정 보 보 호 학 회 지
제 32 권 제3호, 2022. 6

블록암호 기반 랜섬웨어에 대한 분석 사례 동향

김 준 섭*

요 약

랜섬웨어는 2005년부터 알려지면서 지금까지도 전 세계적으로 큰 피해를 입히며, 사회적으로 심각한 문제를 야기하고 있다. 또한, 랜섬웨어 공격 그룹은 개인보다는 금전적 이익을 크게 얻을 수 있는 기업들을 주로 공격하고 있으며, 이에 대응하기 위해 각 국에서는 랜섬웨어에 대한 대응하는 방법과 정보를 제공하고 있다. 따라서 본 고에서는 많은 비중을 차지하고 있는 블록암호 기반 랜섬웨어에 대한 분석 사례 동향을 살펴보고자 한다.

Ⅰ. 서 론

암호기술은 중요한 정보를 읽기 어려운 값으로 변환하여 제3자가 알아볼 수 없도록 하는 기술로, '고대'에서 '제2차 세계 대전'까지 주로 군사적 목적으로 사용하는 것이 1970년대 들어 컴퓨터 사용이 활발해지면서 컴퓨터를 이용한 암호기술로 발전하였다[1]. 컴퓨터와 통신 기술의 발달에 따라 인터넷 뱅킹, 온라인 결제, 암호 화폐, 소셜 네트워크 서비스, 스마트폰 등 우리의 일상에서 중요 정보를 보호하기 위해 암호기술이 널리 사용되고 있다. 이처럼 암호기술은 우리의 일상에서 없어서는 안 될 정도로 중요한 ICT 인프라 보안의 핵심·기반기술이나, 랜섬웨어(Ransomware) 등 암호기술을 악성코드에 악용하는 암호기술의 역기능 사례도 발생하고 있다.

랜섬웨어는 '몸값'(Ransom)과 '소프트웨어'(Software)의 합성어로 피해자의 시스템이나 데이터를 암호화하여 사용할 수 없도록 만든 뒤, 이를 인질로 금전을 요구하는 악성 프로그램이다. 랜섬웨어는 2005년부터 본격적으로 알려지기 시작해, 2013년 들어 전 세계적으로 급증하고 있다[2]. 글로벌 랜섬웨어 피해금액은 2021년 23조6천억, 2026년 84조3천억, 2031년 312조 7천억으로 피해 규모가 천문학적으로 늘어날 것으로 예측하고 있다[3].

랜섬웨어는 파일 암호화를 위해 블록암호 또는 스트림암호를 이용하고 있으며, 파일 암호화 키는 랜섬웨어 안에 하드 코딩되어 있거나 RSA 등의 비대칭키 알고리즘을 이용하여 공격자에게 전송하고 있다. 이에 본 고에서는 2021년과 2022년 블록암호 기반 랜섬웨어에 대한 동향을 살펴보고, 블록암호 기반 Makop 랜섬웨어에 대한 동작 과정과 암호화 과정을 살펴본다.

본 고의 구성은 다음과 같다. 2장과 3장에서는 2021/2022년 블록암호 기반 랜섬웨어에 대한 분기별로 분석 사례 동향을 살펴보고[4, 5, 6, 7, 8], 4장에서는 2020년에 최초 발견되었지만, 2021년에도 꾸준히 변종을 유포한 Makop 랜섬웨어의 동작 과정과 암호화 과정을 살펴본다. 마지막으로 5장에서 결론으로 마무리한다.

Ⅱ. 2021년 블록암호 기반 랜섬웨어 동향

본 장에서는 2021년에 발견된 블록암호 기반 랜섬웨어에 대한 암호화 과정과 복구 도구 개발 등 분석 사례 동향에 대하여 살펴본다.

2.1. 2021년 1분기 랜섬웨어 동향

Pulse Secure VPN 소프트웨어 취약점을 악용한 Black Kingdom 랜섬웨어는 2020년에 처음 발견되었다. 이 후 2021년 3월 ProxyLogon 공격에 취약한 약 1,500개 Exchange 서버에 배포한 웹 쉘을 발견되었다. 보안 연구원인 Marcus Hutchins가 Black Kingdom 랜섬웨어는 윈도우 실행 파일로 컴파일된 파이썬 스크립트임을 밝혔다[9].

