중부대학교

졸업작품전시회 발표자료

랜섬웨어 최근 동향 이슈에 대한 연구

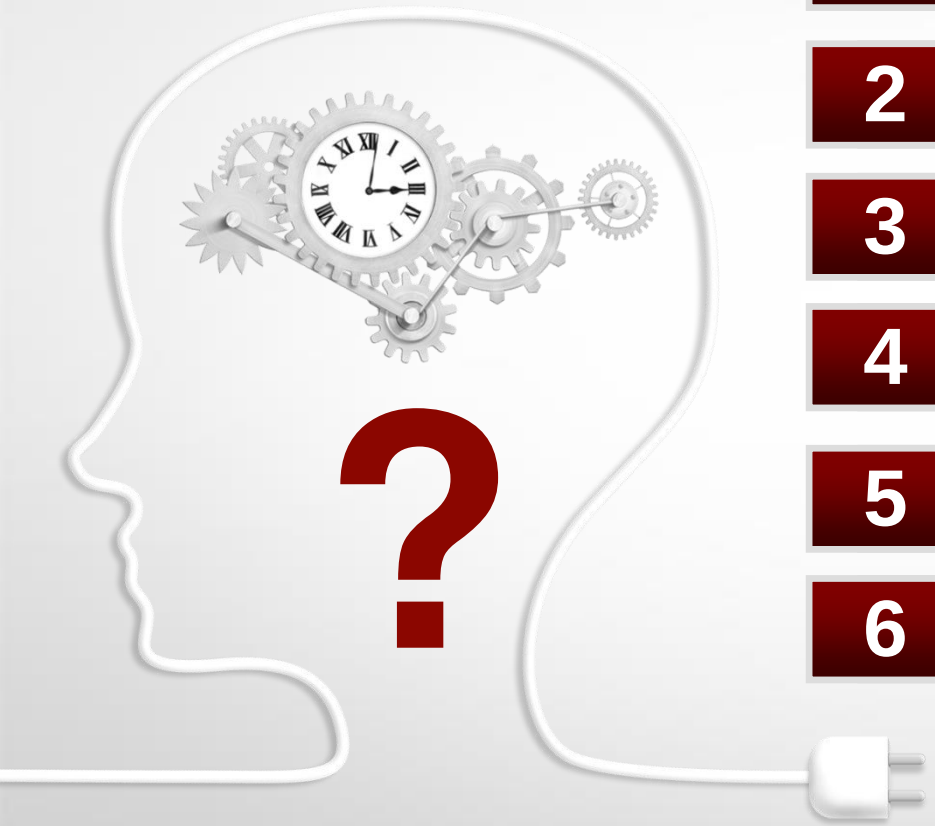
- 최신 랜섬웨어를 중심으로-

2022.11.01

박서현

정보보호전공

Contents



논문목차

연구 목적 및 필요성

- **산업의 발전으로 정보화시대의 도래**
  - 특히 코로나시대가 도래함에 따라 재택근무나 온라인업무의 비중이 커지면서 전 세계의 사이버화가 더욱 가속되었다. 사이버시대가 도래함에 따라 사이버에 저장하는 데이터의 가치가 높아졌으며 그 양도 날로 늘어나고 있다. 이제 정부기관도 글로벌 기업도 모든 정보들을 데이터화 해 서버에 보관할 만큼 정보의 가치는 높아졌고 데이터 보관량도 날로 늘어가고 있다. 이제 정보 데이터는 중요 자산이다. 이에 따라 저장되어있는 데이터파일들을 랜섬웨어 공격으로부터 보호하고 방어 할 필요가 있다.
- **최근 랜섬웨어의 타겟은 정부기관과 글로버기업**
  - 최근에는 방대한 정보를 다루는 기업과 정부기관을 표적으로 하는 위험한 악성해킹 수단인 랜섬웨어가 기승이다. 랜섬웨어의 수익화로 수익시장이 확대되었으며 그에 최적화 된 정부와 기업들이 타겟이 된 것이다. 많은 사람들이 정부와 기업의 서비스를 믿고 이용하는 만큼 정부와 기업을 상대로 하는 랜섬웨어 공격은 앞으로 방어해야 할 1순위 악성해킹수단이 될 것이다.

