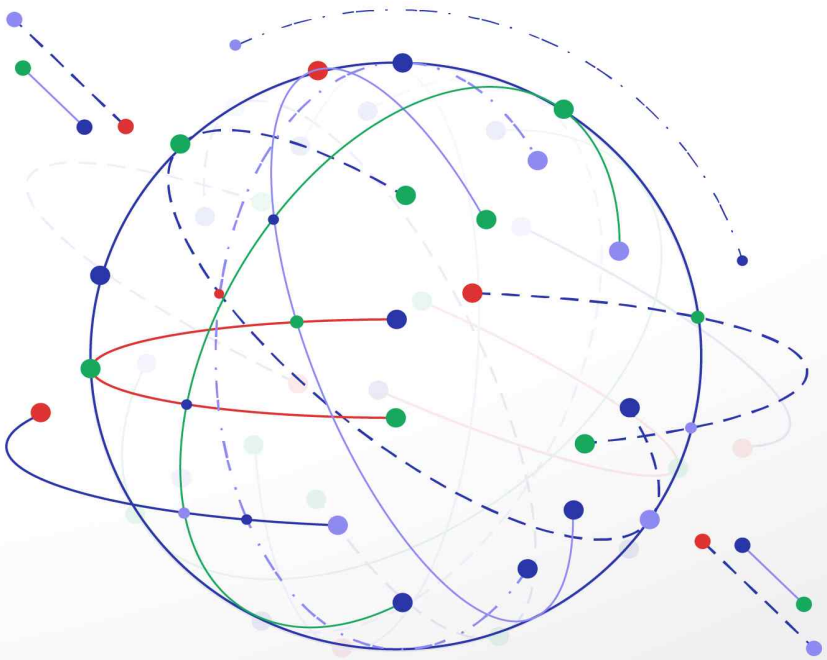
DIGITAL & SECURITY POLICY

KISA Insight

2021 VOL.02

랜섬웨어 최신 동향 분석 및 시사점



KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

www.kisa.or.kr

랜섬웨어 최신 동향 분석 및 시사점

KISA | 민경식·김영직·박진상·장한나

2021. 8. 19.

목 차

『KISA Insight』는 디지털·정보보호 관련 글로벌 트렌드 및 주요 이슈를 분석하여 정책 자료로 활용하기 위해 한국인터넷진흥원에서 기획, 발간하는 심층보고서입니다.

한국인터넷진흥원의 승인 없이 본 보고서의 무단전재나 복제를 금하며 인용하실 때는 반드시 『KISA Insight』라고 밝혀주시기 바랍니다.

본문 내용은 한국인터넷진흥원의 공식 견해가 아님을 알려드립니다.

▶ 작성: 한국인터넷진흥원(KISA) 미래정책연구실 정책분석팀
민경식 팀장(☎061-820-1454, kyoungsik@kisa.or.kr)
김영직 수석연구원(☎061-820-1803, yjkim@kisa.or.kr)
박진상 주임연구원(☎061-820-1195, jinsang@kisa.or.kr)
장한나 주임연구원(☎061-820-1166, hn7462@kisa.or.kr)

요 약

❖ 사이버 침해사고 패러다임 분석

- 코로나 19 확산에 따른 비대면 활동 증가와 맞물려, 우리나라는 물론 세계적으로 랜섬웨어 공격이 유행하여 많은 피해를 주고 있으며, 공격대상도 다양한 산업군으로 확대 중
- 21년 현재, 랜섬웨어가 사이버 위협을 주도하고 있으며, 국내 기업도 랜섬웨어로 인한 피해가 가장 큰 것으로 확인(국내 기업의 59.8%가 랜섬웨어 피해 경험, 20년 정보보호실태조사)

❖ 랜섬웨어 피해 현황 분석

- 랜섬웨어는 악성코드가 삽입된 홈페이지 방문, 이메일 첨부파일, 보안취약점 등을 통해 감염되며, 감염 시 시스템 또는 파일 암호화를 통해 이용을 제한하고 복구비용을 요구
- 랜섬웨어 범죄조직은 더욱 분업화, 전문화되어 가고 있으며, 랜섬웨어로 부당이익을 얻고자 하는 수요가 증가함에 따라, 랜섬웨어를 제작·판매하는 '서비스형 랜섬웨어(RasS)'로 진화

❖ 국내·외 랜섬웨어 대응현황

- (국외) 미국, EU, 영국 등 세계 주요국은 랜섬웨어, 사이버 범죄 등 사이버 침해사고에 대응하기 위한 정부차원의 방지대책 등을 지속적으로 발표하며 대응 중
- (국내) '랜섬웨어 대응 강화방안' 발표('21.8월)를 통해 국가중요시설 관리체계 구축, 정보공유 및 협력, 수사, 대응 기술력 확보 등 종합적인 대응방안을 마련

