정 보 보 호 학 회 지
제34권 제2호, 2024. 4

양자 컴퓨터 등장에 따른 랜섬웨어 대응 기술 동향

위 다 빈*, 김 한 결**, 박 명 서***

요 약

전 세계적으로 막대한 피해를 주고 있는 랜섬웨어는 다양한 방법으로 주요 조직을 대상으로 표적 공격을 펼친다. 랜섬웨어는 일반적으로 공격 대상 시스템의 파일을 암호화하기 위해 블록 암호, 스트림 암호와 같은 대칭키 암호를 사용하고, 해당 파일을 암호화할 때 사용되었던 대칭키를 공개키 암호로 보호한다. 여기서, 대칭키를 암호화할 때 RSA, ECC와 같은 공개키 암호를 주로 사용하는데, 이는 현재 전 세계적으로 이슈가 되고 있는 양자 컴퓨터의 발전과 Shor 알고리즘을 이용하여 무력화할 수 있다. 이러한 이유로 랜섬웨어가 기존의 암호화 구성에서 공개키 암호를 대신하여 양자 후 암호를 적용한다면, 양자 컴퓨터를 통한 랜섬웨어 대응이 불가능해진다. 본 논문에서는 랜섬웨어의 최신 기술 동향을 분석하고, 랜섬웨어의 암호화 구성에 기존 공개키 암호 대신 양자 후 암호를 적용 시 발생하는 공격 대응 원리에 대해 설명한다.

Ⅰ. 서 론

디지털 시대에 진입하면서 디지털 기기 사용이 확산하였으며, 이를 대상으로 한 악성코드가 꾸준히 유포되어 왔다. 1980년 후반 처음 등장한 악성코드의 유형 중 하나인 랜섬웨어(Ransomware)는 피해자의 데이터를 암호화 및 탈취하여 금전적인 이익을 추구한다. 이러한 랜섬웨어의 공격은 우리나라에서 2018년부터 2023년 사이 14배나 증가할 정도로 계속해서 기승을 부리고 있다[1]. 수많은 악성코드 중 랜섬웨어가 인기 있는 이유는 단연 금전적인 동기 때문이다. 해커가 자신의 실력을 과시하거나 재미 삼아 제작한 바이러스나 웜과는 달리, 랜섬웨어는 개인과 기업의 돈을 목표로 만들어졌다. PC나 스마트폰의 기능을 보존하면서도 파일만을 인질로 삼아 개인과 기업에 돈을 요구하는 방식으로 작동한다. 이 구조로 인해 해커는 랜섬웨어를 배포한 뒤 짧은 시간 안에 사용자와 기업의 돈을 탈취할 수 있다[2]. 이러한 상황에서 비트코인과 같은 가상화폐의 등장은 랜섬웨어가 수익을 창출하는 방식으로 확장되었으며, 이는 랜섬웨어의 수요 증가로 이어져 개인 및 기업을 대상으로 한 피해사례가 증가하고 있다. 또한 랜섬웨어는 시간이 흐를수록 더욱 전략적이고 조직적으로 변화하고 있다.

이러한 랜섬웨어의 등장과 더불어 양자 컴퓨터와 양자 후 암호 (PQC, Post Quantum Cryptography) 또한 함께 발전하고 있다. 양자 컴퓨터는 이진 비트 대신 양자비트 즉 큐비트(qubit)를 사용한다. 큐비트는 0과 1의 상태를 동시에 가질 수 있는 양자 중첩(Superposition)이라는 특성이 있어, n개의 큐비트로 2^n개의 값을 동시에 나타낼 수 있다. 이는 모든 가능한 경우를 한 번에 처리할 수 있게 하여, 연산 속도를 혁신적으로 향상시킨다. 양자 후 암호란 양자 컴퓨터를 이용한 공격에도 안전하다고 여겨지는 공개키 암호로, 현재 NIST에서 알고리즘의 표준화를 위한 공모사업을 진행하고 있다. 이러한 양자 컴퓨터의 발전을 통해 기존 랜섬웨어에 대응할 수 있지만, 랜섬웨어가 양자 후 암호를 적용했을 경우 양자 컴퓨터를 통한 대응을 기대하기 어렵다.

