JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 21, No. 10, pp. 1895-1903, Oct. 2020

Check for updates

5ss5c와 Immuni 랜섬웨어의 암호화 프로세스 분석 및 복구 방안 연구

신 수 민[1] · 김 소 람[2] · 윤 병 철[1] · 허 욱[1] · 김 대 운[3] · 김 기 문[3] · 김 종 성[4*]
[1]국민대학교 금융정보보안학과 석사과정
[2]국민대학교 금융정보보안학과 박사과정
[3]한국인터넷진흥원
[4*]국민대학교 정보보안암호수학과&금융정보보안학과 교수

Analysis of Encryption Processes of 5ss5c and Immuni Ransomware, and Their Data Recovery

Sumin Shin[1] · Soram Kim[2] · Byungchul Youn[1] · Uk Hur[1] · Daeun Kim[3] · Kimoon Kim[3] · Jongsung Kim[4*]

[1]Master's Course, Department of Financial Information, Kookmin University

[2]P.HD student, Department of Financial Information, Kookmin University

[3]Korea Internet & Security Agency

[4*]Full Professor, Department of Information Security, Cryptology, and Mathematics & Financial Information, Kookmin University

[요 약]

랜섬웨어는 저장장치의 중요 파일을 암호화한 후 대가로 금전을 요구한다. 공격자들은 기존에 유포했던 랜섬웨어를 변형하거나 신규 랜섬웨어를 개발하여 꾸준히 피해를 주고 있다. 또한, 백신 프로그램 우회하기도 하며, 탐지를 피하거나 복구 가능성을 낮추기 위해 다양한 기법을 적용한다. 이에 대응하기 위해 랜섬웨어 분석 및 복구 가능 여부에 관한 연구는 필수적이다. 본 논문은 2020년 주요 랜섬웨어인 5ss5c와 Immuni의 암호화 프로세스를 분석하여 복구 가능함을 보인다.

[Abstract]

Ransomware encrypts important files on the storage devices and then requires money. Attackers have been steadily damaging the existing ransomware by transforming it or developing new ransomware. It also bypasses vaccine programs and applies various techniques to avoid detection or reduce possibility of recovery. Therefore it is essential to analyze ransomware. In this paper, we analyze encryption processes of the ransomware 5ss5c and Immuni actively spreaded in 2020, their data recovery.

색인어 : 랜섬웨어, 암호화 프로세스, 복구 가능성, 역공학

Key word : Ransomware, Encryption Process, Possibility of Recovery, Reverse Engineering

http://dx.doi.org/10.9728/dcs.2020.2.10.1895

Received 06 October 2020; **Revised** 20 October 2020
Accepted 20 October 2020

***Corresponding Author; Jongsung Kim**

Tel: +82-2-910-5750
E-mail: jskim@kookmin.ac.kr

Ⅰ. 서 론

랜섬웨어는 초기에는 무차별적으로 유포대상을 선정하다가 최근에는 특정 기업 또는 단체를 목표로 삼아 공격하며, 특히 은행, 병원과 기업 등 시스템을 빠른 시간 내에 복구해야 하는 곳을 표적으로 하여 공격을 수행한다[1]. 이와 같은 이유로 처음 랜섬웨어가 유포된 시기에 비해 피해 금액이 월등히 증가하였다. 한국랜섬웨어침해대응센터에 따르면 랜섬웨어에 의한 국내 피해 금액이 2015년에는 1,000억 원이었지만 2019년을 기준으로 피해 금액이 1조 8,000억 원으로 18배 증가했다[2].

최근 대표적인 피해사례는 다음과 같다. 2020년 9월 칠레 최대 규모 은행인 BancoEstado가 랜섬웨어에 감염되었다[3]. 백도어를 통해 은행 네트워크에 잠입해 설치한 것으로 추측되며, 회사 서버 대부분과 워크스테이션이 암호화되었고 이로 인해 은행을 폐쇄했다. 또한, 같은 달 독일의 뒤셀도르프 대학 병원이 랜섬웨어에 감염되었다[4]. 서버 30대가 모두 암호화되어 환자의 긴급 수술을 진행할 수 없게 되어 환자를 다른 병원으로 옮겼으나 사망했다. 국내의 경우, LG 전자와 SK하이닉스가 랜섬웨어에 감염되어 내부 데이터 일부가 유출되는 사고가 있었다[5]. 랜섬웨어는 더 정교한 기술이 적용되고 공격이 더 지능화되고 있으므로, 랜섬웨어에 대한 분석 및 복호화 방안 연구가 지속적으로 필요하다.

본 논문에서는 2020년 랜섬웨어인 5ss5c와 Immuni에 대한 암호화 프로세스를 분석한다. 2장에는 실행 과정 분석 및 암호화 프로세스 분석결과를 보여주며, 3장에서는 복구 방안을 제시한다. 마지막 4장에서 결론으로 마무리한다.