최근 랜섬웨어 동향

- **랜섬웨어의 서비스화 RaaS**
  - 랜섬웨어가 서비스처럼 제공되는 RaaS(Ransomware as a Service)가 시작되었다. 랜섬웨어를 자체 개발 후 타인에게 판매하는 형태로 구매자가 원하는 방향으로 제작과 유포가 가능하도록 거래된다. 사이버 범죄의 진입장벽이 낮아졌고 공격자와 제작자가 분리되어 수익을 나눠가진다.
- **2차피해 증가**
  - 랜섬웨어 피해자가 금전을 지불하지 않을 시 유출 된 데이터를 다크웹에 공개
  - 데이터손실에서 데이터 유출까지 2차피해로 변질
  - 조직화로 인해 랜섬웨어 대금 증가
- **버그바운티 도입**
  - 랜섬웨어에 대한 버그를 공격자들에게 제보하면 포상금 지급
  - 보완을 거듭해 보안프로그램에도 탐지되지 않는 수많은 변종 출시

랜섬웨어 갱단

● 더더욱 조직화되고 치밀해진 랜섬웨어 갱단

- **공격 대상을 정부로 넓혀가는 랜섬웨어 갱단**

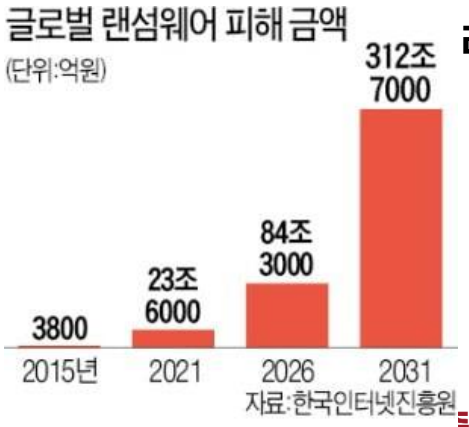
2022-03-03	Lockbit 2.0 랜섬웨어 갱단의 공격으로 미국의 글로벌 타이어기업Bridgestone 생산 중단
2022-04-19	랜섬웨어 갱단 Conti 공격으로 코스타리카 재무부 서비스 제공 중단
2022-04-25	랜섬웨어 갱단 Conti 공격으로 코스타리카 카르타고 전기관리 행정시스템 마비
2022-05-08	랜섬웨어 갱단 Conti, 페루 정보기관 해킹
2022-05-11	Lockbit 2.0 랜섬웨어 갱단, 캐나다 민간 군사훈련업체 Top Aoes 공격
2022-05-12	친러시아 해커그룹 Killnet, 이탈리아 정부 웹사이트에 DDos 공격

● 진화하는 유포 수단

- **개인의 심리를 이용하는 사회공학기반의 랜섬웨어 유포가 성행했다. 입사지원문의, 피고소환통지서 등 자극적인 소재를 주로 이용하였으며 라이나전쟁 등 화제성 있는 키워드를 이용하기도 했다.**

● 점점 증가하는 피해액

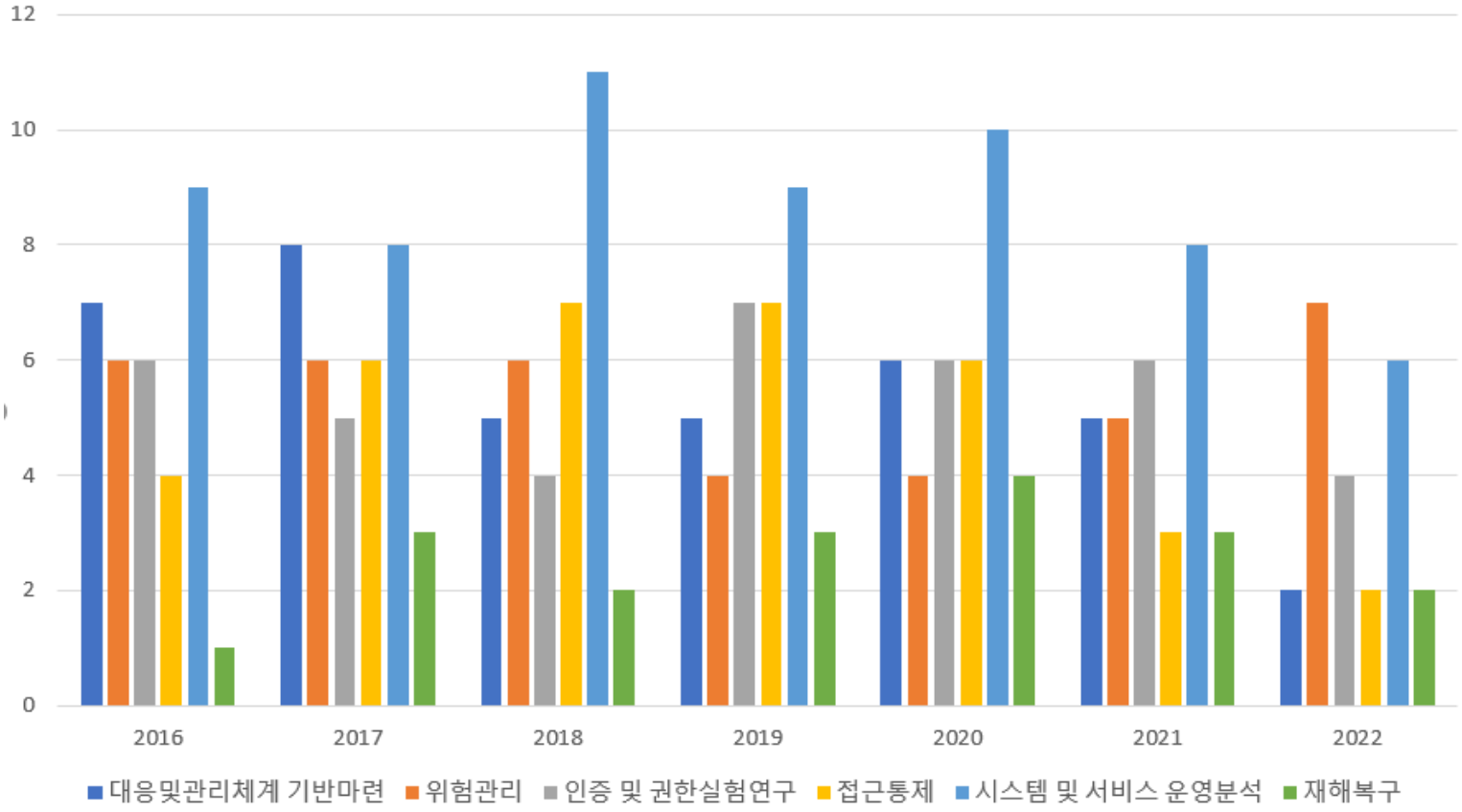
- **매년 피해액수가 증가하고있다.**
- **앞으로 꾸준히 더 늘어 날 것으로 예상된다.**



