KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2021 KISA REPORT

volume 08

www.kisa.or.kr

CONTENTS

ISSUE I. 디지털

ISSUE II. 정보보호

ISSUE III. 개인정보보호

주제 제안 및 정기 메일 신청 | kisareport@kisa.or.kr

인터넷 정보보호 관련 이슈, 현안 등 궁금한 내용을 보내주시면 선별 후 보고서 주제로 선정됩니다.

또한, KISA Report 온라인 서비스 제공을 원하실 경우 신청해주시면 매월 받아보실 수 있습니다.

랜섬웨어 실태와 수사역량 제고방안

김기범 (freekgb02@gmail.com)

성균관대학교 과학수사학과(디지털포렌식), 부교수

새로운 사이버위협, 랜섬웨어의 등장

랜섬웨어는 일반적으로 컴퓨터의 데이터를 암호화한 후에 복호화를 미끼로 가상자산을 요구하는 악성 프로그램을 의미한다.[1] 1989년 컴퓨터의 부팅횟수가 90회에 도달하면 디스크를 암호화하고, 복호화를 위해서는 189불을 송금하라고 설계된 AIDS 트로이잔(AIDS trojan)이 초기의 형태로 알려져 있다.[2] 2008년 사토시 나카모토(Satoshi Nakamoto)가 비트코인의 개념[3]을 제시한 이래 초국가적 범죄로 진화하였고, 우리나라에서도 2015년 이후 피해가 발생하기 시작하였다. 한국인터넷진흥원에서 발표한 랜섬웨어 신고건수는 2018년 22건, 2019년 39건에서 2020년 127건, 2021년 7월 97건으로 꾸준히 증가하고 있다.[4] 개인이나 기업이 신고하지 않은 사건까지 포함하면 피해는 훨씬 많을 것이다. 2021년

1) 랜섬웨어의 법률적 개념에 대한 자세한 사항은 양종모, "랜섬웨어 공격에 대한 형사법적 고찰", 홍익법학 20(1), 2019, 35면 참조.
2) Adam. Young, M. Yung, "Cryptovirology: Extortion-Based Security Threats and Countermeasures". IEEEExplorer 1996, p.131.
3) Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", cryptography mailing list(metzdowd.com), 2018.10.31.

국가정보보호백서에 따르면 사업체의 침해사고 피해유형은 랜섬웨어가 59.8%로 가장 높았고, 그 다음으로 악성코드 42.7%, 해킹 6.6%, 디도스공격 4.1%, 애드웨어·스파이웨어 4.0%, 중요정보유출 1.6% 순으로 나타났다.[5)]

랜섬웨어는 초기에 개인 컴퓨터를 공격하였으나 점차 기업을 거쳐 국가의 주요정보통신기반시설을 대상으로 삼고 있다. 다크웹에서 랜섬웨어가 거래되면서 제작 등 전문지식 없이도 범행을 할 수 있게 되었다. 기업에게 가상자산을 송금하지 않으면 디도스공격을 하겠다는 랜섬디도스(Ransom-DDoS)도 등장하였다.[6)] 제작자와 유포자가 일정한 비율로 가상자산의 수익을 분배하면서 급속도로 조직화·지능화되고 있다. 무엇보다 심각한 것은 랜섬웨어 피해자가 범죄조직에게 가상자산을 송금하는 비율이 높아지고 있다는 점이다. 사이버보안 컨설팅사인 CyberEdge GROUP은 전 세계 17개 나라에서 500명 이상이 근무하는 IT 보안기업 종사자 총 1,182명을 조사한 결과, 비용을 지불한 경우가 2018년 38.7%에서 2019년 45.1%, 2020년 57.5%까지 증가하고 있다고 발표하였다.[7)] 향후에는 기업의 내부자를 매수하여 시스템에 대한 접근 권한을 부여받아 랜섬웨어를 감염시키는 범죄도 가능하고, 범죄조직과 결탁한 자작극도 충분히 상상할 수 있을 것이다. 이처럼 랜섬웨어는 개인과 기업을 넘어 국가안보에 새로운 사이버위협이 되고 있다.