Ⅱ. 랜섬웨어 실행 과정 및 암호화 프로세스 분석

본 장에서는 5ss5c와 Immuni 랜섬웨어의 실행 과정을 분석하며, 특히 암호화 과정에 초점을 맞춰 살펴본다. 실험에 사용한 샘플 파일은 ANYRUN을 통해 다운받았다[6].

2-1 5ss5c

2019년 11월에 처음 등장한 5ss5c 랜섬웨어는 다운로더를 통해 프로세스를 동작시키고 ExternalBlue 익스플로잇을 사용하여 유포된다[7]. 유포방식과 코드 제작 방식이 Satan 랜섬웨어와 유사하여 해당 랜섬웨어에서 파생된 것으로 추정되고, Satan, DBGer, Lucky와 Iron 랜섬웨어 등을 유포한 집단에서 제작한 것으로 추정된다. 분석에 사용한 5ss5c 랜섬웨어의 해시값은 표 1과 같다.

표 1. 5ss5c 랜섬웨어의 해시값
Table 1. 5ss5c ransomware hash value

MD5	853358339279B590FB1C40C3DC0CDB72
SHA1	84825801EAC21A8D6EB060DDD8A0CD902DCEAD25
SHA256	CA154FA6FF0D1EBC786B4EA89CEFAE022E05497D095C2391331F24113AA31E3C

1) 실행 과정

5ss5c 랜섬웨어의 전체 동작 과정은 그림 1과 같다.

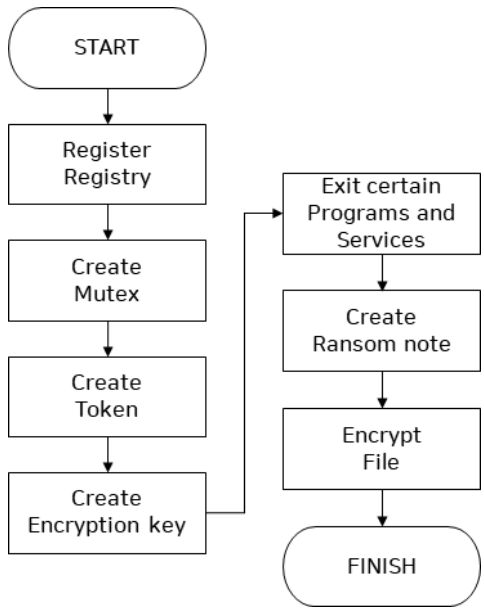


그림 1. 5ss5c 랜섬웨어 동작 과정
Fig 1. Operation process of 5ss5c ransomware

(1) 레지스트리 등록

5ss5c 랜섬웨어의 실행 경로를 레지스트리 "HKEY₩Software₩MicroSoft₩Windows₩CurrentVersion₩Run" 에 등록함으로써 PC 부팅 시마다 랜섬웨어를 자동으로 실행한다.

(2) 뮤텍스 생성

감염대상 PC에 대해 랜섬웨어 실행 시 파일의 중복 감염을 위해 "5ss5c_CRYPT"라는 이름의 뮤텍스를 생성한다.

(3) 토큰 생성

"C:₩ProgramData₩5ss5c_token" 경로에 감염된 PC를 식별하기 위한 토큰이 그림 2와 같이 생성된다. 5ss5c_token 파일이 이미 존재하면 해당 파일을 읽어 토큰으로 사용하며, 없을 경우에만 새로 생성한다. 토큰은 40 bytes 크기이며, 0-9와 A-Z 중에서 랜덤하게 선택한다.

