랜섬웨어 최근 동향 이슈에 대한 연구

-최신 랜섬웨어를 중심으로-

지도교수 김 성 규

이 논문을 공학 박서현 학사 학위 논문으로 제출함.

2023 년 02 월

중부대학교 정보보호학전공

정보보호학과

박서현

◆ 목 차 ◆

◆ 표 목 차 ◆

◆ 그 림 목 차 ◆

Ⅰ. 서 론

1. 연구의 배경 및 목적

산업의 발전으로 디지털화가 가속되며 정보화시대가 도래했다. 특히 코로나 시대가 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 글로벌기업도 모든 정보들을 데이터화 해 서버에 보관할 만큼 정보의 가치는 높아졌고 데이터 보관량도 날로 늘어가고 있다. 이제 정보 데이터는 중요 자산이다. 이에 따라 저장되어 있는 데이터파일들을 공격하는 악성해킹수단인 랜섬웨어가 등장 했다.
랜섬웨어는 몸값을 의미하는 랜섬과 소프트웨어의 합성어이다. 파일을 잠그고 데이터를 암호화해 사용자가 열어보지 못하도록 한 후 협상의 대가로 금전을 요구하는 해킹 공격을 뜻한다. 공격 대상이 특별히 정해지지 않았기에 누구나 공격 대상이 될 수 있다. 인터넷을 사용하는 사람이라면 개인이든 기업이든 정부기관이든 모두가 대상이 될 수 있다는 뜻이다. 현재도 랜섬웨어의 피해가 나날이 증가하고 있으며 이제는 전문적인 랜섬웨어 조직인 갱단들이 등장하는 추세이다. 랜섬웨어는 나날이 발전하고 이에따른 변종도 많이 등장하는 만큼 랜섬웨어로 인한 정보 손실과 금전적 피해, 그리고 데이터가 유출되는 2차피해까지 발생되고 있는 실정이다. 최근에는 방대한 정보를 다루는 기업과 정부기관을 표적으로 하는 위험한 악성해킹수단인 랜섬웨어에의 최신 동향에 대해 분석 및 연구 하고자 한다.

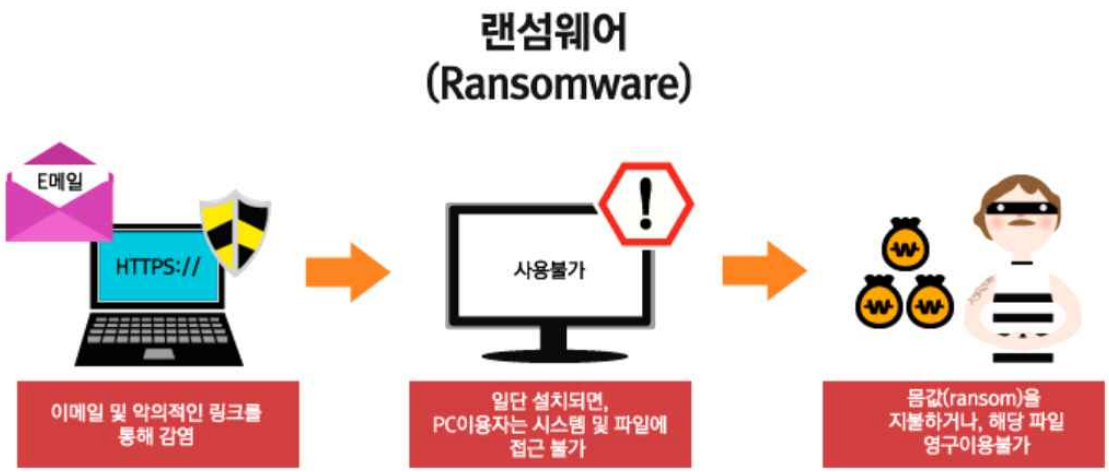
2. 연구범위

본 논문에서는 랜섬웨어에 대한 전반적인 개요와 피해예방수칙 및 예방법을 소개하며 최근 랜섬웨어의 동향은 어떤지 피해사례는 어떤 것이 있는지 좀 더 면밀히 분석하고자 한다. 2장에서는 랜섬웨어의 소개와 주요 피해사례를 정리하며 3장에서는 랜섬웨어와 관련 된 문헌조사를 통해 비교하고 4장에서 비교분석을 통한 연도별 랜섬웨어의 특징을 소개한다. 끝으로 5장에서 결론으로 마무리한다.

Ⅱ. 관련연구

1. 랜섬웨어개요

랜섬웨어는 몸값을 의미하는 랜섬과 소프트웨어의 웨어를 따 온 합성어이다[1]. 컴퓨터에 저장되어있는 사용자의 시스템을 잠그고 데이터를 암호화해서 사용할 수 없도록 만드는 악성 프로그램이다. 이후 해커가 사용자에게 접근을 시도해 데이터를 인질로 금전을 요구한다. 랜섬웨어를 유포 해 불법적인 경로로 금전을 갈취하는 해커들에게 금전을 지불한다고해서 데이터를 복구 할 수 있다는 보장도 없거니와 이 해커들은 주로 해외에 근거지를 두고 있기 때문에 정체가 드러나기 쉽지 않으며 피해를 당했더라도 해커를 추적하는 것이 사실 상 불가능하다[그림 1].



[그림 1] 랜섬웨어의 구성도
(출처 : SK브로드밴드)

2. 랜섬웨어 감염

랜섬웨어는 주로 이메일 첨부파일이나 웹페이지 접속을 통해 들어오기도 하고, 확인되지 않은 프로그램이나 파일을 내려받기 하는 과정에서 감염되기도 한다. 대체적인 랜섬웨어 감염의 흐름은 다음과 같다.

감염 -> 대상파일검색 -> 파일암호화 -> 파일이동 -> 메세지출력 -> 협상

인터넷을 통해 감염이 되면 컴퓨터에 있는 파일들이 전부 암호화 된다. 엑셀이나

워드 등 중요문서들도 암호화 되어서 열리지 않는다. 이 때 연결 된 클라우드나 usb가 있으면 이 또한 감염된다. 그리고 열리지 않는 파일에는 협상을 위한 경로와 금전을 요구하는 메시지가 적혀있다. 감염단계와 협상단계를 제외하면 크게 파일검색, 파일암호화, 파일이동, 메세지출력으로 암호화 부분에서는 고정키 암호화와 다이나믹 암호화 처리 방식에 대해 알아볼 필요가 있다. 특히 다이나믹키 암호화 방식으로 만들어질 경우에는 암호화키 생성과 보관 방법에 따라 피해 복구 가능성에 큰 변화가 발생한다.

3. 랜섬웨어 증상

랜섬웨어 감염 시 가장 먼저 확인되는 증상으로 컴퓨터 부팅이나 로딩중에 표시되는 메세지에 금전을 요구하는 내용과 협상의 경로가 담겨있다. 해커들은 금전적 이득을 위해 랜섬웨어를 배포하기 때문에 모든 폴더와 자료안에는 금전을 요구하는 협박내용과 금전을 지불하는 방법에 대한 내용으로 변하게 된다. 또한 컴퓨터에 있는 파일들은 이전에 정상적으로 열리던 자료들이 암호화가 되어 열리지 않게 되고 파일 확장자 또한 변하게 된다. 랜섬웨어 감염 시 파일이 암호화되면서 확장자가 변하게되는데 .crypted 혹은 .cryptor 로 변경이 되거나 파일 확장자명 자체가 사라진다. 확장자명이 사라질 경우 파일의 형식이 없는 빈 아이콘으로 표시된다. 연결되어있는 클라우드나 서버, usb에 있는 파일들도 암호화 된다. PC에 저장되어 있는 자료들 뿐만 아니라 PC에 연결되어있는 이동식 저장장치(USB 또는 외장하드 등등)에도 감염 될 수 있기 때문에 PC를 넘어서서 이동식 저장장치들까지 파일이 암호화 될 수 있다. 감염이 된 파일들은 더블클릭을 해도 열리지 않으며 금전을 요구하는 메시지만 표시 될 뿐이다.

