정 보 보 호 학 회 지
제 29 권 제6호, 2019. 12

# 2019 국내·외 주요 및 신규 랜섬웨어 동향 분석

박 은 후*, 김 소 람*, 이 세 훈*, 김 종 성**

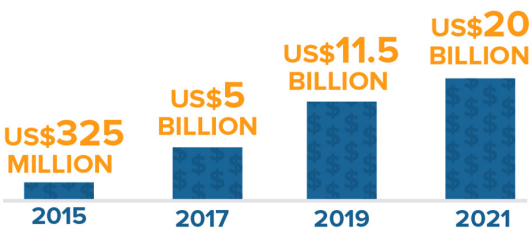
요 약

랜섬웨어(Ransomware)는 몸값(Ransom)과 소프트웨어(Software)의 합성어로 사용자 시스템을 장악하여 중요 문서 및 파일을 암호화하고 암호화된 파일의 복호화를 대가로 가상 화폐를 요구한다. 랜섬웨어로 인한 피해는 매년 증가하고 있으며 새로운 랜섬웨어의 등장과 변종의 출현이 빈번하다. 이에 본 논문은 2019년에 등장하거나 영향을 주고 있는 랜섬웨어에 대한 유포방법, 유포 대상, 알고리즘 사용 현황을 밝히고 국내·외 피해 사례를 소개한다. 그리고 분기 별로 감염율 상위 5개의 랜섬웨어를 살펴보고 평균 요구 금액에 대해 기술한다. 마지막으로 주요 및 신규 랜섬웨어 대해 유포 경로, 특징, 암호화 알고리즘, 복호화 요소 및 복호화 도구에 대해서는 표로 요약하며 자세히 서술한다.

## Ⅰ. 서 론

‘Cybercrime magazine’에 따르면 전 세계 랜섬웨어 피해 금액은 2015년은 324만 달러, 2017년에는 50억 달러, 2019년은 115억 달러로 매년 증가하고 있으며 계속 증가할 것으로 전망하고 있다(그림 1)[1]. ‘한국랜섬웨어침해대응센터’에 따르면 국내 랜섬웨어의 피해 규모 또한 2015년에는 1,090억 원에서 2018년에는 1조 500억 원으로 약 10배 증가하였다[2].

2019년에 새롭게 등장한 랜섬웨어의 수는 작년에 비해 55% 감소했지만, 기존 랜섬웨어에서 파생된 랜섬웨어는 77% 증가하였다[3]. 변종 랜섬웨어는 기존의 랜섬웨어와 비슷한 유포방법을 사용하거나 암호화 알고리즘 및 취약점이 같을 확률이 높다. 따라서 기존 랜섬웨어의 특징을 파악하고, 변종 랜섬웨어와의 차이점을 분석할 필요가 있다.




(그림 1) 전 세계 랜섬웨어 피해 금액

## Ⅱ. 2019 랜섬웨어 특징

본 장에서는 2019년에 자주 사용되거나 새롭게 나온 랜섬웨어의 유포방법, 유포 대상의 변화와 사용한 암호화 알고리즘 현황에 대해 살펴본다.

### 2.1. 랜섬웨어 유포방법

2019년에 주로 사용된 유포방법은 [표 1]과 같이 원격 데스크톱 프로토콜 (RDP, Remote Desktop Protocol), 이메일 피싱(Email Phishing)과 소프트웨어 취약점(Software Vulnerability) 이다[4,5,6].

랜섬웨어를 유포하는 데에 원격 데스크톱 프로토콜이 가장 많이 사용되지만, 그 비율이 점차 감소하고 있는 것에 반해 이메일 피싱과 소프트웨어 취약점을 이용한 유포는 증가하고 있다.

원격 데스크톱 프로토콜은 Windows OS에 기본적으로 탑재된 프로토콜로 Windows 시스템에 원격으로 연결하기 위해 사용된다. 올해에는 원격 데스크톱 프로토콜의 최신 보안 업데이트가 적용되지 않은 시스템을 대상으로 RDP 원격코드 실행 취약점(CVE-2019-0708)이 새롭게 발견되기도 하였다. 원격 데스크톱 프로토콜은 사용하기에 쉽고 해킹된 시스템을 완전히 장악할 수 있

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2019R1F1A1060634).
** 국민대학교 금융정보보안학과 (ehoo410@kookmin.ac.kr, kimsr2040@kookmin.ac.kr, dreamtree304@kookmin.ac.kr)
** 국민대학교 금융정보보안학과, 정보보안암호수학과 (jskim@kookmin.ac.kr)

〔표 1〕 1,2,3분기 랜섬웨어 유포방법 별 비율

| | 1분기 | 2분기 | 3분기 |
|---|---|---|---|
| RDP | 63.5% | 59.1% | 50.6% |
| Email Phishing | 30.4% | 34.1% | 39.0% |
| Software Vulerability (Exploit Kit) | 6.1% | 6.8% | 8.1% |

다는 점에서 랜섬웨어 유포에 많이 활용되고 있다. LockCrypt, Crisis, Samsam과 Phobos를 포함한 다양한 랜섬웨어가 이 방법을 이용하여 유포되었다.

이메일 피싱은 공격자가 랜섬웨어를 포함하고 있는 파일을 첨부한 메일을 불특정 다수 또는 특정 사용자에게 보내 수신자가 직접 악성 파일을 실행하도록 유도하는 방법이다. 다양한 사회공학적 기법을 이용하여 메일 수신자를 쉽게 속일 수 있다는 점에서 지속적으로 사용되고 있다. 5월에 활동한 Sodinokibi를 포함한 다양한 랜섬웨어가 이 방법을 이용하여 유포되었다.