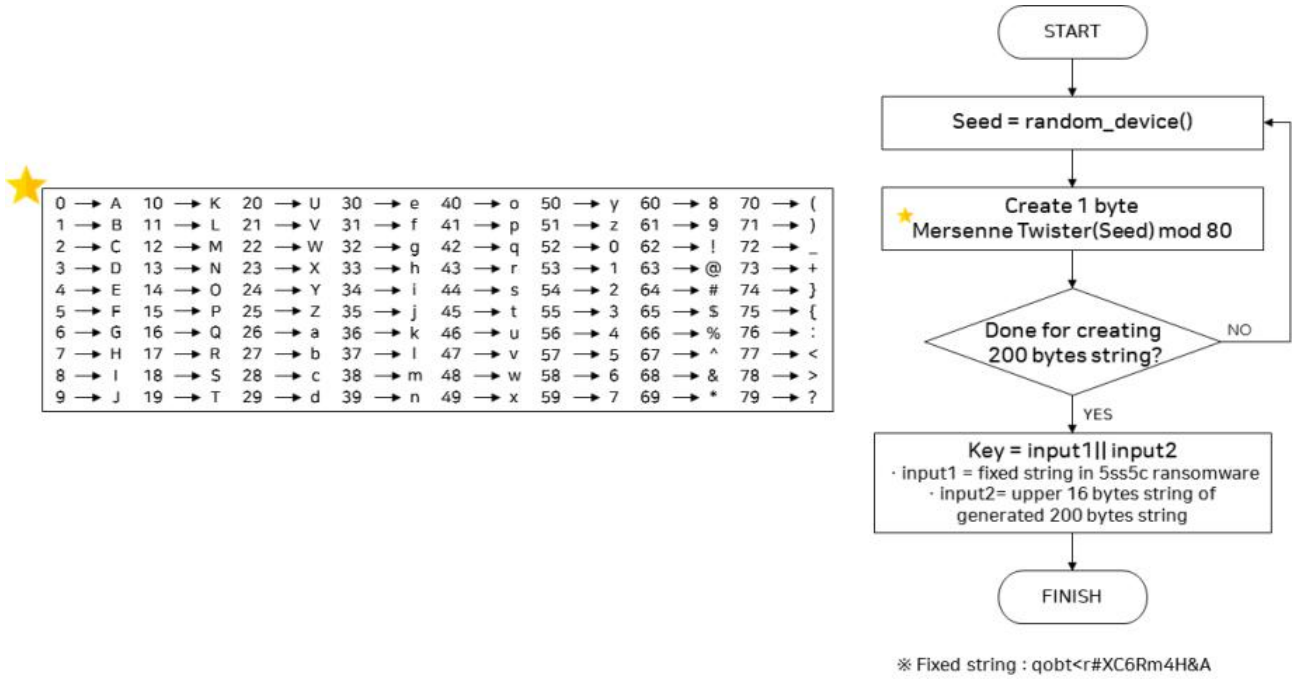


그림 3. 5ss5c 랜섬웨어의 암호키 생성과정
Fig. 3. Generation process of encryption key for 5ss5c ransomware

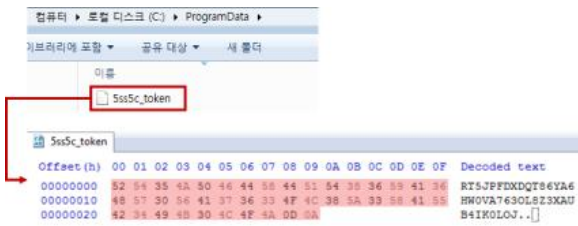


그림 2. 5ss5c 랜섬웨어의 토큰
Fig. 2. 5ss5c ransomware token

(4) 암호키 생성

암호키 생성과정은 그림 3과 같다. random_device 함수를 통해 2 bits의 seed를 생성하여 메르센 트위스터(Mersenne Twister) 알고리즘을 통해 난수를 생성한다. 난수를 modular 80 연산을 거쳐 0부터 79까지의 정수로 계산한 후에 정수를 ASCII 값으로 대응하여 총 200 bytes의 문자열을 생성한다. 마지막으로 실행 파일 내에 고정된 문자열인 16 bytes의 "qobt<r#XC6Rm4H&A"와 생성한 200 bytes 중 상위 16 bytes를 연접하여 암호화 키로 사용한다.

o 암호키 = qobt<r#XC6Rm4H&A || 난수 상위 16 bytes

(5) 특정 프로세스 및 서비스 종료

5ss5c 랜섬웨어는 파일 암호화를 위해 데이터베이스 관련 프로세스와 서비스들을 종료한다. 종료하는 프로세스와 서비스 목록은 표 2와 같다.

표 2. 프로세스 및 서비스 종료 목록
Table 2. Process and service shutdown list

Process list			
Sql	oracle	sqlservr.exe	mysqld.exe
nmesrvc.exe	sqlagent.exe	fdhost.exe	fdlauncher.exe
reportingservicesservice.exe	omtsreco.exe	tnslsnr.exe	oracle.exe
emagent.exe	perl.exe	sqlwriter.exe	mysqld-nt.exe
Service list			
MySQL	MySQLa	SQLWriter	SQLSERVERAGENT
MSSQLFDLauncher	UxSms		

(6) 랜섬노트 생성

랜섬노트는 _如何解密我的文件_.txt로 C:₩ 하위에만 생성되고 다른 경로에는 생성되지 않는다. 내용은 그림 4와 같이 중국어로 작성되어 있으며 일부 파일이 암호화되었다는 문구와 함께 1비트코인을 요구하는 내용이 포함되어있다. 마지막에는 감염 PC마다 생성하는 랜덤 값들을 암호화하여 덧붙인다.

그림 4. 5ss5c 랜섬노트
Fig. 4. 5ss5c ransomnote

랜섬노트에 저장하는 감염 PC 관련 정보는 그림 5와 같다. 암호키 생성 시 사용되는 고정된 16 bytes의 문자열, (4)에서 메르센 트위스터 알고리즘으로 생성한 랜덤한 200 bytes의 문자열과 토큰을 순서대로 연접한다. 연접한 문자열을 실행 파일 내에 하드코딩된 공개키를 사용하여 RSA-4096으로 암호화한다. 암호화된 바이너리 값을 헥사 스트링으로 변환 후 바이트 연산을 거쳐서 나온 결괏값을 base64로 인코딩해 랜섬노트에 저장한다. 바이트 연산은 다음 수식과 같다.

o A = RSA-4096(hardcoreded string||random 200 bytes ||token)

Result = (A[i] XOR 0x19) - 0x7A (i = 0 ~ 1024)

A[i]는 A의 i번째 1 byte 값을 의미한다. 최종적으로 base64로 인코딩된 값을 랜섬노트에 저장한다.