한·미 랜섬웨어 수사사례 분석

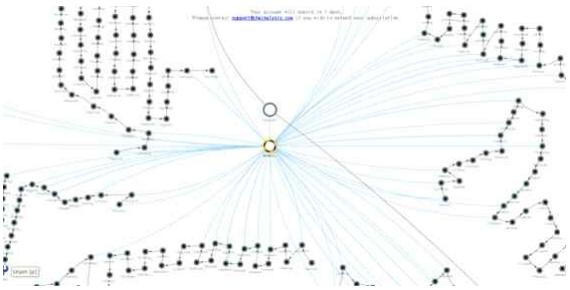
우리나라

2017년 웹호스팅 업체 나야나(Nayana)는 에레버스(Erebus) 랜섬웨어 공격으로 서버 153대가 감염되었고, 이때 범죄조직에게 13억 상당의 비트코인(412.4BTC)을 지불[8)]하여 125대 이상을 복구하였다.[9)] 당시 범죄자는 나야나 홈페이지의 취약점을 이용하여 서버에 침입한 후에 랜섬웨어 공격을 하였다. 경찰청에서 네트워크를 추적하고, 가상자산을 분석하여 유력한 용의자를 특정하였으나 특정국가에서 형사사법공조요청에 미온적으로 대응하여 검거하지 못하고 있다.

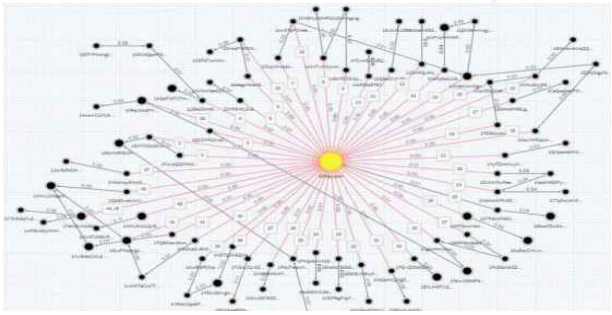
2019년 2월에는 이메일을 이용하여 경찰관서 등의 '출석통지서'로 위장한 갠드크랩(GandCrab) 랜섬웨어가 유포되고, 감염될 경우 복호화를 위해 1,300불을 송금하도록 한 사건이 발생하였다. 경찰청은 약 2년간 10개국과 국제공조 수사를 진행하고, 약 3천만 건의 가상통화 거래내역과 2만 7천 개의 통신

4) 파이낸셜뉴스(2021.6.14.), "'데이터 인질극' 랜섬웨어 '기승' ...표적형 공격 등 진화"(2021.8.14. 최종확인); 과학기술부 보도자료(2021.8.5.), "금품 요구 악성프로그램(랜섬웨어) 대응 역량 결집, 안전한 디지털 전환과 뉴딜지원".
5) 국가정보원등, "2021 국가정보보호백서", 2021, 249면.
6) 한국인터넷진흥원 홈페이지(2021.1.26.), "2021년 사이버 위협 전망"(2021.8.13. 최종확인).
7) CyberEdge GROUP, "2020 Cyberthreat Defense Report", 2020, p.15.
8) 당시 인터넷에서는 회사 측이 범죄조직에게 가상자산을 송금한 사안에 대해 고객의 피해 회복을 위해 불가피하다는 의견과 지불하면 더 많은 공격을 할 수 있다는 반대 의견이 대립하기도 하였다.
9) NAYANA 홈페이지(http://www.nayana.com) 제5차 공지(2017.6.14.), 제14차 공지사항(2017.6.29.) 사항 참고(2021.8.27. 최종확인).