* 한국인터넷진흥원 디지털보안산업본부 융합보안단 차세대암호융합팀 (책임연구원, jskim@kisa.or.kr)

Black Kingdom 랜섬웨어는 해시함수를 사용하여 암호키를 생성하고 파일 암호화 시 AES256-CBC 암호 알고리즘을 사용한다. 영어 대문자와 소문자로 구성된 64개 문자열을 랜덤하게 생성한 후 해시함수 MD5로 해싱하여 암호키를 생성한다. 암호키 생성 후에는 AES256-CBC 암호 알고리즘으로 암호화를 수행한다. 마지막으로 파일 공유 시스템에 암호키를 전송한다. 2021년 3월 23일 이후에는 파일 공유 시스템에 접근할 수 없어 하드 코딩된 암호키를 통해 암호화하므로 이 경우에는 데이터 복구가 가능하다.

현재 공개된 Black Kingdom 랜섬웨어 복구도구는 없지만 Microsoft가 Exchange 서버를 대상으로 하는 사이버 공격을 완화하기 위해 one-click mitigation tool을 개발하였다[10].

Sarbloh 랜섬웨어는 2021년 3월에 처음 발견되었다. Malwarebytes, Cyble, QuickHeal을 포함한 많은 보안 회사에서 발견하였으며, 정치적 메시지가 포함된 악성 워드 문서를 통해 배포되고 있다. 미국의 보안 연구원 Michal Gillespie에 의하면 해당 랜섬웨어는 오픈소스 랜섬웨어인 KhalsaCrypt를 기반으로 제작되었다.

Sarbloh 랜섬웨어는 AES128-CBC 암호 알고리즘을 사용하여 파일을 암호화한다. 파일 암호화에 사용한 암호키는 RSA 암호 알고리즘으로 암호화된다[11]. 현재 복구도구는 공개되어 있지 않다.

2.2. 2021년 2분기 랜섬웨어 동향

전 세계 기업을 대상으로 공격하는 Lorenz 랜섬웨어는 2021년 4월에 처음 발견되었으며, Windows 도메인 관리자의 크리덴셜을 이용하여 유포되고 있다. Lorenz 랜섬웨어는 파일을 암호화하기 전에 피해자의 데이터를 탈취하고 협상에 응하지 않는 경우에 탈취한 데이터를 공개한다. 실제로 공격자는 다크 웹에서 데이터 유출 사이트를 운영하며, 데이터 복구 비용 지불을 거부한 피해자의 데이터를 사이트에 공개하고 있다. ID Ransomware의 Michael 연구원은 해당 랜섬웨어의 암호화 동작이 이전에 발견된 ThunderCrypt 랜섬웨어와 유사하지만 두 종의 랜섬웨어가 동일한 랜섬웨어인지 아니면 변종인지는 확실하지 않다고 밝혔다[12].

Lorenz 랜섬웨어는 AES128-CBC 암호 알고리즘을 사용하여 피해자의 파일을 암호화한다. CryptDeriveKey 함수를 사용하여 암호키를 생성하며 파일 암호화 후에 RSA 암호 알고리즘으로 암호키를 암호화한다[13]. 암호화된 암호키는 일반적인 랜섬웨어와 달리 암호화된 파일의 앞에 추가된다. 암호화된 파일 암호키 앞에는 “.sz40” 문자열을 추가하여 구분한다. 암호화가 완료되면 감염된 파일의 확장자 뒤에 “.Lorenz.sz40” 문자열을 추가한다.

2021년 6월, 네덜란드 사이버 보안회사 Tesorion의 연구원들은 Lorenz 랜섬웨어 복구 도구를 개발하였다[14].