❖ 시사점

- 랜섬웨어의 피해가 큰 시점에 발표된 '랜섬웨어 대응 강화방안'의 추진 효과를 극대화하기 위해서는 지속적인 정책 시행에 대한 관리와 전문가 등의 Feedback 반영이 중요

제 1장 사이버 침해사고 패러다임 분석

❑ 코로나 19 이후 사이버 침해사고 트랜드 변화

▶ 전 세계적으로 코로나 19가 확산하면서 재택근무, 원격교육, 온라인 쇼핑 등 급격한 비대면 활동 증가와 함께 이를 악용한 위장형 공격과 원격근무 시스템을 노린 이메일, 원격접속(RDP)등을 대상으로 하는 **랜섬웨어 공격**이 유행

- 19년에 이어 20년에도 정부 및 기업 등을 대상으로 한 공격에서 서비스, 제조, 의료 등 다양한 산업 분야로 **렌섬웨어의 공격 대상이 다양한 산업군으로 확대**
- 20년, 전세계 랜섬웨어 발생 건수는 약 3억 4백만 건으로 추산*되며, 이는 19년 대비 61.8% 증가한 규모로, 2031년에는 전세계 랜섬웨어 피해 규모가 304조 원에 달할 것으로 전망**

  * (출처) Number of ransomware attacks per year 2016-2020 (Statista ,'21.6월)

  ** (출처) RansomWare Attack (Cybercrime Magazine, '21.6월)

- 지불 여력이 있는 기업 대상의 **선별적인 공격을 통한 금전 갈취 규모가 더욱 커지고 가속화** 되어, 개인 사용자 뿐 아니라 기업 및 국가 차원에서의 **철저한 예방과 대응책 마련 필요**

❑ 21년 사이버 위협, 랜섬웨어가 주도

▶ **(KISA) 국내·외 기관과 '21년 사이버 위협 전망 발표('20.12월)**

- 한국인터넷진흥원은 사이버위협 인텔리전스 네트워크, 한국, 호주, 인도, 스리랑카 침해사고 대응팀과 공동으로 '2021년 사이버 위협 전망(Cyber Threat Signal 2021)' 발표를 통해, **랜섬웨어는 국내·외 공통으로 2021년 가장 주목해야 할 사이버 위협**으로 전망

- (**국내 사이버 위협 전망**) ▲표적 공격과 결합된 랜섬웨어의 위협 확대 ▲거세진 DDoS, 금전까지 요구하는 공격 증가 ▲사회기반시설 및 중요 인프라를 겨냥한 사이버 위협 범위 확대 ▲포스트 코로나 시대 비대면(언택트) 전환 후 보안 사각지대를 노린 사이버 위협 증가 ▲클라우드 서비스 목표한 공격 증가 ▲국가 지원 해킹 그룹의 공격 증가와 위협 대상 확대 및 다양화 ▲5G를 이용한 사물인터넷(IoT) 제품의 활성화로 새로운 보안 위협 대두 ▲보안 솔루션을 우회하기 위한 기법 고도화를 국내 주요 사이버 위협으로 선정

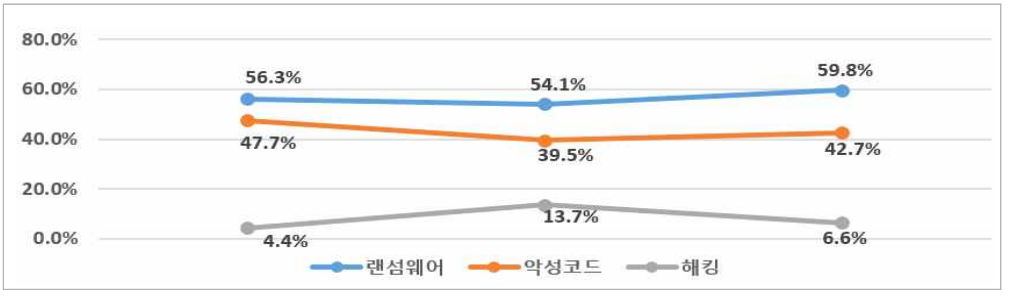
- (**글로벌 사이버 위협 전망**) ▲표적형 공격 랜섬웨어의 확산과 피해규모 증가 ▲고도화된 표적형 악성 이메일 ▲코로나 19 사이버 공격 팬데믹 ▲다크웹 유출 정보를 활용한 2차 공격 기승 ▲기업을 낚는 사이버 스나이퍼를 글로벌 주요 사이버 위협으로 선정