본 논문은 끊임없이 발전하고 변화하는 랜섬웨어에 대해 양자 컴퓨터의 등장으로 인한 영향과 양자 컴퓨터의 발전에 대비하기 위한 랜섬웨어의 동향을 소개한다. 본 논문의 구성은 다음과 같다. 2장에서 랜섬웨어 공격 전략의 동향을 설명한다. 이 과정에서 계속해서 공격이 증가하는 이유를 알아보고 랜섬웨어의 주요 공격 전략을 나열한다. 3장에서는 양자 컴퓨터의 등장으로 인한 랜섬웨어의 암호화 전략에 대한 영

* 한성대학교 융합보안학과 (대학원생, dbwe@hansung.ac.kr)
** 강남대학교 소프트웨어응용학부 (학부생, biequal@kangnam.ac.kr)
*** 한성대학교 융합보안학과 (조교수, pms91@hansung.ac.kr)

향을 설명한다. 이를 위해 다양한 랜섬웨어의 암호화 구성을 분석하고, 랜섬웨어의 암호키 보호를 위한 공개키 암호와 양자 알고리즘과의 관계를 설명한다. 4장에서는 양자 컴퓨터의 암호 해독에 대응하기 위해 양자 후 암호를 적용한 랜섬웨어의 사례를 설명하고, 양자 컴퓨터를 통해 랜섬웨어의 암호를 해독하는 원리를 설명한다. 또한 현재 시점에서 양자 후 암호가 적용된 랜섬웨어에 대한 대응 한계점 및 향후 대응 방법을 설명한다. 마지막으로 5장에서는 결론으로 마무리한다.

Ⅱ. 랜섬웨어의 공격 전략과 기술 동향

2023년에도 랜섬웨어 공격은 여전히 활발하게 이루어졌다. 2023년 1월에는 영국 우편 업체인 Royal Mail이 Lockbit 3.0 랜섬웨어의 공격을 받아 운영에 영향을 받았다[3]. 공격의 배후인 랜섬웨어 그룹 Lockbit은 데이터 유출을 빌미로 피해 기업에 금전적 지불을 요구하였다. 한편, 우리나라도 랜섬웨어로부터 안전하지 않았다. 대표적으로 2023년 5월 16일 국내 기업 오리온이 랜섬웨어 그룹 BlackCat에 피해를 입었다[4]. 공격에 성공한 랜섬웨어 그룹은 1TB에 해당하는 데이터를 탈취했다고 주장했다. 이렇게 세계적으로 2023년 상반기에만 랜섬웨어로 인한 피해액이 4억 4,910만 달러로 많은 피해가 발생하였고[5], 하반기까지 포함한다면 10억 달러가 넘는 피해액이 발생하였다. 이는 랜섬웨어로 인한 피해액 중 최고액이다[6]. 2022년까지만 해도 주요 랜섬웨어 그룹의 운영 중단이나 FBI의 하이브 랜섬웨어 변종 침투와 같은 법 집행 기관의 개입 등 다양한 요인 및 노력으로 랜섬웨어 활동이 감소하였으나, 이러한 노력에도 불구하고 2023년에는 랜섬웨어 활동이 크게 증가하였다. 이는 거액의 몸값을 지불할 수 있는 대규모 조직을 대상으로 공격하는 빅 게임 헌팅 전술이 널리 퍼지고, RaaS (Ransomware as a Service, 서비스형 랜섬웨어) 모델의 확산으로 새로운 공격자들이 사이버 범죄 영역에 진입하는 장벽이 낮아지는 것에 영향을 받았기 때문이다. 전통적으로 랜섬웨어는 암호화 전략에 의존하여 금전적인 활동을 진행하였으나, 피해자의 금전 지불 빈도 하락으로 갈취 전략을 통한 새로운 수익화 전략을 도입하는 추세이다[7]. 이는 단순히 정보를 암호화하는 것보다 민감 데이터 유출 및 서비스 중단 공격 등을 통해 목표 대상에 더 큰 압력을 가하기 위함이다. 또한 랜섬웨어 공격을 활발하게 하는 RaaS의 영향력이 증가하고 있다[8]. 이처럼 랜섬웨어의 전략은 크게 암호화 전략, 갈취 전략, RaaS 전략으로 구성된다.