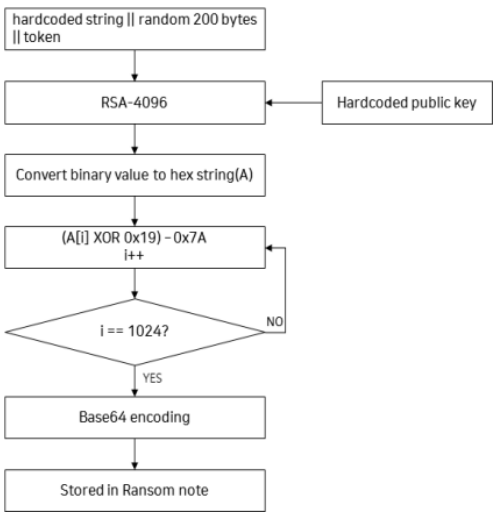


그림 5. 5ss5c 랜섬노트 생성과정
Fig. 5. Creation process of 5ss5c ransom note

(7) 파일 암호화

5ss5c 랜섬웨어는 암호화 전에 감염대상 컴퓨터의 디스크에서 암호화 대상 디렉터리를 선정하여 "C:₩ProgramFiles₩CommonFiles₩System₩tmp" 경로에 그림 6과 같이 저장한다.

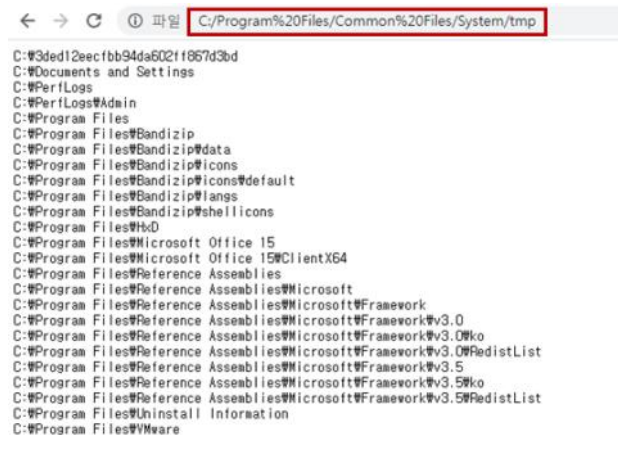


그림 6. 암호화 대상 디렉터리 선정
Fig. 6. Selecting a directory to be encrypted

암호화 제외 대상 디렉터리와 확장자 목록은 표 3과 같다. 윈도우 및 시스템 관련 디렉터리와 중국의 인터넷 보안 회사인 Qihoo360과 관련된 디렉터리는 암호화에서 제외한다.

표 3. 암호화 제외 대상 디렉터리와 확장자 목록
Table 3. List of directory and extension to encryption exclusion

Extension list to exclude encryption	Directory list to exclude encryption
bin, bmp, cab, chm, dat, dll, exe, iso, lib, log, msi, ocx, pbk, pol, sdi, sys, tmp, wim	360rec, 360sec, 360sand, 360safe, 360downloads, favorites, common files, default user, all users, libs, internet explorer, msbuild, public, windows mail, windows media player, windows defender, windows nt, windows photo viewer, windows sidebar, temp

파일 암호화에 대한 자세한 과정은 그림 7과 같다. AES-256-ECB를 이용해 파일 암호화를 수행하며, 패딩을 사용하지 않아 마지막 블록이 16 bytes보다 작은 경우 원본 데이터를 보존한다. 암호화를 마치면 암호화된 데이터 뒤에 (4)에서 생성한 200 bytes를 하드코딩된 공개키를 사용하여 RSA-4096으로 암호화한 값을 덧붙여 감염된 파일을 완성한다. 감염된 파일명은 '[5ss5c@mail.ru]원본 파일명.원본 파일 확장자.토큰.5ss5c'이다.