[참고] 20년 정보보호 실태조사 결과 분석

- (**기업**) 20년 정보보호 실태조사를 통해 조사된 국내 기업의 침해사고 경험률은 2%로 전년대비 0.8% 감소하였으나, 랜섬웨어(54.1%→59.8%), 악성코드(39.5%→42.7%)로 인한 피해는 증가

[표1] 기업 침해사고 경험 유형

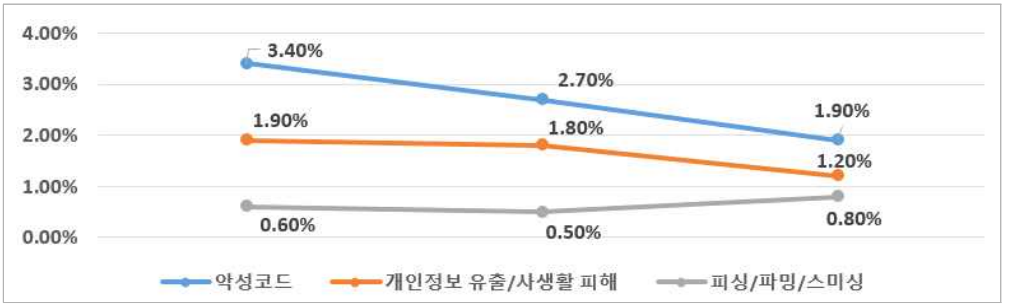
구분	2018	2019	2020	증감률('19~'20)
침해사고 경험률	2.3%	2.8%	**2.0%**	-0.8%p
랜섬웨어	56.3%	54.1%	**59.8%**	**+5.7%p**
악성코드	47.7%	39.5%	**42.7%**	**+3.2%p**
해킹	4.4%	13.7%	**6.6%**	-7.1%p
애드웨어/스파이웨어	12.1%	6.6%	**4.0%**	-2.6%p
내부인력에 의한 중요정보유출	3.9%	1.1%	**1.6%**	+0.5%p
DoS/DDoS 공격	2.5%	0.8%	**4.1%**	+3.3%p



- (**개인**) 국내 PC 이용자의 3.3%가 사이버 침해사고를 경험(전년대비 0.9% 감소)하였고, '악성코드 감염 등으로 인한 피해'가 1.9%로 가장 많았고, '개인정보 유출 및 사생활 침해(1.2%)', '피싱/파밍/스미싱 등으로 인한 금전적 피해(0.8%)'가 그 뒤를 이음

[표2] 개인 침해사고 경험 유형

구분	2018	2019	2020	증감률('19~'20)
침해사고 경험률	4.6%	4.2%	**3.3%**	-0.9%p
악성코드	3.4%	2.7%	**1.9%**	-0.8%p
개인정보 유출/사생활 피해	1.9%	1.8%	**1.2%**	-0.6%p
피싱/파밍/스미싱	0.6%	0.5%	**0.8%**	+0.3%p
랜섬웨어	0.3%	0.2%	**0.3%**	+0.1%p
신용카드 불법결재 등 금전피해	0.4%	0.3%	**0.2%**	-0.1%p



제 2장 랜섬웨어 피해 현황 분석

보안 취약점, 이메일 등을 이용해 감염되는 랜섬웨어는 서비스형 랜섬웨어(RaaS)로 진화하며 전 세계적으로 막대한 피해를 유발하고 있다.

❑ 랜섬웨어 피해 현황

▶ **(국내)** 한국인터넷진흥원에 신고된 최근 3년간 국내 랜섬웨어 현황을 살펴보면, '19년 39건 대비 지난해 '20년 127건으로 325%로 급증

[표3] 최근 3년간 랜섬웨어 침해사고 신고 현황

구 분	'18년도	'19년도	'20년도	'21년도(~7월)
랜섬웨어 침해신고	22건	39건	127건	97건

- 민간 보안업체의 랜섬웨어 통계(월 수만 건)와의 차이는 신고를 기피하는 경향이 원인으로 추정되며, 대부분의 피해는 보안 투자여력이 부족한 중소기업(약 90%)에서 발생한 것으로 확인됨

▶ **(국외)** '21년, 매주 약 950개(1~3월)의 기업이 랜섬웨어 피해를 입고 있으며, 이는 '20년 같은 기간의 약 470여개에 비해 102%가 증가한 수치

※ (출처) The New ransomware Threat : Treat Extortion(Check point, '21.5월)

- 송유관, 병원 등 사회 인프라 운영기관 등을 대상으로 한 랜섬웨어 공격이 지속 발생하여 이를 이용하는 국민들에게 직접적인 피해가 발생

❑ 랜섬웨어 피해 특징·대응

▶ **(전파·감염)** 시스템, SW 취약점 등 보안 취약점, 이용자를 속이는 이메일 첨부파일 등을 이용한 사회공학적 공격기법 등 다양한 경로를 통해 전파·감염됨

