after ransomware hits largest pipeline", BleepingComputer, https://www.bleepingcomputer.com/news/security/us-declares-state-of-emergency-after-ransomware-hits-largest-pipeline/, May. 2021.

[9] "Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers", The New York Times, https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html, May. 2021.

[10] "JBS Paid $11 Million to Resolve Ransomware Attack", The Wall Street Journal, https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781, Jun. 2021

[11] "Kaseya: Roughly 1,500 businesses hit by REvil ransomware attack", BleepingComputer, https://www.bleepingcomputer.com/news/security/kaseya-roughly-1-500-businesses-hit-by-revil-ransomware-attack/, Jul. 2021.

[12] "Hive ransomware attacks Memorial Health System, steals patient data", Bleeping Computer, https://www.bleepingcomputer.com/news/security/hive-ransomware-attacks-memorial-health-system-steals-patient-data/, Aug. 2021.

[13] "Electronics Outlet MediaMarkt Hit by Ransomware Attack Demanding $50M in Bitcoin", Decrypt, https://decrypt.co/85709/electronics-outlet-mediamarkt-hit-ransomware-attack-demanding-240m-bitcoin, Nov. 2021.

[14] "BlackMatter ransomware hits medical technology giant Olympus", BleepingComputer, https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-hits-medical-technology-giant-olympus/, Sep. 2021.

[15] "Iowa Grain Cooperative Hit by Cyberattack Linked to Ransomware Group", The Wall Street Journal, https://www.wsj.com/articles/iowa-grain-cooperative-hit-by-cyberattack-linked-to-ransomware-group-11632172945, Sep. 2021.

[16] "After ransomware attack, company finds 650+ breached credentials from NEW Cooperative employees", ZDNet, https://www.zdnet.com/article/after-ransomware-attack-company-finds-650-breached-credentials-from-new-cooperative-ceo-employees/, Sep. 2021.

[17] "Marketron marketing services hit by Blackmatter ransomware", BleepingComputer, https://www.bleepingcomputer.com/news/security/marketron-marketing-services-hit-by-blackmatter-ransomware/, Sep. 2021.

[18] "Hack of Seattle payments processing firm puts local governments on alert", The Seattle Times, https://www.seattletimes.com/seattle-news/hack-of-seattle-payments-processing-firm-puts-local-governments-on-alert/, Feb. 2021.

[19] Cybersecurity and Infrastructure Security Agency, "RANSOMWARE GUIDANCE AND RESOURCES", https://www.cisa.gov/ransomware. Jan. 2021.

[20] Royal United Services Institute, "Emerging Insights", https://rusi.org/publication/emerging-insights/ransomware-perfect-storm. Mar. 2021.

[21] National Institute of Standards and Technology, "Ransomware Protection and Response", https://csrc.nist.gov/projects/ransomware-protection-and-response, May. 2021

[22] Canadian Centre for Cyber Security, "Ransomware: How to prevent and recover (ITSAP.00.099)", https://cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099, Sep. 2021.

[23] CERTNZ, "Protecting from ransomware", https://www.cert.govt.nz/business/guides/protecting-from-ransomware/, Sep. 2021

[24] Cybersecurity and Infrastructure Security Agency, "DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks", https://www.cisa.gov/uscert/ncas/alerts/aa21-131a, Jul. 2021.

[25] Internet Crime Complaint Center(IC3), "Conti Ransomware Attacks Impact Healthcare and First Responder Networks", https://www.ic3.gov/Media/News/2021/210521.pdf, May. 2021.

[26] Internet Crime Complaint Center(IC3), “Indicators of Compromise Associated with Hive Ransomware”, https://www.documentcloud.org/documents/21049431-fbi-flash-hive-ransomware-iocs, Aug. 2021.

[27] Cybersecurity and Infrastructure Security Agency, “BlackMatter Ransomware”, https://us-cert.cisa.gov/ncas/alerts/aa21-291a, Oct. 2021.

[28] Internet Crime Complaint Center(IC3), “Indicators of Compromise Associated with Cuba Ransomware”, https://www.ic3.gov/Media/News/2021/211203-2.pdf, Dec. 2021.

[29] Internet Crime Complaint Center(IC3), “RagnarLocker Ransomware Indicators of Compromise”, https://www.ic3.gov/Media/News/2022/220307.pdf, Mar. 2022.

[30] Cybersecurity and Infrastructure Security Agency, “FBI and FinCEN Release Advisory on AvosLocker Ransomware”, https://www.cisa.gov/uscert/ncas/current-activity/2022/03/22/fbi-and-fincen-release-advisory-avoslocker-ransomware, Mar. 2022.

[31] Internet Crime Complaint Center(IC3), “BlackCat/ALPHV Ransomware Indicators of Compromise”, https://www.ic3.gov/Media/News/2022/220420.pdf, Apr. 2022.

[32] Cybersecurity and Infrastructure Security Agency, “CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack”, https://www.cisa.gov/uscert/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa, Jul. 2021.

[33] Cybersecurity and Infrastructure Security Agency, “Ransomware Awareness for Holidays and Weekends”, https://us-cert.cisa.gov/ncas/alerts/aa21-243a, Aug. 2021.

[34] Cybersecurity and Infrastructure Security Agency, “2021 Trends Show Increased Globalized Threat of Ransomware”, https://www.cisa.gov/uscert/ncas/alerts/aa22-040a, Feb. 2022.

[35] U.S. Federal Bureau of Investigation (FBI), “2021 Internet Crime Report”, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf, Mar. 2022.

[36] Cybersecurity and Infrastructure Security Agency, “2021 Top Routinely Exploited Vulnerabilities”, https://www.cisa.gov/uscert/ncas/alerts/aa22-117a, Apr. 2022.

[37] “Stop Ransomware”, https://www.cisa.gov/stopransomware

[38] “KISA Stop Ransomware”, https://boho.or.kr/ransom/main.do

[39] “Establishment of the Bureau of Cyberspace and Digital Policy”, U.S. Department of State, https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/, Apr. 2022.

[40] “Shields Up”, https://www.cisa.gov/shields-up

[41] Department of Home Affairs, “RANSOMWARE ACTION PLAN”, https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf, Oct. 2021.

[42] GOV.UK, “National Cyber Strategy 2022”, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022, Feb. 2022.

〈저 자 소 개〉

강 수 진 (Soojin Kang)

정회원

2018년 2월 : 국민대학교 정보보안암호수학과 졸업

2022년 2월 : 국민대학교 금융정보보안학과 석사

2022년 3월 ~ 현재 : 국민대학교 금융정보보안학과 박사과정

<관심분야> 디지털 포렌식, 정보보호

김 종 성 (Jongsung Kim)

종신회원

2006년 11월 : K.U.Leuven, ESAT/SCD-COSIC 정보보호 공학박사

2007년 2월 : 고려대학교 정보보호대학원 공학박사

2009년 9월~2013년 2월 : 경남대학교 e-비즈니수학과 교수

2013년 9월~2017년 2월 : 국민대학교 수학과 교수

2017년 3월 ~ 현재 : 국민대학교 정보보안암호수학과/금융정보보안학과 교수

<관심분야> 정보보호, 암호 알고리즘, 디지털 포렌식