정 보 보 호 학 회 지
제 32 권 제3호, 2022. 6

최신 랜섬웨어 동향 및 발전 방향

문 기 운*, 이 종 혁*

요 약

전 세계적으로 다양한 피해를 입히고 있는 랜섬웨어는 사이버 공간에서 가장 위협적인 공격으로 인식되고 있다. 최근 랜섬웨어는 단순히 데이터를 암호화하는 것 뿐만 아니라 데이터 유출, DDoS 공격을 수행하는 등 고도화 되고 있다. 최근 랜섬웨어 공격 조직들은 서비스형 랜섬웨어를 제작/판매하고 있으며, 그에 따라 전문 지식이 없는 악의적인 사용자들도 랜섬웨어 공격이 가능한 실정이다. 본 논문은 지능화 되고 있는 랜섬웨어의 최신 동향을 분석하고 세대별 발전 방향을 살펴본다.

Ⅰ. 서 론

기존 악성코드 제작자들은 악성코드를 통하여 특정 사용자의 개인정보 및 민감 정보를 탈취해, 이를 통한 판매 및 협상 등을 통해 수익을 얻었다. 하지만 특정 사용자/단체/기관을 목표로 하는 공격은 금전적 보상을 달성하기 위한 높은 공격 비용 대비 그 수익률은 높지 않았다. IT 기술의 발전으로 거래 추적이 어려운 가상화폐가 등장하였고, 그 가치는 폭등하였다. 가상화폐의 등장으로 악성코드 제작자들은 랜섬웨어 개발로 탈바꿈하고 탈취한 데이터 및 정보 자체를 볼모로 삼아 가상화폐 등을 통한 금전적 요구를 하고 있다. 데이터와 정보의 복구를 위하여 사용자들은 비싼 값의 가상화폐를 지불하게 되고 공격자들은 쉽게 고수익을 얻는다. 최근 랜섬웨어들은 공격 기법이 더욱더 다양해지고 교묘하며 공격 횟수 또한 기하급수적으로 증가하고 있다. 본 논문에서는 갈수록 발전하고 있는 랜섬웨어에 대한 최신 동향을 분석하고 세대별 발전 방향을 살펴보고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 랜섬웨어의 피해 현황 및 주요 피해 사례를 살펴본다. 3장에서는 랜섬웨어들을 세대별로 분류하여 발전 현황을 분석하고 4장에서 본 논문의 결론을 맺는다.

Ⅱ. 랜섬웨어 최신 동향

2.1. 랜섬웨어 개요

랜섬웨어는 몸값(Ransom)을 의미하는 단어와 소프트웨어(Software)의 합성어이다. 랜섬웨어는 피해자의 시스템이나 데이터 및 정보들을 인질로 삼아 피해자들에게 금전적인 요구를 하는 악성 소프트웨어이다. 랜섬웨어 피해의 증가 요인은 비트코인과 같은 가상화폐의 등장을 꼽을 수 있다. 가상화폐는 익명성을 보장하며, 공격자의 계좌 추적이 어렵기 때문에 랜섬웨어 공격자들은 몸값의 대가로 가상화폐를 요구하고 있다. 가상화폐의 가치는 천문학적으로 높아지고 있으며, 공격자들은 제작 시간 대비 고수익을 얻을 수 있다. 또한 서비스형 랜섬웨어(RaaS, Ransomware as a Service)의 등장으로 랜섬웨어 공격의 진입 장벽이 낮아졌다. 전문 지식이 없는 사람도 만들어진 랜섬웨어를 구매하여 쉽게 공격을 수행할 수 있다. 그 결과 수많은 변종 랜섬웨어가 등장하고 있으며, 공격 사례는 지속적으로 증가하고 있다.