기록을 분석한 끝에 유포자를 검거하였다.[10] 2020년에는 이랜드그룹은 클롭(Clop) 랜섬웨어[11]의 공격을 받아 오프라인 점포 23곳의 영업을 중단하였고, 복호화를 위해서는 444억원 상당의 가상자산을 송금하라는 협박을 받았다. 범죄조직은 스피어피싱, MS의 AD 서버의 취약점을 이용하여 랜섬웨어를 유포하였다. 이랜드그룹은 시스템 암호화에 대한 피해를 감수하기로 하고, 범죄조직에게 가상자산을 송금하지 않기로 결정하였다.[12] 경찰청은 우크라이나, 미국(FBI)과 국제공조수사를 실시하였고, 형사사법공조 절차를 통해 우크라이나에 소재한 가상자산 관리책을 검거하고, 이를 바탕으로 제작·유포한 상선을 추적하고 있다.



[그림 1] 나야나 사건 가상자산 추적(경찰청, 2017)



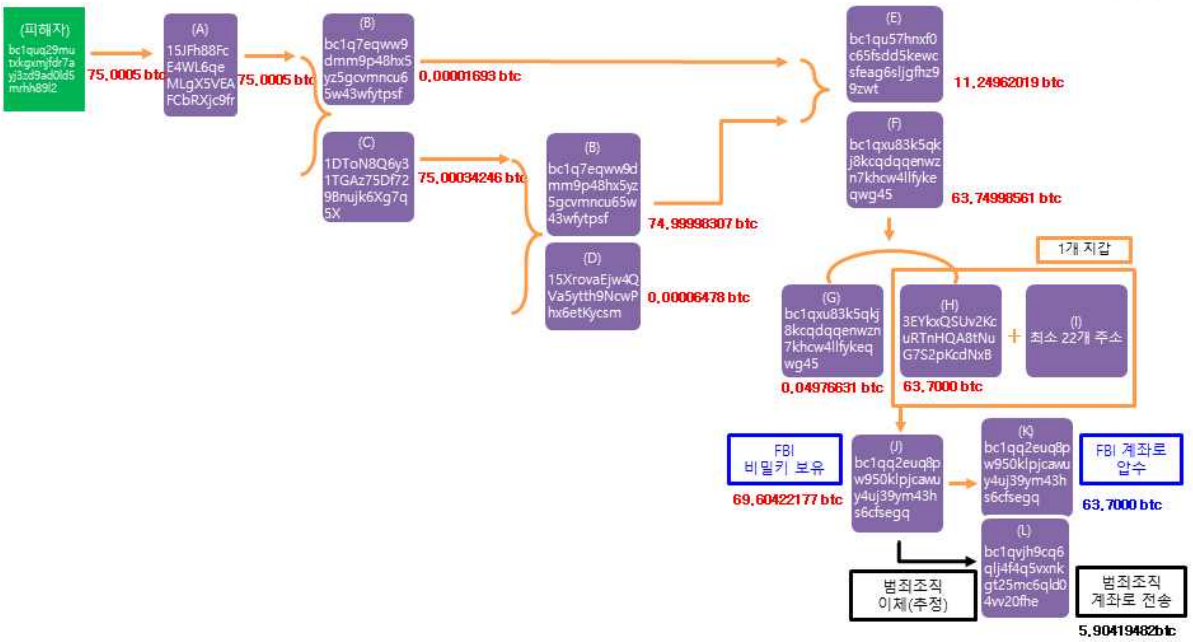
[그림 2] 갠드그랩 랜섬웨어 가상자산 추적(경찰청, 2021)

미국

연방수사국(FBI) 크리스토퍼 레이(Christopher Wray)는 2021년 현재 100가지 유형의 랜섬웨어를 수사하고 있고, 사이버공격의 위협이 2001년 9.11 테러 수준이라고 경고했다.[13] 2021년 5월 'JBS SA'는 자회사가 공격을 받아 생산시설 일부가 3일간 중단되자, 복호화 키를 받기 위해 범죄조직에게 1,100만 달러 상당의 비트코인을 지불하였다.[14] 무엇보다도 2021년 5월 6일 송유관 운영사인 콜로니얼 파이프라인(Colonial Pipeline)이 랜섬웨어 공격을 받아 5월 7일부터 5월 12일까지 6일간 송유관을 운영하지 못해 휘발유 가격이 급증하는 혼란을 야기하였다.[15] 콜로니얼 파이프라인(Colonial Pipeline)은 사건 발생 다음날 연방수사국(FBI)에 신고하였고, 범죄조직에게 75BTC를 지불하였다.[16] 조 바이든 대통령은 5월 9일 비상사태를 선포하였고, 연방수사국(FBI)는 5월 10일 범죄조직으로 다크사이드(Darkside)를 지목하였다. 이후 콜로니얼 파이프라인은 5월 12일 송유관 시스템을 재가동하였고, 연방수사국(FBI)은 6월