2.3. 2021년 3분기 랜섬웨어 동향

전 세계 다양한 산업 분야에서 활동하는 기업을 대상으로 공격하는 LockFile 랜섬웨어는 2021년 7월 20일에 처음 발견되었다. 정확한 유포 경로는 확인되지 않았으나 보안 연구원 Kevin Beaumont에 따르면 ProxyShell 취약점을 이용하여 Microsoft Exchange 서버에 접근하여 유포한 것으로 추측하고 있다[15]. 공격자는 특정 IP 주소(209.14.0[.]234)를 이용하여 서버에 접근하였으며 LockFile 랜섬웨어의 제어하에 있는 원격 NTLM 릴레이에 대한 인증을 강제하기 위해 새로운 PetitPotam 방법을 이용하여 기업의 도메인 컨트롤러를 장악하였다.

LockFile 랜섬웨어는 WastedLocker 랜섬웨어, Maze 랜섬웨어처럼 파일을 암호화하기 위해 Memory Mapped File Input/Output(I/O)을 이용한다. 그리고 간헐적 암호화(Intermittent Encryption) 방식을 이용하여 파일을 16 bytes마다 한 번씩만 암호화함으로써 랜섬웨어 보호 솔루션에 쉽게 탐지되지 않는다[16]. LockFile 랜섬웨어는 AES 암호 알고리즘으로 암호화하며, 파일의 16 bytes 크기의 영역을 암호화한 후 다음 16 bytes 크기의 영역은 암호화하지 않는 간헐적 암호화 방식을 사용한다. 이때, 파일의 처음 블록 일부는 암호화하지 않아 다른 랜섬웨어와 차별된다.

2021년 10월, Jiri Vinopal은 AtomSilo 랜섬웨어의 취약점을 이용하여 랜섬웨어 몸값을 지불하지 않고도 파일을 복구할 수 있다고 알렸으며, 그 이후 LockFile 랜섬웨어 정보도 분석하여 공개하였다. Avast社는 이러한 정보를 이용하여 LockFile 랜섬웨어 복구 도구를 개발하였다[17].

2.4. 2021년 4분기 랜섬웨어 동향

2021년 9월에 처음 발견된 AtomSilo 랜섬웨어는 브라질의 한 제약회사를 공격하였고, 해당 기업으로부터 탈취한 900GB 크기의 데이터를 공개하였다. 해당 랜섬웨어는 Atlassian 社에서 개발한 자바 기반의 상용 위키 소프트웨어인 컨플루언스(Confluence)의 서버에 대한 취약점을 이용하여 접근권한을 획득하고 공격을 수행한다[18].

AtomSilo 랜섬웨어는 파일을 암호화하기 위해 XOR과 AES 암호 알고리즘을 사용하며[19], ‘AESKEYGENASSIST’ 인스트럭션을 이용하여 AES 라운드 키를 생성한다. 암호키의 크기는 240bytes이며 첫 32bytes는 페이로드에 의해 무작위로 생성되고, 나머지 208bytes는 ‘AESKEYGENASSIST’ 인스트럭션을 통해 생성된다. AtomSilo 랜섬웨어는 파일 암호화 시 파일 전체를 암호화하지 않는다. 대상 파일의 첫 16bytes를 암호화한 후, 다음 32bytes는 그대로 남겨두고 다음 16 bytes를 암호화하는 방식을 반복하여 파일을 암호화한다. AES 암호키는 RSA 암호 알고리즘으로 암호화되어 암호화된 파일 끝(End of File)에 저장된다.

2021년 10월, LockFile 랜섬웨어와 함께 AtomSilo 랜섬웨어 복구 도구를 개발하였다[17].

Ⅲ. 2022년 블록암호 기반 랜섬웨어 동향

본 장에서는 2022년 1분기에 발견된 블록암호 기반 랜섬웨어에 대한 암호화 과정과 복구 도구 개발 등 분석 사례 동향에 대하여 살펴본다.

3.1. 2022년 1분기 랜섬웨어 동향

연방정보기술보안청(BSI)의 내부 보고서에 따르면 BlackCat 랜섬웨어 그룹은 독일 북부에서 수백 개의 주유소를 운영하는 독일 석유 기업 2개를 공격하였다. 해당 기업들은 식별되지 않은 게이트웨이를 통해 BlackCat 랜섬웨어에 감염되었다. 2개 기업 중 하나인 Oiltanking 社는 이번 랜섬웨어 공격으로 인해 석유 공급에 차질이 생겨 모든 방법을 동원하여도 손해의 발생을 막을 수 없다고 밝혔다[20, 21]. 이밖에도 BlackCat 랜섬웨어는 이탈리아 패션 브랜드인 Moncler 社, 스위스 항공 서비스 기업 Swissport 社 등 다양한 기업을 대상으로 공격하였다[22, 23].