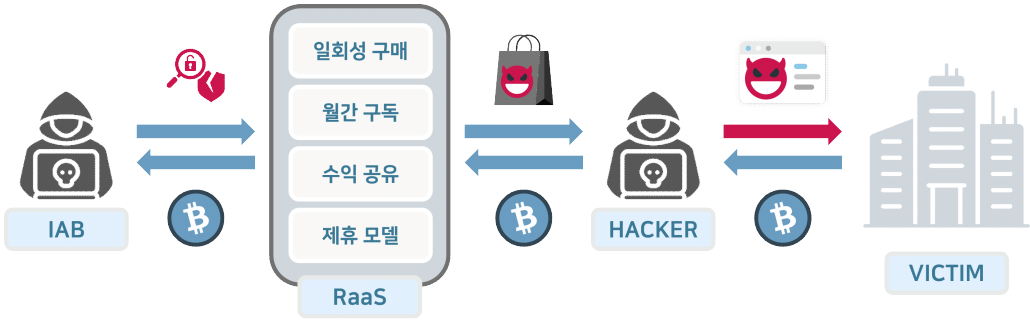
랜섬웨어의 암호화 전략은 랜섬웨어의 대표적인 전략으로 대상 시스템의 데이터를 암호화한 후 복호화 키를 제공하는 대가로 금전을 요구하는 방식을 의미한다. 과거에는 단순히 암호화 전략만을 사용하였지만, 최신의 랜섬웨어는 갈취 전략과 서비스 형태의 랜섬웨어 등 다양한 전략을 사용하고 있다. 최근에는 피해자로부터 금전을 요구하는 데 있어서 [표 1]과 같이 다중 갈취 기법을 사용하나 모든 갈취 기법에는 데이터를 암호화한 후 복호화를 위한 금전적 대가를 요구하는 암호화 전략을 포함한다.

첫 번째 기법인 이중 갈취기법은 암호화를 포함하고, 해커가 데이터를 유출하거나 공개하지 않는 대가로 금전을 요구한다. 두 번째 기법인 삼중 갈취기법은 이중 갈취 기법에 적용된 기술을 포함하고, 피해조직의 공급망 또는 벤더에 대한 서비스 거부 공격을 통해, 피해자 조직이 자신들의 요구를 충족시키도록 압력을 가한다. 이러한 삼중 갈취 공격은 피해조직의 운영을 방해하고, 장기적인 경제적 손실을 초래한다. 마지막으로 사중 갈취 기법은 삼중 갈취 기법을 실행함과 동시에, 피해조직과 고객사와의 비즈니스 관계에 악의적인 영향을 끼쳐 피해조직에 더 큰 압력을 가하는 방법을 말한다[9]. 이렇듯 랜섬웨어는 끊임없이 피해자를 압박하기 위한 다중 갈취 기법을 사용하고 있다.

RaaS란 제3자의 랜섬웨어 공격 행위를 위해 서비스 형태로 제공되는 랜섬웨어를 의미한다. RaaS는 익명 네트워크를 통해 거래되는 특성을 보유하고 있다. 랜섬웨어 제작자가 제공하는 RaaS 키트는 SaaS (Software as a Service) 공급자가 제공하는 것과 유사하게 랜섬웨어 공격 서비스를 제공하며, 해당 키트

〔표 1〕 랜섬웨어의 갈취 전략

전략	적용 기술			
	암호화	정보유출	서비스 거부 공격	비즈니스 관계 공격
이중 갈취	O	O	X	X
삼중 갈취	O	O	O	X
사중 갈취	O	O	O	O



