정 보 보 호 학 회 지
제 31 권 제6호, 2021. 12

2021년 랜섬웨어 현황 및 대응/예방 정책 동향

김 소 람*, 강 수 진*, 최 용 철*, 박 귀 은**, 이 민 정**, 김 종 성***

요 약

랜섬웨어는 2021년 가장 주목해야 할 사이버 위협으로 여겨지며, 전 세계적으로 큰 피해를 입혔다. 특히 국가 핵심 인프라 시설과 기업을 대상으로 대규모 공격을 지속하였으며, 파일을 암호화하는 것 뿐만 아니라 기업의 기밀 정보를 유출함으로써 2차 피해 우려를 낳고 있다. 이에 따라 세계 각국에서는 랜섬웨어를 대응 및 예방하고자 다양한 지침을 발표하였다. 본 논문에서는 2021년 국내·외에서 발생한 랜섬웨어 사건·사고와 새롭게 등장한 랜섬웨어에 대해 알아보고, 국가별 랜섬웨어 대응 및 예방 정책에 관해 소개한다.

Ⅰ. 서 론

과학기술정보통신부가 발표한 ‘21년 사이버 위협 분석 및 ‘22년 전망 분석에는 모두 랜섬웨어 공격에 대한 내용이 포함되어 있다[1]. 이처럼 랜섬웨어는 국내·외 기관과 기업들이 주요하게 여겨야 할 사이버 위협으로 분류되며, 갈수록 고도화/지능화되는 형태를 보인다. 피싱 공격보다는 취약점을 통해 공격하는 비율이 높으며, 공급망 공격 등을 통하여 광범위한 피해를 일으키는 형태로 변화하고 있다[2].

랜섬웨어 피해 규모가 커짐에 따라 세계 주요 국가들은 랜섬웨어에 대응 및 예방하기 위한 방안을 지속적으로 발표하고, 랜섬웨어 공격 그룹을 추적하기 위해 공조 수사 등을 펼치고 있다. 국내에서는 경찰 조직이 루마니아, 필리핀과 미국 등 10개국과 공조 수사를 진행해 최초로 갠드크랩(GandCrab) 유포 사범을 검거하였다[3]. 또한 향후에 발생할 랜섬웨어 공격에 대응하고자 정부 기관에서는 랜섬웨어 대응 웹 서비스와 24시간 대응할 수 있는 지원반을 운영하고 있다[4].

본 논문의 2장에서는 2021년에 발생한 랜섬웨어 사건·사고를 국내와 국외로 나누어 정리하였으며, 3장에서는 2021년에 새롭게 등장한 랜섬웨어에 대한 특징을 살펴본다[5,6,7]. 4장에서는 랜섬웨어를 대응 및 예방하기 위해 세계 각국에서 제시한 지침을 소개한다. 5장에서는 2021년에 공개된 랜섬웨어의 복구 도구에 관해 소개하며 마지막 6장을 결론으로 마무리한다.

Ⅱ. 2021년 랜섬웨어 사건·사고

2021년에는 기아자동차, LG전자 및 CJ셀렉타 등 국내 대기업의 국외 법인들이 랜섬웨어에 피해를 보았다. 또한, 미국 송유관 시설 공격에 이어 IT 자동화 관리 소프트웨어인 카세야(Keseya) 공급망 공격이 발생하는 등 국가 핵심 인프라 시설 및 기업을 대상으로 하는 대규모 공격이 다수 발생하였다.

2.1. 국내 랜섬웨어 피해사례

랜섬웨어 피해를 본 국내 주요 기업은 [표 1]과 같다[8,9,10]. CJ 제일제당의 브라질 자회사인 CJ 셀렉타는 Avaddon 랜섬웨어에 감염되었다. 감염 이후 일정 시간 서버를 중단하고 초기 대응을 하였으며, 감염 이후 컴퓨터를 포맷하여 공격자들의 몸값 요구에 대응하지 않았다.