4. 랜섬웨어 해킹조직 및 갱단

최근 코로나로인해 재택근무와 온라인업무 비중이 증가하면서 랜섬웨어도 또다시 기승을 부리고 있다. 게중에는 랜섬웨어 해킹조직 이른바 갱단을 만들어서 활동하는 조직들이 생겨났다. 최근 랜섬웨어 동향을 조사한 결과 국내외에서 이들에 의한 피해가 다수 발견되었다. 갱단에는 록비트(Lockbit), 콘티(Conti), 랩서스

(Lapsus) 등이 있는데 특히 최근 국제 랜섬웨어 해커조직 1위로 부상 중인 록비트는 최근 2년 동안 국내 기업 5곳을 해킹했다. 록비트는 랜섬웨어 해킹 프로그램 3.0 버전을 지난달 출시하고 제휴사를 모집하며 공격적으로 랜섬웨어 해킹에 나서고 있어 보안업계에서 가장 예의 주시하는 해커조직 중 하나다. 콘티(Conti)는 위자드 스파이더(Wizard Spider)라고 불리는 러시아 사이버 범죄 조직에 의해 운영되고 있다. 우크라이나 연구원이 콘티 랜섬웨어와 관련 한 정보를 유출 한 적이 있어 이슈가 됐었다. 랩서스는 2021년 12월부터 온라인에 본인들만의 개인채널을 생성하고 홍보를 통해 대중들에게 알려지게 되었는데 최근에는 글로벌기업들의 가상 사설망(VPN)과 다단계 인증(MFA)을 우회하는데 집중됐고 해당 기업의 내부직원을 통해 기업에 온라인망에 접속가능 한 ID를 구매 한 후 기업 내부 네트워크에 접속 해 랜섬웨어를 유포 및 데이터를 탈취하는 방법을 주로 이용하고 있다. 블랙바이트(BlackByte)라는 랜섬웨어 갱단도 있는데 이 조직은 올해 꾸준한 활동량을 보이고 있다. 이 랜섬웨어 조직은 작년 10월 경 보안업체인 TrustWave에 의해 디크립터가 제작 된 이력이 있으며 미국연방수사국(FBI)에서는 이들에 관련한 보고서를 발표 한 이슈가 있다. 블랙바이트가 미국의 핵심 인프라 분야의 업체를 공격했다며 주의를 요하는 경고 글을 발표했었다.

공격 대상을 정부로 넓혀가는 러시아 사이버 범죄 집단 - 록비트, 콘티, 킬넷[표 1].

[표 1] 랜섬웨어 갱단들에 의한 2022년 공공기관 및 정부의 주요 피해사례

2022-03-03	Lockbit 2.0 랜섬웨어 갱단의 공격으로 미국의 글로벌 타이어기업 Bridgestone 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

2월 27일 전 세계에 수십 개의 생산 단위와 13만명 이상의 직원이 일하는 미국의 글로벌 타이어업체 브리지스톤이 랜섬웨어 공격을 받아 북미와 남미 전역의 공장에서 생산 중단되었고 브리지스톤은 공격을 받은 지 열흘만인 3월 9일에 시스템을 모두 복구했다고 발표했다.

3월 11일 러시아 랜섬웨어 갱단 Lockbit 2.0은 브리지스톤에 대한 공격이 자신들의 소행이라고 주장하면서 2022년 3월 15일 23시 59분까지 몸값을 지불하지 않으면 훔친 데이터를 공개하겠다고 협박했다.

4월 18일 Conti의 해킹으로 코스타리카 재무부의 과세 시스템과 통관, 관세업무 시스템이 마비되고 납세자 정보 1TB가 유출되었다.
4월 23일 Conti의 공격으로 카르타코시의 전기를 관리하는 카르타고 전기서비스관리위원회(JASEC)에서 조직의 웹사이트, 이메일, 관리시스템 등 조직의 모든 행정시스템이 마비되었다고 공지했다.
5월 7일 Conti는 페루의 국가정보국(DIGIMIN)을 해킹해 9.41GB의 데이터를 훔쳤다고 주장했다. 국가 정보기관에 대해 해킹은 국가기밀 유출로 이어져 국가안보와 위험을 초래할 우려가 있다.
5월 8일 차베스 대통령은 코스타리카가 사이버테러를 당하고 있다면서 5월 11일 국가 비상사태를 선언했다. 특히 재무부의 디지털 서비스가 복구되지 못해 전체 생산부문에 영향을 미치는 것이 큰 문제였다.
5월 11일 전투기 훈련서비스를 제공하는 캐나다의 글로벌 민간 군사훈련업체 Top Aces가 Lockbit 2.0의 공격을 받은 것으로 드러났다. Lockbit 2.0 갱단은 탈취한 44GB의 데이터에 방위산업 정보가 포함됐을 가능성을 우려했다.
2022년 1사분기 공격 성공수가 가장 많다고 주장하는 랜섬웨어 톱3 갱단에는 록비트와 콘티 그리고 블랙캣이 있다. 록비트는 220건의 랜섬웨어 공격을 성공했다고 주장하고 콘티는 117건 블랙캣은 59건의 공격성공을 주장한다. LockBit는 35.8%, Conti는 19%, BlackCat은 9.6%일 정도로 랜섬웨어 갱단들의 활동이 활발하다.

5. 최근 랜섬웨어 주요 피해사례

랜섬웨어가 발생한지도 몇 년이 지났는데 여전히 랜섬웨어는 개인에게도 기업에게도 큰 위협이다. [표 2].

[표2] 랜섬웨어 갱단들에 의한 2022년 기업의 주요 피해사례

2022-01-19	이탈리아 패션 브랜드 몽클레르가 BlackCat 랜섬웨어 공격 당해 국내 고객 개인정보도 유출되었다.
2022-02-07	스위스 대형 항공서비스업체 스위스포트가 BlackCat 랜섬웨어 공격으로 IT 서비스가 일부 중단되었다.
2022-02-22	글로벌 물류업체 엑스 피다이터스가 랜섬웨어의 공격을 받아 운영 중단되었다.
2022-03-01	협력사에 대한 랜섬웨어 공격으로 3월 1일 하루동안 도요타 생산이 전면 중단되었다.
2022-03-14	도요타 부품 계열사 덴소가 또 해킹되어 도면 등 15만7천건이 도난되었다.

새로 등장한 BlackCat의 공격으로 인한 피해가 발생했다. 1월에는 이탈리아 패션 브

랜드 몽클레르가 지난해 12월 블랙캣 AlphV 라는 랜섬웨어의 공격을 받아 데이터가 유출되었다.[72] BlackCat 갱단은 몽클레르에게 300만 달러(약 35억원)을 요구했으니 응하지않자 몽클레르와 협력 업체의 직원, 고객정보 등 중요 정보를 유출, 이로인해 2020년 몽클레르 그룹에 인수 된 국내 스톤아일랜드의 일부 고객정보도 함께 유출됐다. 2월, 전 세계 50개국에 307개의 지점이 있는 스위스의 대형 항공서비스 회사 Swissport International 역시 BlackCat의 공격으로 IT 인프라가 일부 작동하지 않았고, 이로 인해 파트너사인 취리히 공항에서 일부 항공편이 지연되는 등 연쇄적으로 피해가 발생했다.[73][74] BlackCat 갱단은 또한 Swissport에서 1.6TB의 데이터를 유출했다고 주장했다. 2월에 또 미국글로벌 물류업체인 Expeditors가 랜섬웨어 공격으로 막대한 피해가 발생했다.[75] 전 세계 350개 지점이 있고 연간 매출액이 100억 달러(약 12조원)에 이르는 미국의 글로벌 물류회사 엑스피다이터스(Expeditors)가 랜섬웨어 공격을 받아 약 3주 동안 배송 준비, 세관 및 유통 활동 관리, 회계 기능 등을 수행하는 데 문제가 발생해 글로벌 운영이 중단되었다. 완전히 복구하는 데에는 1달 이상 소요가 되었다. 이로인해 엑스피다이터스는 체선료 증가분 4000만 달러(약 480억 원), 조사 및 복구비용 2000만 달러(약 240억원) 등의 대규모 손실이 발생했고, 항공 화물 톤수 18%, 해상 컨테이너 물량 3%가 감소했다. 일본 도요타 자동차가 협력업체에 대한 랜섬웨어 공격으로 하루 동안 전면 생산이 중단됐다.[76] 일본의 세계적 자동차 회사 도요타의 자동차 부품 협력사 고지마프레스 공업이 랜섬웨어 공격을 받아 시스템장애를 일으켜 3월 1일 하루 동안 도요타의 일본 내 14개 공장 가동이 전면 중단되었다. 또한 도요타의 계열사로서 세계적인 자동차 부품회사인 덴소의 독일 법인이 랜섬웨어 공격을 받았다.[77] Pandora 랜섬웨어 갱단은 자신들이 이 공격을 수행했고, 15만 7000건 이상의 도면 등 1.4TB의 데이터를 유출했다고 주장했다.

일정 수준 이상의 보안을 갖추고 있으리라 생각되는 글로벌 기업에서도 전형적인 암호화 방식의 랜섬웨어 공격으로 비즈니스가 중단되어 수백억 원에 달하는 막대한 피해 사례가 계속 발생하고 있다. 특히 본사보다 취약한 협력사, 계열사 등 약한 고리를 공격함으로서 본사에 피해를 주는 방식은 협력업체가 많은 제조업에 피해가 클 수 있으므로 공급망 공격의 일부로 고려해 대책 강구가 필요하다.

현대자동차그룹은 현대오토에버를 비롯해 계열사를 중심으로 협력업체 공급사슬에 대한 보안위기 여부를 긴급 점검했다. 지난 3월 도요타 1차 협력업체(자동차 내외장재 생산회사)가 랜섬웨어 해킹을 당하면서 벌어진 일 때문이다. 협력사 해킹으로 당시 도요타 생산라인 전체가 하루 동안 셧다운되면서 자동차 약 1만3000대를 생산하는 데 영향을 받아 초유의 완성차 업계 해킹 사태를 보면서 현대차그룹도 긴급 점검을 실시한 셈이다.