- ▲악성코드가 삽입된 홈페이지 방문, ▲이메일 첨부파일, ▲시스템 취약점 등을 이용해 전파·감염

[표4] 랜섬웨어 주요 전파 경로

구 분	악성코드 삽입 홈페이지 방문	이메일, SNS	시스템, NW, SW 보안 취약점
감염 경로	해킹을 통해 악성코드가 설치된 홈페이지 접속 시 악성코드에 감염	(이메일) 첨부파일 실행 (SNS) 링크 등을 통한 악성코드 실행·감염	취약점을 이용한 침투, 악성코드 설치
원 인	OS 보안패치 미설치, SW 취약점 방치 등	이용자 보안인식 미비, 실수 등	운영·관리 체계 미비, 이용자 교육 부족 등

▶ **(피해 복구)** 사전에 백업된 데이터 활용, 일부 공개된 복구도구를 활용하는 경우가 있으나, 대부분 복구가 어려운 것이 현실(중요 데이터에 대한 정기적인 백업이 매우 중요한 의미를 가짐)

- ▲사전에 백업된 데이터를 이용, ▲공개된 복구 도구를 이용하는 경우 → 백업 데이터가 없는 경우, 현실적으로 복구가 어려움

▶ **(운영·예방)** ▲최신버전 SW 사용 및 보안 업데이트 적용 ▲출처가 불명확한 이메일과 URL 링크 클릭 주의 ▲파일 공유 사이트 등에서 다운로드 주의 ▲중요한 자료는 정기적으로 백업

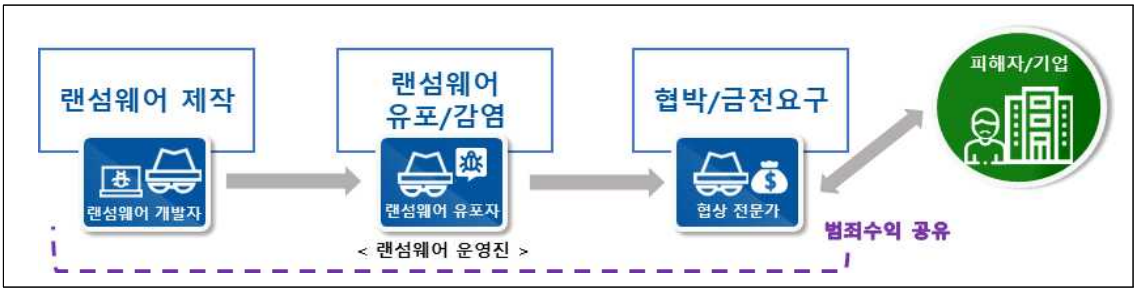
❑ 랜섬웨어 피해 유형 및 진화

▶ 랜섬웨어의 피해 유형

- **(①시스템, DB 등 이용제한)** 랜섬웨어는 감염 시 시스템 화면 또는 파일을 암호화해 사용자의 시스템 이용을 제한하고, 공격자는 피해자(기업)에게 복구를 위한 돈을 요구
- **(②정보 삭제·유통·판매)** 만일, 피해자(기업)가 금전 요구에 응하지 않을 경우, 암호화한 파일을 삭제하거나, 다크웹 등을 통해 정보를 무단 유통, 판매하여 2차 피해를 유발

▶ 랜섬웨어의 진화

- 보이스 피싱 범죄자들이 조직화, 분업화를 통해 범죄수익을 극대화하고 있는 것과 유사하게, **랜섬웨어 공격자** 또한 수익 극대화를 위해 세부 역할을 분배하여 담당하는 **조직화가 진행**되고 있음
  - **(RaaS의 등장)** 랜섬웨어로 금전적 수익을 얻을 수 있다는 것이 알려지면서, 랜섬웨어를 찾는 수요가 생기게 되었고, 이는 랜섬웨어를 제작하여 공급·판매하는 방식인 RaaS(Ransomware as a Service)의 등장을 촉발
  - **(협상전문가 등장)** 이러한 랜섬웨어의 조직화, 분업화는 피해 기업을 전문적으로 협박하고 언어장벽 등의 문제를 넘어 협상을 진행하기 위한 협상전문가까지 등장



❑ 랜섬웨어 피해 사례

〈 국내 피해 사례 〉

▶ (**유통기업 피해**) 백화점, 아울렛 등 OO그룹의 주요 매장이 클롭(Clop) 랜섬웨어 조직의 공격으로 영업 중단되는 사태 발생('20.11월)

- 랜섬웨어 감염 시스템은 일부 매장의 포스(POS) 단말기 등과 연동되어, 백화점과 아울렛의 매장 50여개 중 23개의 운영에 영향을 미침

▶ (**부품기업 피해**) 부품 제조기업의 서버 및 직원 PC 데이터 암호화(1차 공격), 임직원 개인정보, 해외사업 데이터 다크웹 유출(2차 공격), DDoS 공격으로 홈페이지 마비(3차 공격)('21.5월)