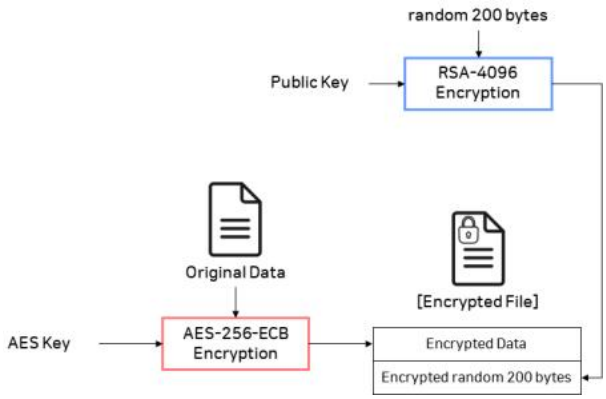


그림 7. 5ss5c 랜섬웨어의 암호화 과정
Fig. 7. Encryption process of 5ss5c ransomware

2-2 Immuni

코로나19 바이러스를 악용한 Immuni 랜섬웨어는 2020년 5월경 유포되었다[8]. Immuni는 이탈리아 정부에서 개발한 코로나 접촉자 추적 애플리케이션 이름이다[9]. 공격자들은 이탈리아 약사 연맹(Federazione Ordini farmacisti Italiani, FOFI) 웹사이트를 위조하여 가짜 웹사이트를 제작했다. 이를 통해 Immuni 애플리케이션의 PC 버전을 다운로드할 수 있다는 메일을 유포해 웹사이트에서 랜섬웨어를 다운받도록 유도한 후 감염시킨다. Immuni 랜섬웨어는 감염 후 변경된 바탕화면에 나타나는 문구와 같이 FUCKUNICORN이라는 이름으로도 불린다. 분석에 사용한 Immuni 랜섬웨어의 해시값은 표 4와 같다.

표 4. Immuni 랜섬웨어의 해시값
Table 4. Hash value of Immuni ransomware

MD5	B226803AC5A68CD86ECB7C0C6C4E9D00
SHA1	110301B5F4ECED3C0D6712F023D3E0212515BF99
SHA256	7980EF30B9BED26A9823D3DD5746CDEFE5D01DE2B2EB2C5E17DBFD1FD52F62BF

1) 실행 과정

Immuni 랜섬웨어의 전체 동작 과정은 그림 8과 같다.

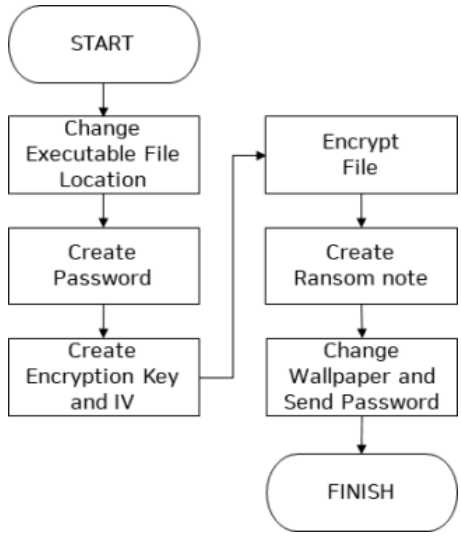


그림 8. Immuni 랜섬웨어 동작 과정
Fig. 8. Operation process of Immuni ransomware

(1) 실행 파일 위치 변경

Immuni 랜섬웨어는 "C:₩<username>₩Rand123" 경로로 실행 파일의 위치를 변경하고 이름을 local.exe로 변경한다. 감염 종료 후에도 실행 파일은 삭제되지 않는다.

(2) 패스워드 생성

패스워드는 암호키와 IV 생성 시 사용되며, 생성과정은 그림 9과 같다. Random 함수를 통해 생성한 4 bytes의 tickcount를 seed로 사용한다. 이를 통해 알파벳 소문자, 대문자, 숫자와 일부 특수문자를 포함한 62개의 문자열에서 15개가 랜덤하게 선택된다. 이때 초기 seed가 동일하면 항상 같은 15자리의 문자열이 생성된다.

```
public string CreatePassword(int length)
{
    StringBuilder stringBuilder = new StringBuilder();
    Random random = new Random();
    while (0 < length--)
        stringBuilder.Append("abcdefghijklmnopqrstuvwxyz
                              ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*!=?()"
        [random.Next("abcdefghijklmnopqrstuvwxyz
                      ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*!=?()".Length)]);
    return stringBuilder.ToString();
}
```

그림 9. Immuni 패스워드 생성과정
Fig. 9. Password generation process of Immuni ransomware

(3) 암호키 및 IV 생성

암호키와 IV를 생성하는 과정은 그림 10과 같다. (2)에서 생성한 패스워드를 SHA-256을 통해 해시값을 계산한다. 계산한 해시값은 키 유도 함수인 PBKDF2 함수의 입력값으로 사용한다. salt는 0x0102030405060708가 고정으로 사용되며, iteration은 1,000회이다. 최종 결괏값의 상위 32 bytes는 암호키로 사용하며, 다음 16 bytes는 IV로 사용한다.