소프트웨어 취약점은 소프트웨어를 개발할 때 결함이 될 수 있는 논리적인 오류나 버그를 의미한다. 이러한 취약점을 이용하여 공격을 자동화하는 소스코드 및 도구가 익스플로잇 킷이다. 이를 악용하면 정보를 유출하거나 데이터를 변경할 수 있어 랜섬웨어의 유포방법으로 사용되고 있다. 올해는 폴아웃(Fallout) 익스플로잇 킷의 최신 버전이 나타났으며 제로데이 취약점이 추가되었다. 1월에 등장한 Vidar이 이 방법을 사용하여 유포되었다.

하나의 유포방법만을 사용하는 것이 아니라 여러 가지 유포방법을 융합해서 사용하는 랜섬웨어가 등장하였다. 그 예로는 Sodinokibi와 Nemty, Nemty Revenge v2가 이메일 피싱과 익스플로잇 킷을 이용하여 유포된 바가 있다. 이는 5장에서 자세히 다룬다.

### 2.2. 유포 대상의 변화

‘2018년 정보보호 실태조사 결과’에 따르면 랜섬웨어의 피해를 경험한 기업의 비율이 2016년에는 18.7%, 2017년은 25.5%, 2018년에는 53.6%로 증가하였다[7]. 기존의 랜섬웨어는 주로 개인을 대상으로 유포되었다. 하지만 주기적인 OS 패치, 백신 프로그램 업데이트 등 다양한 방법으로 랜섬웨어 감염을 방지하고 있고 피해를 받더라도 금액을 지불하지 않는 경우가 많아 이로 인한 수익이 감소하였다. 이에 공격자들은 유포 대상을 개인 사용자에서 기업으로 변경하고 있다. 또한, 2019년에는 기업 뿐만 아니라 네트워크 스토리지(NAS, Network Attached Storage)를 대상으로 공격하는 랜섬웨어가 등장하였다.

2019년 랜섬웨어는 제조업이나 공공기관과 같은 기업을 목표로 공격하는 랜섬웨어가 다수 출현하였다. 그 예로는 2019년 3월에 노르웨이 알루미늄 회사인 Norsk나 Hydro가 LockerGoga에 감염되었으며 국내 주요 제조 기업이 Clop에 감염되어 일부 기업이 시스템 내부, 백업 시스템에 피해를 본 사건이 있다.

하반기에는 기존의 개인용 PC가 아닌 네트워크 스토리지를 대상으로 하는 랜섬웨어가 등장하였다. eCh0raix 랜섬웨어는 초기에 QNAP 사의 NAS만을 공격 대상으로 하였으나, 하반기부터는 Synlogy 사의 NAS와 Lenovo사의 Lomega NAS 피해사례도 보고되었다.

### 2.3 암호 알고리즘 사용 현황

본 절에서는 2019년에 등장한 랜섬웨어 중 사용한 암호 알고리즘이 밝혀진 것을 대상으로 사용 현황을 살펴본다.

2019년에 가장 많이 사용된 암호화 알고리즘은 AES와 RSA 알고리즘이다. 그 외 기타 알고리즘으로는 Chacha20이나 Salsa20과 같은 스트림 암호와 타원 곡선 암호 알고리즘인 ECIES (Elliptic Curve Integrated Encryption Scheme)가 있다.

2019년에 사용한 알고리즘을 ‘AES, RSA 알고리즘 모두 사용’, ‘AES 알고리즘을 사용’, ‘기타’ 총 3가지로 나누어 정리한 결과는 [표 2]와 같다. 그 결과 22종이 AES와 RSA를 모두 사용하였으며, 18종은 AES만 사용하였고 나머지 12종이 기타 알고리즘을 사용하였다.

〔표 2〕 2019 랜섬웨어 암호화 알고리즘 사용 현황

| 알고리즘 | 랜섬웨어 명 | |
|---|---|---|
| AES, RSA 알고리즘 모두 사용 (22종) | LockerGoga | Tellyouthe pass |
| | Gotcha | Gandcrab (v1~v3) |
| | JSWorm | SCR |

| 알고리즘 | 랜섬웨어 명 | |
|---|---|---|
| AES, RSA 알고리즘 모두 사용 (22종) | Koratos | JCry |
| | Major | Croc |
| | Phobos | Djvu |
| | HildaCrypt | Viagra |
| | JSWorm 4.0 | COOT |
| | MedusaLocker | Mike |
| | D00mEd | Pay-or-Lost |
| | InfoDot | HDMR |
| AES 알고리즘을 사용 (18종) | Marozka | CrazyCrypt 2.1 |
| | Chech | Gorgon |
| | Rapid | Blitzkrieg |
| | LooCipher | Basillisque Locker |
| | Ims00rry | ZeroFucks |
| | Syrk | PyLock |
| | SYRK | Muhstik |
| | GeBigBosRoss | CCryptor |
| | Noos | Lulz |
| 기타 (12종) | Cr1ptT0r | Chacha |
| | Jokeroo | GandCrab (v4~v5.2) |
| | Sodinokibi | Maze |
| | Clop | Relock |
| | Koko (Mailto) | ERIS |
| | Estemani | OnyxLocker |

## Ⅲ. 국내·외 랜섬웨어 피해사례

본 장에서는 2019년에 발생했던 국내·외 랜섬웨어 피해사례에 대해 서술한다.