LG생활건강 베트남법인도 Avaddon에 감염되었으며, 내부 계약 문건과 고객사 명단 등 기업 내부 문서를 다크웹을 통해 유출되는 피해를 당하였다. 그러나 이후에 자료 백업 및 포맷, 운영체제(OS) 재설치 작업

본 연구는 2021년도 과학기술정보통신부(암호이용활성화)의 재원으로 한국인터넷진흥원의 지원을 받아 수행되었습니다.
* 국민대학교 금융정보보안학과 (대학원생, kimsr2040@kookmin.ac.kr, szin31@kookmin.ac.kr, chldydcjf@kookmin.ac.kr)
** 국민대학교 정보보안암호수학과 (대학생, dhnr16@kookmin.ac.kr, jenna0825@kookmin.ac.kr)
*** 국민대학교 정보보안암호수학과/금융정보보안학과 (교수, jskim@kookmin.ac.kr)

〔표 1〕 2021년 국내 랜섬웨어 주요 피해사례

시기	기업명	랜섬웨어명	피해내용
2월	기아자동차 북미법인	DoppelPaymer	자동차 도면, 재무자료 등 유출
4월	CJ셀렉타	Avaddon	직원 이메 일 정보 등 유출
4월	LG생활건강 베트남법인	Avaddon	내부 계약 문건, 고객사 명단 유출
5월	SL 코퍼레이션	Avaddon	개인 여권 사본, 신용카드 정보 유출
5월	LG전자 북미법인	Conti	테스트 제품 관련 파일, 직원 컴퓨터 이름 유출
8월	진양오일씰	LockBit 2.0	-
8월	풀무원 미국법인	LockBit 2.0	-

을 진행하였다고 밝혔다.

국내 자동차 부품업체 SL 코퍼레이션 또한 Avaddon 랜섬웨어에 감염돼 여권 사본, 신용카드 정보를 포함한 임직원 개인정보와 함께 물품 계약서, 문서 등 해외 사업 관련 데이터를 다크웹을 통해 유출되는 피해를 보았다.

LG전자의 북미법은 Conti 랜섬웨어에 공격당해 내부 계약 문건, 고객사 명단 등의 민감한 데이터 약 28MB의 7개의 파일이 다크웹을 통해 유출되었다.

2.2. 국외 랜섬웨어 피해사례

국외 피해사례 중 주요한 사건은 [표 2]와 같다[11]. 일부 기업은 시스템 복구 및 데이터 유출을 막기 위해 몸값을 지불하기도 하였다.

미국 최대의 송유관 관리 업체인 Colonial Pipeline은 DarkSide 랜섬웨어에 공격으로 네트워크를 종료하고 5,500마일의 연료 파이프라인을 폐쇄하였다[12]. 이로 인해 해당 지역의 연료 공급이 절반 가까이 중단되었으며, 이후 시스템 재개를 위해 공격자들에게 75 비트코인(거래 당일 기준 약 440만 달러)을 지급하여 데이터를 복구하였지만, FBI의 수사를 통해 63.7 비트코인을 회수하였다[13].

세계 최대의 육류 생산 회사인 JBS Foods가 Revil

〔표 2〕 2021년 국외 랜섬웨어 주요 피해사례

시기	기업명	랜섬웨어명	피해내용
3월	CNAFinacial	Phoenix	4천만 달러 지불
4월	Brenntag	Darkside	440만 달러 지불
5월	Colonoal Pipeline	Darkside	440만 달러 지불
5월	JBS Foods	REvil	약 천만 달러 지불
7월	Kaseya	REvil	-

랜섬웨어로 인해 호주 및 북미 지부의 IT 시스템 일부가 암호화되었다. 이에 영향을 받는 모든 시스템이 중단되고 식품 생산 사이트가 폐쇄되었으나, 백업 시스템을 통해 시스템을 복구하였다. 그러나 공격자가 탈취한 고객들의 데이터 유출을 막기 위해 협상을 통해 1,100만 달러를 몸값으로 지급하였다[14].

REvil 랜섬웨어는 Kaseya VSA를 공격하여 수많은 관리형 서비스 제공업체 MSP[1] (Managed Service Provider)를 감염시켰다[15]. 공격자들이 몸값으로 7,000만 달러를 요구하였지만 이에 대응하지 않았다.