2.2. 랜섬웨어 피해 현황

최근의 랜섬웨어 공격자들은 큰 수익을 얻기 위하여 규모가 큰 기업을 대상으로 공격을 수행하고 있다. 피해

본 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2022-0-00796, 상시적 보안품질 보장을 위한 6G 자율보안 내재화 기반기술 연구).
* 세종대학교 정보보호학과 & 지능형드론 융합전공 (대학원생, kiwoon@pel.sejong.ac.kr, 부교수, jonghyouk@sejong.ac.kr)

〔표 1〕 글로벌 랜섬웨어 피해금액

년도	2015	2017	2019	2021	2031
피해 금액	$ 3억	$50억	$115억	$200억	$2,650억

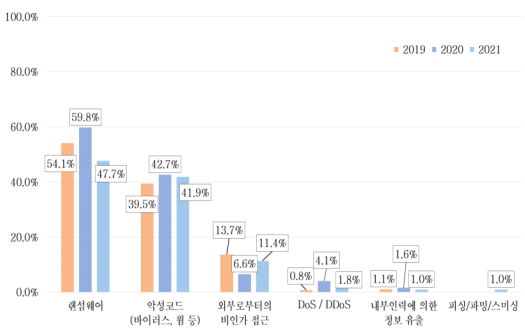
를 입은 기업들은 이미지 실추 문제, 벌금 및 과태료에 이르기까지 많은 리스크들을 고려해야 한다. 그 결과 공격자들은 보상 가능성이 높은 기업을 공격 대상으로 삼고 있다. 다음 [표 1]은 글로벌 랜섬웨어 피해 금액을 나타낸다.

Cybersecurity Ventures의 보고서에 따르면 랜섬웨어로 인한 피해액은 2015년 약 $3억 에서 2017년 $50억으로 약 15배 증가하였다고 분석하였다. 이후 폭발적으로 증가하여 2031년까지 $2,650억 이상의 규모로 증가할 것으로 예상하였다[1].

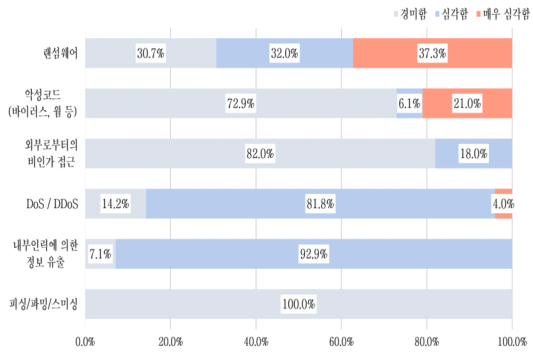
과학기술정보통신부가 발표한 '2021년 정보보호실태조사' 에 따르면 2020년 1년 동안 국내 사업체의 약 1%는 해킹 및 악성코드, DDoS, 랜섬웨어 등의 침해사고를 경험한 것으로 나타났다. 침해사고는 2021년에 랜섬웨어(47.7%), 악성코드(41.9%), 외부로부터의 비인가 접근(11.4%), DoS/DDoS 공격(1.8%) 순으로 집계되었다[2]. 다음 [그림 1]는 국내 기업의 침해사고 경험 유형을 나타낸다.

국내 기업의 경험한 침해사고의 심각성 정도는 랜섬웨어(37.3%), 악성코드(21.0%), DoS/DDoS 공격(4.0%) 순으로 '매우 심각'한 정도로 집계되었다[2]. 다음 [그림 2]는 국내 기업들이 겪은 침해사고 유형의 심각도를 나타낸다. 2019년 집계된 이후로 랜섬웨어는 국내 기업들에게 가장 위협적인 공격으로 나타났다.