10) 경찰청 보도자료(2021.3.9.), "랜섬웨어 '갠드그랩' 유포자 검거, 구속".
11) 자세한 내용은 이영주, "랜섬웨어 암호기능 및 복구 가능성 분석", 정보보호학회지 30(3), 2020, 47~48면.
12) 한겨레(2020.11.27.), "이랜드 부회장 "랜섬웨어 해커 계속 협박…굴복 않겠다"(2021.8.27. 최종확인).
13) THE WALL STREET JOURNAL(2021.6.4.), "FBI Director Compares Ransomware Challenge to 9/11", (2021.8.27. 최종확인).
14) THE WALL STREET JOURNAL(2021.6.9.), "JBS Paid $11 Million to Resolve Ransomware Attack"(2021.8.27. 최종확인).
15) Bloomberg(2021.6.5.), "Hackers Breached Colonial Pipeline Using Compromised Password" (2021.8.27. 최종확인).
16) United States DEPARTMENT of JUSTICE(June 7, 2021), "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside"(2021.8.13. 최종확인).

7일 캘리포니아 북부 연방지방법원(US District Court for the Northern District of California)에서 압수·수색영장을 발부받아 63.7BTC(약 230만 달러)를 회수하였다.[17] 연방수사국(FBI)의 가상자산 압수 과정을 살펴보면 범죄조직이 자금세탁에 사용하는 지갑주소의 비밀키(Private Key)를 확보한 것으로 보인다. 하지만 비밀키를 어떻게 확보하였는지에 대해서는 공개하고 있지 않다.[18] 피해자가 전송한 약 75BTC는 63.74998561BTC와 11.24962019BTC로 나뉘어졌는데, 여기에서 11.24962019BTC는 전체의 15%에 해당하는 금액으로 공범과 사전 계약에 따라 송금된 것으로 보인다. 마지막으로 연방수사국(FBI)이 비밀키(Private Key)를 보유하고 있던 지갑주소에 약 69.6BTC가 있었지만 범죄와 관련된 63.7BTC만 압수한 것으로 보인다. 그리고 연방수사국(FBI)이 압수한 직후 나머지 잔액이 제3의 지갑 주소로 전액 송금된 것으로 보아 범죄조직은 압수를 미처 예상하지 못한 것으로 해석된다.



[그림 3] 콜로니얼 파이프라인 가상자산 자금세탁 (출처: FBI Affidavit와 인터넷자료 활용)

정부의 종합대책과 아쉬운 지점

정부는 랜섬웨어의 피해가 심각하다고 판단하고, 2021년 과학기술정보통신부, 국가정보원, 기획재정부, 외교부, 국방부, 산업통상자원부, 보건복지부, 중소벤처기업부, 금융위원회, 경찰청 등 10개 부처가 참여하여 "랜섬웨어 대응 강화방안"을 마련하였다.[19] 강화방안은 크게 1) 국가중요시설-기업-국민 수요

17) United States DEPARTMENT of JUSTICE(June 7, 2021), "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside"(2021.8.13. 최종확인).
18) FBI Affidavit(2021.6.7.), Case3-21-mj-70945-LB, https://www.justice.gov/opa/press-release/file/1402056 /download (2021.8.27. 최종확인)
19) 이하의 내용은 관계부처 합동(2021.8.5.), "랜섬웨어 대응 강화방안"(비상경제 중앙대책본부 21-42-5)과 과학기술정보통신부