BlackCat 랜섬웨어는 파일 암호화 시 AES 블록 암호 또는 ChaCha20 스트림 암호를 사용한다. 자동 모드(Auto)에서 랜섬웨어 실행파일은 AES 블록 암호의 암·복호화에 대해 하드웨어 가속 지원 여부를 검사한다. 지원하는 경우 AES 블록 암호를 사용하고 그렇지 않은 경우 ChaCha20 스트림 암호를 사용한다[24]. 사용한 암호키는 RSA-2048 공개키 암호로 암호화된다. 현재 복구도구는 공개되어 있지 않다.

2022년 1월 26일, DeadBolt 랜섬웨어 공격이 최고조에 달했을 때 인터넷에 있는 13만 개의 QNAP 社 장비 중 4,988개의 장비가 해당 랜섬웨어에 감염되었다[25]. QNAP 社는 문제를 해결하기 위해 펌웨어를 업데이트 하였고, 이후 몇 달 동안은 DeadBolt 랜섬웨어에 감염된 장비는 300대 미만으로 줄어들었다. DeadBolt 랜섬웨어 공격 그룹은 QNAP 社 NAS 장비의 제로 데이 취약점을 이용하여 공격 중이라고 주장하고 있다.

DeadBolt 랜섬웨어는 파일을 암호화하기 위해 AES-128 블록 암호를 사용한다. Emsisoft 社는 DeadBolt 랜섬웨어 복구 도구를 개발하였다.

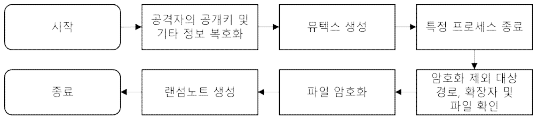
Ⅳ. Makop 랜섬웨어 분석

본 장에서는 2020년에 발견되었지만, 2021년에도 꾸준히 변종을 유포하고 있는 Makop 랜섬웨어의 동작 과정과 암호화 과정을 살펴본다,

Makop 랜섬웨어는 다양한 랜섬웨어를 유포시킨 비너스락커(VenusLocker) 그룹에서 유포한 것으로 추정하고 있으며, 이력서로 위장한 피싱 메일을 통해 공격하고 있다[26]. 2020년 4월에 처음 등장하였지만 2021년 9월(현재)까지도 꾸준히 변종을 생성해내며 유포하고 있다. 기업들이 직원 채용을 하는 기간에 맞춰 채용 담당자를 목표로 해 유포하는 특징이 있다[27]. 또한, 백신 탐지 등을 우회하고자 이중 압축을 한 후 파일을 유포한다.

4.1. 동작 과정

Makop 랜섬웨어의 전체적인 동작 과정은 그림 1과 같다.



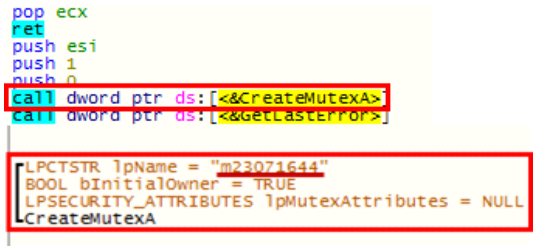
〔그림 1〕 Makop 랜섬웨어의 전체 동작 과정

4.1.1. 공격자의 공개키 및 기타 정보 복호화

Makop 랜섬웨어는 악성코드 실행을 위해 필요한 정보와 공격자의 RSA-1024 공개키를 AES-256 암호 알고리즘으로 암호화한 상태로 가지고 있으며, 랜섬웨어 실행파일 내부에 하드코딩 된 AES-256 암호키로 복호화한다. 해당 정보는 뮤텍스 이름, 암호화 제외 대상 경로/파일/파일 확장자 목록 등을 포함하고 있다.