국내에서도 랜섬웨어 해킹 피해 신고가 증가하고 있다. 과학기술정보통신부에 따르면 2019년 39건에 불과했던 랜섬웨어 신고 건수는 2020년 127건, 지난해에는 223건까지 치솟았다.

6. 랜섬웨어 피해예방 및 대응

랜섬웨어의 피해를 입지 않기 위한 예방에는 확인되지 않은 주소의 이메일이나 스팸 메일은 열어보지 않아야 하며 파일을 내려 받기 할 때에도 도메인이 정확히 확인 된 공식 사이트에서만 내려 받아야 한다. 또한, 운영체제를 주기적으로 업데이트 해야하며 운영체제와 모든 소프트에어의 업데이트를 최신버전으로 유지하고 있어야 한다. 중요자료는 정기적으로 백업하고 외부 저장장치 등을 이용한 2차 백업을 하거나 접근을 아예 차단하거나 보안백업 소프트웨어 등을 통해 쉽게 접근하기 어렵도록 설정한다. 연결되어있는 서버나 usb들은 사용하지 않을때는 연결해제 해놓는다. 이러한 예방수칙들에도 불구하고 랜섬웨어에 감염되었을 경우에 그에 따른 대응절차가 필요하다. 감염사실 확인 시 네트워크를 즉시 차단한다. 랜섬웨어는 인터넷을 통해 감염되기 때문에 연결 되어 있는 네트워크를 통해 랜섬웨어가 확산 될 위험이 있으므로 랜선을 뽑거나 해서 네트워크를 단절시킨다. 랜섬웨어에 아직 감염되지 않은 새로운 usb나 외장하드에 감염 된 데이터를 백업한다. 추후에 복구 될 가능성이 있기 때문이다. 감염 된 데이터들을 백업 및 이동했으면 감염 된 PC를 포맷하고 운영체제를 재설치한다. 운영체제를 비롯한 모든 소프트웨어는 최신 보안 업데이트를 적용한다. 새로운 운영체제가 설치되었으면 이전에 백업해둔 새 이동식 저장장치를 연결해 데이터 복구를 시도 해본다. 위 방법으로도 데이터복구 확률은 희박하다. 데이터복구가 되지 않았을 경우 백신소프트웨어 제조사 홈페이지 등을 통해 복구가능 여부를 확인한다. 모든 파일복구가 지원되는 경우는 드물어도 부분적인 복구를 지원하는 보안업체가 있을 수도 있다. Crypto Sheriff와 같은 도구를 사용하여 컴퓨터에 어떤 변종이 감염되었는지 확인하고 No More Ransan 과 같은 리소스를 검색하여 암호 해독 키가 생성 되었는지 확인한다. 이 방법은 흔한 랜섬웨어 변종의 공격을 받았다면 누군가 그 변종을 제거하고 파일을 복구 할 수 있는 가능성이 있다. 긱 스쿼드를 사용해 보거나 랜섬웨어 공격을 현지 경찰이나 미국연방수사국(FBI)에 신고한다. FBI는 인터넷 범죄고충센터를 통해 사이버 공격을 추적하게 된다. 랜섬웨어는 데이터복구율이 희박한 악성프로그램이다. 데이터 복구에 실패하더라도 해커와의 협상은 하지 않는다. 해커와의 협상한다고 하더라도 파일복구를 보장할 수 없고 또 합법적 거래가 아니므로 법의 보호도 받을 수 없다. 또한 한번 금전을 지불 한 피해자는 해커들로 하여금 금전을 지불 할 수 있는 대상으로 인식되어 이후 또 다른 해킹행위에 노출 될 가능성이 크다. 실제로 해커에게 금전을 지불 해도 암호키를 제공받지 못한 경우도 있고 금전을 지불한 후에 다시 공격 대상이 되는 경우도 있다. 이럴 경우 처음 공격보다 더 많은 금액을 요구한다. 이는 해킹행위를 장려하는 행위이므로 지양한다.

Ⅲ. 실험방법론 - 문헌조사

실험방법은 전체 71편의 논문을 리서치를 하여 비교조사하였고 2016년부터 올해 2022년도까지 총 6년의 자료를 분석 하였다.

[표 3] 항목,연도별 문헌조사 [1]~[71]

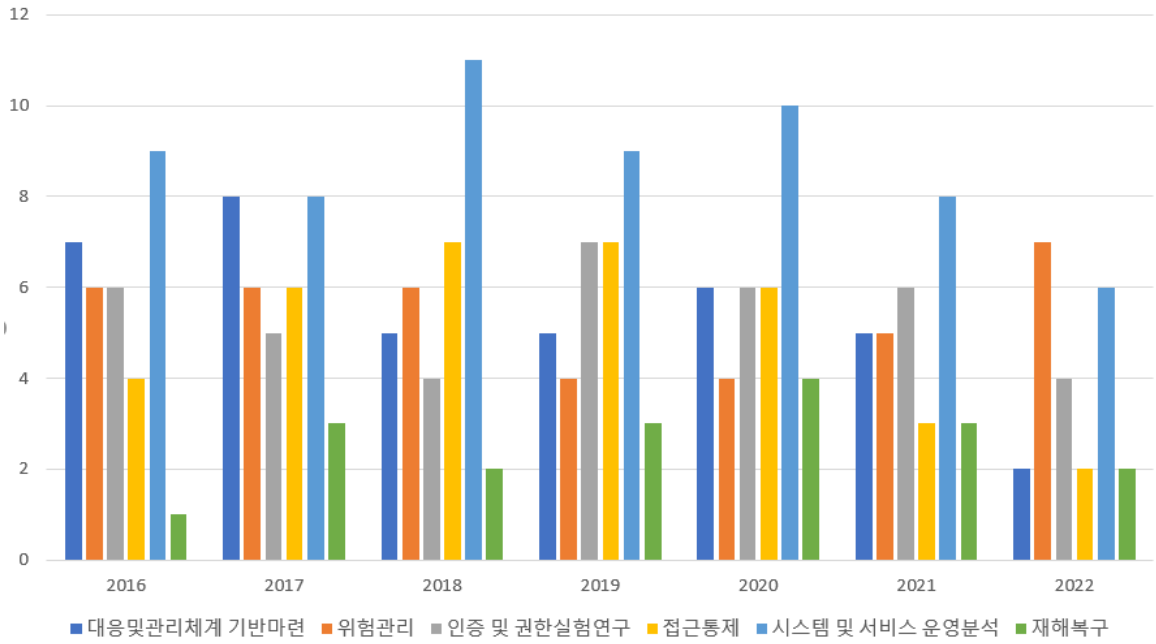
SEQ	Title Digital Library	Year	대응및관리체계기반마련	위험관리및동향분석	인증및권한실험연구	접근통제	시스템및서비스운영분석	재해복구
1	PC에 랜섬웨어 바이러스에 대한 경고	2016		●			●	
2	랜섬웨어의 종류와 앞으로의 동향	2016		●			●	
3	랜섬웨어 분석과 피해 최소화 방향	2016	●				●	
4	랜섬웨어 Cryptolocker에 대한 분석과 대응방안	2016	●		●		●	
5	윈도우즈에서의 랜섬웨어 악성행위 탐지방안에 대한 연구	2016	●	●	●	●	●	
6	랜섬웨어에 의한 보안위협 및 대응방안	2016	●	●	●	●	●	●
7	파일 I/O Interval을 이용한 랜섬웨어 공격차단 방법론	2016	●	●	●	●	●	
8	포렌식 기법 및 침해 지표를 활용한 랜섬웨어 대응 방안에 대한 연구	2016	●		●		●	
9	정적 및 동적 분석 툴을 활용한 랜섬웨어 탐지방안 연구	2016	●	●	●	●	●	
10	랜섬웨어와 북한의 사이버위협	2017	●	●				
11	통계적기법을 이용한 악성소프트웨어 분류	2017	●	●	●		●	
12	$UsnJrnl 기반 랜섬웨어 암호화 패턴 유형화 및 탐지 모델	2017	●	●	●	●	●	
13	효율적으로 랜섬웨어 탐지를 위한 미끼 파일	2017			●	●	●	
14	실시간 파일행위 분석을 통한 랜섬웨어 침해복구 방안 연구	2017	●	●	●		●	●
15	파일 암호화 기반 랜섬웨어 탐지에 대한 연구	2017	●		●	●	●	
16	대표적인 랜섬웨어 탐지 기법들의 취약점 분석	2017	●			●	●	
17	랜섬웨어 분석 및 탐지패턴 자동화모델에 관한 연구	2017	●	●		●	●	

