정 보 보 호 학 회 지
제 32 권 제3호, 2022. 6

랜섬웨어의 파일 암호화 키 관리 방법 분류와 그에 따른 분석 대상 식별

박 명 서*

요 약

랜섬웨어는 시스템을 잠그거나 데이터를 암호화해서 사용할 수 없도록 한 뒤 피해자에게 대가로 금전을 요구하는 악성 프로그램이다. 랜섬웨어는 암호학적으로 안전하다고 알려진 암호 알고리즘들을 이용하여 파일을 암호화하기 때문에 암호 알고리즘 분석만으로는 감염된 파일을 복구할 수 없다. 따라서, 감염된 파일의 복구를 위해서는 암호 알고리즘 안전성 측면이 아닌 별도의 방법을 마련할 필요가 있다. 랜섬웨어는 파일 암호화 키를 이용하여 대상 파일들을 암호화하기 때문에 이를 복구할 수 있다면, 감염된 파일 복구가 가능하다. 하지만, 랜섬웨어들은 각각 다른 방법으로 파일 암호화키를 관리하기 때문에 일반적인 파일 암호화키 관리 방법을 미리 숙지하지 못한다면 파일 암호화키 복구를 위한 역공학 분석 시 비효율이 발생할 수 있다.

본 논문에서는 랜섬웨어가 파일 암호화키를 암호화하는 방식에 따라 세 가지로 분류하여 설명한다. 또한, 향후 랜섬웨어 분석가가 효율적인 분석을 할 수 있도록 각 관리 방법에 따라 파일 암호화키 복구를 위한 분석 대상을 식별하였다.

Ⅰ. 서 론

몸값(Ransom)과 소프트웨어 (Software)의 합성어인 랜섬웨어는 개인보다 기업을 공격 대상으로 유포되고 있다. 2020년 11월 이랜드그룹은 클롭 랜섬웨어 감염되어 추가 확산을 막기 위한 네트워크 차단으로 이랜드 매장 영업이 중단되는 사건이 발생하였다[1]. 2021년 2월 기아차 북미법인은 도플페이머 랜섬웨어에 감염되었으며, 공격자는 내부 데이터 유출을 빌미로 2,000만 달러를 요구하였다[2]. 2021년 3월 대만 컴퓨터 제조사 에이서가 소디노키비로 잘 알려진 레빌 랜섬웨어에 의해 공격 받은 뒤 5,000만 달러를 요구하는 협박을 받았다[3]. 랜섬웨어는 개발자와 배포자의 역할을 분담하는 서비스형 랜섬웨어 (RaaS, Ransomware as a Service) 형태로 진화하여 더욱 손쉽게 공격이 가능해졌다. 이로 인해 랜섬웨어의 공격으로 인한 국제적인 피해 금액은 2015년 한화 3,800억원에서 기하급수적으로 증가하여 2031년에는 312조 7천억으로 증가할 것으로 예측되었다[4]. 랜섬웨어는 더욱 정교화된 기술과 지능화된 공격 방법으로 피해를 입히고 있으므로 피해 예방 차원에서 랜섬웨어의 암호화 기술 및 복호화 방법에 대한 연구가 지속적으로 수행되어야 한다.

본 논문에서는 랜섬웨어가 파일 암호화에 사용되는 파일 암호화키를 관리하는 방법에 대해 설명하고, 각 파일 암호화키 관리 방법에서의 분석 대상을 식별하였다. 2장에서는 일반적인 랜섬웨어 감염 프로세스와 비용 지불 시 복구 프로세스를 보여주고, 3장에서는 랜섬웨어의 파일 암호화키 관리 방법 및 각 방법에 따른 파일 암호화키 복구를 위한 분석 대상에 대해 설명한다. 마지막 4장에서 결론짓는다.