4.1.2. 뮤텍스 생성

Makop 랜섬웨어는 파일의 중복 암호화를 방지하기 위해 그림 2와 같이 뮤텍스(Mutex)를 생성한다. 생성된 뮤텍스 이름은 ‘m23071644’이다.



〔그림 2〕 Makop 랜섬웨어의 뮤텍스 생성

4.1.3. 암호화 제외 대상 확인

Makop 랜섬웨어는 “Windows”, “system32”, “ProgramData”, “all users”, “caches” 등의 특정 경로를 암호화 대상에서 제외한다. 그 다음 “exe”, “dll”와 같이 알려진 확장자뿐만 아니라 “makop”, “zbw”, “shotlock” 등 특정 확장자 파일을 암호화 대상에서 제외한다. 마지막으로 “boot.ini”, “ntldr”, “io.sys” 등의 특정 파일을 암호화 대상에서 제외한다.

4.1.4. 특정 프로세스 종료

Makop 랜섬웨어는 표 1과 같이 암호화 대상 파일

〔표 1〕 종료 대상 프로세스

msftesql .exe	sqlagent .exe	sqlbrowser .exe	sqlservr .exe	sqlwriter .exe	oracle.exe
ocssd.exe	dbsnmp .exe	synctime .exe	agntsrvc .exe	mydesktop qos.exe	isqlplussvc .exe
xfssvccon .exe	mydesktop service.exe	ocautoupds .exe	encsvc.exe	firefoxconfig .exe	sqbcore service.exe
ocomm.exe	mysqld.exe	mysqld-nt .exe	mysqld-opt .exe	dbeng50 .exe	tbirdconfig .exe
excel.exe	infopath .exe	msaccess .exe	mspub.exe	onenote .exe	outlook .exe
powerpnt .exe	steam.exe	thebat.exe	thebat64 .exe	thunderbird .exe	visio.exe
winword .exe	wordpad .exe				

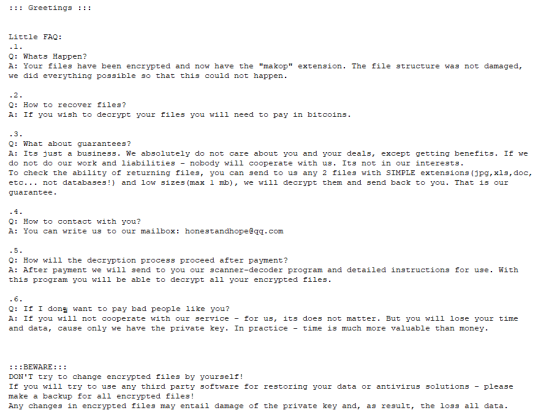
에 대한 접근 권한을 제한할 수 있는 프로세스를 종료한다.

4.1.5. 공격자의 공개키 및 기타 정보 복호화

Makop 랜섬웨어는 고정 디스크, 이동식 디스크, 네트워크 드라이브를 대상으로 파일 암호화를 수행한다. 이때, Microsoft CryptoAPI에서 제공하는 함수를 사용하여 AES-256-CBC 암호 알고리즘으로 파일을 암호화한다. 암호화된 파일에는 ‘[8글자 헥사값].[honestandhope@qq.com].makop’ 형태의 확장자가 추가된다. 8글자 헥사값은 Product ID를 기반으로 생성된다.

4.1.6. 공격자의 공개키 및 기타 정보 복호화

Makop 랜섬웨어는 파일 암호화가 완료된 후 그림


::: Greetings :::

Little FAQ:
.1.
Q: Whats Happen?
A: Your files have been encrypted and now have the "makop" extension. The file structure was not damaged, we did everything possible so that this could not happen.

.2.
Q: How to recover files?
A: If you wish to decrypt your files you will need to pay in bitcoins.

.3.
Q: What about guarantees?
A: Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will cooperate with us. Its not in our interests.
To check the ability of returning files, you can send to us any 2 files with SIMPLE extensions(jpg,xls,doc, etc... not databases!) and low sizes(max 1 mb), we will decrypt them and send back to you. That is our guarantee.