18	클라우드기반 랜섬웨어 복구시스템 설계 및 구현	2017	●			●	●	●
19	랜섬웨어의 비즈니스	2017		●				●
20	파일 시스템 모니터링을 통한 클라우드스토리지 기반 랜섬웨어 탐지 및 복구시스템	2018	●	●	●	●	●	●
21	최신 랜섬웨어에 대한 암호키 복구 방안 연구	2018	●	●			●	●
22	최신 랜섬웨어 특징 분석	2018		●			●	
23	의료산업에서의 랜섬웨어 대응 방법	2018	●	●			●	
24	소셜 빅데이터 마이닝 기반 실시간 랜섬웨어 전파감지 시스템	2018				●	●	
25	바이너리 시각화와 기계학습을 이용한 랜섬웨어 탐지	2018			●	●	●	
26	랜섬웨어 탐지율을 높이기 위한 블록암호 알고리즘 식별방법에 관한 연구	2018			●	●	●	
27	랜섬웨어 유형별 특징분석 및 위협에 대한 연구	2018		●			●	
28	MacOS에서 화이트리스트를 이용한 랜섬웨어 탐지 연구	2018	●		●	●	●	
29	랜섬웨어 방어 SSD에서의 감염 데이터 분리 및 고속 쓰레기 수집 연구	2018	●	●		●	●	
30	Erebus 랜섬웨어에 대한 암호학적 분석 연구	2018				●	●	
31	플랫폼 독립적인 행위기반 랜섬웨어 대응 기술에 관한 연구	2019	●	●	●	●	●	●
32	랜섬웨어 특징정보 추출 및 탐지 연구	2019			●	●	●	
33	랜섬웨어 탐지를 위한 효율적인 미끼파일 배치방법	2019			●	●	●	
34	메모리 분석을 통한 Donut 랜섬웨어 복호화 방안 연구	2019		●	●		●	●
35	암호화 기반의 랜섬웨어로부터 사용자 데이터 보호 방안	2019	●			●	●	
36	랜섬웨어 공격에 대한 형사법적 고찰	2019	●	●				
37	동적 분석 및 기계학습을 활용한 랜섬웨어 탐지	2019			●	●	●	
38	데이터 복원이 가능한 사용자 요구사항 분석기반 랜섬웨어 탐지 시스템에 관한 연구	2019			●	●	●	
39	2019년 랜섬웨어 암호화 프로세스 분석 및 복호화 방안 연구	2019	●		●	●	●	●
40	2019 국내·외 주요 및 신규 랜섬웨어 동향 분석	2019	●	●			●	
41	클러스트링을 이용한 랜섬웨어에 사용 된 비트코인 주소 분석	2020		●	●		●	
42	차세대 랜섬웨어의 공격유형과 대응방안	2020	●				●	
43	모티프 찾기 알고리즘을 이용한 랜섬웨어 탐지에 관한 연구	2020			●	●	●	
44	랜섬웨어 대응을 위한 소규모 기업의 백업매카니즘의 비교분석	2020	●	●			●	
45	랜섬웨어 암호기능 및 복구 가능성 분석	2020	●			●	●	●
46	디스크 IO 분포를 활용한 랜섬웨어 탐지 및 무손실 복원 방법	2020			●	●	●	●
47	기업환경에서 백업 소프트웨어를 통한 랜섬웨어 대응	2020	●		●		●	●

	방안에 관한 연구							
48	기계학습을 이용한 랜섬웨어 조기 탐지	2020			●	●	●	
49	국방정보시스템에서의 랜섬웨어 위협 대응방안; 정보보안 위험관리 관점에서	2020	●	●				
50	Endpoint level의 효과적인 랜섬웨어 대응방안 연구	2020	●	●	●	●	●	
51	5ss5c와 Immuni 랜섬웨어의 암호화 프로세스 분석 및 복구 방안 연구	2020				●	●	●
52	커넥티드 의료기기 해킹 및 랜섬웨어 대응기술동향	2021	●	●			●	
53	Magniber v2, Ragnar Locker, Donut 랜섬웨어에 대한 복호화 연구 및 암호키 검증 방안	2021			●		●	●
54	랜섬웨어 탐지를 위한 그래프	2021			●	●	●	
55	랜섬웨어 해커의 공격	2021		●				
56	2021년 랜섬웨어 현황 및 대응예방 정책 동향	2021	●	●				●
57	미국의 사이버안보 거버넌스 구축과 대응 : ‘워너크라이(WannaCry)’를 중심으로	2021	●	●			●	
58	키 재사용 공격을 통한 Ragnar Locker 랜섬웨어 감염 파일 복호화 및 활용 방안 연구	2021			●		●	●
59	랜섬웨어 피해현황 및 대응방안	2021	●	●				
60	랜섬웨어 대응 및 데이터 유출 보호를 위한 파일 접근 로그 기반 파일 접근 제어 시스템	2021			●	●	●	
61	디지털트윈 기반의 스마트공장에서 랜섬웨어 공격과 피해 분석을 위한 정보보안 실습콘텐츠 시나리오 개발	2021			●		●	
62	Google Rapid Response 기반 랜섬웨어 공격 대응 방안	2021	●		●	●	●	
63	타깃 랜섬웨어 그룹 동향	2022		●				
64	최신 랜섬웨어 동향 및 발전 방향	2022		●			●	
65	스트림 암호 기반 랜섬웨어에 대한 기술적 분석 동향	2022		●	●		●	
66	블록암호 기반 랜섬웨어에 대한 분석 사례 동향	2022		●	●		●	
67	랜섬웨어에서 메모리 덤프를 통한 파일 복호화에 관한 연구	2022			●		●	●
68	랜섬웨어를 이용한 암호화폐 탈취 및 자금세탁 방법에 대한 대응방안 연구 동향 분석	2022		●			●	
69	랜섬웨어 특징 분석을 통한 탐지 기술 조사 연구	2022			●	●	●	
70	랜섬웨어 피해 저감을 위한 공격 타임라인별 대응전략 및 기술	2022	●	●		●		●
71	2021년 및 2022년 상반기 주요 랜섬웨어 대응 정책	2022	●	●				

2016년도 9편, 2017년도 10편, 2018년도 11편, 2019년도 10편, 2020년도 11편, 2021년도 11편, 2022년도 8편으로 총 71 편의 논문과 참고문헌을 조사 비교 했으며 그 중 대응 및 관리체계 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. 랜섬웨어의 복호화가 어려운 만큼 재해복구가 포함되어있는 문헌은 적은 모습을 보였다. [그림 2]



[그림 2] 연도별 항목별 참고문헌조사 그래프

Ⅳ. 실험결과 - 문헌조사

1. 2016년도

약 3000억원 피해

랜섬웨어가 본격화되기 시작한 시점이라 2015년 대비 2배가량 많은 피해가 발생했고 랜섬웨어도 급속도로 진화했다. 이전에는 PC의 아이콘과 시작버튼을 선택할 수 없는 화면잠금형 랜섬웨어가 주류였다면 이 시점부터는 사용자의 데이터를 암호화하는 데이터잠금형 랜섬웨어가 시작됐다. 랜섬웨어 종류로는 록키와 케르베르가 성행. 초반에 성행하던 테슬라크립트와 크립트XXX는 소멸하는 모습을 보임. 이 외 공격자 측면에서 수익화를 성공한 랜섬웨어로는 케르베르, 록키, 크립토락커, 테슬라크립트, 크립트XXX, CTB-락커, 크립토월 등이 있다.[78][79] 이전에 비해 급작스러운 피해량 증가해 피해금액이 상대적으로 많다. 2016년도의 가장 큰 특이사항으로는 랜섬웨어의 수익화가 가능한 점을 대중적으로 알리기 시작했다는 점이다. 랜섬웨어가 서비스처럼 제공되는 RaaS(Ransomware as a Service)가 시작되었다. 랜섬웨어를 자체 개발 후 타인에게 판매하는 형태로 구매자가 원하는 방향으로 제작과 유포가 가능하도록 거래된다. 또한 집단지성을 이용한 랜섬웨어의 오픈소스가 이루어졌는데 유포방식에는 스팸메일, 익스블로잇킷, 멀버타이징 등이 있으며 최근에는 원격 데스크톱 프로토콜을 이용한 유포도 확산되고 있다.

이전 유포방식은 스팸 메일을 통해 전통적인 악성코드 유포, 이메일 제목 및 내용 첨부 파일 등으로 사용자를 속여 메일 또는 첨부 파일을 열도록 유도하는 방법이 있었다면 2016년 들어서는 익스플로잇킷(EK) 웹 취약점(Drive-by-download)을 이용하는 유포방식도 발견되었다. 또한 멀버타이징기법으로 EK와 광고 모듈이 결합된 방식을 이용하기도 한다. 이 유포방식은 불특정 다수의 감염에 효과적이다.