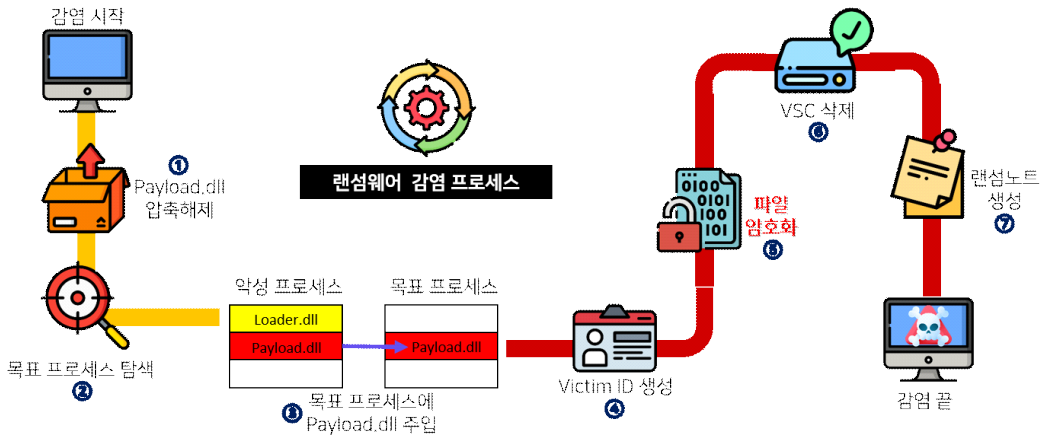
Ⅱ. 랜섬웨어 감염 프로세스

본 장에서는 대략적인 랜섬웨어 감염 프로세스와 비용 결제 시 복구 프로세스에 대해 설명한다.

2.1. 랜섬웨어 전체 감염 프로세스

[그림 1]은 랜섬웨어 감염 프로세스를 총 7단계로 나타낸 것이다. 랜섬웨어 감염이 시작되면 악성 프로세스 역할을 수행하는 Payload.dll을 압축 해제한다(1). 그 다

* 강남대학교 ICT융합공학부 (조교수, pms91@kangnam.ac.kr)



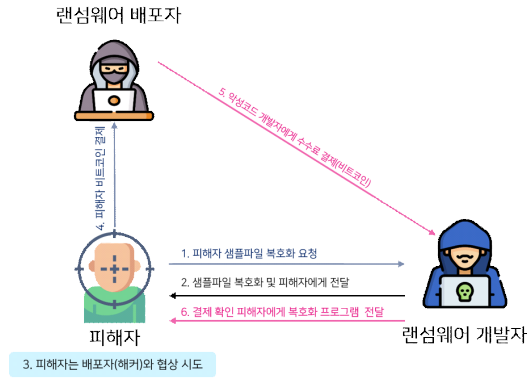
〔그림 1〕 랜섬웨어 감염 프로세스

음 목표 프로세스를 탐색(2)하여 악성 프로세스를 목표 프로세스에 주입한다(3). 이로써, dll을 프로세스의 로드된 모듈로 등록하지 않아도 되어 dll 로드 모니터링 툴을 우회할 수 있다. 이후 피해자를 특정할 수 있는 Victim ID를 생성(4)하고, 파일 암호화를 수행한다(5). 5단계에서 파일 암호화키를 생성하여 파일들을 암호화한다. 파일 암호화키 관리 방법과 파일 암호화 방식은 랜섬웨어마다 다르기 때문에 감염된 파일 복구를 위해서는 이 부분에 대해 면밀히 분석할 필요가 있다. 파일 암호화가 완료되면, 시스템 복원을 막기 위해 VSC (Volume Shadow Copy)를 삭제한다(6). 마지막으로 비용 지불 방법을 포함한 랜섬노트를 생성하여 시스템에 출력하고 감염이 완료된다.

2.2. 비용 결제 시 복구 프로세스

피해자는 랜섬웨어 감염 이후 감염된 파일 복구를 위해 비용을 지불할 수 있다. 이때 화면에 출력되는 랜섬노트를 통해 랜섬웨어 개발자에게 연락하는 파일 복구를 수행하게 되는데 [그림 2]는 이 과정에 대한 구체적인 프로세스를 나타낸다.