금전을 목적으로 공격을 수행하는 랜섬웨어의 급증



〔그림 1〕 국내 기업의 침해사고 경험 유형



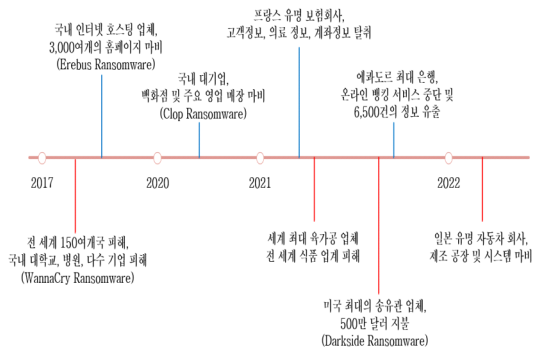
〔그림 2〕 침해사고 유형의 심각도

으로 국내 기업에서는 랜섬웨어를 가장 위협적인 침해사고로 인식하고 있음을 알 수 있다.

2.3. 주요 피해 사례

랜섬웨어의 공격이 증가함에 따라 산업 및 의료체계의 마비, 정보의 유출 등 큰 피해를 받고 있다. 최근 몇 년간 발생한 주요 랜섬웨어 피해 사례들을 소개한다. 다음 [그림 3]은 최근에 발생한 랜섬웨어 피해 사례의 타임라인을 나타낸다.

2017년 전 세계 150여개국에서 워너크라이(WannaCry) 랜섬웨어에 공격을 받았다. 국내에서도 대학교 및 대형병원, 다수의 기업들이 공격당하였다고 알려졌다. 해당 랜섬웨어는 SMB 서비스 취약점을 이용하여 공격을 수행하였다. 한국인터넷진흥원(KISA)에 따르면 감염된 피해 시스템들은 모두 SMB(포트번호 445) 서비스를 실행하고 있었고, 보안 업데이트를 수



〔그림 3〕 주요 랜섬웨어 피해 사례

행하지 않았다[3].

2017년 국내의 웹호스팅 업체가 Erebus 랜섬웨어에 공격당하였다. 이 인터넷호스팅 업체에서 관리하는 153대의 Linux 서버를 대상으로 공격을 수행하였으며 그 결과 약 3,000여개의 홈페이지가 마비되는 사태가 발생하였다. 이 업체에서는 복호화 키를 전달받기 위하여 약 13억원에 해당하는 금액을 지불하였다. 이후 공격자에게 복호화 키를 전달받았지만, 피해받은 데이터들을 완벽하게 복구하지 못하였다[4].

2020년 국내의 대기업이 클롭(Clop) 랜섬웨어에 공격을 받았다. 랜섬웨어 감염된 시스템은 일부 매장의 포스(POS) 단말기 등과 연동되어, 백화점 등 약 20여 곳의 매장이 영업을 중단하였다. 그룹의 사내 네트워크에서 랜섬웨어 감염이 발생되었으며 전산 복구 작업에만 수 주일의 시간이 필요하였다. 공격을 수행한 해킹 그룹은 약 200만 건의 카드 정보를 획득하였다고 주장하였으며, 약 4천만 달러의 금액을 요구하였다[5].

2021년 랜섬웨어의 공격을 받아 미국 최대의 송유관 운영업체가 마비상태에 이르렀다. Darkside 라는 해킹 그룹이 공격한 것으로 알려져 있으며, 해당 공격으로 송유관 약 8,850㎞ 구간 폐쇄되었다. 그 결과 미국 동부 지역 석유 공급 약 45%를 담당하는 업체의 마비로 인하여 석유값이 폭등하기도 하였다[6]. 이 업체는 복구를 위하여 약 500만달러의 금액이 지불하기도 하였고, 미국은 비상사태를 선포하며 이번 사건을 유례없는 일로 규정하였다[7].

2021년 미국의 세계 최대의 육류 가공 업체가 랜섬웨어에 공격받았다. 이 기업은 호주와 미국, 캐나다와 브라질에 생산 시설을 두고 있는 대기업으로서 식품 업계 전체에 큰 피해가 예상되었다[8].