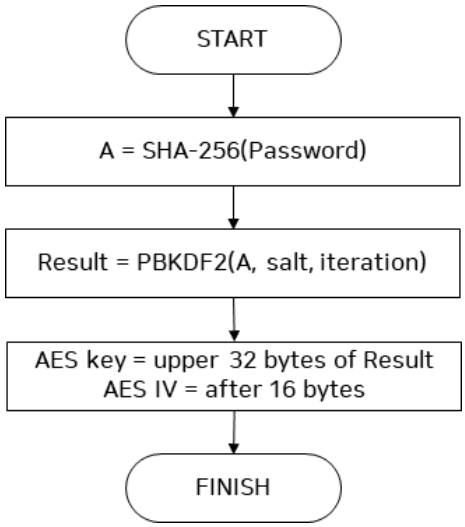


그림 10. Immuni 랜섬웨어 암호키 및 IV 생성과정
Fig. 10. Encryption and IV generation process of Immuni tansomware

(4) 파일 암호화

C 드라이브를 대상으로 암호화가 진행되며, 자세한 암호화 대상 경로 및 확장자는 표 5와 같다.

표 5. 암호화 대상 경로 및 확장자 목록
Table 5. List of path and extension to encryption

Encryption target path (C:₩Users₩<username>₩)	Encryption target extensions
Desktop	.txt, .jar, .exe, .dat, .contact,
Links	.xls, .xlsx, .settings, .doc, .docx,
Contacts	.ppt, .pptx, .odt, .jpg, .png,
Desktop	.csv, .py, .sql, .mdb, .sln, .php,
Documents	.asp, .aspx, .html, .htm, .xml,
Downloads	.psd, .pdf, .dll, .c, .cs, .mp3,
Pictures	.mp4, .f3d, .dwg, .cpp, .zip,
Music	.rar, .mov, .rtf, .bmp, .mkv, .avi,
OneDrive	.apk, .lnk, .iso, .7-zip, .ace, .arj,
Saved Games	.bz2, .cab, .gzip, .lzh, .tar,
Favorites	.uue, .xz, .z, .001, .mpeg, .mp3,
Searches	.mpg, .core, .crproj, .pdb, .ico,
Videos	.pas, .db, .torrent

최종적으로 그림 11과 같이 AES-256-CBC 암호 알고리즘과 PKCS7 패딩을 사용하여 파일 암호화를 진행한다. 암호화 후 파일명은 '원본 파일명.원본 파일 확장자.fuckunicornhtrhrtjrjy'이다.

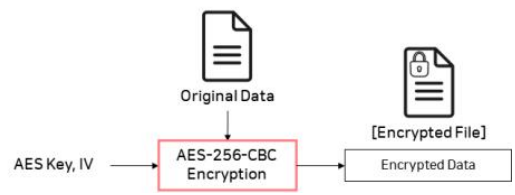
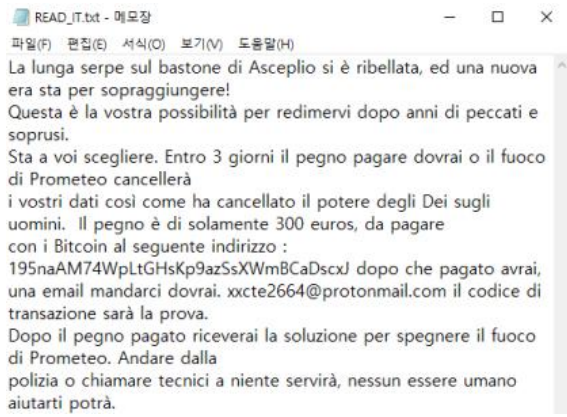


그림 11. Immuni 랜섬웨어 암호화 과정
Fig. 11. Encryption process of Immuni ransomware

(5) 랜섬노트 생성

파일 암호화를 완료한 후 바탕화면에 READ_IT.txt 파일명으로 그림 12와 같이 랜섬노트가 생성된다. 파일 복호화를 위해 300유로를 요구하며 비트코인 주소와 공격자의 메일 정보가 포함되어 있다.


READ_IT.txt - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

La lunga serpe sul bastone di Asceplio si è ribellata, ed una nuova era sta per sopraggiungere!
Questa è la vostra possibilità per redimervi dopo anni di peccati e soprusi.
Sta a voi scegliere. Entro 3 giorni il pegno pagare dovrai o il fuoco di Prometeo cancellerà
i vostri dati così come ha cancellato il potere degli Dei sugli uomini. Il pegno è di solamente 300 euros, da pagare
con i Bitcoin al seguente indirizzo :
195naAM74WpLtGHsKp9azSsXWmBCaDscxJ dopo che pagato avrai, una email mandarci dovrai. xxcte2664@protonmail.com il codice di transazione sarà la prova.
Dopo il pegno pagato riceverai la soluzione per spegnere il fuoco di Prometeo. Andare dalla
polizia o chiamare tecnici a niente servirà, nessun essere umano aiutarti potrà.

그림 12. Immuni 랜섬노트
Fig. 12. Immuni ransom note

(6) 바탕화면 변경 및 패스워드 전송

Immuni 랜섬웨어는 감염 후 그림 13과 같이 코로나 감염 현황 차트를 띄워주고 바탕화면을 변경한다. 바탕화면 이미지는 "https://i.imgur.com/6bDNKfs.jpg"에서 다운로드하여 "C:₩<username>₩ransom.jpg"에 저장한다.