.4.
Q: How to contact with you?
A: You can write us to our mailbox: honestandhope@qq.com

.5.
Q: How will the decryption process proceed after payment?
A: After payment we will send to you our scanner-decoder program and detailed instructions for use. With this program you will be able to decrypt all your encrypted files.

.6.
Q: If I dont want to pay bad people like you?
A: If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause only we have the private key. In practice - time is much more valuable than money.

:::BEWARE:::
DON'T try to change encrypted files by yourself!
If you will try to use any third party software for restoring your data or antivirus solutions - please make a backup for all encrypted files!
Any changes in encrypted files may entail damage of the private key and, as result, the loss all data.

〔그림 3〕 Makop 랜섬웨어의 뮤텍스 생성

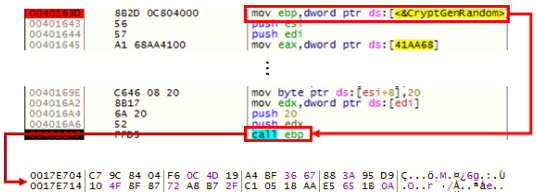
3과 같이 이메일 주소, 경고 문구 등이 포함된 랜섬노트를 생성한다. 랜섬노트명은 'readme-warning.txt'이다.

4.2. 암호화 과정

Makop 랜섬웨어의 파일 암호화 과정은 그림 4와 같다.

4.2.1. 파일 암호키 생성

Makop 랜섬웨어는 그림 5와 같이 CryptoAPI의 CryptGenRandom 함수를 사용하여 32 Bytes 크기의 랜덤한 값을 2개 생성하고 이를 파일 암호키로 사용한다. 파일 암호화 시 파일 암호키 2개를 번갈아가며 사용한다.



〔그림 5〕 파일 암호키 생성

4.2.2. 파일 암호키 암호화

Makop 랜섬웨어는 CryptImportKey 함수를 사용하여 실행파일 내부에 하드코딩된 상태인 공격자의 공개키를 가져온다. 해당 키는 파일 암호키 2개를 각각 RSA-1024 암호 알고리즘으로 암호화하는데 사용된다. 이때 0x80 크기로 고정된 구조체 형태로 암호화된다.

〔표 2〕 AES 암호키 저장 구조체

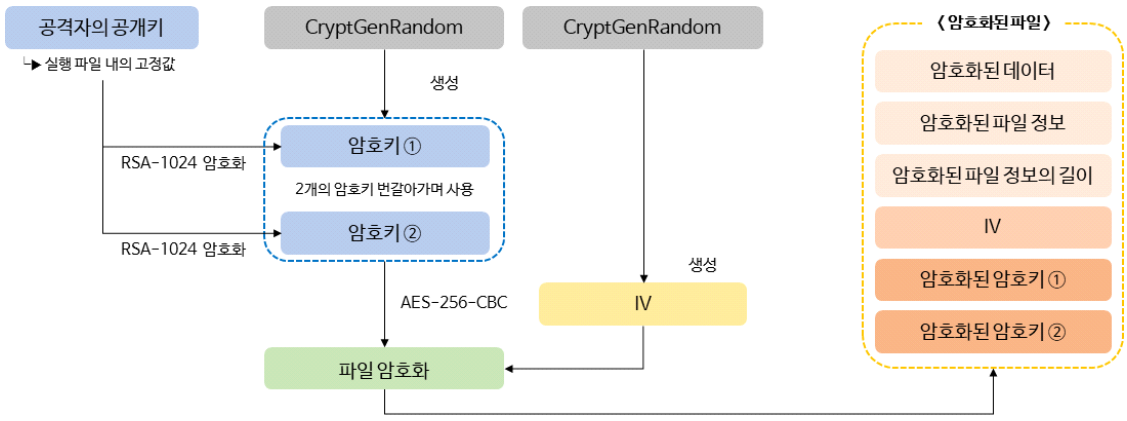
크기 (Bytes)	의미	비고
0x8	고정값	0xADAD37A1
0x4	암호화된 파일명에 포함되는 랜덤 8글자	ProductID를 기반으로 생성된 값
0x4	0 또는 랜덤값	
0x4	플래그	3 또는 4
0x20	AES 파일 암호키	
0x4	CRC32	
0x4C	패딩	0x0000...0000

4.2.3. IV 생성

Makop 랜섬웨어는 CryptGenRandom 함수를 사용하여 랜덤한 값을 생성한다. 그리고 생성한 값을 CryptSetKeyParam 함수를 사용하여 IV로 설정한다. IV 값은 파일마다 다른 값으로 사용된다.