2021년 프랑스 보험사의 아시아 지사(태국, 말레이시아, 홍콩, 필리핀 지역 등)들이 랜섬웨어로부터 공격을 받았다. Avaddon 이라는 해킹 그룹은 자신들이 공격을 수행하였으며 3TB의 데이터를 갈취하였다고 밝혔다. 탈취된 정보들은 고객들의 개인정보, 의료 정보, 은행 계좌 등이 포함된 것으로 알려졌다[9].

2021년 에콰도르의 최대 은행이 랜섬웨어에 공격을 받아 온라인 뱅킹, 모바일 앱, ATM 네트워크 등의 서비스가 중단되었다. 공격을 수행한 해킹 그룹 HotarusCorp은 탈취한 약 6,500 여개의 정보를 공개하였다. 공개된 정보에는 고객들의 개인정보, 비밀번호, 금융정보 등이 포함되었다[10].

2022년 일본의 유명 자동차 회사의 부품 제조사가 랜섬웨어 공격을 받아 설계 도면, 발주 서류 등 약 15만 건의 정보가 유출된 것으로 파악되고 있다. 공격을 수행한 해킹 그룹은 '기밀 데이터를 탈취하였으며, 정보들을 공개하겠다.'고 협박하였다. 또한 비슷한 시기에 주요 부품 거래처도 공격을 받았다. 그 결과 부품 공급 데이터 시스템이 마비되었고, 일본 내의 전 공장이 멈춰서는 피해를 입었다[11].

Ⅲ. 랜섬웨어의 세대별 특징

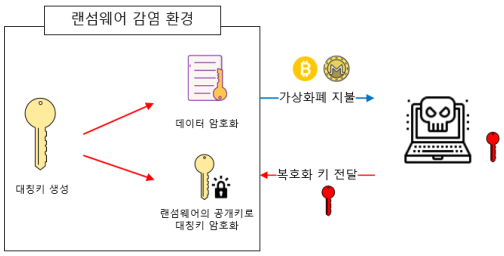
앞서 살펴본 바와 같이 랜섬웨어의 피해 규모는 급격하게 증가하고 있으며, 랜섬웨어는 계속적으로 진화하고 있다. 본 절에서는 랜섬웨어를 세대별로 나누어 살펴본다.

3.1. 랜섬웨어의 등장 - 1세대

1989년 등장한 PC Cyborg Trojan(AIDS Trojan)은 Virus Bulletin[1]의 헤드라인을 장식하였으며, 악성코드의 디지털 갈취(Digital Extortion) 개념을 세상에 처음 알리게 되었다. 최초의 랜섬웨어 PC Cyborg Trojan은 우편으로 송부된 디스켓의 랜섬웨어가 실행되면 PC의 루트 디렉터리를 암호화하였으며, 복호화의 대가로 약 $189~$378를 요구하였다[12]. 당시의 배포 방식의 한계와 제한된 공격 대상 수로 인하여 큰 피해를 입히지 않았지만 많은 사람들의 이목을 집중시키게 되었다.

1세대 랜섬웨어는 락커(Locker) 계열과 크립토(Crypto) 계열로 나눌 수 있다. 락커 계열 랜섬웨어는 단순하게 로그인이나 장치에 대한 접근을 차단하여 사용자에게 잠금 해제에 필요한 코드를 받으려면 금액을 지불하라고 요구한다. 크립토 계열 랜섬웨어는 시스템 상의 데이터 및 정보을 암호화하여 사용자에게 복호화 키를 받으려면 금액을 지불하라고 요구한다. 현재의 랜섬웨어는 크립토계열의 랜섬웨어가 계속적으로 진화하고 있다. 다음 [그림 4]는 1세대 랜섬웨어의 행위를 단순화하여 나타낸 것이다.