### 3.1. 국내

2019년 5월 11일, 국내 학원 관리 프로그램 DB가 Frogo 랜섬웨어에 감염되었다[8]. 해당 프로그램 개발 업체는 일부 고객의 DB 서버는 복구하는데 성공했지만 출석 연동, 모바일 알림 톡 결제, 가상계좌 등의 일부 연동 기능들은 사용이 불가능했다. 서버 복구를 위해 해커와 두 차례 걸쳐 협상했지만 1차 협상만 성공했으며, 감염된 9대의 서버 중 1대를 복구하는 데에 성공하였다. 해커가 요구한 금액에 대해서는 알려진 바가 없다.

2019년 8월에 우리 은행을 사칭하는 이메일을 통해 특정 기관이 Sodinokibi 랜섬웨어에 감염되었다[9]. 공격자는 '지불 정지·우리 은행'이라는 제목을 사용하였으며 메일에는 압축 파일인 '우리_은행.zip'이 첨부되어 있었다. 이를 압축 해제하면 '결제 정보-세부 정보가 잘못 입력되었습니다'라는 제목의 MS 워드 파일이 있다. 그러나 이 파일의 실제 형식은 exe 실행 파일로 내용을 확인하기 위해 파일을 실행하면 암호화가 수행된다. 해커가 요구한 금액 및 피해 현황에 대해서는 알려진 바가 없다.

### 3.2. 국외

2019년 3월, 조지아주 잭슨 카운티 시 정부의 컴퓨터들이 Ryuk 랜섬웨어에 감염되어 업무가 마비되었다[10,11]. 이로 인해 압출 공정이 중단되었으며 모든 공장과 운영 네트워크가 글로벌 네트워크로부터 분리되었다. 이 과정에서 일부 자동화 공정이 수동으로 전환되었으며, 그 결과 전 세계 알루미늄 가격이 변동되었다. 해당 랜섬웨어 감염으로 인한 피해액은 약 4,100만 달러로 알려져 있다.

미국 볼티모어시는 5월에 Robbinhood의 공격을 받았다[12]. 이로 인해 공항, 병원과 현금 자동 인출기 등의 서비스 장애를 겪었다. 또한, 상수도나 교통 요금 납부 서비스가 불가능하여 오프라인으로 진행되었다. 공격자는 PC 복호화를 대가로 최대 13비트코인을 요구하였다.

## Ⅳ. 분기별 주요 활동 랜섬웨어

1,2,3분기에 전 세계적으로 활동한 랜섬웨어를 순위별로 정리한 결과는 [표 3]과 같다. 각 분기에 새롭게 등장한 랜섬웨어는 굵게 표시한다.

각 분기의 상위 5개의 랜섬웨어는 70% 이상을 차지한다. Ryuk는 2,3분기 연속해서 1위를 유지하고 있다. Sodinokibi, Phobos의 감염 비율이 증가하고 있으며 Dharma와 Gandcrab은 감소하였다.

1분기에는 Dharma, Gandcrab, Ryuk가 가장 많이 활동하였다. 그리고 1월에 처음 등장한 Phobos가 4위를 차지하였다. Dharma는 2016년에 처음 출현하였으며 같은 해에 등장한 Crysis 랜섬웨어의 변종이다. 주로 이메일 피싱을 통해 유포되며 컴퓨터를 실행하는데 필요한 파일들을 제외한 모든 파일을 가리지 않고 암호화

〔표 3〕 1,2,3분기 랜섬웨어 순위

| 순위 | 1분기 | | 2분기 | | 3분기 | |
|---|---|---|---|---|---|---|
| | 랜섬웨어 | 비율 | 랜섬웨어 | 비율 | 랜섬웨어 | 비율 |
| 1 | Dharma | 27.8 | Ryuk | 23.9 | Ryuk | 22.2 |
| 2 | Gandcrab | 20.0 | Phobos | 17.0 | Sodinokibi | 21.1 |
| 3 | Ryuk | 18.3 | Dharma | 13.6 | Phobos | 19.9 |
| 4 | **Phobos** | 5.2 | **Sodinokibi** | 12.5 | Dharma | 8.8 |
| 5 | Rapid | 5.2 | Gandcrab | 10.2 | GlobeImposter | 5.3 |

비율의 단위는 %

하여 큰 피해를 준다. 복호화를 위해 평균 9,742달러를 요구한다고 알려져 있다. Gandcrab은 2018년 초에 등장하여 지속적으로 발전해왔으며 평균 7,994달러를 요구한다. 같은 해 8월에 활동하기 시작한 Ryuk는 지능형 표적 공격(APT, Advanced Persistent Threat)으로 유포된다. 전 세계의 대형 기업을 대상으로 감염시키며 평균 28만 6,556달러를 요구한다.

2분기는 Ryuk, Phobos와 Dharma가 가장 많이 활동하였다. 새롭게 등장한 Sodinokibi가 4위 차지하였으며 활동 종료를 선언한 Gandcrab의 비율은 절반으로 감소하였다. Ryuk는 전 분기에 비해 감염 비율이 증가하였으며 26만 7,742달러로 가장 많은 금액을 요구하는 것으로 알려졌다. Phobos는 비율이 약 3배 이상 증가하였으며 평균 13,925달러를 요구한다. Dharma의 감염 비율은 약 2배 감소하였으며 평균 13,295달러를 요구한다. Sodinokibi는 랜섬웨어 감염 순위는 4위지만 피해 요구액은 2위인 56,577달러를 기록하였다.