Ⅲ. 2021년 신규 랜섬웨어

2021년에 새롭게 등장한 주요 랜섬웨어 목록과 특징은 [표 3]과 같다. 암호 알고리즘 또는 암호화 방식이 발견된 경우, 주로 파일 암호화에 사용하는 대칭키 알고리즘은 AES 알고리즘이 파일 암호키 암호화에 사용하는 비대칭키 알고리즘에는 RSA 알고리즘을 활용한다. 대부분이 윈도우에서 동작하며, 15개 랜섬웨어 중 복구 및 복호화 가능한 랜섬웨어는 Black Kingdom, Lorenz, Hive와 AtomSilo 4종이다.

Black Kingdom 랜섬웨어는 2021년 3월 23일 이후 암호키 공유시스템에 접근할 수 없어 랜섬웨어 내부에 고정된 키로 암호화하므로 복호화 가능하였다. AtomSilo 랜섬웨어는 공격자가 복호화 키를 공개하였고, Hive 랜섬웨어는 암호화 과정의 취약점이 발견되어 복호화 가능하였다.

1) 기업의 컨텐츠 및 네트워크 컨설팅, 네트워크 시스템 구축, 모니터링 및 관리를 제공하는 업체

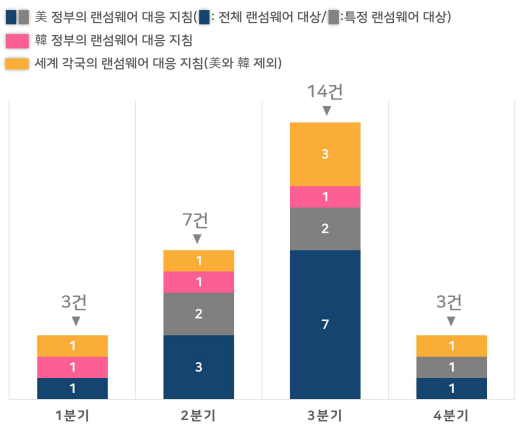
〔표 3〕 2021년도 신규 랜섬웨어

랜섬웨어	대칭키		비대칭키		동작 환경	복구/복호화 가능 여부
	키 생성방식	알고리즘	키생성방식	알고리즘		
DeroHE〔16〕	-	-	-	-	윈도우	X
Babuk Locker〔17〕	RtlGenRandom /SHA256	ChaCha8	-	-	윈도우	X
Black Kingdom〔18〕	MD5	AES256CBC	-	-	윈도우	O*
Sarbloh〔19〕	-	AES128CBC	-	RSA	윈도우	X
Lorenz〔20〕	CryptDeriveKey	AES128CBC	-	RSA	윈도우	O
AstroLocker〔21〕	-	ChaCha20	-	RSA	윈도우	X
N3TW0RM〔22〕	-	-	-	-	윈도우	X
Epsilon Red〔23〕	-	-	-	-	윈도우	X
LockFile〔24〕	-	AES	-	-	윈도우	X
Hive〔25〕	-	XOR	-	RSA	윈도우	O
BlackMatter〔26〕	RDRAND	Salsa20	-	RSA1024	윈도우	X
AtomSilo〔27〕	AESKEYGENA SSIST	AES256	-	RSA	윈도우	O
Chaos〔28〕	-	-	-	-	윈도우	X
MacawLocker〔29〕	-	-	-	-	윈도우	X
Yanluowang〔30〕	-	-	-	-	윈도우	X

- : 알려지지 않음
*: 2021년 3월 23일 이후 감염된 경우 복구 가능

Ⅳ. 2021년 랜섬웨어 대응 및 예방 지침

랜섬웨어로 인한 피해 규모가 증가 및 확대됨에 따라 세계 각국에서는 랜섬웨어 대응 및 예방 지침을 발표하였다. 2021년 분기별 랜섬웨어 대응 및 예방 지침 건수는 (그림 1)과 같다. 총 27건 중에서 22건은 전반적인 랜섬웨어에 관련한 정책이며, 5건은 특정 랜섬웨어 대한 지침이다.