자별 선제적 예방 지원, 2) 정보공유·피해지원·수사 등 사고대응 전주기 지원, 3) 진화하는 금품요구 악성프로그램에 대한 핵심 대응 역량 제고 등 3가지로 구성되어 있다. 1) 수요자별 예방지원은 주요정보통신기반시설에 대하여 정유사(공정제어시스템), 자율주행 관제시스템 등을 추가하는 방안과 랜섬웨어 예방을 위해 '백업 시스템 구축'하는 사업을 포함하고 있다. 중소기업에게 데이터 이중화를 지원하는 클라우드 기반의 '데이터금고' 지원 사업도 추진한다. 2) 사고대응 전주기 지원은 공공·민간의 사이버위협 정보공유시스템과 의료·금융 등 분야별 정보공유분석센터(ISAC)를 연동하고, 주요국의 인터넷 보안기관(CERT)과 사이버보안 협의체를 통해 국가 간 랜섬웨어에 대한 정보공유를 강화하는 방안을 포함하고 있다. 다크웹 모니터링으로 해킹조직에 대한 감시를 강화하고, 경찰청·시도청의 사이버테러수사대(팀)에 랜섬웨어 전담 수사체계를 구축한다. 인터폴 회원국들과 해킹조직 분석 및 범죄자 공동검거를 강화하고 유로폴과의 실무협약도 추진한다. 마지막으로 3) 랜섬웨어 핵심 대응역량 제고는 랜섬웨어 탐지·차단 기술과 복구 기술 개발에 투자를 확대하고, 해킹조직 근원지 및 가상자산 흐름 추적 기술 등을 개발하는 방안을 포함하고 있다. 정부의 종합대책은 2018년 청와대 국가안보실에서 수립한 국가사이버안보전략과 이행전략 하에 랜섬웨어에 대한 보다 구체적인 대책을 수립한 것으로 보인다.

하지만, 랜섬웨어 범죄조직을 추적하기 위한 수사정책은 다소 부족해 보인다. 강화대책에서 3대 전략 18개 과제를 제시하고 있는데 수사정책은 "랜섬웨어 해킹조직 수사역량 강화", "근원지 추적기술 개발 강화" 등 2개뿐이다. 시스템에 대한 침해사고 예방정책만으로는 랜섬웨어를 근절할 수 없다. 범죄조직은 검거되지 않으면 범행을 계속하게 되고, 피해가 보안이 취약한 다른 시스템으로 전이될 뿐이다. 따라서 예방정책에 수사정책을 포함하지 않을 경우 국제화·지능화·조직화되고 있는 랜섬웨어에 대응하는데 한계가 있을 것이다.

랜섬웨어 수사역량 제고를 위한 제언

과거에는 랜섬웨어를 검거한 사례가 많지 않았지만, 최근에는 우리나라를 비롯하여 일부 국가에서 성과를 내고 있어 수사역량을 강화하는 정책이 중요해지고 있다.

이를 위해 먼저 모든 피해가 신고되고 분석되어 추적할 수 있는 여건이 마련되어야 한다. 개인과 기업이 피해를 당할 경우 신고하도록 인식을 개선해야 한다. 피해복구 조치로 끝내고 수사로 연결되지 않으면 근절할 수 없다. 특히, 주요정보통신기반시설의 경우에는 반드시 수사기관에 신고 되어야 한다. 랜섬웨어에 대한 신고보상금도 수 억 원대로 확대하여 시민들의 적극적인 신고를 유도해야 한다.[20] 미국 연방수사국(FBI)은 랜섬웨어 용의자를 검거하거나 가상자산을 더 쉽게 추적 또는 차단할 수 있는 정보를 제공한 자에 대해서 1천만 달러의 신고보상금을 지급하겠다고 발표하였다.[21] 나아가 과학기술정보통신

보도자료(2021.8.5.), "금품 요구 악성프로그램(랜섬웨어) 대응 역량 결집, 안전한 디지털전환과 뉴딜지원"을 요약한 것임.