3분기는 Ryuk, Sodinokibi, Phobos 순으로 가장 많이 활동하였으며 Dharma는 계속해서 비율이 감소하여 4위를 차지하였다. 5위를 기록한 GlobeImposter 랜섬웨어는 2017년에 처음 등장하였으며 주로 이메일 피싱으로 유포된다. Ryuk는 지속적으로 감염 비율이 증가하고 있으며 평균 37만 7,026만 달러로 전 분기 대비 요구하는 금액이 증가하였다. Sodinokibi와 Phobos는 각각 15만 7,445달러와 31,864달러를 요구한다.

〔표 4〕 2019년 주요 및 신규 랜섬웨어 월별 요약

| 등장 시기 | 랜섬웨어 | 유포 경로 | 특징 | 암호화 알고리즘 | 복호화 요소/도구 |
|---|---|---|---|---|---|
| 1월 | LockerGoga | 멀버타이징 | - Boost C++ Libraries 사용 | RSA-1024<br>AES-128-CTR | X |
| | Gorgon | - | - FilesLocker 변종<br>- 분석 방해 (코드 난독화)<br>- 한글 랜섬노트 | AES | X |
| | RickRoll Lcoker | 이메일 피싱 | - Aurora 변종<br>- 오프라인 상태에서 암호화 가능 | RSA-2048 | O |
| | Phobos | RDP 취약점 | - 파일 크기 1.5MB 이상은 암호화하지 않음 | AES-256-CBC<br>RSA-1024 | X |
| | Anatova | 위장 애플리케이션 | - 네트워크 공유 자원 감염<br>- 분석 방해 (코드 난독화)<br>- 탐지 우회 (VM 탐지) | - | X |
| 2월 | Clop | 이메일 피싱<br>APT | - 탐지 우회 (유효한 인증서 사용)<br>- 특정 언어 암호화 대상 제외<br>- 공유 드라이브 파일 암호화<br>- 기업을 대상으로 유포됨 | RC4<br>RSA | X |
| | B0r0nt0k | 사회 공학적 기법 | - 파일 암호화 후 Base64 인코딩<br>- 랜섬노트 없음<br>- 기업(웹 사이트, 서버) 대상으로 유포됨 | - | X |
| | Cr1ptT0r | D-Link DNS-320 NAS 백도어 | - 사용된 256 비트의 공개키가 로그 파일에 저장됨<br>- NAS를 대상으로 유포됨 | Curve25519<br>Salsa20<br>Poly1305 | X |

| 등장 시기 | 랜섬웨어 | 유포 경로 | 특징 | 암호화 알고리즘 | 복호화 요소/도구 |
|---|---|---|---|---|---|
| 2월 | Gandcrab (v5.2) | 이메일 피싱 | - 탐지 우회 (가짜 인증서 포함)<br>- 실행중인 백신 프로그램 기록<br>- 특정 프로세스 강제 종료<br>- 시스템 정보 탈취<br>- 볼륨 섀도 복사본 삭제 | RSA-2048<br>Salsa20 | O |
| 3월 | Rapid 변종 | - | - 1분마다 재실행하여 새 파일도 암호화 | AES | X |
| | JNEC.a | 익스플로잇 킷 | - 분석 방해 (VM 탐지)<br>- 재부팅 후 실행 파일 자동실행<br>- 마지막 접근 14일 이내 파일만 암호화<br>- Gmail을 이용해 복호화 암호키 전달 | - | X |
| | djvu | 가짜 소프트웨어 | - 개인 정보 탈취 | AES-256-CFB<br>RSA | -/O |
| | JCry | 어도비 플래시 플레이어 업데이트 메시지 | - Go 언어로 개발됨 | AES-128-GCM | X |
| 4월 | Specialist | 익스플로잇 킷<br>멀버타이징<br>드라이브 바이 다운로드 | - Magniber 변형<br>- 국내 URL을 통해 유포됨<br>- C&C 서버와의 통신을 숨기기위해 다수 IP 접속 | - | X |
| | Sodinokibi | 익스플로잇 킷<br>이메일 피싱 | - 감염된 시스템을 대상으로 Gandcrab v5.2 추가 설치<br>- 프로세스 종료<br>- 시스템 정보 탈취<br>- 볼륨 섀도 복사본 삭제 | Salsa20<br>ECIES | X |
| 5월 | Maze | 익스플로잇 킷 | - ChaCha 랜섬웨어 변종 | Chacha20<br>RSA-2048 | X |
| 6월 | LooCipher | 이메일 피싱 | - 원본 파일의 크기를 0KB로 변화시킴<br>- 고정 문자열을 이용한 랜덤키 생성 | AES-128-ECB | O |
| 7월 | eCh0raix | 무차별 대입 공격 | - Go 언어로 개발됨<br>- NAS를 대상으로 유포됨 | AES-256-CFB | O |
| | LuckyJoe | - | - C와 파이썬 언어로 개발됨<br>- Linux 기기를 대상으로 공격함 | AES-256-CBC<br>RSA-2048 | - |
| 8월 | Sodinokibi 변종 | 이메일 피싱 | - 한국 IP를 사용하여 유포됨<br>- 유포 시, 저장된 쿠키값과 암호 화폐 지갑 관련 정보 추가 수집<br>- 랜섬노트에 한글 추가 | Salsa20<br>ECIES | X |
| | Nemty | 이메일 피싱<br>익스플로잇 킷 | - 감염 대상 국가 확인 후, PC 정보를 공격자에게 전송 | AES-128-CBC<br>RSA-2048<br>RSA-8192 | O |
| | JSWorm | - | - C++ 언어로 개발됨<br>- MS Excel 사용 시 랜섬노트 자동실행 | AES-256<br>RSA-4096 | O |
| 10월 | Nemty Revenge v2 | 이메일 피싱<br>익스플로잇 킷 | - 감염 대상 국가 확인 후, PC 정보를 공격자에게 전송 | - | X |
| | FuxSocy | - | - Cerber 랜섬웨어와 유사 | - | - |