〔그림 1〕 2021년 세계 각국에서 발표한 랜섬웨어 대응 및 예방 지침 통계

4.1 국내 랜섬웨어 대응 및 예방 지침

2월 18일, 과학기술정보통신부에서는 디지털상 존재하는 여러 보안 위협에 대응하기 위한 “K-사이버 방역 추진전략”을 발표하였다. 이를 통해 사이버 위협정보를 실시간으로 수집하고 공유하며, 침해사고 발생 시 신속한 피해 복구 및 재발 방지를 위한 지원을 수행하는 것을 목표로 하였다[31].

5월 21일, 한국인터넷진흥원에서는 랜섬웨어를 포함한 사이버 위협을 예방하고자 인공지능 및 빅데이터 기술을 활용한 위협 정보 공유 체계 및 예방 시스템의 확립 계획인 “랜섬웨어 예방 체계 구축”을 발표하였다[32].

8월 5일, 한국인터넷진흥원에서는 랜섬웨어 대응을 위해 랜섬웨어 대응 방안 및 복구 프로그램 관련 사이

트를 제공하는 한국형 Stop Ransomware 사이트를 개설하였다. 기존 여러 사이트에 흩어져 있던 랜섬웨어 관련 자료를 하나로 모아 사용자의 정보 접근성을 높이며, 랜섬웨어에 관한 보안 공지, 최신 동향과 같은 다양한 정보를 제공하고 있다[33].

4.2 국외 랜섬웨어 대응 및 예방 지침

1월 21일, 미국의 국토안전부 산하의 사이버보안 및 인프라 보안국인 CISA (Cybersecurity and Infrastructure Security Agency)는 랜섬웨어에 대한 인식을 높이고 랜섬웨어의 위협에 대응하고자 랜섬웨어 위협 완화 캠페인을 진행하였다[34].

4월 29일, 2021년 초 글로벌 랜섬웨어 위협에 대응하기 위해 설립된 미국의 Ransomware Task Force (RTF)는 랜섬웨어 예방 및 대응을 위해 정부 및 업계에서 취할 수 있는 자세한 행동 지침을 설명하는 보고서를 발행하였다[35].

5월 4일, NIST는 “Ransomware Protection and Response” 프로젝트를 발표하여 이 프로젝트를 통해 기업이 랜섬웨어 공격에 대비하기 위한 팁과 대응 방안, 랜섬웨어로부터 데이터를 보호하는 방법에 대한 정보와 랜섬웨어 사고 대응 능력 향상을 위한 정보를 제공하였다[36].

5월 12일에는 미국 백악관에서는 국가의 사이버 보안을 개선하고 연방 정부 네트워크를 보호하기 위해 “FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation’s Cybersecurity and Protect Federal Government Networks”를 발행하였다[37].

6월 11일부터 3일간 영국에서 열린 G7 정상회담에서 영국, 미국, 캐나다, 일본, 독일, 프랑스 및 이탈리아의 지도자들은 랜섬웨어에 대응하기 위한 국가 간의 협력을 강조하는 계획을 밝혔다[38].

7월 12일, 인터폴(Interpol, 국제형사경찰기구)의 사무총장은 기업이 단독으로 랜섬웨어 관련 문제를 해결하기보다 경찰 기관과 기업들이 글로벌 연합을 구성하여 협력할 것을 촉구하였다[39].

7월 14일, CISA와 FBI, NIST 등 모든 美 연방 정부 기관에서 수집한 랜섬웨어에 대한 정보를 제공하는 최초의 공동 웹사이트인 StopRansomware 사이트를 개설하였다[40].

7월 15일, 美 국무부의 국제 테러를 방지하기 위해 설립된 대테러 보상 프로그램인 RFJ (Rewards for Justice)는 RFJ 프로그램을 확대하여 악의적인 사이버 활동을 수행하는 사람의 신원이나 위치를 알려주는 정보에 대해 최대 1,000만 달러의 보상을 제공하기로 하였다[41].

7월 28일, 美 대통령은 중요 인프라와 사이버 보안 강화를 위한 국가 차원의 보안 각서인 “National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems”를 발표하였다[42].

8월 5일, 미국의 CISA는 랜섬웨어 및 기타 사이버 위협으로부터 미국의 중요 기반 시설을 보호하는 데 중점을 둔 공공 및 민간 부문의 파트너십인 JCDC를 발표하였다[43].