20) 미국 FBI는 2012년 12개 국가에 'Cryptolocker'와 'CTB-Locker' 등의 악성코드를 배포하여 약 1억달러 가량의 피해를 입힌 러시아 해커 Evgeniy Mikhailovich Bogachev를 은행사기, 컴퓨터사기, 돈세탁 등의 혐의로 지명수배하고 현상금을 300만 달러를 걸었다.

부(한국인터넷진흥원)와 경찰청은 랜섬웨어에 대한 정보를 공유하고, 프로파일링 시스템을 구축하여 분석과 추적역량을 확충해 나가야 한다.

둘째, 추적기술에 대한 지속적인 연구가 필요하다. 정보보호 분야는 다양한 연구가 이루어지고 있지만, 다크웹·가상자산·네트워크 추적 등 수사에 필요한 기술에 대한 연구는 부족하다. 추적기술을 전담으로 연구하는 대학·연구소를 지정하고, 인텔리전스 기업을 육성하여야 한다. 경찰청에서 클롭(Clop) 랜섬웨어를 검거할 때, 범죄조직인 TA-505에 대해서 1년 이상 지속적으로 정보를 수집하고 분석해 온 금융보안원의 사이버위협 인텔리전스 보고서가 많은 도움이 되었다.[22)]

셋째, 국제공조 수사역량을 대폭 확충해야 한다. INTERPOL, UNODC, ICANN, FATF 등 다양한 국제기구에 진출하여 국제공조 수사를 위한 네트워크를 개척해야 한다. 유로폴(EUROPOL)에도 수사관을 파견하여 정보공유, 공동수사 등을 통해 협력 네트워크를 확충해야 한다. 국내·외 금융·통신사, 정보보안업체, 가상자산 분석 업체, 암호화폐 거래소, 도메인등록 업체와도 협력체계를 구축해야 한다.

넷째, 중단 없는 수사체계를 구축해야 한다. 살인사건 등 강력범죄보다 해킹·디도스·랜섬웨어에 대한 미제사건 수사와 관리체계가 부족하다. 랜섬웨어에 대한 범죄정보를 지속적으로 수집·분석하여 용의자를 식별해 나가는 노력을 계속해야 한다.

다섯째, 가상자산 사업자는 랜섬웨어 자금세탁에 대한 모니터링을 강화해야 한다. 우리나라뿐만 아니라 바이낸스, 후오비 등 전 세계적인 가상자산 사업자들의 적극적인 협조가 필요하다.

여섯째, 실체법·절차법 등 입법적 뒷받침도 필요하다. 정보통신망법상 악성프로그램 전달·유포죄에 제작까지 포함하여 랜섬웨어 개발행위를 처벌하고, 영리를 목적으로 악성프로그램을 유포하는 행위에 대해서는 가중처벌이 필요하다.[23)]

나아가 랜섬웨어 추적수사를 위해 전기통신감청도 허용할 필요가 있다. 이를 통해 정부가 랜섬웨어로 인한 개인과 기업 그리고 국가의 안보를 확실하게 지키고, 국제사회에서 랜섬웨어 대응을 리딩하는 선도국으로서 위상을 확립하기를 기대한다.

---

21) New York Times(2021.7.15.), "Biden makes a new push in fight against ransomware, including a $10 million reward" (2021.8.16. 최종확인).
22) 금융감독원, "TA505 위협 그룹 프로파일링", 2020, 1~126면.
23) 최호진, "정보통신망법의 악성프로그램에 대한 형법정책", 형사정책 32(2), 2020.7, 91면; 양종모, "랜섬웨어 공격에 대한 형사법적 고찰", 홍익법학 20(1), 2019, 41~50면.

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

발 행 일	2021년 9월
발 행 처	한국인터넷진흥원 (전라남도 나주시 진흥길 9)
기 획	한국인터넷진흥원 미래정책연구실 정책분석팀
편 집	㈜ 해리