O : 존재함, X : 존재하지 않음, - : 알려지지 않음

## Ⅴ. 2019 국내·외 주요 및 신규 랜섬웨어

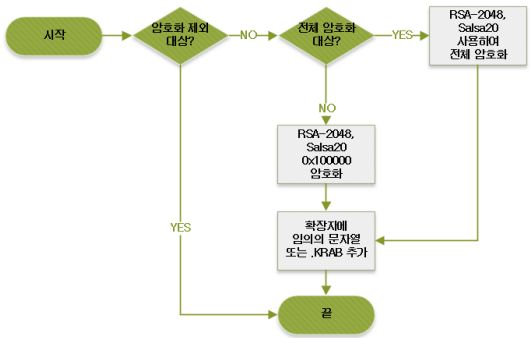
본 장에서는 올해 새롭게 등장하거나 기존 랜섬웨어의 변종 랜섬웨어 24종을 대상으로 유포방법, 동작 특징, 복호화 도구 및 복호화 요소 여부를 요약한다[표 4]. 그리고 그 중, 전 세계적으로 큰 피해를 입히거나, 암호화하는 파일 중 '.hwp'가 포함되고 한국에 피해사례가 존재하는 등 한국을 대상으로 활동한 랜섬웨어를 선별하여 자세히 서술한다.

### 5.1. Gandcrab v5.2

2018년 1월에 처음 출현한 Gandcrab은 서비스형 랜섬웨어(RaaS, Ransomware as a Service)로 다크웹을 통해 판매 및 유통되었으며, 지속적으로 새로운 변종을 등장시켜 전 세계를 위협하였다. 2019년 1분기에 국내에서도 Gandcrab이 가장 많이 탐지되었다[13]. Gandcrab은 이메일 피싱, 웹 어플리케이션의 취약점을 이용한 워터링 홀, 멀버타이징 등의 다양한 방식을 사용하여 유포된다.

Gandcrab의 동작 과정은 (그림 2)와 같다. [표 5]와 같이 암호화 대상 확장자에 'hwp'가 있으며 이를 통해 암호화 대상 국가에 한국이 포함되어 있음을 알 수 있다.

Gandcrab v5.2는 2019년 2월에 등장하였으며 [표 6]과 같이 v5와 v5.1과는 확장자, 사용하는 알고리즘, 백신 무력화 기능 유무 등 다양한 점이 같지만 내부 코드,




(그림 2) Gandcrab의 동작 과정

〔표 5〕 Gandcrab 감염 대상 파일 확장자 일부

| |
|---|
| , .fodt, .fountain, .fpt, .frt, .fwd, .fwdn, .gmd, .gpd, .gpn, .gsd, .gthr, .gv, .hbk, .hht, .hs, **.hwp**, .hz, .idx, .iil, .ipf, .ipspot |

〔표 6〕 Gandcrab 버전별 비교

| | v5 | v5.1 | v5.2 |
|---|---|---|---|
| 등장 시기 | 2018. 9. | 2019. 1. | 2019. 2. |
| 유포 경로 | 멀버타이징, 익스플로잇 킷, RDP Brute-force, Botnets | | |
| 확장자 | 임의의 문자열 or .KRAB | | |
| 암호화 알고리즘 | RSA-2048, Salsa20 | | |
| 백신 무력화 여부 | O | | |
| 바탕화면 | 암호화 후, 랜섬웨어 메시지로 변경됨 | | |
| 복호화 도구 | O | | |
| 특징 | HTML 형식의 랜섬노트 사용 | 바탕화면 파일명 변경 | - 닷넷(.NET) 외형으로 유포<br>- 탐지 우회<br>- 내부 코드 변경<br>- 랜섬노트명 변경 |

유포 외형과 랜섬노트 명이 다르다.

Gandcrab은 백신 탐지를 우회하기 위해 다양한 파일 외형을 이용하여 유포된다. v5와 v5.1은 UPX (Ultimate Packer for eXecutables)로 실행 압축된 형태이었지만 v5.2는 '.NET' 외형을 사용하여 유효하지 않은 가짜 인증서를 포함한다. 그리고 샌드박스 탐지 회피를 위해 Sleep 함수 호출을 통해 실행을 지연시킨다. 여러 번의 Sleep 호출 이후에는 RUNPE 방식으로 '.NET' 내부에 있는 Gandcrab을 실행시킨다.

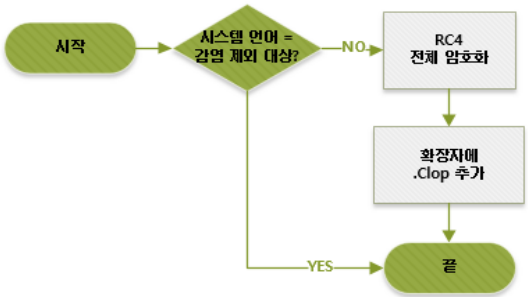
Gandcrab은 2019년 6월에 RaaS 운영 중단을 밝혔으며 v5.2까지 모두 복호화 가능하다[14]. 도구는 BitDefender에 공개되어 있으며 사용하기 위해서는 네트워크가 연결되어있어야 하며 경로를 지정하거나 시스템을 검사한 후, 암호화된 파일을 복호화할 수 있다.