▶ (**성형외과 피해**) 국내 성형외과 의원이 랜섬웨어 공격을 받아, 병원 고객연락처를 탈취한 공격자는 고객들과 직접 연락을 취한 정황이 파악되는 등 2차 피해 발생, 해당 병원은 홈페이지 상에 피해 사실을 공지하고, 경찰 등 수사기관에 사건을 의뢰('21.5월)

〈 국외 피해 사례 〉

▶ (**미국**) 최대 송유관 업체인 콜로니얼 파이프라인社가 랜섬웨어 공격을 받아 시스템 마비로 인해 송유관 가동이 전면 중단('21.5월)

▶ (**독일**) 뒤셀도르프대 병원 서버 30대가 랜섬웨어 공격으로 인해 마비, 병원 IT 서비스 운용이 불가능하게 되어, 여성 응급환자를 받지 못해 인근 도시 병원으로 이송했으나 결국 사망('20.9월)

▶ (**영국**) 영국 '국민건강서비스(NHS)'가 워너크라이 공격을 당해 당시 16개 병원 폐쇄됐으며, 최소 6,900건에 달하는 국민건강서비스 진료예약이 취소('17.5월)

▶ (**스페인**) 스페인 정보 노동기관 SEPE가 렌섬웨어 공격을 받아 네트워크 시스템이 암호화되어 일부 서비스가 중지되는 피해 발생하였으나 개인 및 급여정보 등이 탈취되지는 않음('21.3월)

▶ (**네덜란드**) 네덜란드 연구위원회 NWO(Netherlands Organization for Scientific Research)가 랜섬웨어 공격으로 인해 내부 자료가 탈취되고 연구 보조금 관련업무가 중단('21.2월)

▶ (**일본**) 후지필름社가 랜섬웨어 공격을 받아, 공격 확산을 막기 위해 일부 네트워크를 차단하는 등의 조치를 통해 손상된 시스템을 복구하였다고 밝히고, 외부로의 정보 유출은 없다고 발표 ('21.6월)

제 3장 주요 국가 사이버 침해사고 대응 현황

세계 주요 국가들은 사이버 침해사고로 인한 피해가 증가함에 따라 국가 차원의 디지털 안전 정책 마련을 진행 중에 있음

❑ (미국) 미 행정부, 산업계에 랜섬웨어 대응 강화 촉구 및 방지대책 발표

▶ 바이든 대통령이 정부와 민간 분야의 사이버보안 역량을 강화하는 내용의 행정명령에 서명한 데 이어, 교통안전국(TSA)은 주요 송유관 시설 소유자와 운영자를 대상으로 보안지침 발표('21.5월)

- (보안 지침) 사이버 사고 발생 시 사이버보안 및 기반시설보안청(CISA)에 보고 요구, 사이버보안 전담관 지정 및 24시간 배치, 30일 내에 기존 사이버보안 관행 검토해 격차 현황과 위험 해소를 위한 보완 조치를 파악해 TSA와 CISA에 보고 등

- (산업계 권고) ①바이든 대통령이 사이버 행정명령에서 연방기관에 요구한 ▲다중요소인증 ▲엔드포인트 탐지·대응 ▲암호화 ▲보안팀의 역량과 권한 보장 등의 모범관행 이행, ②데이터, 시스템 이미지, 환경설정의 백업, ③운영시스템, 애플리케이션, 펌웨어 등 신속 업데이트, ④사고대응계획 점검, ⑤보안팀의 역량 확인, ⑥비즈니스 운영과 제조/생산 부문 네트워크 분리

▶ 바이든, 푸틴에게 랜섬웨어 조치 요구 후, 랜섬웨어 방지 대책 발표('21.7월)

- (진행 경과) ①세계 최대 정육업체 JBS 해킹 등 최근 미국에서 발생한 사이버 테러 배후를 러시아로 지목, ②미 상무장관, 랜섬웨어 공격에 군사대응도 불사 발언, ③바이든-푸틴 전화 회의를 통해 랜섬웨어 조치 요구, ④미 행정부, 랜섬웨어 방지대책 발표

- (주요 내용) ▲위협행위자 식별정보 제공 시 1천만 달러 보상, ▲미 금융범죄단속국, 금융기관 등과 랜섬웨어 지불문제 대응, ▲랜섬웨어에 중점을 둔 사이버 보안 교육 웹사이트 오픈·운영 등

❑ (EU) 사이버 범죄 대응을 중심으로 미래 보안 환경 구축

▶ 디지털 기술·인프라 의존도 증가 및 사이버 범죄에 대응하기 위해 유럽 연합 보안 전략(EU Security Union Strategy for 2020-2025)을 발표('20.7월)