4.2.4. 파일 정보 암호화

Makop 랜섬웨어는 암호화 대상 파일의 정보를 구조체 형태로 저장한 후 AES-256 암호 알고리즘으로 암호화한다. 구조체 크기는 가변적이며 그림 6과 같이 아래의 수식에 따라 결정된다.



〔그림 4〕 Makop 랜섬웨어의 파일 암호화 과정

o 구조체 크기 = LCM((파일 이름 길이 * 2) + 0x1C, 0x10)

〔그림 6〕 Makop 랜섬웨어의 구조체 크기

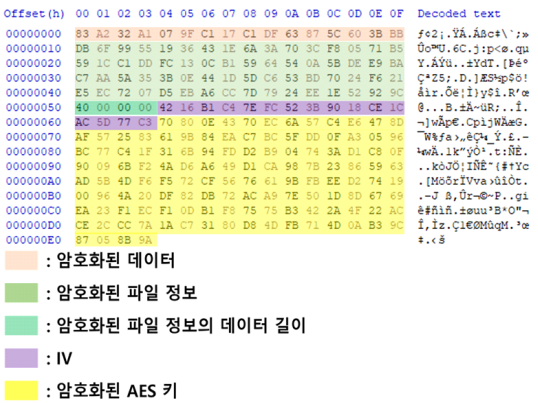
구조체는 결정된 크기만큼 고정값(0x0DF0ADBA)으로 초기화된다. 이후 표 3과 같이 데이터를 덮어씌우며, 파일 정보의 크기가 구조체 크기보다 작은 경우 고정값으로 초기화된 값 일부가 구조체에 그대로 남아 있다.

〔표 3〕 파일 정보 저장 구조체

크기 (Bytes)	의미	비고
12	고정값	0x0
4	원본 파일 크기	Little-Endian
4	고정값	0x0
4	원본파일 이름 길이(Bytes)	
가변	원본 파일명	Unicode
4	CRC32	
가변		파일 정보의 크기가 16의 배수가 아닌 경우 존재

4.2.5. 파일 데이터 암호화

Makop 랜섬웨어는 AES-256 암호 알고리즘으로 파일 데이터를 암호화한다. 암호화된 파일 데이터와 앞서 암호화된 파일 정보를 결합하여 암호화된 파일을 생성한다. 암호화된 파일의 구조는 그림 7과 같다.



〔그림 7〕 암호화된 파일 구조

V. 결 론

본 고에서는 2021년/2022년 블록암호 기반 랜섬웨어에 대한 분석 사례 동향을 살펴보고, Makop 블록암호 기반 랜섬웨어에 대한 동작 과정과 암호화 과정을 살펴봤다. 블록암호 기반 랜섬웨어를 확인해보면, 랜섬웨어 안에 파일 암호화 키가 하드코딩된 경우에는 해당 키를 이용하여 복구 도구를 개발하였거나, 암호화 과정 시 취약점으로 인해 파일 암호화 키가 복구 가능한 경우 복구 도구를 개발하였다. 그러나 RSA 암호 알고리즘을 이용하여 파일 암호화 키를 암호화하여 공격자에게 전송하였다면, 공격자가 파일 암호화 키를 공개하지 않는 이상 복구 도구이 불가능하다. 이처럼 랜섬웨어 방식이 점점 분업화 전문화되고 있기 때문에 랜섬웨어에 감염될 경우 이를 다시 복구하기 어렵다. 따라서 사용자들은 과기정통부·KISA의 랜섬웨어 피해 예방 5대 수칙에 따라 랜섬웨어 피해 예방을 위해 노력을 기울여야 하겠다.