### 5.2. Phobos

2019년 1월에 발견된 Phobos는 2016년에 발견된 Dharma와 Crysis 랜섬웨어의 변종이다[15]. Dharma 랜섬웨어는 2016년 11월에 등장하였으며 Crysis 랜섬웨어를 기반으로 만들어진 패밀리 랜섬웨어다. Phobos는 원격 데스크톱 프로토콜의 취약한 비밀번호 사용자들을 대상으로 사전공격 및 무작위 대입 방식을 통해

PC에 접근한 후, 사용자도 모르게 악성 파일을 실행시켜 유포한다[16].

Phobos 동작 과정은 (그림 3)과 같으며 11월 기준, 밝혀진 복호화 가능 요소 및 도구는 존재하지 않는다.

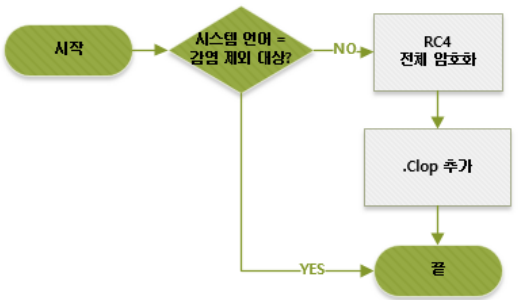



(그림 3) Phobos 동작 과정

### 5.3. Clop

2019년 2월에 국내를 대상으로 등장한 Clop은 악성 메일을 이용하여 사전에 중앙관리 서버 (AD, Activity Directory) 환경의 관리자 계정을 확보한 관리 서버에 연결된 시스템에 랜섬웨어를 삽입하는 APT 방식으로 유포된다[17].

Clop의 동작 과정은 (그림 4)와 같다. Clop은 프로세스들의 점유율이 높아 암호화를 실패하는 것을 방지하기 위해 실행되자마자 많은 프로세스들을 검색한 후 종료한다는 특징이 있다. 또한, 다른 랜섬웨어와는 다르게 유효한 저자 서명을 포함하고 있어 백신 탐지를 우회한다는 점에서 주목할 필요가 있다. 11월 기준, 복호화 가능 요소 및 개발된 복호화 도구는 없다.



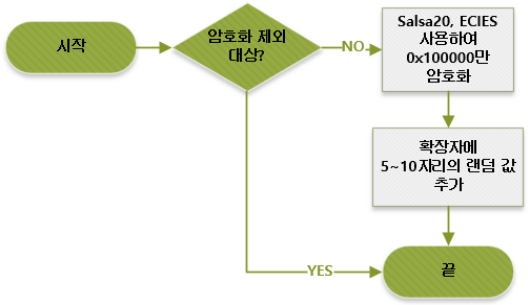

(그림 4) Clop 동작 과정

### 5.4. Sodinokibi / Sodinokibi 변종

2019년 4월에 발견된 Sodinokibi는 스피어 피싱, 익스플로잇 킷, 웹 로직 취약점 등의 다양한 방법을 통해 유포되고 있다. 또한 암호화에 사용하는 키, 변경되는 확장자 정보를 레지스트리에 저장하며 Gandcrab 유사한 유포방법을 사용한다[18]. 취약점을 이용하여 유포하고 있어 사용자가 직접 랜섬웨어를 실행하지 않더라도 취약한 시스템을 사용하고 있으면 자동으로 감염될 수 있다.

Sodinokibi의 동작 과정은 (그림 5)와 같다. 2019년 8월 말에 유포방법, 수집 정보 및 랜섬노트가 업데이트된 Sodinokibi 변종이 유포되었다[19]. 기존에는 구글 지메일이나 호스팅을 직접 구축해서 악성 메일을 보냈던 것에 반해, KT와 같은 한국 IP를 통해 메일을 발송하여 유포하였다. 또한, 이전에는 악성 실행 파일을 메일에 첨부하여 파일을 실행하면 바로 Sodinokibi가 설치되었지만 변종은 브라우저에 저장된 쿠키 값과 암호화폐 지갑 관련 정보를 추가 수집한 후 설치된다. 랜섬노트와 변경되는 바탕화면에는 영어 메시지 외에 한국어와 중국어 문구가 포함되었다.

Sodinokibi는 2019년 6월에 활동을 종료한 Gandcrab과 코드가 유사하다. 그리고 이메일 내 첨부파일, 멀버타이징, 익스플로잇 킷, WordPress 취약점을 악용한 포털 검색 상위 노출을 통해 유포된다는 점이 같다. 두 랜섬웨어를 혼용하는 공격도 발견되고 있으며 유포 시 사용된 메일의 형태가 비슷하다는 점에서 주의가 요구된다. 11월 기준, 복호화 가능 요소 및 복호화 도구는 없다.