먼저 피해자는 랜섬웨어 개발자에게 감염된 파일의 복구 능력을 확인하기 위해 감염 파일 중 하나를 샘플 파일로 복호화 요청한다(1). 랜섬웨어 개발자는 감염된 파일 내에 있는 파일 암호화 키를 복구하여 샘플 파일을 복호화한 후 피해자에게 전달한다(2). 복구 능력을 확인한 패해자는 무료 복호화 도구 제공 및 가격 협상을 랜섬웨어 배포자와 시도한다(3). 피해자가 비트코인으로 비용을 결제(4)하면, 랜섬웨어 배포자는 그 중 일부를 수수료로 랜섬웨어 개발자에게 전달한다(5). 이 후 랜섬웨어 개발자가 피해자에게 복호화 프로그램을 전달(6)하면, 피해자는 그 프로그램을 이용하여 감염된 파일을 복구하게 된다.



〔그림 2〕 비용 지불 시 랜섬웨어 복구 프로세스

Ⅲ. 랜섬웨어의 파일 암호화키 관리 방법

본 장에서는 랜섬웨어를 파일 암호화키 관리 방법에 따라 분류하고, 각 관리 방법별 파일 암호화키 복구를 위한 분석 대상에 대해 설명한다. 랜섬웨어는 파일 암호화키를 대칭키 암호 알고리즘의 비밀키로 사용하여 파일을 암호화한다. 파일 암호화키를 복구할 수 있다면, 그것을 이용해 암호화된 파일을 복호화할 수 있다. 따라서, 랜섬웨어에 대한 파일 암호화키 관리 방법을 파악하

〔표 1〕 파일 암호화 키 관리 방법별 분석 대상 식별

구분	관리 방법 1		관리 방법 2	관리 방법 3
	case 1	case 2		
고정된 암호화 키 확인	O	X	X	X
메모리 분석	X	O	O	O
키생성 알고리즘의 취약성 분석	X	O	O	O
복호화 도구 역공학 분석	X	X	O	X

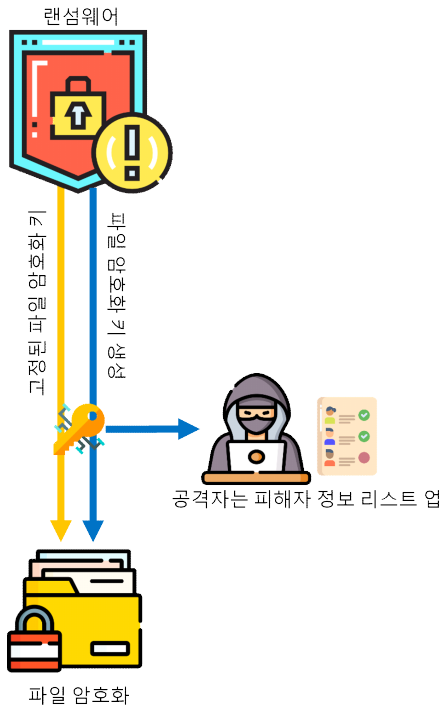
고, 각 방법에 따른 파일 암호화키의 복구 가능 요소에 대해 살펴봐야 한다. 우리는 랜섬웨어의 파일 암호화키 암호화 여부에 따라 관리 방법을 세 가지로 분류하였으며, 각 방법에 대해 파일 암호화키 복구를 위해 분석해야 하는 대상을 식별하였다. [표 1]은 파일 암호화키 관리 방법에 대해 식별된 분석 대상을 정리한 것이다.

3.1. 파일 암호화키 관리 방법 1

랜섬웨어의 파일 암호화키 관리 방법 1은 별도의 공개키 암호 알고리즘을 활용하여 파일 암호화키를 암호화하지 않는다. 파일 암호화키 관리 방법 1에 대한 구체적인 감염 과정은 [그림 3]과 같이 나타낼 수 있다.

고정된 파일 암호화키(case 1) 또는 별도의 키생성 알고리즘을 통해 생성된 파일 암호화키(case 2)를 이용하여 대상 파일을 암호화한다. caes 1은 랜섬웨어에 파일 암호화키가 내장된 상태로 배포되고, case 2는 감염 대상마다 별도로 파일 암호화키를 생성한다. case 2에서 생성된 파일 암호화키는 공격자에게 전송되고, 공격자는 전송받은 파일 암호화키를 기반으로 피해자 정보를 관리하게 된다.