〔그림 1〕 RaaS를 이용한 랜섬웨어 공격 구조

에는 월간구독, 일회성 코드 구매, 제휴모델, 이익공유 등의 수익모델이 삽입되어 있다[10]. RaaS의 구조는 [그림 1]과 유사한 모델을 기반으로 하며, 다양한 형태로 존재한다. IAB (Initial Access Broker)는 SSH, VPN, RDP 등 네트워크 접근 권한이나 내부 인프라의 취약점을 찾아 침투 경로를 제공하는 개인 또는 그룹을 의미한다. 이들은 오직 침투 경로만 제공하고 랜섬웨어 공격이나 협상에 관여하지 않는다는 특징이 있다. 이는 초기 침투 과정에 많은 시간과 노력을 투자해 온 랜섬웨어 조직이 수고를 줄이기 위해 외주를 맡기는 것으로 볼 수 있다[11]. 이렇게 얻은 경로를 통해 랜섬웨어를 제작한 후 다른 해커에게 다양한 서비스 모델을 판매한다. 그 후 RaaS 키트를 제공받은 해커는 기업 및 정부 조직과 같은 귀중한 데이터를 보유한 적절한 피해자 대상에게 공격을 실시한다[12]. 이러한 과정을 통해 RaaS 키트 사용자는 일반적인 소프트웨어 사용자처럼 전문적인 지식이 없어도 랜섬웨어 공격을 수행할 수 있다.

Ⅲ. 양자 컴퓨터를 통한 랜섬웨어 복호화

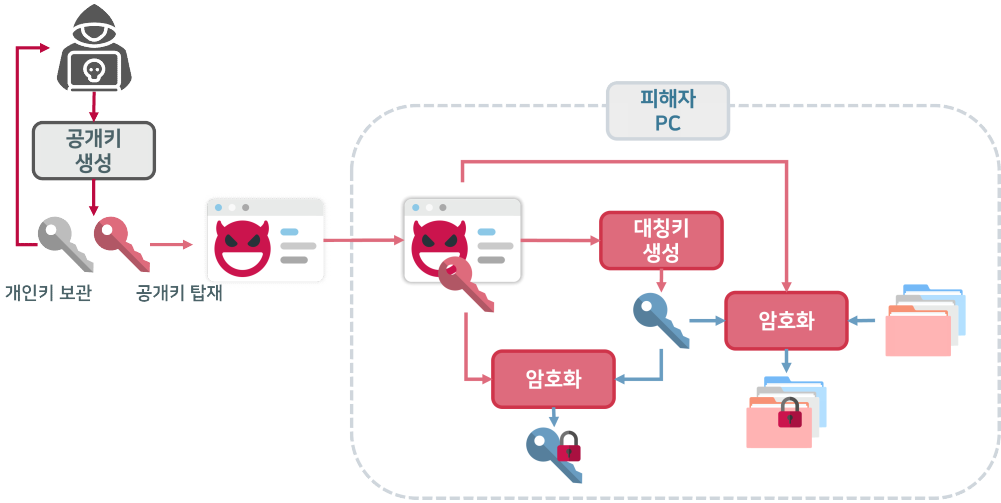
3.1. 랜섬웨어의 암호화 구성

랜섬웨어의 전략이 다양한 형태로 변화하고 있지만, 모든 전략에 있어서 대상 시스템에 존재하는 파일을 암호화한다. 따라서 랜섬웨어 대응에 있어서 복호화 과정은 중요한 쟁점이다. 현재에도 많은 랜섬웨어 공격에서 이러한 형태를 식별할 수 있다. 2019년 2월에 출현한 Clop 랜섬웨어는 동작 초기에 동작 조건을 충족하는지를 런타임에서 확인하는 로직이 존재하며, 네트워크를 통해 확산할 수 있는 장치를 식별하였다[13]. 이후 파일 암호화를 진행하며 암호화에 사용한 AES 암호키를 RSA 공개키로 암호화하여 제3자의 해독을 방지한다. Royal 랜섬웨어는 OpenSSL 라이브러리와 함께 AES 암호화 방식을 사용하여 대상 파일을 암호화한다. 이 과정에서 사용된 AES 암호화 키는 랜섬웨어에 내장된 RSA 공개키를 통해 암호화된다. 이렇게 암호화된 AES 키는 암호화된 파일 하위에 위치하여 저장된다[14]. Rhysida 랜섬웨어는 256비트 키와 IV가 요구되는 스트림 암호 방식인 ChaCha20을 통해 파일 암호화를 진행한다[15]. 암호화 준비 단계에서 랜섬웨어에 내장된 RSA 공개키를 불러온 후 암호화를 진행하고, 암호화에 사용한 암호화키와 IV를 불러온 RSA 공개키로 암호화한다. RaaS로 알려진 Lockbit 3.0은 피해자의 파일을 암호화한 후 로그 파일, 휴지통 파일, 볼륨 섀도 복사본 등을 삭제한다[16]. 암호화 과정에서 사용된 AES 암호키는 RSA 공개키를 통해 암호화된다.