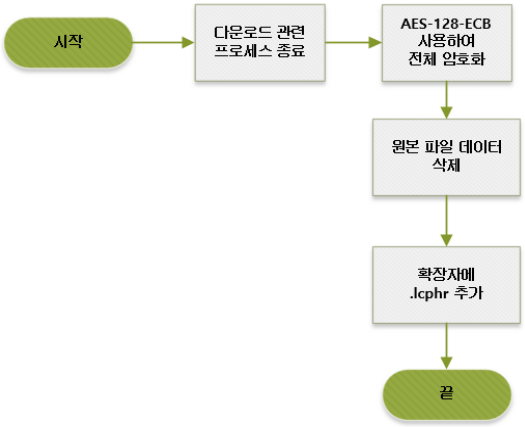



(그림 5) Sodinokibi 동작 과정

### 5.5. LooCipher

LooCipher는 2019년 6월에 MS 워드 문서인 'Info_BSV_2019.docm'을 통해 유포되었다[20]. 동작 과정은 (그림 6)과 같다.

LooCipher 복호화 도구는 2019년 7월에 Emsisoft에서 개발하여 공개하였다. 복호화하기 위해서는 암호화된 파일과 원본 파일이 필요하며 전수 조사를 통해 암호키를 찾아 복호화한다.

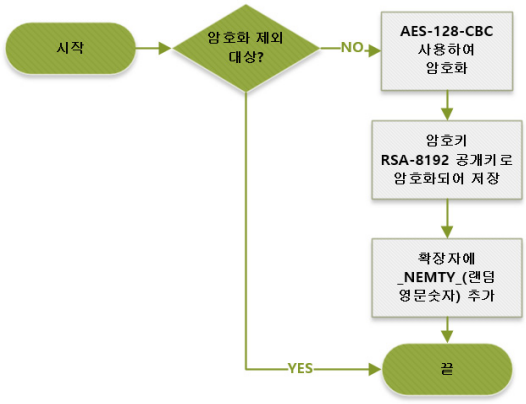



(그림 6) LooCipher 동작 과정

### 5.6. Nemty / Nemty Revenge v2

Nemty는 2019년 8월에 원격 데스크톱 프로토콜과 악성 메일을 이용하여 처음 유포되었으며 9월에는 RIG 익스플로잇 킷을 사용하였다[21,22]. 악성 메일은 한글로 작성되어 있으며 첨부된 압축 파일의 내부에는 아이콘이 한글 문서나 우편인 포트폴리오와 이력서가 있다. 이는 악성 실행 파일로, 실제 확장자와 가짜 확장자 사이의 긴 공백과 가짜 아이콘을 이용하여 정상 파일인 것처럼 위장한 것이다.

10월 초 Tesorion 회사에서 복호화 도구인 Nemty Decryptor를 공개하였다[23]. Tesorison은 랜섬웨어 개발자들이 복호화 도구를 분석하여 자신들이 사용한 알고리즘의 취약한 점을 파악하는 것을 막기 위해 Tesorison 서버에서 복호화 키를 생성하여 도구로 보낸다. 11월 기준, 도구가 지원하는 복호화 가능한 버전은 1.4와 1.6이며 도구를 사용하기 위해서는 암호화된 파일 중 'docx, gif, pdf, png, pptx, xlsx, zip' 확장자를



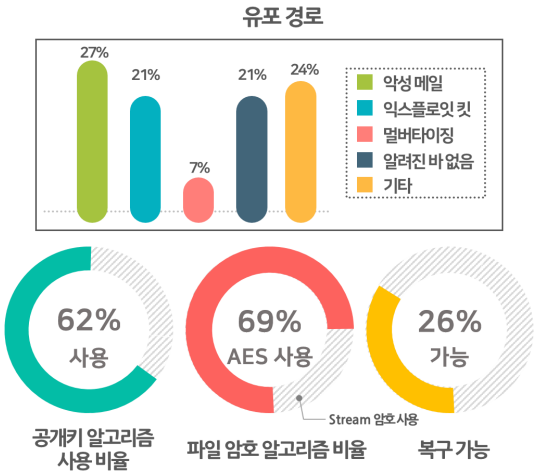

(그림 7) Nemty 동작 과정

〔표 7〕 Nemty 복호화 가능 대상 확장자 일부

| |
|---|
| avi, bmp, gif, mp3, jpeg, jpg, mov, mp4, qt, 3qp, mpeg, mpg, doc, docb, docm, docx, dotm, dotx, dot, ole, pot, pps, ppt, wbk, xlm, xls, xlsb, xlt, pdf, png, tif, tiff, pptm, pptx, xlsm, xlsx, xltm, xltx, zip |

가진 파일들을 업로드해야한다. 복호화 가능 대상 확장자는 [표 7]과 같다.

10월 29일, Nemty Revenge v2가 경력직 입사지원서로 위장하여 등장하였다[24]. 메일의 제목으로 다양한 지원자의 이름을 사용하였지만, 내부 내용은 같다. 기존 버전과 마찬가지로 가짜 확장자와 실제 확장자 사이에 긴 공백을 넣어 파일을 위장하고 있다. 기존의 랜섬노트는 'NEMTY PROJECT V1.X'로 시작하며 복호




(그림 8) 2019 주요 및 신규 랜섬웨어 특징

화를 위해 브라우저에 공격자가 정한 URL을 입력하도록 안내하였다. 하지만 Revenge v2는 'NEMTY REVENGE 2.0'으로 시작하며 공격자가 지정한 이메일 주소로 메일을 전송해야 한다.

Nemty는 한글로 작성된 메일 내부에 악성 첨부 파일 열람 및 악성 링크 클릭을 유도하여 랜섬웨어 파일을 실행시킨다는 점에서 기존의 Gandcrab이나 Sodinokibi와 유사하다.