8월 31일, 미국 FBI와 CISA는 최근 기업의 주말과 휴일 동안에 랜섬웨어 공격이 증가하는 것을 발견하여, 이에 대응할 것을 촉구하는 권고 사항을 발표하였다[44].

9월 13일, 캐나다의 사이버 보안 센터인 Canadian Centre for Cyber Security은 조직을 랜섬웨어로부터 보호하기 위한 사전 예방 방안과 공격 발생 이후 수행해야 할 조치사항을 발표하였다[45].

9월 14일, 뉴질랜드의 사이버 보안을 대처하기 위해 설립된 CERT는 기업을 위해 랜섬웨어의 일반적인 공격 경로, 랜섬웨어 작동 방식 및 랜섬웨어로부터 장치를 보호하는 방법 등을 포함한 랜섬웨어 보호 가이드를 출시하였다[46].

9월 21일, 美 재무부는 지난해 10월 발행한 랜섬웨어 공격 주의 권고문을 갱신하여, 랜섬웨어의 공격에 대응하는 방안으로 다른 부서, 기관 및 해외 기관과 협력하여 불법적인 목적으로 사용되는 가상화폐의 거래 제재를 발표하였다[47].

10월 6일, 미국에서 랜섬웨어 공격의 피해자가 몸값을 지급한 지 48시간 이내에 몸값 지급 사실과 지급 금액 정보를 국토안보부에 제공하는 ‘랜섬웨어 몸값 공개법(Ransom Disclosure Act)’이 발의되었다. 랜섬웨어 운영 방식에 대한 정보를 수집하고 몸값의 이동을 파악하여, 효과적인 랜섬웨어 대응 및 예방 전략을 개발하고 구현하고자 하였다[48].

10월 13일, 호주 내무부 장관은 지난 2016년과 2020년에 발표된 사이버 보안 전략의 주요 내용을 기

반으로 증가하는 랜섬웨어 위협에 대하여 대응하기 위해 국가 차원에서 새로운 랜섬웨어 대응 계획인 'Ransomware Action Plan'을 발표하였다[49].

4.3 특정 랜섬웨어 대응 및 예방 지침

5월 20일, FBI는 증가하는 Conti 랜섬웨어의 공격으로부터 조직의 네트워크를 방어할 수 있도록 사이버 보안 전문가와 시스템 관리자를 위한 행동 지침을 발행하였다[50].

5월 11일, 미국의 CISA와 FBI는 미국의 주요 인프라 기업을 대상으로 수행되고 있는 랜섬웨어에 대한 공격을 대비하기 위해 DarkSide 랜섬웨어 경고문을 발행하였다[51].

7월 4일, 미국의 CISA와 FBI는 Kaseya VSA 소프트웨어의 취약성을 이용하여 공격을 수행한 REvil 랜섬웨어에 영향을 받은 MSP 업체들과 그 고객을 위한 행동 지침을 발표하였다[52].

8월 25일, 美 FBI는 Hive 랜섬웨어 공격에 관한 기술적 세부 정보와 침해 지표(IoC)인 Hive Ransomeware IoCs를 발표하였다[53]. FBI는 보고서를 통해 Hive 랜섬웨어 공격 기술 세부사항과 침해 지표(IOC)를 설명하며 Hive 랜섬웨어의 공격을 대비하기를 권장하였다.

10월 18일, 미국의 FBI, CISA와 국가안보국인 NSA (National Security Agency)는 BlackMatter 랜섬웨어의 활동, 공격 기술 및 방법에 대하여 설명하는 BlackMatter 랜섬웨어 공격에 대한 경고문을 발행하였다[54].

Ⅴ. 2021년 랜섬웨어 복구 도구

2021년에는 총 10종에 대한 랜섬웨어 복구 도구가 공개되었다 [표 4]. Emsisoft 社에서 Ziggy, Avaddon, SynAck와 Ragnarok 랜섬웨어, Bitdefender 社에서 Fonix 랜섬웨어, DarkSide와 Revil/Sodinokibi 랜섬웨어, Tesorion 社에서 NoCry와 Lorenz 랜섬웨어, Trustwave 社에서 BlackByte 랜섬웨어, Avast 社에서 Babuk, AtomSilo와 LockFile 랜섬웨어에 대한 복호화 도구를 각각 개발하였다.