2. 2017년

약 7000억원 피해

2017년은 RaaS(Ransomware as a Service)로 인해 랜섬웨어의 종류가 더더욱 다양해지고 많은 변종이 생겨났다. 잠시 활동이 없던 Locky와 Cerber가 다시 활동을 시작했으며 특히 Cerber는 방화벽 차단 목록으로 PC에 설치 된 보안제품 업데이트를 방해하는 기능을 추가한 버전6으로 더욱 강력하게 활동했으며 5월초에는

SMB(Server Message Blcok)의 취약점을 악용한 WannaCryptor 유포에 이용되었던 Petya라는 새로운 랜섬웨어가 기승을 부리며 세계 곳곳의 주요기관을 마비시켰다. Petya는 일반적이게 데이터들을 암호화하는 것은 물론 부팅이 필요한 정보를 담고 있는 MBR(Master Boot Record)를 변조하고 파일의 메타정보 MFT(Master File Table) 영역을 암호화하는 새로운 기술을 선보였다.[82] 2016년부터 랜섬웨어의 본격화로 인해 수익시장이 형성 된 것이 기폭제가 되어 2017년에는 더더욱 고수익을 추구하는 수익시장의 확대가 이루어졌다. 시장이 확대됨에 따라 랜섬웨어 대상이 세계적으로 확대되었으며 그로 인해 다국어를 지원했으며 지불 옵션도 스포라를 통해 다양화 되었다.[81] 스포라는 랜섬웨어 피해자들을 대상으로 한 대금 지불 소프트웨어인데 전체복구와 재감염 방지기능까지 금전을 통해 거래가 가능하다. 랜섬웨어를 통한 사회공학 해킹기법도 등장했다. 기관과 기업 사용자를 대상으로 사내 내부지침과 블로그 사진 수정을 요구하는 고소장으로 위장한 개인의 심리를 타겟으로 한 사회공학기반 랜섬웨어 유포사례도 생겨났다. 2017년도의 두드러지는 랜섬웨어의 특징은 본격적으로 랜섬웨어가 진화했으며 수익 시장도 더욱 더 커졌다. 랜섬웨어 오픈소스의 대중화가 이루어졌으며 서비스형 랜섬웨어 RaaS가 보편화 되었으며 이로인해 다양한 변종이 발생했고 랜섬웨어는 더욱 진화했다.[83]

3. 2018년도

약 1조 500억원 피해 [86].

수많은 변종들이 탄생하며 공격기법이 진화되었다. 변종으로 공격을 해 보안기술을 무력화 시켰으며 복구가 불가능하도록 암호화 기법이 지능화 되고 키 관리체계가 향상되었다. 2018년 갠드크랩(Gandcrab)이라는 랜섬웨어가 처음 등장했는데 갠드트랩은 전체피해의 약 53% 정도 비율을 차지했다.[84] 갠드크랩은 서비스형 랜섬웨어(RaaS)로 다크웹을 통해 판매 및 유통되어 지속적으로 새로운 변종을 제작하였다. 갠드크랩은 NSA 툴에 탑재된 이터널블루(EternalBlue) 취약점을 활용했으며 북한 폰트파일로 위장하여 유포 된 바 있다. 공정거래위원회를 사칭하거나 안랩의 V3 Lite 제거를 유도하는 기능도 발견되었다. 2018년 한해 최악의 랜섬웨어로 볼 수 있다. 또 다른 악명높은 랜섬웨어는 파일리스(Fileless)형태로 활동하는 메그니베르(Magniber)가 있다. 또 요구하는 랜섬머니의 종류가 다양화 되었다. 기존에는 대부분 랜섬웨어 대금을 비트코인으로 지불하였지만 비트코인캐시, 모네로, 제트캐시 등 다양한 납부방식이 생겨났다.[85]

공격대상이 다양화 되었다. 2017년 본격적인 랜섬웨어의 발전으로 공격대상을 기업 및 기관들로 확장해갔는데 그 때문에 2018년에는 특히나 기업 및 기관들을 노리는 현상이 생겼다. 정보가 중요할 수 밖에 없는 기업 및 기관들이 수익화에 최적이라고 판단 했다.[88] 실제로 전 세계 공장들 뿐 아니라 거대 해운회사 COSCO, 각 국

의 공항, 병원 등 수많은 기업 및 기관들이 랜섬웨어에 감염되었다. 수법은 더욱 더 악랄해졌는데 입사지원문의나 피고소환통지서, 쇼핑몰 쿠폰발송, 택배 등등의 내용으로 사용자들의 클릭을 유도했다.[87]

4. 2019년

약 13조 피해액

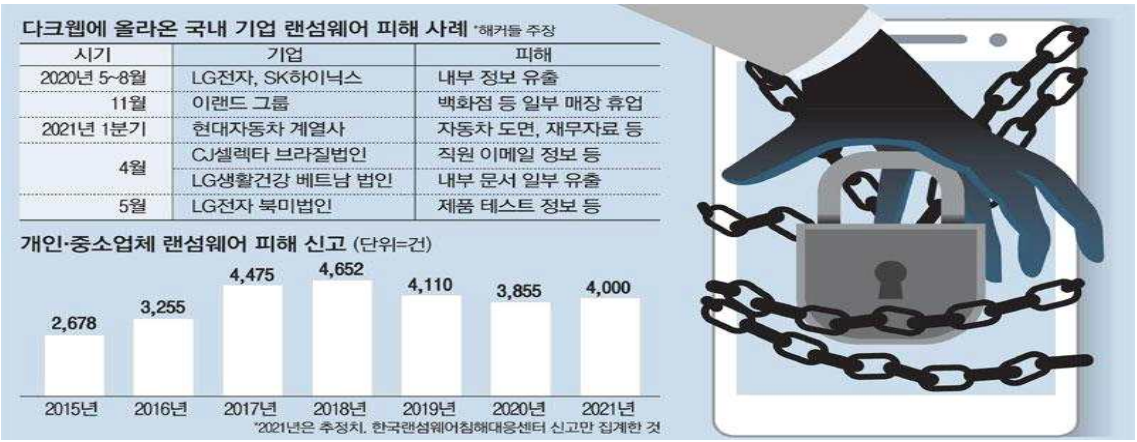
개인들이 다양한 방법으로 랜섬웨어를 사전 방지하고 피해를 당하였다고 해도 대금을 지불하지 않자 공격자들의 수익이 감소하였다. 이에 공격자들은 기업을 주로 공격하게 된다. 이것이 2018년 초 이후부터 광범위한 무차별 랜섬웨어 공격 발생은 현저히 줄어들었지만 랜섬웨어 공격으로 인한 피해액 자체는 크게 증가하게 된 이유다. 제조업이나 공공기간과 같은 기업을 집중적으로 목표하는 랜섬웨어가 다수 출현하였다. 작년 등장한 갠드크랩 랜섬웨어가 여전히 기승을 부리고 있는 와중에 신규 랜섬웨어인 Clop이 새로 등장했는데 클롭은 기업을 표적으로 하는 신규랜섬웨어다.[93] 클롭은 기업에서 사용하는 중앙관리서버(AD서버 Active Directory)에 침투한다. 기업 윈도우 서버를 타깃으로 침투 한 후 기업 내부망과 연결 된 백업서버의 자료를 손상시키며 AD domain controller 관리자 계정을 탈취 해 연결 된 하위 시스템들을 감염시킨다. 하반기 랜섬웨어는 네트워크 스토리지(NAS, Network Attached Storage)를 공격하기에 이르른다. [89]~[92]

5. 2020년

약 23조 피해 코로나 이후로 조금더 증가

대표적인 랜섬웨어 류크, 소디노키비, 메이즈, 코로나바이러스[94]

2020년부터는 세계적인 코로나 사태로 인해 랜섬웨어 공격자들에게는 황금같은 기회의 해다. 실제로 코로나를 키워드로 하는 랜섬웨어 유포도 다수 발생했고 스스로 랜섬웨어 명칭을 Coronavirus로 변경하는 경우도 발생했다.[95] 기존 Nemty & Makop 랜섬웨어에 의한 공격과 재택근무 확산으로 RDP 취약점을 노리는 공격이 발생했다. 실제로 2019년 한국인터넷진흥원(KISA)에 신고된 랜섬웨어 피해사례는 39건이지만, 2020년에는 127건으로 3배 이상 급증했다. 한국랜섬웨어 침해대응센터에 신고 된 랜섬웨어 피해사례는 아래와 같다.[그림 3]



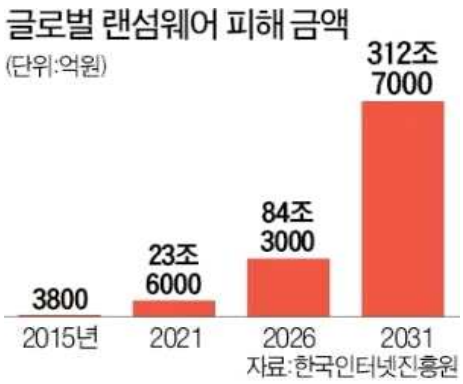
[그림 3] 국내 개인, 중소기업 랜섬웨어 연도별 피해수치
출처 : 한국랜섬웨어침해대응센터 매일경제 보안뉴스 중