랜섬웨어의 파일 암호화키 관리 방법 1에서는 감염된 파일 복구를 위해 랜섬웨어 분석 과정에서 파일 암호화키를 복구 가능 여부를 파악해야 한다. case 1은 고정된 파일 암호화키가 랜섬웨어에 내장되어 있기 때문에 비교적 쉽게 파일 암호화키 복구가 가능하다. Jigsaw[5]는 파일 암호화에 사용된 비밀키와



〔그림 3〕 파일 암호화키 관리 방법 1에 대한 감염 과정

IV(Initialization Vector)가 프로그램 내에 내장되어 있어 감염된 파일 복구가 가능하였다. 반면, case 1에 비해 분석이 어려운 case 2는 두 가지 측면에서 파일 암호화키 복구 가능 여부를 확인할 필요가 있다. 첫 번째는 파일 암호화키의 메모리 상 존재 여부를 확인하는 것이다. 대부분의 랜섬웨어는 감염이 완료되면 파일 암호화키를 제로화하고 메모리 상에서 삭제한다. 하지만, Donut[6]과 같은 일부 랜섬웨어가 파일 암호화키 제로화를 수행하지 않고 메모리 해제만을 수행하여 파일 암호화키 복구가 가능하였다. 두 번째는 파일 암호화키 생성에 사용된 키생성 알고리즘의 취약점을 활용하는 것이다. 암호화키 생성은 보통 시스템의 자원을 엔트로피로 활용하는 난수 발생기를 이용한다. 충분한 엔트로피와 암호학적으로 안전한 난수 발생기를 사용하여 생성된 파일 암호화키는 복구가 불가능하다. 대다수의 랜섬웨어는 앞선 상태를 만족하는 난수 발생기로 간단히 운영체제에서 제공하는 난수 발생기 API를 이용한다. 하지만, 5ss5c[7], Immuni[7] 및 Magniber v2[8]와 같은 일부 랜섬웨어는 랜섬웨어 개발자가 직접 개발한 난수 발생기를 통해 암호화키를 생성하였다. 이 랜섬웨어들

은 충분하지 못한 엔트로피 사용 및 난수 발생기의 취약점으로 인해 파일 암호화키 복구가 가능하였다.

3.2. 파일 암호화키 관리 방법 2

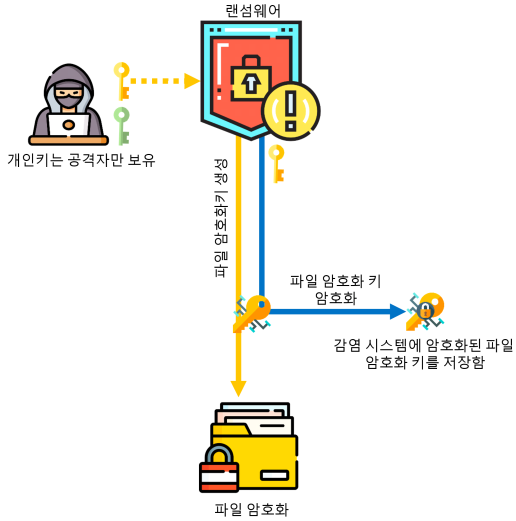
랜섬웨어의 파일 암호화키 관리 방법 2은 파일 암호화키 관리 방법 1의 case 2에 대한 파일 암호화키를 공격자의 공개키를 이용하여 암호화하는 방식이다. 파일 암호화키 관리 방법 2에 대한 구체적인 감염 과정은 [그림 4]와 같이 나타낼 수 있다.