그림 13. Immuni 랜섬웨어 감염 후 변경된 바탕화면
Fig. 13. Wallpaper after infected Immuni ransomware

이후에 암호키 생성 시 사용한 패스워드, computername과 username을 “http://116.203.210.127/write.php”로 전송한다. 감염대상 PC가 네트워크에 연결되어 있지 않은 경우에는 바탕화면이 변경되지 않으며, 패스워드도 전송되지 않는다.

Ⅲ. 랜섬웨어 복구 방안 제시

3-1 5ss5c

1) 볼륨 섀도 복사본 이용

5ss5c 랜섬웨어는 감염 후에 볼륨 섀도 복사본을 삭제하지 않는다. 볼륨 섀도 복사본이 활성화되어 있으며, 랜섬웨어 감염 이전 시점에 대한 파일이 저장된 경우 원본 파일을 복구할 수 있다. 볼륨 섀도 복사본 파일은 Shadow Explorer 프로그램을 통해 분석할 수 있다. Shadow Explorer 프로그램은 Windows Vista/7/8/10에서 생성한 볼륨 섀도 복사본에 접근 가능하게 해주는 프로그램이다[10]. 이를 통해 원본 파일을 획득할 수 있다. 감염 후 볼륨 섀도 복사본을 통해 원본 파일을 획득한 모습은 그림 14와 같다.

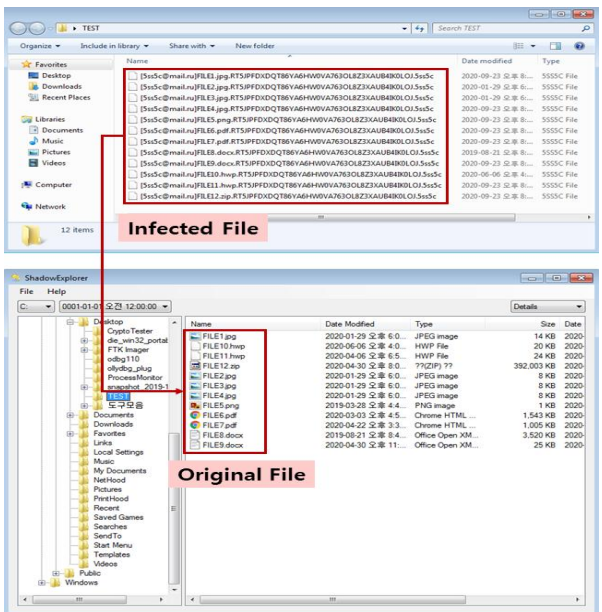


그림 14. 5ss5c 랜섬웨어를 Shadow Explorer를 통해 복구한 모습
Fig. 14. Recovering 5ss5c ransomware through Shadow Explorer

3-2 Immuni

1) 볼륨 섀도 복사본 이용

Immuni 랜섬웨어는 감염 후에 볼륨 섀도 복사본을 삭제하지 않는다. 따라서 볼륨 섀도 복사본을 통해 그림 15와 같이 원본 파일을 획득할 수 있다.

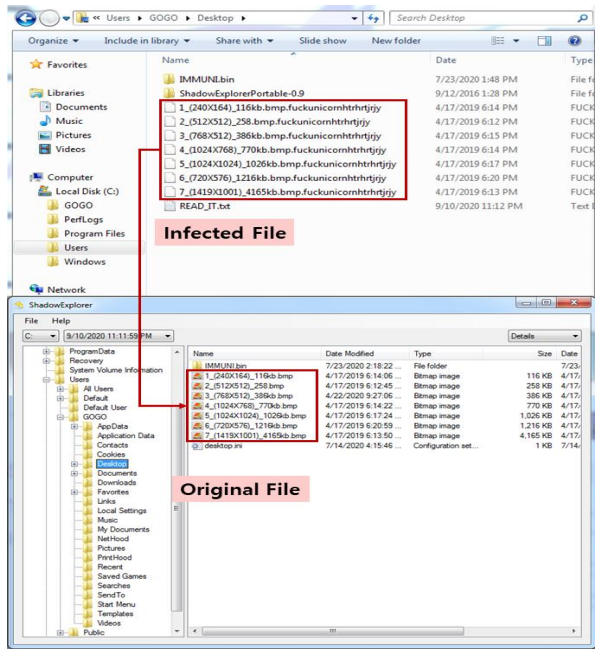


그림 15. Immuni 랜섬웨어를 Shadow Explorer를 통해 복구한 모습
Fig. 15. Recovering Immuni ransomware through Shadow Explorer

2) 메모리 이용

파일 암호화 후에 암호키 영역에 대해 메모리 제로화를 수행하지 않는다. 또한, 감염 종료 후에 실행 파일을 삭제하지 않으므로 해당 프로세스에 대한 메모리 덤프를 획득할 수 있다. 메모리 덤프 내에 암호화 키와 IV가 남아있으며, 구조는 그림 16과 같다. 고정값인 0x004A6804 뒤에 암호키 또는 IV의 길이가 저장되며, 이후에 실제 암호키 또는 IV 값이 존재한다. 메모리 덤프에서 암호키와 IV를 획득하여 AES-256-CBC 암호 알고리즘으로 파일을 복호화할 수 있다.