지난 수년 간 랜섬웨어 공격은 더욱 정교하고 신박한 기술을 적용하면서 발전을 거듭해왔다. 2020년 랜섬웨어 공격 빈도수는 전년도와 비슷하게 유지되고 있지만 기업을 타겟으로 공격 방식이 점점 더 표적화되고 정교해져서 피해비용은 계속 증가하고 있는 추세다. 일부 공격은 새로운 데이터 유출 방법을 획득했는데 세계적인 보안 컨설팅 업체인 크롤(Kroll)은 2020년 올해에는 랜섬웨어 공격자들 사이에서 파일 암호화와 정보 유출을 동시에 진행하는 현상이 발생했다고 진단했다. 데이터를 도용해 인터넷에 공개하려고 위협하는 새로운 공격방법으로 랜섬웨어 공격과 더불어 정보유출을 통한 협박을 동시 진행하고 있는 것이다. 랜섬웨어 메이즈(Maze)는 랜섬웨어 대금 지불을 거부할 경우 유출 된 정보를 공개하겠다고 위협했다. 실제로 Revil 랜섬웨어는 6월 경 훔친 정보를 경매하기 시작했고 11월 경 메이즈 랜섬웨어는 피해자들로부터 훔친 정보를 다크웹사이트에 일부 공개하기도 했다.[96] 이로 인해 기업들의 더욱 많은 피해를 입게 되었다. 올해 처음 등장한 이 특이한 전략은 모든 랜섬웨어 공격의 약 2/5 확률로 발견되고 있으며 점차 증가할 것으로 예상했다.[97]

6. 2021년

코로나 사태로 인해 증가된 사이버 활동이 증가함에 따라 랜섬웨어 공격 범위와 피해규모도 함께 증가하고 있다. 과거에는 랜섬웨어 공격자가 개인인 경우가 많았지만 지금은 거대조직을 중심으로 해커들이 뭉치면서 이른바 갱단으로 불리우는 조직화 된 랜섬웨어 공격자 집단이 등장하게 된다.[99] 대표적인 갱단으로는 Conti와 Locky가 있다. 그만큼 대응도 어려워지고 랜섬웨어 대금도 커지고 있다. 2019년 건당 8만4116달러(약 9800만원) 수준이던 몸값은 지난해 15만4108달러(약 1억8000만원), 올해 22만298달러(약 2억5700만원)로 해마다 두 배 가까이 커지고 있

다. 2021년에는 랜섬웨어 공격의 77%가 데이터 유출 위협을 포함했는데, 이는 작년보다 10% 증가한 수치다.[그림 4].[98][100]

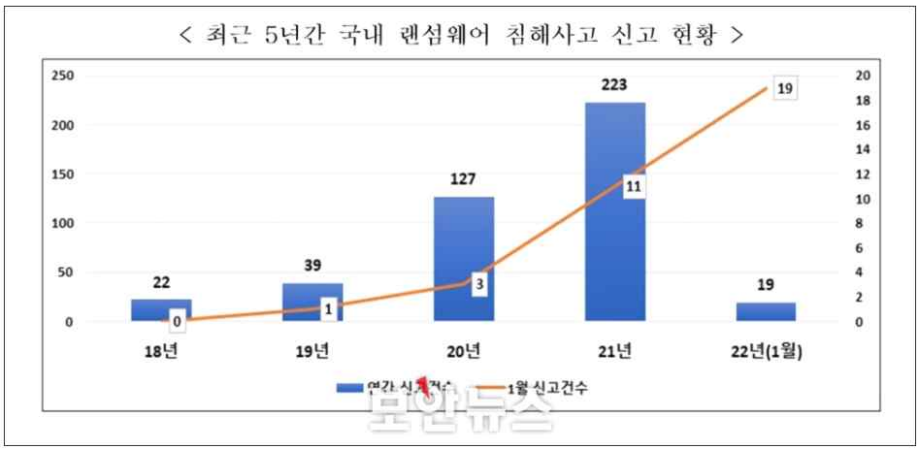


[그림 4] 글로벌 랜섬웨어 피해금액 - 예측 수치
출처 : 한국인터넷진흥원

대기업과 의료기관 등 기업을 대상으로 한 랜섬웨어 공격이 지속되고 있으며 법원과 경찰서 등 형사사법기관을 대상으로 하는 사례도 발견되었다. 4월 미국 워싱턴 DC 경찰서도 Babuk 랜섬웨어에 감염되었으며 5월에는 미국 최대 송유관 업체 Colonial Pipeline 이 DarkSide 랜섬웨어에 공격당해 연료 공급망이 마비되었는데 이는 미국에서 가장 큰 랜섬웨어 공격으로 화제가 되었다. 이로인해 미국 연방 운송회사 언전청인 FMCSA(Federal Motor Carrier Safety Administration)는 17개 주와 콜롬비아 특별구에 즉각적인 석유 공급을 위해 지역 비상 선언을 발표하였다. 6년만에 휘발유 가격이 최고치를 기록하였고 미국의 추적과 압수수색 끝에 DarkSide 랜섬웨어는 운영이 중단되었고 지불한 몸값을 일부 회수 한 첫 번째 사례이다.[101] 세계적인 대기업 및 국가 주요 인프라를 대상으로 하는 랜섬웨어 공격이 다수 발생함에 따라 미국을 포함한 세계의 다양한 국가기관에서 직접 나서 랜섬웨어 대응책을 발표하게 되었다. 한국인터넷진흥원(KISA)는 Stop Ransomeware 사이트를 개설했으며 인터폴은 랜섬웨어 대응을 위한 국제적인 협력촉구를 발표했으며 미국은 랜섬웨어에 대한 국가 보안각서 및 주의보 등등을 발표했다.

7. 2022년

랜섬웨어가 날이 갈수록 정교해지고 조직화되어 더욱 기승을 부리고 있다. 특히나 공공기관과 기업을 대상으로 하는 공격이 더욱 집중적으로 발생하고있고 러시아와 우크라이나간에 발생한 전쟁상황을 악용하여 랜섬웨어를 유포하기도 한다. 한국인터넷진흥원(KISA)에 접수된 랜섬웨어 피해신고 건수 2020년 127건, 2021년 223건, 2022년(8월기준) 225건으로 올해는 상반기에만 작년보다 많은 피해건수를 보이고 있다. [그림 5].



[그림 5] 최근 5년간 국내 랜섬웨어 침해사고 신고 현황
출처 : 과학기술정보통신부 보안뉴스의 인용

최근 랜섬웨어들은 RaaS(Ransomeware as a Service) 형태로 랜섬웨어에 제작에 대한 전문지식이 없어도 비용만 지급하면 되는 서비스 형태의 공격으로 진화하고 있어 사이버 범죄의 진입장벽이 점차 낮아졌다. RaaS 서비스로 최근 랜섬웨어들은 공격자와 제작자가 구분되어 수익을 나눠가지는 구조를 통해 더욱 더 조직화 된 하나의 기업처럼 움직이는 갱단이 늘고 있다. 대표적인 갱단으로는 Lockbit 가 있는데 이 Lockbit는 1차적으로 RaaS 형태의 랜섬웨어를 유포하여 감염을 시키고 2차적으론 다크웹으로 훔친 정보를 유출한다. 그야말로 수년간 랜섬웨어가 가진 특징을 종합적으로 탑재한 랜섬웨어의 최종 진화라고 할 수 있다. 록비트는 여러차례 업데이트를 거치면서 랜섬웨어 최초로 버그바운티를 도입하여 록비트 랜섬웨어에 대한 버그를 제보해주면 현상금을 지불한다고 대대적으로 홍보하였으며 랜섬웨어 대금을 Zcash 코인으로 지불 할 수 있게 암호화폐를 추가 도입했고 다양한 Anti-Analysis & Evasion 기능을 도입하여 활발히 활동 중이다. 이렇게 랜섬웨어 공격은 갈수록 사업화 되고 있다. 이처럼 랜섬웨어 피해사례가 기하급수적으로 증가함에 따라 보안업계는 2023년 랜섬웨어 피해액이 300조가 넘을 것으로 예측하고 있다.[102]

[표 4] 연도별 주요 랜섬웨어 및 최신동향

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, 기업등으로 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