[표 2]와 같이 앞서 설명한 랜섬웨어는 파일 암호화를 위해 AES 또는 ChaCha20을 사용하며, 파일 암호화에 사용된 암호키는 RSA의 공개키를 통해 보호한다. 따라서 [그림 2]와 같이 랜섬웨어의 암호화 구성을 보았을 때, 결과적으로 공격자의 RSA 개인키를 획득한 경우 랜섬웨어의 파일 복호화가 가능해진다.

〔표 2〕 랜섬웨어별 암호화 구성

랜섬웨어	파일 암호화 알고리즘	파일 암호키 보호 알고리즘
Clop	AES	RSA
Royal	AES	RSA
Rhysida	ChaCha20	RSA
Lockbit 3.0	AES	RSA



〔그림 2〕 랜섬웨어의 파일 및 대칭키 암호화 전략

3.2. 양자 알고리즘과 공개키 암호의 관계

양자 컴퓨팅의 발전은 RSA 및 ECC와 같은 기존의 암호화 알고리즘을 무력화시킬 수 있다. 1994년 피터 쇼어에 의해 고안된 쇼어 알고리즘(Shor's Algorithm)은 소인수분해 문제와 이산 대수 문제를 다항식 시간 안에 풀 수 있는 양자 알고리즘이다. 전통적인 컴퓨터에서 이 문제를 해결하는 데에는 지수 시간이 소요되지만, 양자컴퓨터를 활용한 쇼어 알고리즘은 다항식 시간 내에 문제를 해결할 수 있기 때문에 기존의 암호 체계에 큰 영향을 준다. RSA-2048을 합리적인 시간 내에 공격하기 위한 최소한의 큐비트 수가 4,098로 알려져 있는데[17], 2023년 11월 기사에 따르면 Atom Computing은 1,000개 이상의 장벽을 최초로 돌파한 1,225큐비트 양자 컴퓨터를 발표했으며[18], IBM은 2026년까지 수만 큐비트를 처리하는 양자 프로세서를 개발하겠다는 계획을 발표하였다. 랜섬웨어의 동향을 살펴보았을 때 암호화된 파일을 해독하기 위해 공격자의 RSA 개인 키가 필요하다. 그런데 양자 컴퓨팅의 발전으로 인해 기존의 공개키 암호로 제작된 공격자의 개인 키는 해독이 가능해진다. 하지만 랜섬웨어 또한 이러한 상황에 대비하여 양자 후 암호를 적용하고 있다.