1) Virus Bulletin: 세계 3대 보안인증으로 꼽히는 'VB100'을 심사하는 보안 인증기관. 심사 이외에도 글로벌 보안업체들의 연구 결과 및 분석 보고서들을 게재



〔그림 4〕 랜섬웨어 단순 흐름도

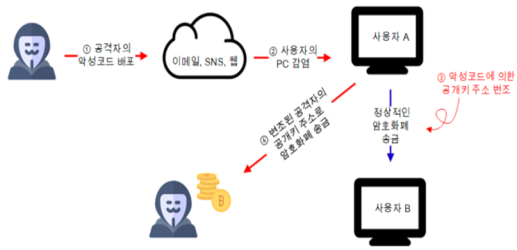
랜섬웨어의 행위를 단순화하여 살펴보면 다음과 같은 과정으로 수행된다. 우선적으로 랜섬웨어에 감염된 환경에서 랜섬웨어가 실행되면 정보 및 데이터 암호화에 사용할 대칭키를 생성한다. 암호화에 사용된 대칭키는 랜섬웨어의 자체에 존재하는 공개키로 암호화되어 은닉된다. 암호화 수행이 완료되면 바탕화면 변조나 랜섬노트를 생성하여 사용자에서 감염 사실을 알린다. 랜섬노트에는 지불해야할 가상화폐 금액과 공격자의 가상화폐 주소가 기록되어 있다. 공격자는 금액이 지불되면 사용자에게 복호화 키를 전달한다.

3.2. 이중 갈취 - 2세대

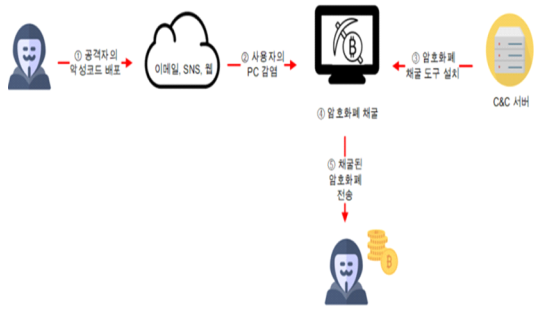
2세대 랜섬웨어는 이중 갈취를 목적으로 공격을 수행하고 있다. 공격자들은 암호화 이전에 데이터를 우선적으로 확보한 후, 공격 대상 환경의 데이터 및 시스템을 암호화한다. 암호화된 시스템을 인지한 사용자들이 요구 금액을 지불하지 않을 때, 공격자는 우선적으로 입수한 사용자의 데이터 및 정보를 다크웹이나 자신들이 운영하는 웹사이트에 공개하기 시작한다. 순차적으로 탈취한 정보를 공개함으로써 금액을 지불하도록 유도한다.

또 다른 랜섬웨어 제작자들은 자신들의 수익을 높이기 위하여 부가적인 공격 방법을 강구하였다. 랜섬웨어 제작과 더불어 크립토재킹 악성코드를 제작하여 배포한다. 크립토재킹 악성코드는 지갑 탈취형, 채굴형 악성코드로 나눌 수 있다. 다음 [그림 5]는 지갑 탈취형 악성코드의 행위 예시를 나타낸다.

KimChenIn과 Cyptoshuffler는 대표적인 지갑 탈취형 악성코드이다. 지갑 탈취형 악성코드는 피해자가 암호 화폐를 송금하기 위하여 수신자의 지갑 주소를 입력할 때, 해당 주소를 공격자 자신의 지갑 주소로 바꿔치기한다. 이때 공격자는 약 1만개의 지갑 주소를 악성코드에 심어 놓았으며, 피해자가 입력하는 송신자의 지갑 주소와 가장 유사한 것을 선택하여 바꿔치기한다. 결과적으로 피해자가 송금하는 암호 화폐는 공격자에게 전달된다[13][14]. 다음 [그림 6]은 채굴형 악성코드의 행위 예시를 나타낸다.