참 고 문 헌

[1] KISA 암호이용활성화, “https://seed.kisa.or.kr/”
[2] 네이버 지식백과, “https://terms.naver.com/e ntry.naver?docId=3581192&cid=59088&categoreyId=59096/”
[3] KISA, “2021년 랜섬웨어 스페셜 리포트”, 2021
[4] KISA, “2021년 1분기 랜섬웨어 동향 보고서”, 2021
[5] KISA, “2021년 2분기 랜섬웨어 동향 보고서”, 2021
[6] KISA, “2021년 3분기 랜섬웨어 동향 보고서”, 2021
[7] KISA, “2021년 4분기 랜섬웨어 동향 보고서”, 2021
[8] KISA, “2022년 1분기 랜섬웨어 동향 보고서”, 2022
[9] Alyac Blog, “https://blog.alyac.co.kr/3654”
[10] Microsoft Security Response Center, “htt ps://msrc-blog.microsoft.com/2021/03/15/one-click-microsoft-exchange-on-premises-mitigation-tool-march-2021/”
[11] Quick Heal Blog, “https://blogs.quickhe l.com/act

ivists-turn-hacktivists-new-ransomware-that-does-not-demand-money/“
[12] Alyac Blog, “https://blog.alyac.co.kr/3770”
[13] Tesorion, “https://www.tesorion.nl/en/po sts/lorenz-ransomware-analysis-and-a-free-decryptor/“
[14] The Record, “https://therecord.media/free-decrypter-available-for-lorenz-ransomware/”
[15] Bleeping Computer, “https://www.bleepi ngcomputer.com/news/security/lockfile-ransomware-uses-petitpotam-attack-to-hijack-windows-domains/“
[16] SOPHOS, “https://news.sophos.com/en-u s/2021/08/27/lockfile-ransomwares-box-of-tricks-intermittent-encryption-and-evasion/“
[17] Avast, “https://decoded.avast.io/threatin tel/decryptor-for-atomsilo-and-lockfile-ransomware/”
[18] SOPHOS NEW, “https://news.sophos.co m/en-us/2021/10/04/atom-silo-ransomware-actors-use-confluence-exploit-dll-side-load-for-stealthy-attack/“
[19] Zscaler, “https://www.zscaler.com/blogs/ security-research/atomsilo-ransomware-enters-league-double-extortion/“
[20] BlackCat ransomware implicated in attack on German oil companies, ZDNet, “https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/“
[21] Major German oil supplier confirms cyber-attack −“Oiltanking” says incident has crippled inland supply, The Stack, “https://thestack.technology/oiltanking-cyber-attack/?utm_source=rss&utm_medium=rss&utm_campaign=oiltanking-cyber-attack&mid=1#cid=452270/“
[22] Moncler group becomes the first victim of ALPHV (BlackCat) RaaS following the data leak, “https://www.secureblink.com /cyber-security-news/moncler-group-becomes-the-first-victim-of-alphv-(blackcat)-raas-following-the-data-leak/“
[23] BlackCat (ALPHV) claims Swissport ransomware attack, leaks data, Bleeping Computer, “https://www.bleepingcomput er.com/news/security/blackcat-alphv-claims-swissport-ransomware-attack-leaks-data/“
[24] ALPHV BlackCat - This year's most sophisticated ransomware, Bleeping Computer, “https://www.bleepingcomput er.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/“
[25] Deadbolt Ransomware is Back, “https://censys.io/deadbolt-ransomware-is-back/“
[26] 보안뉴스, “https://www.boannews.com/media/view.asp?idx=100516/”
[27] AhnLab, “https://asec.ahnlab.com/ko/27 025/”

〈저 자 소 개〉

김 준 섭 (Jun-Sub Kim)
정회원
2010년 2월 : 순천향대학교 정보보호학과 졸업
2012년 2월 : 순천향대학교 정보보호학과 석사
2015년 2월 : 순천향대학교 정보보호학과 박사
2015년 3월~2016년 1월 : 성균관대학교 IT융합연구원 박사후연구원
2016년 2월~2016년 11월 : 한국지역정보개발원 책임연구원
2017년 3월~현재 : 한국인터넷진흥원 책임연구원
<관심분야> 정보보호, 암호 알고리즘