Fonix, Avaddon, SynAck, Ragnarok, Babuk, AtomSilo와 LockFile 랜섬웨어는 공격자가 암호키를 공개했으며, REvil/Sodinokibi 랜섬웨어의 경우에는 Bitdefender 社가 별도로 복호화 키를 획득하여 복호화가 가능하였다.

〔표 4〕 2021년에 공개된 랜섬웨어 복호화 도구

랜섬웨어명	복호화 대상 확장자	참고
Ziggy	.id=[〈id〉].email=[〈mail〉].ziggy	[55]
Fonix	.Email=[〈mail〉@〈server〉.〈domain〉]ID=[〈id〉].XINOF .Email=[〈mail〉@〈server〉.〈domain〉]ID=[〈id〉].FONIX	[56]
DarkSide	.e392d905	[57]
Avaddon	.aCCAceacEc	[58]
NoCry	.Cry	[59]
Lorenz	.Lorenz.sz40	[60]
SynAck	.{10 Digit Alphabet Random Extension}	[61]
Ragnarok	.thor/.hela	[62]
REvil/Sodinokibi	.{Alphabet&Number Random Extension}	[63]
BlackByte	.blackbyte	[64]
Babuk	.babuk/.babyk/.doydo	[65]
AtomSilo	.ATOMSILO	[66]
LockFile	.lockfile	[66]

Ⅵ. 결 론

2021년, 랜섬웨어는 Colonial Pipeline과 Kaseya 공급망 등 국가 필수 인프라 시설 및 공급망 공격을 수행해 큰 피해를 주었다. 또한 다양한 기업들을 공격해 파일을 암호화하고 중요 데이터를 탈취해 몸값 획득을 위한 협박 수단으로 삼았다. 이에 대응하고자 세계 각국에서는 약 27건의 랜섬웨어 대응 및 예방 정책을 발표하였다. 전반적인 랜섬웨어에 대응 방안을 제시할 뿐만 아니라 피해가 큰 다섯 가지의 특정 랜섬웨어에 대해서는 그에 맞는 행동 지침을 제공하였다. 그럼에도 불구하고 랜섬웨어는 향후에도 주목해야할 사이버 위협으로 여겨지고 있다. 따라서 이러한 랜섬웨어 동향 분석을 기반으로 다양한 랜섬웨어에 관한 대응 및 예방 방안 연구가 더욱 활발히 진행되어야 할 것으로 보인다.

참 고 문 헌

[1] 과학기술정보통신부, “ ’21년 사이버위협 분석 및 ’22년 전망 분석”, pp.1-8, 2021

[2] DATANET, “https://www.datanet.co.kr/news/articleView.html?idxno=164714”

[3] 보안뉴스, “https://www.boannews.com/media/view.asp?idx=97701”

[4] 대한민국 정책브리핑, “https://www.korea.kr/news/policyNewsView.do?newsId=148887607”

[5] 한국인터넷진흥원 (KISA), “2021년 1분기 랜섬웨어 동향 보고서”, pp.1-38, 2021

[6] 한국인터넷진흥원 (KISA), “2021년 2분기 랜섬웨어 동향 보고서”, pp.1-37, 2021

[7] 한국인터넷진흥원 (KISA), “2021년 3분기 랜섬웨어 동향 보고서”, pp.1-42, 2021

[8] 매일경제, “https://www.mk.co.kr/news/it/view/2021/06/553716/”

[9] 보안뉴스, “https://www.boannews.com/media/view.asp?idx=100023&direct=mobile”

[10] 동아일보, “https://www.donga.com/news/Economy/article/all/20210601/107203283/1”

[11] Cnet, “https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/”

[12] BleepingComputer, “https://www.bleepingcomputer.com/news/security/us-declares-state-of-emergency-after-ransomware-hits-largest-pipeline/”

[13] ESTSecurity, “https://blog.alyac.co.kr/3825”

[14] The Wall Street Journal, “https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781”

[15] 보안뉴스, “https://www.boannews.com/media/view.asp?idx=98830”

[16] ESTSecurity, “https://blog.alyac.co.kr/3527”