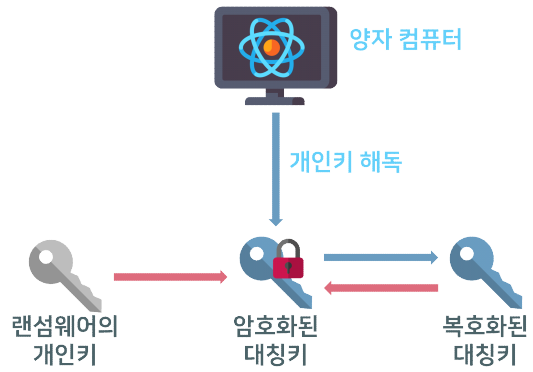
Ⅳ. 랜섬웨어의 양자 후 암호 적용

4.1. 양자 후 암호가 적용된 랜섬웨어의 등장

양자 컴퓨터의 발전은 빠른 연산속도를 통해 기존 랜섬웨어에 대한 대응 가능성을 제공한다. 랜섬웨어가 암호키 보호를 위해 기존의 RSA와 ECC와 같은 공개키 암호가 아닌, 양자 후 암호를 적용한다면 양자 컴퓨터를 통한 대응이 불가능하다. 러시아어 해킹 포럼에서 유출된 'HelloKitty' 랜섬웨어 소스 코드에서는 'hellokitty.zip' 아카이브 내에 파일 암호화에 사용되는 NTRUEncrypt 라이브러리와, HelloKitty 랜섬웨어의 암호화 및 복호화 도구를 구축하기 위한 Microsoft Visual Studio 솔루션이 포함되어 있음이 밝혀졌다[19]. NTRUEncrypt는 격자 기반의 문제를 이용한 공개키 암호 시스템인 NTRU의 일환으로, 양자 컴퓨팅 공격에 저항력이 있는 알고리즘이다. 이는 양자 컴퓨팅에 대응하는 암호화 기술이 이미 랜섬웨어에 적용되기 시작했음을 시사한다.

4.2. 양자 컴퓨터를 활용한 랜섬웨어 암호키 해독

양자 컴퓨터를 통해 랜섬웨어에 대응하는 원리는 랜섬웨어의 암호화 구성에 있다. 랜섬웨어는 빠른 암호화를 위해 대칭키 알고리즘을 사용하고, 공개 키 암호 알고리즘으로 암호화 키를 보호하는 하이브리드 암호 방식을 사용한다. 이는 빠른 연산속도와 키 배송



〔그림 3〕 양자 컴퓨터를 통한 랜섬웨어 대칭키 복호화 과정

문제를 모두 해결할 수 있는 효율적인 방법으로, 암호키 보호는 공개키 알고리즘에 의존한다. 양자 컴퓨터는 기존의 공개키 암호를 해독할 수 있으며 이를 통해 [그림 3]과 같이 랜섬웨어 공격자의 개인 키를 해독할 수 있다. 랜섬웨어 공격자의 개인 키를 획득하였을 때, 감염된 시스템 또는 암호화된 파일에 존재하는 암호화된 암호화 키를 복호화하여, 최종적으로 파일 복호화에 사용되는 암호키를 획득할 수 있게 된다.

그러나 해당 부분에서 랜섬웨어가 기존의 공개키 알고리즘이 아닌 양자 후 암호를 적용하였을 때, 랜섬웨어 공격자의 개인 키 해독이 불가능하게 된다. 따라서 랜섬웨어에 양자 후 암호가 적용되면, 양자 컴퓨터의 활용으로도 대응이 불가능해진다. 하지만 양자 컴퓨터를 양자 후 암호가 적용되지 않은 랜섬웨어에 HNDL (Harvest Now, Decrypt Later) 공격을 통해 역이용할 수 있다. HNDL은 공격 대상으로부터 암호화된 데이터를 수집하고, 이후 복호화 가능한 정보 또는 방법을 사용해 암호화된 데이터를 복호화하는 것을 의미한다. 즉, 현재 랜섬웨어로부터 공격당해 암호화된 파일을 복호화하지 못하였다면 암호화된 데이터 중 공개키와 암호화된 파일을 따로 저장해 둔 뒤 이후 충분한 성능의 양자컴퓨터가 개발되었을 때 복호화를 시도할 수 있다.

Ⅴ. 결 론

이전의 랜섬웨어와 다르게 최신 랜섬웨어 조직은 암호화뿐만 아니라 정보 탈취 및 협박, 랜섬웨어 서비스 등과 같이 다양한 전략을 사용하고 있다. 이러한 랜섬웨어를 통한 피해사례는 꾸준히 증가하고 있다. 모든 랜섬웨어 전략에는 기본적으로 암호화 전략이 포함되어 있기 때문에 랜섬웨어 피해 복구를 위해선 파일 복호화가 핵심이 된다.