V. 결론

본 논문은 랜섬웨어에 대한 소개와 피해예방법, 대응방안 등을 제시하고 최신 랜섬웨어의 동향을 분석하였다. 최근에는 랜섬웨어 감염사례가 더 빈번하게 발생하고 있으며 이로 인한 금전적 피해와 데이터 손실 및 유출 등 2차피해마저 계속 증가하는 추세다. 디지털시대에 사용자들이 마음껏 인터넷을 사용 할 수 없는 정신적인 고통을 겪고 있는 것이다. 이전에는 많은 사람이 대기업에는 보안팀이 있고 해커들이 침입하기 힘들다고 생각했었지만 수많은 랜섬웨어들이 기업과 공공기관 공격에 성공해 엄청나고 방대한 피해를 주고 있다. 많은 사이버 범죄자가 기업과 공공기관에 눈을 돌렸으며 디지털시대에 살고있는 우리들은 모두 기업의 이용자들이다. 대부분의 이용자들은 글로벌기업들의 보안성을 신뢰하고 사용하고 있다. 그러나 앞서 살펴 본 바와 같이 공공기관과 글로벌기업들이 최신 랜섬웨어의 주요 타겟이며 그로 인해 랜섬웨어 공격에 더 쉽게 당할 수 있다. 랜섬웨어의 잠재적인 위협에 대한 공격 코드 또한 지속적으로 공개되고 있다. 따라서 기업과 공공기관에서 앞서서 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. 안전한 네트워크 환경의 제공과 이용자의 이용반경에 대한 보안솔루션의 운영과 관리에 대한 관심이 필수적이다. 앞으로 또 어떤 공격 기법이 생겨나고 성행할지는 알 수 없다. 그러나 랜섬웨어가 지속해서 발전하고 다크웹에서의 입지가 넓혀가고 있기때문에 랜섬웨어 방어에 더 많은 자원을 투자해야 할 것이다. 앞으로 랜섬웨어는 모든 기업의 1순위 방어대상이 될 것이다. 이를 극복하기 위해서 랜섬웨어에 대한 전반적인 지식이 필요하며 최근동향을 살펴볼 필요가 있다. 또한 올바른 인식과 예방수칙이 필요하며 이러한 내용을 시스템에 적용해 랜섬웨어에 대한 피해를 최소화 시켜야 할 것이다. 최근 화이트햇 해커들과 사이버보안 전문가들이 새로운 랜섬웨어 변종들과 랜섬웨어 갱단들에 대응하기 위해 부지런히 연구하고 있으니 더 좋은 대응절차가 나오리라 기대해본다.

참고문헌

[1] 곽수동. (2016) “PC에 랜섬웨어 바이러스에 대한 경고”
[2] 서규원. 김호원, (2016) “랜섬웨어의 종류와 앞으로의 동향”
[3] 문재연, 장영현, (2016) “랜섬웨어 분석과 피해 최소화 방향”
[4] 김용기, 함동균, 주영환, 이근호, (2016) “랜섬웨어 Cryptolocker에 대한 분석과 대응방안”
[5] 박지요, (2016) “윈도우즈에서의 랜섬웨어 악성행위 탐지방안에 대한 연구” 학위논문
[6] 박병태, (2016) “랜섬웨어에 의한 보안위협 및 대응방안, 2016” 학위논문
[7] 윤정무, (2016) “파일 I/O Interval을 이용한 랜섬웨어 공격차단 방법론”
[8] 이지영, (2016) “포렌식 기법 및 침해 지표를 활용한 랜섬웨어 대응 방안에 대한 연구” 학위논문
[9] 오예지, (2016) “정적 및 동적 분석 툴을 활용한 랜섬웨어 탐지방안 연구” 학위논문
[10] 장노순, (2017) “랜섬웨어와 북한의 사이버위협”
[11] 김현주, (2017) “통계적기법을 이용한 악성소프트웨어 분류”
[12] 김형규, 정동호, 진필근, 한채민, 김기범, (2017) “$UsnJrnl 기반 랜섬웨어 암호화 패턴 유형화 및 탐지 모델”
[13] 이정환. (2017) “효율적으로 랜섬웨어 탐지를 위한 미끼 파일” 학위논문
[14] 김재용. (2017) “실시간 파일행위 분석을 통한 랜섬웨어 침해복구 방안연구” 석사학위논문, 고려대학교
[15] 황상엽. (2017) “파일 암호화 기반 랜섬웨어 탐지에 대한 연구” 석사학위논문, 숭실대학교
[16] 김종현, 박기성, 박영호. (2017) “대표적인 랜섬웨어 탐지 기법들의 취약점 분석” 학술논문, 경북대학교
[17] 이후기, 성종혁, 김유천, 김종배, 김광용. (2017) “랜섬웨어 분석 및 탐지패턴 자동화모델에 관한 연구” 한국정보통신학회논문지
[18] 하상민, 김태훈, 정수환. (2017) “클라우드기반 랜섬웨어 복구시스템 설계 및 구현” 숭실대학교
[19] 이진천. (2017) “랜섬웨어의 비즈니스” ㈜디씨에스
[20] 김주환, 최민준, 윤주범. (2018) “파일 시스템 모니터링을 통한 클라우드스토리지 기반 랜섬웨어 탐지 및 복구시스템” 세종대학교
[21] 김소람. (2018) “최신 랜섬웨어에 대한 암호키 복구 방안 연구” 석사학위논문, 국민대학교
[22] 문기운, 이종혁. (2018) “최신 랜섬웨어 특징 분석”

[23] 전인석, 김동원, 한근희. (2018) “의료산업에서의 랜섬웨어 대응 방법”
[24] 김미희, 윤준혁. (2018) “소셜 빅데이터 마이닝 기반 실시간 랜섬웨어 전파감지 시스템”
[25] 지환태. (2018) “바이너리 시각화와 기계학습을 이용한 랜섬웨어 탐지” 석사학위논문, 한양대학교
[26] 윤세원, 전문석. (2018) “랜섬웨어 탐지율을 높이기 위한 블록암호 알고리즘 식별방법에 관한 연구” 숭실대학교
[27] 조성준, 강승용, 노봉남. (2018) “랜섬웨어 유형별 특징분석 및 위협에 대한 연구” 한국정보기술학회, 한국디지털콘텐츠학회
[28] 윤정무. (2018) “MacOS에서 화이트리스트를 이용한 랜섬웨어 탐지 연구” 석사학위논문, 충남대학교
[29] 민동현, 안진우, 김영재. (2018) “랜섬웨어 방어 SSD에서의 감염 데이터 분리 및 고속 쓰레기 수집 연구” 서강대학교
[30] 김소람, 김지훈, 박명서, 김대운, 김종성. (2018) “Erebus 랜섬웨어에 대한 암호학적 분석 연구” 국민대학교, 한국인터넷진흥원
[31] 고용선. (2019) “플랫폼 독립적인 행위기반 랜섬웨어 대응 기술에 관한 연구” 박사학위논문, 숭실대학교
[32] 이규빈. (2019) “랜섬웨어 특징정보 추출 및 탐지 연구” 석사학위논문, 이규빈
[33] 이진우, 김용민, 이정환, 홍지만. (2019) “랜섬웨어 탐지를 위한 효율적인 미끼파일 배치방법”
[34] 이세훈, 김소람, 김기윤, 김대운, 박해룡, 김종성. (2019) “메모리 분석을 통한 Donut 랜섬웨어 복호화 방안 연구”
[35] 김성수. (2019) “암호화 기반의 랜섬웨어로부터 사용자 데이터 보호 방안” 석사학위논문, 숭실대학교
[36] 양종모. (2019) “랜섬웨어 공격에 대한 형사법적 고찰” 영남대학교
[37] 이승환. (2019) “동적 분석 및 기계학습을 활용한 랜섬웨어 탐지” 석사학위논문, 인하대학교
[38] 고용선, 박재표. (2019) “데이터 복원이 가능한 사용자 요구사항 분석기반 랜섬웨어 탐지 시스템에 관한 연구” 숭실대학교
[39] 이세훈, 윤병철, 김소람, 김기윤, 이영주, 김대운, 박해룡, 김종성. (2019) “2019년 랜섬웨어 암호화 프로세스 분석 및 복호화 방안 연구”
[40] 박은후, 김소람, 이세훈, 김종성. (2019) “2019 국내·외 주요 및 신규 랜섬웨어 동향 분석” 정보보호학회지
[41] 김보선,신무곤, 이민성,백의준,김명섭. (2020) “클러스트링을 이용한 랜섬웨어에 사용 된 비트코인 주소 분석” 고려대학교
[42] 우성희. (2020) “차세대 랜섬웨어의 공격유형과 대응방안” 한국교통대학교