[17] Chuong Dong Security Blog, “http://chuongdong.com/reverse%20engineering/2021/01/03/BabukRansomware/”

[18] ESTSecurity, “ https://blog.alyac.co.kr/3654”

[19] Quick Heal Blog, “https://blogs.quickheal.com/activists-turn-hacktivists-new-ransomware-that-does-not-demand-money/”

[20] ESTSecurity, “https://blog.alyac.co.kr/3770”

[21] INCA Blog, “https://isarc.tachyonlab.com/3942”

[22] Bleeping Computer, “https://www.bleepingcomputer.com/news/security/n3tw0rm-ransomware-emerges-in-wave-of-cyberattacks-in-israel/”

[23] 보안뉴스, “https://www.boannews.com/media/view.asp?idx=98010”

[24] Bleeping Computer, “https://www.bleepingcomputer.com/news/security/lockfile-ransomware-uses-petitpotam-attack-to-hijack-windows-domains/”

[25] SentinelLABS, “https://www.sentinelone.com/labs/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/”

[26] Tesorion, “https://www.tesorion.nl/en/posts/analysis-of-the-blackmatter-ransomware/”

[27] SOPHOS NEW, “https://news.sophos.com/en-us/2021/10/04/atom-silo-ransomware-actors-use-confluence-exploit-dll-side-load-for-stealthy-attack/”

[28] CYWARE SOCIAL, “https://cyware.com/news/chaos-ransomware-targeting-minecraft-gamers-in-japan-6ec628e2”

[29] BleepingComputer, “https://www.bleepingcomputer.com/news/security/evil-corp-demands-40-million-in-new-macaw-ransomware-attacks/”

[30] BleepingComputer, “https://www.bleepingcomputer.com/news/security/new-yanluowang-ransomware-used-in-targeted-enterprise-attacks/”

[31] 과학기술정보통신부, “https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&bbsSeqNo=94&nttSeqNo=3179937”

[32] 연합뉴스, “https://www.yna.co.kr/view/AKR20210521125700017"

[33] KISA stop RANSOMWARE, “https://boho.or.kr/ransom/main.do"

[34] CISA, “https://www.cisa.gov/news/2021/01/21/cisa-launches-campaign-reduce-risk-ransomware”

[35] Institute for Security and Technology, “https://securityandtechnology.org/ransomwaretaskforce/report/”

[36] NIST, "https://csrc.nist.gov/Projects/ransomware-protection-and-response"

[37] The White House, "https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-i

mprove-the-nations-cybersecurity-and-protect-federal-government-networks/"

[38] CARBIS BAY G7 SUMMIT COMMUNIQUE, "https://www.g7uk.org/wp-content/uploads/2021/06/Carbis-Bay-G7-Summit-Communique-PDF-430KB-25-pages-5.pdf"

[39] Interpol, "https://www.interpol.int/News-and-Events/News/2021/Immediate-action-required-to-avoid-Ransomware-pandemic-INTERPOL"

[40] CISA, "https://www.cisa.gov/stopransomware“

[41] U.S. DEPARTMENT of STATE, "https://www.state.gov/rewards-for-justice-reward-offer-for-information-on-foreign-malicious-cyber-activity-against-u-s-critical-infrastructure/"

[42] The White House, "https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/"

[43] CISA, "https://www.cisa.gov/sites/default/files/publications/JCDC%20Slick%20Sheet_09.15.2021_508_0.pdf"

[44] CISA, "https://us-cert.cisa.gov/ncas/alerts/aa21-243a"

[45] Canadian Centre for Cyber Security, "https://cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099"

[46] CERTNZ, "https://www.cert.govt.nz/business/guides/protecting-from-ransomware/"

[47] U.S. DEPARTMENT OF THE TREASURY, "https://home.treasury.gov/news/press-releases/jy0364"

[48] warren.senate.gov, "https://www.warren.senate.gov/newsroom/press-releases/warren-and-ross-introduce-bill-to-require-disclosures-of-ransomware-payments"

[49] Department of Home Affairs, "https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf"

[50] FBI FLASH, "https://www.cyber.nj.gov/alerts-advisories/conti-ransomware-attacks-impact-healthcare-and-first-responder-networks"