〔그림 5〕 지갑 탈취형 악성코드의 행위 예시



〔그림 6〕 채굴형 악성코드의 행위 예시

채굴형 악성코드로는 대표적으로 Digmine과 KJU와 같은 악성코드들이 존재한다[15][16]. 채굴형 악성코드들은 랜섬웨어에 감염된 사용자의 환경에 가상화폐 채굴 도구를 설치한다. 감염된 환경에서 채굴된 가상화폐를 공격자 자신의 계좌로 전송하여 가상화폐를 획득한다. 공격자는 감염 환경의 컴퓨팅 자원을 사용하여 부가적인 수익을 얻을 수 있다.

3.3. 3중 협박 (RDDoS) - 3세대

앞서 살펴본 2세대 랜섬웨어들은 사용자의 데이터 및 정보를 암호화하고 볼모로 삼아 금전적인 요구를 하였다. 사용자들이 금전을 지불하지 않는다면 사전에 미리 유출한 정보들을 순차적으로 공개하며 협박하기도 하였다. 3세대 랜섬웨어는 3중 협박 형태로 랜섬디도스

(RDDoS) 공격을 수행한다.

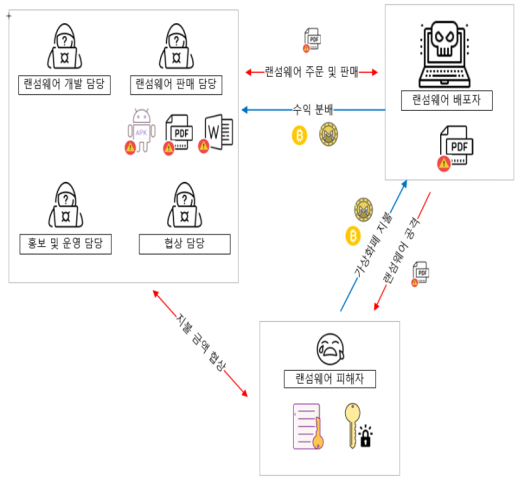
랜섬디도스(RDDoS)는 랜섬웨어 공격과 더불어 디도스(DDoS) 공격을 혼합한 형태를 말하며 특정한 서비스나 전체적인 네트워크를 디도스 공격을 수행하여 중단시키겠다고 협박한다. 디도스 공격을 먼저 수행하고 공격 중단을 위하여 금전을 요구하거나, 디도스 공격 이전에 희생자에게 먼저 연락하여 금전을 요구하는 방식을 사용한다. 보통은 개인보다는 기업을 대상으로 공격을 수행하며, 공격 받은 기업의 이메일이나 보안담당자에게 이메일로 협박을 수행한다. 기업에서 대응하지 않거나 금전을 지불하지 않을 경우에는 실제로 작은 규모의 디도스 공격을 수행하기도 한다.

랜섬디도스 공격은 특정 분야에 국한되지 않고 공기업, 금융기관, 전자상거래 전문 기업과 같이 다수의 고객을 대상으로 서비스하는 기업들을 선정한다. 2020년 6월에는 대형 유럽 은행을 대상으로 809Mpps(Million Packets Per Second)에 달하는 공격이 수행되었으며[17], Armada Collective라는 해킹 그룹이 국내 금융사를 대상으로 공격을 수행하겠다고 협박 메일을 보낸 사례도 존재한다[18].

3.4. 서비스형 랜섬웨어 (RaaS) - 4세대

랜섬웨어 제작자들은 서비스형 랜섬웨어를 제작하여 판매하며 직접 공격을 수행하지 않고도 수익을 거둘 수 있다. 전문 지식이 없는 개인도 랜섬웨어 제작자로부터 배포 키트를 대여하거나 구매하여 랜섬웨어를 이용해 수익을 거둘 수 있다. 서비스형 랜섬웨어 제작자는 랜섬웨어 인프라 제작 및 구축, 지속적인 업데이트 및 지원 등을 제공하는 대가로 구매자에게 수익을 배분받는다. 다음 [그림 7]은 서비스형 랜섬웨어 조직화의 예 나타낸다.