[43] 윤영진. (2020) “모티프 찾기 알고리즘을 이용한 랜섬웨어 탐지에 관한 연구” 석사학위논문, 한양대학교
[44] 박홍진. (2020) “랜섬웨어 대응을 위한 소규모 기업의 백업매카니즘의 비교분석”
[45] 이영주. (2020) “랜섬웨어 암호기능 및 복구 가능성 분석” 정보보호학회지
[46] 백성하. (2020) “디스크 IO 분포를 활용한 랜섬웨어 탐지 및 무손실 복원 방법” 박사논문학위, 인하대학교
[47] 조영훈. (2020) “기업환경에서 백업 소프트웨어를 통한 랜섬웨어 대응방안에 관한 연구” 석사학위논문, 아주대학교
[48] 조영훈. (2020) “기계학습을 이용한 랜섬웨어 조기 탐지” 석사학위논문, 국민대학교
[49] 유진철,문상우,김종화. (2020) “국방정보시스템에서의 랜섬웨어 위협 대응방안; 정보보안 위험관리 관점에서”
[50] 유다선. (2020) “Endpoint level의 효과적인 랜섬웨어 대응방안 연구” 석사학위논문. 고려대학교
[51] 신수민, 김소람, 윤병철, 허욱, 김대운, 김기문, 김종성. (2020) “5ss5c와 Immuni 랜섬웨어의 암호화 프로세스 분석 및 복구 방안 연구”
[52] 권혁찬, 정병호, 문대성, 김익균. (2021) “커넥티드 의료기기 해킹 및 랜섬웨어 대응기술동향”
[53] 이세훈. (2021) “Magniber v2, Ragnar Locker, Donut 랜섬웨어에 대한 복호화 연구 및 암호키 검증 방안” 석사학위논문, 국민대학교
[54] 최도현. (2021) “랜섬웨어 탐지를 위한 그래프”
[55] 허영섭. (2021) “랜섬웨어 해커의 공격”
[56] 김소람, 강수진, 최용철, 박귀은, 이민정, 김종성. (2021) “2021년 랜섬웨어 현황 및 대응예방 정책 동향” 정보보호학회지
[57] 홍건식. (2021) “미국의 사이버안보 거버넌스 구축과 대응 : ‘워너크라이(WannaCry)’를 중심으로” 중앙대학교
[58] 강수진, 이세훈, 김소람, 김대운, 김기문, 김종성. (2021) “키 재사용 공격을 통한 Ragnar Locker 랜섬웨어 감염 파일 복호화 및 활용 방안 연구”
[59] 김기범. (2021) “랜섬웨어 피해현황 및 대응방안” 성균관대학교
[60] 이한수, 김동주, 이혁준, 황동혁. (2021) “랜섬웨어 대응 및 데이터 유출 보호를 위한 파일 접근 로그 기반 파일 접근 제어 시스템”
[61] 남수만, 이승민, 박영선. (2021) “디지털트윈 기반의 스마트공장에서 랜섬웨어 공격과 피해 분석을 위한 정보보안 실습콘텐츠 시나리오 개발”
[62] 오세욱, 손태식. (2022) “Google Rapid Response 기반 랜섬웨어 공격 대응 방안” 아주대학교
[63] 박태환. (2022) “타깃 랜섬웨어 그룹 동향”

[64] 문기운, 이종혁. (2022) “최신 랜섬웨어 동향 및 발전 방향” 정보보호학회지
[65] 이영주. (2022) “스트림 암호 기반 랜섬웨어에 대한 기술적 분석 동향” 정보보호학회지
[66] 김준섭. (2022) “블록암호 기반 랜섬웨어에 대한 분석 사례 동향” 정보보호학회지
[67] 김승환, 손태식. (2022) “랜섬웨어에서 메모리 덤프를 통한 파일 복호화에 관한 연구” 아주대학교
[68] 김금보, 허신욱, 김호원. (2022) “랜섬웨어를 이용한 암호화폐 탈취 및 자금세탁 방법에 대한 대응방안 연구 동향 분석” 정보보호학회지
[69] 정혜림, 박기웅. (2022) “랜섬웨어 특징 분석을 통한 탐지 기술 조사 연구”
[70] 이슬기, 김동욱, 이태우. (2022) “랜섬웨어 피해 저감을 위한 공격 타임라인별 대응전략 및 기술” 정보보호학회지
[71] 강수진, 김종성. (2022) “2021년 및 2022년 상반기 주요 랜섬웨어 대응 정책” 정보보호학회지
[72] 보안뉴스, 블랙캣 랜섬웨어, 패션 거물 업체 몽클레르 정보 유출
https://www.boannews.com/media/view.asp?idx=104213
[73] 조선비즈, [유통가 해킹 전쟁]① “500억 내놔” 이랜드 협박사건...샤넬・풀무원도 뚫렸다
https://biz.chosun.com/distribution/channel/2021/08/27/KCWPF4II5BFILNF6WKP6XNQLWU/
[74] 시큐리티어페어스, Swissport International, 랜섬웨어 공격 받아 항공편 지연
https://securityaffairs.co/wordpress/127655/cyber-crime/swissport-international-ransomware-attack.html
[75] Expeditors, Expeditors 랜섬웨어 공격으로 운영 시스템 폐쇄
https://www.expeditors.com/022022-downtime-notification
http://www.cargopress.co.kr/korean/news_view.php?nd=2950
[76] 한경뉴스, 교묘해진 랜섬웨어…도요타 대신 협력사 공격
https://www.hankyung.com/international/article/2022030167731
[77] 글로벌비즈, 도요타 부품업체 덴소, 독일 현지법인 랜섬웨어 사이버공격 받아
https://news.g-enews.com/article/Global-Biz/2022/03/202203140730023896b5d048c6f3_1?md=20220314080626_U
[78] Ahnlab, 최신 랜섬웨어 동향 분석 보고서
https://download.ahnlab.com/kr/site/library/Report_Ransomware_Trend_Analysis.pdf
[79] 데일리시큐, 2016년 랜섬웨어 침해분석과 2017년 침해 전망
https://www.dailysecu.com/news/articleView.html?idxno=18369
[80] Ahnlab, 2017년 랜섬웨어 동향 보고서
https://www.ahnlab.com/kr/site/securityinfo/asec/asecView.do?groupCode=VNI001&seq=

26596
[81] Ahnlab, 2017년 1분기 랜섬웨어 동향
https://asec.ahnlab.com/ko/1065/
[82] Ahnlab, 2017년 상반기 랜섬웨어 동향
https://asec.ahnlab.com/ko/1073/
[83] 2017년 상반기, 랜섬 위협 쓰나미에 휩쓸리다
https://byline.network/2017/08/1-836/
[84] Ahnlab, 2018년 랜섬웨어 동향
https://asec.ahnlab.com/ko/1188/
[85] 2018년 랜섬웨어 동향 및 특징
https://www.estsecurity.com/enterprise/security-info/column/view/1150
[86] 보안뉴스, 2018년 랜섬웨어 피해, 1조 500억원 규모 이를 듯
https://www.boannews.com/media/view.asp?idx=74441
[87] 보안뉴스, 입사지원서 사칭한 갠드크랩 랜섬웨어 또 등장, 이메일로 유포중!
https://www.boannews.com/media/view.asp?idx=74699
[88] 보안뉴스, 전 세계 기업 타깃 랜섬웨어로 글로벌 업체들 피해 속출, Norsk, Hydro 등등
https://www.boannews.com/media/view.asp?idx=78088
[89] 한국인터넷진흥원(KISA) 19년 1분기 랜섬웨어 동향 보고서
https://seed.kisa.or.kr/kisa/Board/54/detailView.do
[90] 한국인터넷진흥원(KISA) 19년 2분기 랜섬웨어 동향 보고서
https://seed.kisa.or.kr/kisa/Board/61/detailView.do
[91] 한국인터넷진흥원(KISA) 19년 3분기 랜섬웨어 동향 보고서
https://seed.kisa.or.kr/kisa/Board/66/detailView.do
[92] 한국인터넷진흥원(KISA) 19년 4분기 랜섬웨어 동향 보고서
https://seed.kisa.or.kr/kisa/Board/78/detailView.do
[93] ASEC 2019년 상반기 랜섬웨어 동향
https://asec.ahnlab.com/ko/1241
[94] 보안뉴스 2020년의 가장 큰 사이버 위협은 압도적으로 랜섬웨어
https://www.boannews.com/media/view.asp?idx=91741
[95] 보안뉴스 2020년 1분기 최악의 신규 랜섬웨어 5종 꼽아보니... ‘코로나’ 키워드 악용
https://www.boannews.com/media/view.asp?idx=89122
[96] 보안뉴스 메이즈 랜섬웨어의 은퇴 기념 트롤링? 자체 웹 사이트에 유출자료 공개
https://www.boannews.com/media/view.asp?idx=92570
[97] 아이티월드 2020 랜섬웨어 현황과 방어 전략 “지능화되고 표적화된 공격으로

피해 비용 증가”
https://www.itworld.co.kr/news/143876
[98] Betanews 2020년 랜섬웨어의 영향과 피해금액
https://betanews.com/2020/10/09/ransomware-in-2020/
[99] ‘갱단’으로 커진 랜섬웨어 악당
https://www.chosun.com/economy/tech_it/2021/05/15/QE7WH67DBVEIVNQ5TQ6EO3QJOM/
[100] 전세계서 2초마다 랜섬웨어 공격・・・ “올해 상반기 피해액 24조원”
https://www.vanchosun.com/news/main/frame.php?main=1&boardId=17&bdId=73728
[101] 보안뉴스 콜로니얼 파이프라인 랜섬웨어 사건, 파이프라인 OT 취약성 드러내
https://www.boannews.com/media/view.asp?idx=97355
[102] Cloudwards 랜섬웨어 통계, 동향 및 2022 이후 전망
https://www.cloudwards.net/ransomware-statistics/