관련연구

● 참고문헌 비교분석

- 2016년도 9편, 2017년도 10편, 2018년도 11편, 2019년도 10편, 2020년도 11편, 2021년도 11편, 2022년도 8편으로 총 71 편의 논문과 참고문헌을 조사 비교했다.



그 중 대응 및 관리 체계 기반마련이 포함되어있는 문헌은 총 38편, 위험관리 및 동향분석이 포함되어 있는 문헌은 총 38편, 인증 및 권한실험 연구가 포함되어있는 문헌은 총 38편, 접근 통제가 포함되어있는 문헌은 총 35편, 시스템 및 서비스 운영 분석이 포함되어있는 문헌은 총 61편, 재해복구가 포함되어있는 문헌은 18편이었다.

연구결과

● 연도별 대표 랜섬웨어 및 특징

연도	대표 랜섬웨어	공격대상	글로벌 피해금액	특징
2016년	Locky, Cerber	무차별	약 3000억원	▪ 랜섬웨어의 본격화 ▪ 데이터 잠금형 등장 ▪ 진화의 시작
2017년	Petya	무차별	약 7000억원	▪ RaaS 서비스의 대중화 ▪ 수익시장 형성
2018년	Gandcrab, Magniber	공공기관, 기업 등으로 확장	약 1조 500억원	▪ 랜섬웨어의 본격적 수익화 ▪ 수익화에 적합화된 공공기관과 기업쪽으로 타겟 변경
2019년	Clop	공공기관, 기업	약 13조억원	▪ 본격적으로 기업들만 공격하기 시작. (개인은 타겟에서 제외)
2020년	Ryuk, Maze	공공기관, 기업	약 24조억원	▪ 코로나시대로 인한 랜섬웨어 확산 ▪ 랜섬웨어 갱단의 출현 ▪ 고도의 지능탑재 및 전략화
2021년	Darkside, Conti	공공기관, 기업		▪ 랜섬웨어의 기업화 ▪ 탈취한 정보유출로 2차피해 발생 ▪ 국가차원에서 랜섬웨어에 대응하기 시작
2022년	Blackcat, Lockbit	공공기관, 기업	현재 진행중	▪ 랜섬웨어의 사업화 ▪ 버그바운티 등 각종 운영제도 도입 및 지능화 ▪ RaaS 서비스를 이용해 제작자와 공격자 분리

결론 및 시사점

● 기업 및 정부기관들의 방어체계 구축

- 대부분의 이용자들은 기업과 정부기관의 보안성을 신뢰하고 사용하고 있지만 최근 랜섬웨어 공격자들은 기업과 공공기관에 눈을 돌렸다. 따라서 기업과 정부기관에서 앞장서서 완벽한 안전함이란 존재하지 않을 수 있음에 대해 인정하고 최신 취약점 공지에 대한 관심과 함께 공격의 트렌드 또한 살핌으로서 잠재된 위협에 대응 할 수 있는 상시적인 준비가 필요하다.

● 시사점

- 기업과 정부기관의 경계를 촉구
- 랜섬웨어 방어에 많은 투자를 함으로서 보안시장의 확대

THANK YOU