파이어아이는 해킹그룹 다크사이드(DARKSIDE)의 랜섬웨어 운영에 대한 보고서를 발표하였다. 다크사이드는 2020년 8월부터 15개국 이상의 조직과 산업 전반을 대상으로 공격을 진행하였으며 희생자들의 데이터를 사전에 탈취한 뒤 랜섬웨어 공격을 수행한다. 유출된 데이터 및 정보를 블로그에 공개하겠다고 협박하는 등 희생자들이 금전을 지불하도록 만든다. 이러한 2중 협박과 더불어 서비스형 랜섬웨어를 제작하여 판매한다[19].



〔그림 7〕 서비스형 랜섬웨어의 조직화의 예

서비스형 랜섬웨어는 랜섬웨어를 제작하여 판매하는 조직과 실제로 랜섬웨어를 배포하는 배포자가 수익을 분배한다. 원활한 협상이 필요하다면 조직의 협상 전문가가 협상을 진행하기도 한다. 2020년 11월부터 RaaS 랜섬웨어 구매자를 모집하는 광고를 자신들의 블로그에 게시하였다. 광고 내용에 따르면, 구매자가 공격을 수행하여 50만 달러 미만의 랜섬웨어 몸값을 받는 데 성공할 경우에 수익의 25%를 랜섬웨어 제작자에게 분배하여야 한다. 또한 수익이 500만 달러가 넘는 경우에는 10%의 수익을 분배한다는 계약 조건이 명시되어 있었다. 이러한 명시된 조건에 해당하지 않는 작은 금액이라도 수익은 분배하고 있으며, 박리다매 형식으로 광범위하게 공격을 수행하여 큰 수익을 거둘 수 있다[18].

Ⅳ. 결 론

본 논문에서는 랜섬웨어의 최신 동향을 파악하기 위하여 피해 현황 및 주요 피해 사례들을 살펴보았다. 랜섬웨어의 피해는 계속적으로 증가하고 있으며, 국내의 기업들은 랜섬웨어를 가장 위협적인 침해사고로 인식하고 있는 실정이다. 단순히 데이터를 볼모로 금전을 요구하는 방식에서 데이터 유출, DDoS 공격에 이르기까지 3중으로 협박하며 공격을 수행한다. 최근의 랜섬웨어들은 불특정 다수를 대상으로 공격을 수행하던 방식과 다르게 특정 기업이나 기관을 노린 표적형 랜섬웨어 공격이 많아지고 있다. 세계의 최대 석유 공급 업체나 육가

공 업체가 랜섬웨어의 공격을 받는 사례를 통하여 제조 및 공급망을 대상으로 공격을 수행하는 사례가 늘어나고 있음을 알 수 있다. 또한 조직화된 해킹 그룹들이 서비스형 랜섬웨어를 제작하여 배포함으로써 공격 횟수와 피해 규모는 날로 늘어날 것이다. 교묘하고 조직적으로 발전하고 있는 랜섬웨어는 기관 및 조직의 규모나 산업의 형태를 가리지 않고 있다. 이러한 위협에 대응하기 위해서는 랜섬웨어에 대한 지속적인 관심을 가지고 피해를 사전 예방하고자 하는 노력이 필요할 것으로 사료된다.

참 고 문 헌

[1] Cybersecurity Ventures, “Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031”, https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/. Accessed on March 2022.

[2] 과학기술정보통신부. “2021 정보보호 실태조사.” 2022.

[3] 보안뉴스, “워너크라이 랜섬웨어 국내 피해현황 집계해보니...21곳 감염 신고”, https://www.boannews.com/media/view.asp?idx=57452&kind=1. Accessed on March 2022.

[4] 한겨레, “랜섬웨어 감염 웹호스팅업체 인터넷나야나, 결국 해커에 굴복”, https://www.hani.co.kr/arti/economy/it/798812.html. Accessed on March 2022.

[5] 세이프타임즈, “[시큐리티] '랜섬웨어 감염' 이랜드 그룹 사태를 보는 시각”, http://www.safetimes.co.kr/news/articleView.html?idxno=90335. Accessed on March 2022.