- 안전한 디지털 세상을 위해 ①미래 보안 환경 구축, ②보안위협 대응, ③테러 및 범죄 대응, ④강력한 보안 생태계 구축 등으로 구성

❑ (영국) 안전기술 산업 육성을 중심으로 이용자의 사이버 안전 도모

▶ 사용자 보호 및 안전기술 산업 육성을 위해 사이버보안 지침(Safer technology, safer users: The UK as a world-leader in Safety Tech)을 마련('20.5월)

- 안전기술 산업 육성을 위해 산업에 대한 인식제고, 투자 기반 마련, 정책 및 표준 개발, 데이터 접근성 확대, R&D 확대 관련 10가지 권고사항 제시

❑ (호주) 사이버보안 분야 투자 확대를 통한 국가 사이버 보안수준 강화

▶ 사이버 위협에 대응 및 안전한 사이버 환경 조성을 위해 사이버안보 전략 (Australia's Cyber Security Strategy 2020)을 발표('20.8월)

- ①산업·개인의 온라인 안전 확보, ②핵심 인프라의 회복력 강화, ③온라인 안전 관련 지역사회 이해 제고, ④사이버안보 사법집행 역량 구축을 위해 사이버보안 예산으로 10년간 1.67B 달러(약 1조 4100억 원)를 투입

❑ (일본) 언택트 비대면 환경에 대응하기 위한 사이버 보안 전략 수립

▶ 코로나 19로 인한 사회 환경 변화에 적극 대응하기 위해 "IoT, 5G 보안 종합대책 2020"을 발표('20.7월)

- ①코로나 19로 인한 재택근무 환경에 대응하기 위한 보안 대책 추진, ②5G 통신네트워크 보안 대책 추진, ③사이버 공격에 대한 통신사업자의 능동적 대응 추진, ④사이버 보안정보 수집·분석 능력 향상을 위한 산·학·연 협력 추진

❑ (중국) 데이터 보안 및 개인정보보호 보장 기반의 데이터 사용 촉진

▶ 데이터 보안 및 개인정보보호를 보장하면서 데이터 개발 및 사용 촉진을 위해 데이터 보안법(Data Security Law) 초안을 발표('20.7월)

- ①데이터 보안관리의 제반 기본제도 확립, ②조직·개인의 데이터 보안 의무 명확화, ③데이터 보안과 발전을 촉진, ④정부 데이터 개방 등으로 구성

제 4장 국내 랜섬웨어 대응 현황

정부는 관계부처 합동으로 랜섬웨어로부터의 피해를 최소화하기 위한 예방·대응·기반의 3단계 전략으로 구성된 「랜섬웨어 대응 강화방안」을 수립·발표

❑ 정부, 관계부처 합동 「랜섬웨어 대응 강화방안」 발표('21.8월)

▶ 랜섬웨어에 안심할 수 있는 디지털 환경구축을 위해, 예방·대응·기반의 종합대책을 수립·발표

- **(전략 1)** 국가중요시설-기업-국민 수요자별 선제적 예방
  - ①튼튼한 국가중요시설 관리 체계 구축, ②중소기업 보안역량 지원 강화, ③대국민 랜섬웨어 면역력 향상
- **(전략 2)** 정보공유-복구-수사 등 사고대응 全주기 지원
  - ①정보공유·협력 채널 강화, ②확산방지 및 신속한 피해지원, ③2차 피해 방지를 위한 사이버 공격 수사 강화
- **(전략 3)** 진화하는 랜섬웨어에 대한 핵심 대응 역량 제고
  - ①랜섬웨어 등 사이버공격 대응 핵심기술력 확보 ②사이버보안 생태계 강화 기반 마련

▶ 랜섬웨어 정보를 통합 제공하는 한국형 'Stop Ransomware' 사이트 오픈·운영

- 랜섬웨어 감염 시 대응방안부터 복구 프로그램 사이트 링크까지 랜섬웨어 정보 일괄 제공

※ (사이트 주소) https://www.boho.or.kr/ransom/main.do

〈 「랜섬웨어 대응 강화방안」 세부 내용 〉

(전략 1) 국가중요시설-기업-국민 수요자별 선제적 예방

1 튼튼한 국가중요시설 관리 체계 구축

- 미 송유관, 육가공 업체의 랜섬웨어 피해 사례와 같은, 대형 인프라를 대상으로 하는 사고는 사회 전반에 막대한 피해 전파, 지속적인 안전 제고 필요