공격자는 공개키와 개인키로 이루어진 공개키 쌍을 생성한다. 공격자의 개인키는 공격자만이 보유하고, 공격자의 공개키는 배포될 랜섬웨어에 내장시킨다. 랜섬웨어는 파일 암호화키를 생성하여 파일을 암호화시킨 후 내장된 공격자의 공개키를 이용해 파일 암호화키를 암호화하여 감염 시스템에 저장하게 된다. 일반적인 저장 방법으로 감염된 파일에 암호화된 파일 암호화키를 연접하는 방법을 이용한다. 감염된 파일 복구를 위해서는 공격자만이 가지고 있는 공격자의 개인키를 이용하여 암호화된 파일 암호화키를 복호화해야 한다. 파일 암호화키 관리 방법 2에서는 파일 암호화키 관리 방법 1에서 파일 암호화키 복구를 위해 고려하였던 메모리 분석 및 키생성 알고리즘의 취약점 외에 추가적으로 공격자의 개인키 복구 여부에 대해 확인할 필요가 있다. 공격자의 개인키 복구를 위해 공개키 암호 알고리즘을 대상으로 분석한다고 가정했을 때, 알려진 정보는 랜섬웨어에 내장된 공격자의 공개키이다. 하지만, 암호학적으로 공개키만으로 개인키 복구는 불가능하다. 공격자의 개인키 복구를 위해 고려할 또 다른 방법은 공격자가 제공한 랜섬웨어 복호화 도구를 이용하는 것이다. 랜섬웨어의 피해자가 공격자에게 비용을 지불하고 랜섬웨어 복호화 도구를 제공받는다. 이 랜섬웨어 복호화 도구에는 감염된 파일 복구를 위해 공격자의 개인키가 내장되어야 한다. 따라서, 랜섬웨어 복호화 도구를 역공학 분석하면 공격자의 개인키 복구가 가능하다. 랜섬웨어 공격자는 이러한 복구 방법을 무력화시키기 위해 대다수가 다음 절에서 설명하는 파일 암호화키 관리 방법 3을 이용한다.

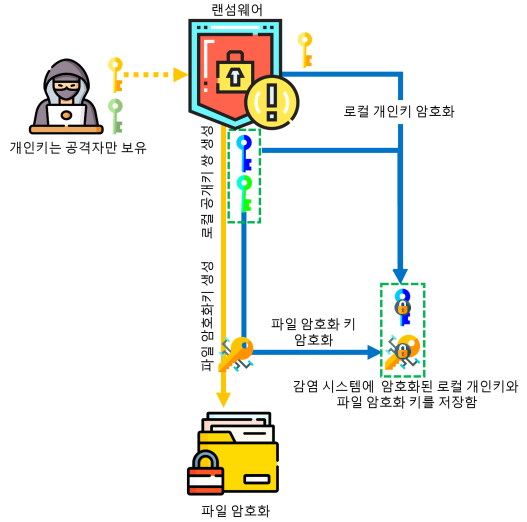
3.3. 파일 암호화키 관리 방법 3

랜섬웨어의 파일 암호화키 관리 방법 3은 동적으로 생성된 파일 암호화키를 감염 시스템 상에서 생성한 로컬 개인키 쌍의 로컬 공개키로 암호화하는 방식을 사용한다. 파일 암호화키 관리 방법 3에 대한 구체적인 감염 과정은 [그림 5]와 같이 나타낼 수 있다.

파일 암호화키 관리 방법 3은 파일 암호화키 관리 방법 2와 마찬가지로 공격자의 공개키를 랜섬웨어 내장하는 것은 동일하다. 여기에 부가적으로 감염된 시스템 상에서 로컬 공개키와 로컬 개인키로 이루어진 로컬



〔그림 4〕 파일 암호화키 관리 방법 2에 대한 감염 과정



〔그림 5〕 파일 암호화키 관리 방법 3에 대한 감염 과정

공개키 쌍을 생성한다. 랜섬웨어는 파일 암호화키를 생성하여 파일을 암호화시킨 후 로컬 공개키를 이용해 파일 암호화키를 암호화한다. 그 다음, 로컬 개인키를 공격자의 공개키를 이용하여 암호화하여 암호화된 파일 암호화키와 같이 감염된 시스템에 저장한다.