[51] CISA, "https://us-cert.cisa.gov/sites/default/files/publications/AA21-131A_Darkside_Ransomware.pdf"

[52] CISA, "https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa"

[53] FBI, "https://www.documentcloud.org/documents/21049431-fbi-flash-hiveransomware-iocs"

[54] CISA, "https://us-cert.cisa.gov/ncas/alerts/aa21-291a"

[55] Emsisoft, “https://www.emsisoft.com/ransomware-decryption-tools/ziggy”

[56] Bitdefender, “https://labs.bitdefender.com/2021/02/fonix-ransomware-decryptor/”

[57] Bitdefender, “https://labs.bitdefender.com/2021/01/darkside-ransomware-decryption-tool/”

[58] Emsisoft, “https://www.emsisoft.com/ransomware-decryption-tools/avaddon”

[59] Nomoreransome, “https://www.nomoreransom.org/ko/decryption-tools.html#JudgeNoCry”

[60] Nomoreransome, “https://www.nomoreransom.org/en/decryption-tools.html#Lorenz”

[61] Emsisoft, “https://www.emsisoft.com/ransomware-decryption-tools/synack”

[62] Emsisoft, “https://www.emsisoft.com/ransomware-decryption-tools/ragnarok”

[63] Bitdefender, “https://www.bitdefender.com/blog/labs/bitdefender-offers-free-universal-decryptor-for-revil-sodinokibi-ransomware/”

[64] Trustwave, “https://github.com/SpiderLabs/BlackByteDecryptor”

[65] Avast, “https://www.avast.com/ransomware-decryption-tools#babuk”

[66] Avast, “https://files.avast.com/files/decryptor/avast_decryptor_atomsilo.exe”

[67] Avast, “https://www.avast.com/ransomware-decryption-tools#babuk”

[68] Avast, “https://files.avast.com/files/decryptor/avast_decryptor_atomsilo.exe”

〈저 자 소 개〉

김 소 람 (Soram Kim)
정회원
2016년 2월 : 국민대학교 수학과 졸업
2018년 2월 : 국민대학교 금융정보보안학과 석사
2018년 3월~현재 : 국민대학교 금융정보보안학과 박사과정
<관심분야> 디지털 포렌식, 정보보호

강 수 진 (Soojin Kang)
정회원
2018년 2월 : 국민대학교 정보보안암호수학과 졸업
2020년 3월~현재 : 국민대학교 금융정보보안학과 석사과정
<관심분야> 디지털 포렌식, 정보보호

최 용 철 (Yongcheol Choi)
정회원
2021년 2월 : 서원대학교 정보보안학과 졸업
2021년 3월~현재 : 국민대학교 금융정보보안학과 석사과정
<관심분야> 디지털 포렌식, 정보보호

박 귀 은 (Gwuieun Park)
정회원
2016년 3월~현재 : 국민대학교 정보보안암호수학과 학사과정
<관심분야> 디지털 포렌식, 정보보호

이 민 정 (Minjeong Lee)
정회원
2018년 3월~현재 : 국민대학교 정보보안암호수학과 학사과정
<관심분야> 디지털 포렌식, 정보보호

김 종 성 (Jongsung Kim)
종신회원
2000년 8월/2002년 8월 : 고려대학교 수학 학사/이학석사
2006년 11월 : K.U.Leuven, ESAT/SCD-COSIC 정보보호 공학박사
2007년 2월 : 고려대학교 정보보호대학원 공학박사
2007년 3월~2009년 8월 : 고려대학교 정보보호기술연구센터 연구교수
2009년 9월~2013년 2월 : 경남대학교 e-비즈니스학과 조교수
2013년 3월~2015년 8월 : 국민대학교 수학과/일반대학원 금융정보보안학과 조교수
2015년 9월~2017년 2월 : 국민대학교 수학과 부교수
2015년 9월~2020년 8월 : 국민대학교 일반대학원 금융정보보안학과 부교수
2017년 3월~2020년 8월 : 국민대학교 정보보안암호수학과 부교수
2020년 9월~현재 : 국민대학교 정보보안암호수학과/일반대학원 금융정보보안학과 교수
<관심분야> 정보보호, 암호 알고리즘, 디지털 포렌식