구 분	주요 내용
주요정보통신기반시설 예방 체계 강화	정보통신기반시설 범위 확대, 공공분야 정보시스템 대상 점검 강화, 통신사, IDC 등 핵심 기반시설 대상 모의훈련 추진, 점검결과 개선 조치 근거 마련 등
軍, 연구기관 등	국방정보체계, 군 기반시설 대상 취약점 점검, 사이버 특별훈련, 교육 등 강화, 출연연(26개), 4대 과기원 대상 사이버 보안대책 수립·적용
공급망 및 공공 이메일 보안 강화	기반시설에 구축된 SW·시스템의 공급망(SW업체 등)에 대한 보안 점검 체계 구축, SW 개발보안 허브 구축 등

2 중소기업 보안역량 지원 강화

- 보안여력이 부족한 중소기업을 대상으로 데이터 백업, 랜섬웨어 대응 패키지 지원 등 강화

구 분	주요 내용
데이터 금고를 통한 백업 지원	랜섬웨어에 취약한 중소기업을 대상으로 중소기업 데이터 유실 예방을 위한 데이터 금고 구축·제공
중소기업 보안역량 강화 패키지 지원	랜섬웨어 3종 패키지(메일보안SW, 백신, 탐지·차단SW) 지원, 원격 서버점검, 맞춤형 컨설팅 등
기업의 랜섬웨어 예방활동 강화	ISMS 인증 기업의 사후·갱신 심사 시 랜섬웨어 예방활동 평가, 정보보호공시 내 업무지속계획 포함 추진, 정보보호최고책임자 대상 랜섬웨어 교육 강화 등

3 대국민 랜섬웨어 면역력 향상

- 코로나 팬데믹으로 인한 IT 서비스 활용도 증가에 따라, 랜섬웨어로 인한 위험이 더욱 증가

구 분	주요 내용
국민들의 정보통신 기기 보안성 향상 지원	PC·IoT 기기의 랜섬웨어 취약 여부를 원격으로 진단·개선하는 '내 PC 돌보미 서비스' 지원
랜섬웨어 예방 인식제고 및 예방수칙 보급	'예방 플레이북' 보급 등 전방위 예방 캠페인 전개

(전략 2) 국가중요시설-기업-국민 수요자별 선제적 예방

1 정보공유·협력 채널 강화

- 민·관간, 국가간 랜섬웨어 위협·탐지 정보공유 활성화하여 국가 전체의 랜섬웨어 대응 강화

구 분	주요 내용
민·관간 정보공유·협력 채널 활성화	민간(C-TAS), 공공(NCTI) 사이버위협 정보공유 시스템 상호 연동, 가상자산거래소, 유통·제조 분야 기업 등의 사이버위협 정보공유 참여 확대, 웹사이트 랜섬웨어 위협 탐지·공유
국가간 정보공유 강화	해외 정보기관, 주요국가 인터넷 보안기관(CERT)간 정보공유 통해 신종 랜섬웨어 및 다크웹 등 정보 신속 입수·분석, '한미 사이버 워킹그룹' 등 사이버보안 협의체를 통해 랜섬웨어 정보, 위협 대응 사례 공유, 수사공조 등 협력 강화 추진

2 확산방지 및 신속한 피해지원

- 랜섬웨어 공격의 확산 방지를 위해 AI기술 활용 악성도메인 차단, 다중이용시설 취약점 개선, 전국단위 피해지원 체계 구축 등 추진

구 분	주요 내용
랜섬웨어 공격의 확산 방지	AI 기반 악성도메인 차단, 가상자산거래소 등 대량 이용자 서비스 대상 취약점 점검 지원, 백신 배포, 랜섬웨어 대응사례 수집·공유, 랜섬웨어 사고 분석·대책 마련·권고 제도 개선
신속한 사고·피해 극복 지원	지역정보보호 지원체계(지역정보보호센터, 지역보안 전문업체 등)와 연계, 피해 시 인력·장비를 현장 파견, 피해 극복 지원 및 적극 수사 의뢰

3 2차 피해 방지를 위한 사이버공격 수사 강화

- 랜섬웨어로 인해 발생한 피해사고 대상 수사 및 공격자 활동 감시 강화 등을 통한 피해 저감

구 분	주요 내용
다크웹 모니터링 통한 해킹조직 활동 감시 강화	다크웹 상에 노출된 피해자 개인정보 등을 관계부처에 신속 공유, 피해자의 2차 피해 방지 지원, 민간(과기정통부, ☎118), 공공(국정원, ☎111) 기관과 실시간 정보공유
랜섬웨어 해킹조직 수사 역량 강화	인터폴 회원국들과 해킹조직 분석, 범죄자 공동 검거 강화 및 공조 확대