파일 암호화키 관리 방법 3에서는 파일 암호화키 관리 방법 1에서의 메모리 분석 및 키생성 알고리즘의 취약점을 파일 암호화키 복구를 위해 고려해야 한다. 다만, 메모리 분석에서 파일 암호화키 관리 방법 1이 파일 암호화키에 대해서만 분석했던 것과 달리 로컬 공개키 쌍에 대한 메모리 분석이 포함되어야 한다. 이 분석에는 로컬 공개키 쌍뿐 아니라 로컬 공개키 쌍 생성을 위해 사용되었던 재료도 분석 대상에 포함해야 한다. WannaCry[9]는 로컬 공개키 쌍 생성 시 사용된 소수 관련 데이터가 메모리 해제 전 소수를 제로화하지 않아 공개키 쌍 복구가 가능하였다. 또한, 파일 암호화키 관리 방법 3은 파일 암호화키 관리 방법 2와 다른 방식의 복호화 도구 제공으로 인해 복호화 도구 역공학 분석을 통한 공격자의 개인키 복구가 불가능하다. 공격자는 비용을 지불한 피해자로부터 암호화된 로컬 개인키를 전달받는다. 이는 일반적으로 암호화된 로컬 개인키가 포함된 감염된 파일을 전달하는 것으로 가능하다. 공격자는 암호화된 로컬 개인키를 공격자의 개인키로 복호화한 후 로컬 개인키를 이용해 랜섬웨어 복호화 도구를 개발하여 피해자에게 전달한다. 이 랜섬웨어 복호화 도구에는 오직 해당 피해자 개인에만 적용할 수 있는 로컬 개인키가 포함되어 있기 때문에 역공학 분석을 수행하더라도 공격자의 개인키 복구는 불가능하다.

Ⅳ. 결 론

본 논문에서는 랜섬웨어의 파일 암호화키 관리 방법을 암호화 여부에 따라 세 가지로 분류하여 설명하고, 각 관리 방법에 따라 감염된 파일 복구를 위해 분석해야 하는 대상에 대해 설명하였다. 다양한 랜섬웨어가 사회 여러 분야에 피해를 주는 현 상황에서 랜섬웨어에 대한 효율적인 분석을 통해 복호화 여부를 빠르게 판단할 필요가 있다. 본 연구 결과는 감염된 파일의 복호화에 반드시 필요한 파일 암호화키 복구를 위해 각 랜섬웨어의 파일 암호화키 관리 방법을 미리 숙지하고, 분석 대상을 미리 식별할 수 있어 효율적인 분석이 가능할 것으로 판단된다.

참 고 문 헌

[1] 보안뉴스, “랜섬웨어 공격으로 이랜드 매장 영업 중단사태 발생했다.”, https://www. boannews. com/media/view.asp?idx=92816& kind=1, 2021

[2] 아시아경제, “기아차 美”법인 랜섬웨어 공격받아 232억 비트코인 요구“, https://www.asiae. co.kr /article/2021021820184911105, 2021

[3] 테크데일리, “에이서, 랜섬웨어 피해 몸값은 사상 최대인 5천만 달러“, http://www.techdaily.co.kr /news/articleView.html?idxno=9917, 2021

[4] Cybercrime Magazine, “Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031,” https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/, 2021

[5] ESTsecurity, “Jigsaw 랜섬웨어 복호화 툴 공개”, https://blog.alyac.co.kr/603, 2016

[6] 이세훈, 김소람, 김기윤, 김대운, 박해룡, 김종성, “메모리 분석을 통한 Donut 랜섬웨어 복호화 방안 연구”, *디지털포렌식연구*, 13(1), pp. 13-22, 2019

[7] 신수민, 김소람, 윤병철, 허욱, 김대운, 김기문, 김종성, “5ss5c와 Immuni 랜섬웨어의 암호화 프로세스 분석 및 복구 방안 연구”, *디지털콘텐츠학회논문지*, 21(10), pp. 1895-1903, 2020

[8] Sehoon Lee, Myungseo Park, Jongsung Kim, “Magniber v2 Ransomware Decryption: Exploiting the Vulnerability of a Self-Developed Pseudo Random Number Generator,” electronics, 10(1), pp. 1-17, 2021

[9] ESTsecurity, “WannaCry 랜섬웨어 복호화 툴 공개! 돈을 지불하지 않고도 파일 잠금해제 가능”, https://blog.alyac.co.kr/1105, 2017

〈저 자 소 개〉

박 명 서 (Park Myungseo)

정회원

20013년 2월 : 국민대학교 수학과 졸업

2015년 2월 : 국민대학교 금융정보보안학과 석사

2014년 12월~2017년 2월 : 국가보안기술연구소 연구원

2021년 8월 : 국민대학교 금융정보보안학과 박사

2021년 9월~2022년 2월 : 국민대학교 금융정보보안학과 박사후연구원

2022년 3월~현재 : 강남대학교 ICT융합공학부 조교수

<관심분야> 정보보호, 디지털포렌식