양자 컴퓨터가 등장하면서 빠른 연산 속도를 통해 기존 랜섬웨어의 파일 암호화에 대한 대응이 가능해진다. 기존 랜섬웨어는 대칭키 암호 알고리즘을 통해 파일을 암호화하고, 공개키 암호 알고리즘을 통해 암호화에 사용한 암호키를 보호한다. 이 과정에서 사용되는 공개키 알고리즘은 양자 컴퓨터의 연산을 통해 해독될 수 있으며 결과적으로 대칭키 획득에 영향을 준다. 이후에 등장할 다양한 랜섬웨어는 금전적 이익 창출을 위해 양자 후 암호를 적용할 것으로 예상되며, 이를 위한 대응 방법이 모색되어야 한다.

참 고 문 헌

[1] 부산일보,"'랜섬웨어' 공격 4년간 14배 증가…"피해 대부분 중소기업·.정부는 외면", https://www.busan.com/view/busan/view.php?code=2023101618234737125

[2] 동아일보,"랜섬웨어가 활개치는 3가지 이유", https://www.donga.com/news/It/article/all/20161228/82078263/1

[3] 잉카인터넷 시큐리티대응센터 블로그, https://isac.tachyonlab.com/5450

[4] 아이뉴스24, https://www.inews24.com/view/1595642

[5] 보안뉴스, https://www.boannews.com/media/view.asp?idx=120221

[6] 데일리시큐, https://www.dailysecu.com/news/articleView.html?idxno=153448

[7] IT WORLD, https://www.itworld.co.kr/news/290809, 2023

[8] 정보통신신문, https://www.koit.co.kr/news/articleView.html?idxno=101896

[9] Trend Micro, Trend Micro Security Predictions for 2022, pp.21-22, 2021

[10] What is ransomware-as-a-service (RaaS)?, https://www.ibm.com/topics/ransomware-as-a-service

[11] 랜섬웨어 조직에 최초 접근 권한 판매하는 브로커 'IAB' 활개, https://m.boannews.com/html/detail.html?idx=119767

[12] Ransomware-as-a-Service, https://www.sophos.com/en-us/cybersecurity-explained/ransomware-as-a-service
[13] Clop Ransomware", https://www.quorumcyber.com/, https://www.quorumcyber.com/malware-reports/clop-ransomware
[14] Royal Rumble: Analysis of Royal Ransomware", https://www.cybereason.com/, https://www.cybereason.com/blog/royal-ransomware-analysis
[15] Max Kersten, Leandro Velasco, "Rhysida Ransomware",https://www.trellix.com/ko-kr/,https://www.trellix.com/blogs/research/rhysida-ransomware/,2023
[16] "Dark Web Profile: LockBit 3.0 Ransomware", https://socradar.io/ ,https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/
[17] 보안뉴스, “제113차 CISO포럼, 최근 보안 핫 키워드 ‘양자컴퓨터’와 ‘다크웹’ 논의”, https://www.boannews.com/media/view.asp?idx=101658
[18] AI넷, “[1,000개 이상의 큐비트 양자컴퓨터 발표]”, http://www.ainet.link/12618
[19] https://www.bleepingcomputer.com/, "HelloKitty ransomware source code leaked on hacking forum", https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-source-code-leaked-on-hacking-forum/

〈저 자 소 개〉

위 다 빈 (Dabin We)

2024년 2월 : 강남대학교 소프트웨어응용학부 졸업
2024년 3월 : 한성대학교 융합보안학과 석사과정
<관심분야> 정보보호, 디지털포렌식

김 한 결 (Han-gyeol Kim)

학생회원

2019년 3월~현재 : 강남대학교 소프트웨어응용학부 재학
<관심분야> 정보보호, 디지털포렌식

박 명 서 (Myungseo Park)

종신회원

2013년 2월 : 국민대학교 수학과 이학사
2015년 2월 : 국민대학교 금융정보보안학과 이학석사
2014년 12월~2017년 2월 : 국가보안기술연구소 연구원
2021년 8월 : 국민대학교 금융정보보안학과 이학박사
2021년 9월~2022년 2월 : 국민대학교 금융정보보안학과 박사후연구원
2022년 3월~2023년 8월 : 강남대학교 ICT융합공학부 조교수
2023년 9월~현재 : 한성대학교 융합보안학과 조교수
<관심분야> 정보보호, 디지털 포렌식