(전략 3) 진화하는 랜섬웨어에 대한 핵심 대응 역량 제고

1 랜섬웨어 등 사이버공격 대응 핵심기술력 확보

- 신형 랜섬웨어의 신속한 탐자복구 지원 기술 확보, 공격근원지 및 가상자산 흐름 추적기술 개발 등

구 분	주요 내용
신형 랜섬웨어 탐지·복구 기술 확보	랜섬웨어 공격 탐지·차단' 기술 개발, 랜섬웨어 복구기술 개발, 산업계 신속 배포
근원지 추적기술 개발 강화	해킹조직 프로파일링 시스템 구축. 해킹조직 서버·이메일 역추적 기술 등 개발, AI 기반 부정 가상자산 거래 기록 축적·학습, 흐름 추적 기술 개발
데이터·네트워크 및 AI 기반 보안기술 개발 강화	개인·금융 정보 등 민감정보 노출방지 암호기술 확보, 5G 네트워크 全영역(코어망, 엣지망, 디바이스) 보안 기술 개발, AI 기반의 첨단 보안 기술 심층 육성

2 사이버보안 생태계 강화 기반 마련

- 사이버보안 생태계 강화를 위해 기본법 제정 추진, 민·관 협의체 확대를 통해 랜섬웨어 대응 역량 결집

구 분	주요 내용
사이버보안 기본 법제 마련	사이버보안 법제도 체계화 및 산업분야간 협력 강화하기 위한 기본법 제정 추진
「민·관 랜섬웨어 대응 협의체」확대 운영	연구기관·지자체·지역 중소기업 등의 「민·관 랜섬웨어 대응 협의체」 참여 확대 운영

제 5장 시사점

「랜섬웨어 대응 강화방안」 발표를 통해 랜섬웨어로 인한 국가 차원의 피해 저감과 정책 추진 효과의 극대화를 위한 지속적인 관리·보완 필요

▶ 정부는 민간, 공공, 전 영역을 거쳐 심각한 피해를 유발하고 있는 랜섬웨어에 대한 종합적 대응방안이 필요한 시점에, 사전예방·대응 등 전단계를 아우르는 랜섬웨어 종합대책을 발표*

* 국내외 주요 기관, 보안업체 등이 21년 보안 이슈로 랜섬웨어를 선정하고 있는 시점에 발표

▶ 정책 추진효과의 극대화를 위해, 발표 후 강화방안이 적절히 추진되고 있는지 철저한 관리와 함께 동향 등 상황 변화에 따른 기존 정책 보완 등 지속 관리*가 중요하며,

* 산·학·연 등 관련 기관 등의 추가적인 의견 feedback 수렴을 통한 정책 관리·보완·개선 등

▶ 아울러 「랜섬웨어 대응 강화방안」의 지속적인 추진에도 불구하고 현재와 같은 피해상황이 지속 될 경우, 이용자 보호, 랜섬웨어 대응 강화 등 추가적인 보완대책의 마련·추진 등도 검토 필요

〈 랜섬웨어 정책제언(안) 〉

① (**이용자 보호 강화**) 랜섬웨어 감염 파일의 자동화 분석을 통해, 이용자가 사용할 수 있는 복구도구를 제공하는 '**랜섬웨어 감염자료 분석서비스**'를 구축·운영하여 랜섬웨어 피해자 신속 지원(Stop ransomware 사이트에서 서비스를 제공)

- (**감염자료 등록**) 랜섬웨어 피해자가 감염된 파일을 보관소에 업로드(등록)
- (**복구여부 판별**) 감염자료에 대한 AI 기반 분석을 통해 복구가능 여부 판단
- (**복구도구 제공**) 복구가능 확인 시, 피해자에게 즉시 복구도구를 제공하고, 복구 불가능 시 피해자에게 해당 랜섬웨어명 통보(추후 복구도구 개발 시 사후 제공)

⇒ (**장점**) 이용자가 개별적으로 랜섬웨어 복구도구를 검색, 복구여부를 확인해야 하는 어려움을 해결하고, 복구도구 개발 시 통보, 신규 랜섬웨어 정보 제공 등 사후 지원

② (**대응조직 신설 검토**) KISA 내에 ▲온·오프라인 신고접수 채널 운영(KISA, 보안업체), ▲상담 및 원격 기술지원(KISA, 보안업체), ▲피해 신고, 수사(사이버수사대)을 전담하는 **"랜섬웨어 원스톱 대응센터**(가칭)" 신설

- (**지원 내용**) 피해 상담·접수, 복구 등 기술지원, 피해 신고, 대국민 홍보 및 예방 교육

⇒ (**장점**) 랜섬웨어 피해자가 한번의 신고·상담을 통해 피해상담, 기술지원, 원격분석, 신고 가능

발 행 일	2021년 8월
발 행 처	한국인터넷진흥원 (전라남도 나주시 진흥길 9)
기 획	미래정책연구실 정책분석팀