## Ⅵ. 결 론

본 논문은 2019년에 주로 사용한 유포 방법, 대상 및 암호화 알고리즘을 살펴보았다. 그리고 올해 등장한 신규 및 주요 랜섬웨어 24종의 유포방법, 유포 대상 변화 및 암호화 알고리즘 사용 현황에 대해 요약하였다. 또한, 국내·외 피해 사례와 분기별 랜섬웨어 감염 비율 및 복호화를 대가로 요구하는 금액을 조사하였다. 마지막으로 24종의 랜섬웨어 중 주목해야 할 랜섬웨어를 선별하여 자세히 기술하였다.

올해는 2018년부터 지속적으로 큰 피해를 주던 Gandcrab의 활동이 종료되면서 후속 랜섬웨어로 주목받고 있는 Sodinokibi와 Nemty와 Gandcrab의 공통점을 언급하였다.

24종 랜섬웨어의 특징을 정리하면 (그림 8)과 같다. 유포 경로는 악성 메일과 익스프로잇 킷이 각각 27%와 24%로 가장 높았다. 사용한 알고리즘 중 62%가 공개키 알고리즘을 사용하였으며 파일 암호화에는 AES를 69%로 가장 많이 사용하였다. 또한 복구 가능한 랜섬웨어는 26%로 RickRoll Locker, Gandcrab, djvu, LooCipher, eCh0raix, JSWorm이 있다.

## 참 고 문 헌


[1] Financesonline, https://financesonline.com/cybersecurity-statistics/

[2] Boannews, https://www.boannews.com/media/view.asp?idx=74441

[3] Trendmicro, 2019 중간 보안 위협 보고서, 2019.

[4] Coveware, https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases

[5] Coveware, https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

[6] Coveware, https://www.coveware.com/blog/q3-ransomware-marketplace-report

[7] 과학기술정보통신부, "2018년 정보보호 실태조사 결과", 2019.

[8] Boannews, https://www.boannews.com/media/view.asp?idx=79785&page=1&kind=1

[9] Boannews, https://www.boannews.com/media/view.asp?idx=82485

[10] Bleeping Computer, https://www.bleepingcomputer.com/news/security/ransomware-attack-on-jackson-county-gets-cybercriminals-400-000/

[11] EST security, https://blog.alyac.co.kr/1944

[12] Etnews, https://www.etnews.com/20190607000209

[13] Ahnlab, blog.ahnlab.com/ahnlab/2448

[14] Bitdefender, https://labs.bitdefender.com/2019/06/good-riddance-gandcrab-were-still-fixing-the-mess-you-left-behind/

[15] Zdnet, https://www.zdnet.com/article/new-phobos-ransomware-exploits-weak-security-to-hit-targets-around-the-world/

[16] Tachyon ISARC, https://isarc.tachyonlab.com/2501

[17] EST security, https://blog.alyac.co.kr/2212

[18] "2019년 상반기 랜섬웨어 동향", IGLOO security, 2019.

[19] Checkmal, http://blog.checkmal.com/221641761655

[20] Bleeping Computer, https://www.bleepingcomputer.com/news/security/new-loocipher-ransomware-spreads-its-evil-through-spam/

[21] Bleeping Computer, https://www.bleepingcomputer.com/news/security/new-nemty-ransomware-may-spread-via-compromised-rdp-connections/

[22] Bleeping Computer, https://www.bleepingcomputer.com/news/security/nemty-ransomware-gets-distribution-from-rig-exploit-kit/

[23] Bleeping Computer, https://www.bleepingcomputer.com/news/security/nemty-ransomware-decrypt

or-released-recover-files-for-free
[24] Bleeping Computer, https://www.bleepingcomputer.com/news/security/nemty-ransomware-decryptor-released-recover-files-for-free/

## 〈저 자 소 개〉

**박 은 후 (Eunhu Park)**
학생회원
2018년 7월 : 국민대학교 정보보안암호수학과 졸업
2018년 8월~현재 : 국민대학교 금융정보보안학과 석사과정
<관심분야> 디지털포렌식, 데이터분석, 정보보호

**김 소 람 (Soram Kim)**
학생회원
2016년 2월 : 국민대학교 수학과 졸업
2018년 2월 : 국민대학교 금융정보보안학과 석사
2018년 3월~현재 : 국민대학교 금융정보보안학과 박사과정
<관심분야> 디지털포렌식, 정보보호

**이 세 훈 (Sehun Lee)**
학생회원
2019년 2월 : 경북대학교 전자공학부 졸업
2019년 3월~현재 : 국민대학교 금융정보보안학과 석사과정
<관심분야> 디지털포렌식, 정보보호

**김 종 성 (Jongsung Kim)**
종신회원
2000년 8월/2002년 8월 : 고려대학교 수학 학사/이학석사
2006년 11월 : K.U.Leuven, ESAT/SCD-COSIC 정보보호 공학박사
2017년 2월 : 고려대학교 정보보호학원 공학박사
2007년 3월~2009년 8월 : 고려대학교 정보보호기술연구센터 연구교수
2009년 9월~2013년 2월 : 경남대학교 e-비즈니스학과 조교수
2013년 3월~2017년 2월 : 국민대학교 수학과 부교수
2014년 3월~현재 : 국민대학교 일반대학원 금융정보보안학과 부교수
2017년 3월~현재 : 국민대학교 정보보안암호수학과 부교수
<관심분야> 정보보호, 암호 알고리즘, 디지털 포렌식