[6] 연합뉴스. “공격당한 미 송유관업체, 해커들에 57억원 가상화폐로 지급(종합)”, https://www.yna.co.kr/view/AKR20210514005051072. Accessed on March 2022.

[7] CCTVNEWS, “콜로니얼 파이프라인, 랜섬웨어 공격으로 “5800여 명 개인정보 유출”, CCTVNEWS. https://www.cctvnews.co.kr/news/articleView.html?idxno=229908. Accessed on March 2022.

[8] 보안뉴스, “세계 최대 육류 가공 업체인 JBS, 사이버 공격으로 마비돼” https://www.boannews.com/media/view.asp?idx=97969. Accessed on March 2022.

[9] CCTVNEWS, “AXA, 랜섬웨어 이어 디도스 공격까지...'국내 기업'도 당했다”, https://www.cctvnews.co.kr/news/articleView.html?idxno=225863. Accessed on March 2022.

[10] 보안뉴스, “에콰도르 최대 은행, 랜섬웨어 공격 피해 이후 여전히 서비스 중단.” https://www.boannews.com/media/view.asp?idx=101605&page=10&kind=1. Accessed on March 2022.

[11] “日기업, 랜섬웨어 사이버 공격 피해 잇따라.” 파이낸셜뉴스. https://www.fnnews.com/news/202204071559099396. Accessed on March 2022.

[12] Jim Bates. “Trojan horse: AIDS information introductory diskette version 2.0” Virus Bulletin, 1990.

[13] HAURI Official hompage, “비트코인 지갑 정보를 탈취하는 김정은 악성코드”, https://www.hauri.co.kr/security/issue_view.html?intSeq=277&page=6&article_num=218, Accessed on March 2022.

[14] CoinWire hompage, “Be All Ears: CyptoShuffler Trojan Quietly Alters Wallet Address”, https://www.coinwire.com/be-all-ears-cryptoshuffler-trojan-quietly-alters-wallet-address, Accessed on March 2022.

[15] TrendLabs Security Intelligence Blog, “Digmine Miner Spreading via Facebook Messenger”, https://blog.trendmicro.com/trendlabs-security-intelligence/digmine-cryptocurrency-miner-spreading-via-facebook-messenger/, Accessed on March 2022.

[16] Anlab Official hompage, “가상화폐 채굴 후 김일성대 서버로 이전하는 악성코드 발견”, http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=27098, Accessed on March 2022.

[17] ITDAILY, “유럽 은행 노린 사상 최대 규모 디도스 공격 발생”, http://www.itdaily.kr/news/articleView.html?idxno=101966, Accessed on April 2022.

[18] KrCERT, “해커그룹 'Armada Collective'의 비트코인 요구 협박 및 DDoS 공격 주의”, https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=25964, Accessed on April 2022.
[19] FireEye Mandiant blog, "Shining a Light on DARKSIDE Ransomware Operations",https://www.mandiant.com/resources/shining-a-light-on-darkside-ransomware-operations, Accessed on April 2022.

〈저 자 소 개〉

문 기 운 (Kiwoon Moon)
2016년 2월 : 상명대학교 컴퓨터소프트웨어공학과 졸업
2021년 9월~현재 : 세종대학교 정보보호학과 석사과정
<관심분야> 시스템 보안, 네트워크 보안, 취약점 진단

이 종 혁 (Jong-Hyouk Lee)
정회원
2010년 2월 : 성균관대학교 공학박사
2009년 6월~2012년 2월 : 프랑스 INRIA 연구원
2012년 3월~2013년 8월 : 프랑스 TELECOM Bretagne 조교수
2013년 9월~2020년 2월 : 상명대학교 소프트웨어학과 부교수
2020년 3월~현재 : 세종대학교 정보보호학과 부교수
<관심분야> 프로토콜 엔지니어링 및 정보보호