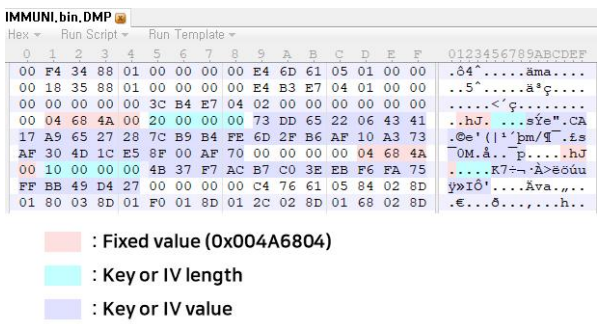


그림 16. Immuni 랜섬웨어의 메모리 덤프 구조
Fig. 16. Structure of Immuni ransomware’s memory dump

3) seed 전수조사

패스워드 생성 시 사용하는 seed는 tickcount 값을 사용하는데, 0부터 2,147,483,647 사이의 값을 사용하기 때문에 2^{31} 계산량으로 전수조사할 수 있다. seed를 전수조사한 후 알려진 확장자를 가진 암호화된 파일을 이용해 키를 찾는다. 본 논문에서는 JPG 파일을 이용하였다. 자세한 과정은 그림 17과 같다. seed 전수조사를 통해 암호키와 IV를 계산하고 하나의 암호화된 JPG 파일을 AES-256-CBC 암호 알고리즘으로 복호화한다. 복호화한 파일의 상위 4 bytes가 JPG 시그니처인 0xFFD8FFE0과 동일하면, 암호키와 IV를 올바르게 획득하였다고 간주하고 전체 파일에 대해 복호화를 수행한다.

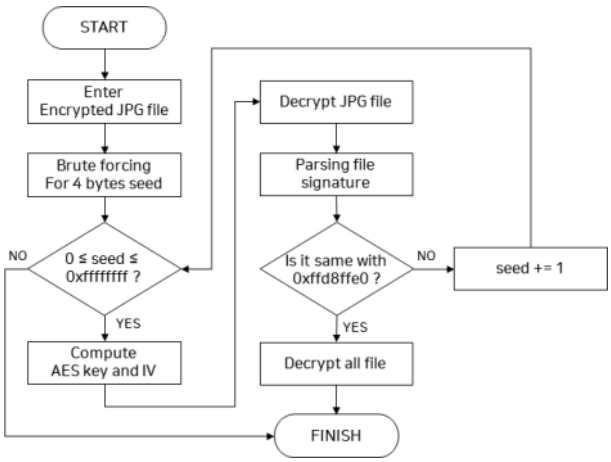


그림 17. seed 전수조사를 통한 복구 방법
Fig. 17. Recovery method through brute forcing of seed

본 논문에서는 위의 과정을 PoC 구현을 통해 복호화 가능함을 확인하였다.

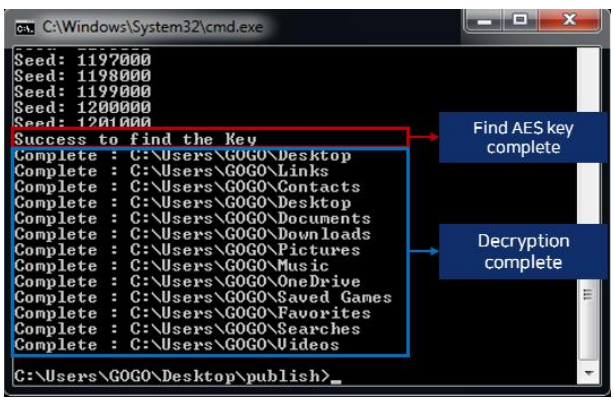


그림 18. PoC를 통한 복호화 과정 검증 완료
Fig. 18. Decryption process verification completed through PoC

Ⅳ. 결론

본 논문에서는 2020년에 주요하게 활동한 랜섬웨어인 5ss5c와 Immuni에 대해 암호화 프로세스를 분석하고 복구 방안을 제시하였다. 5ss5c 랜섬웨어는 AES-256-ECB 알고리즘을 사용하여 파일 암호화를 진행하고, Immuni 랜섬웨어는 AES-256-CBC 알고리즘을 사용하여 파일 암호화를 진행하였다. 그러나 볼륨 섀도 복사본 삭제를 하지 않거나 암호키 생성 시 취약한 seed를 사용하였으며, 암호화 종료 후 암호키에 대한 메모리를 제로화하지 않아 암호화된 파일에 대한 복구 가능성을 발견하였다. 이에 따라 볼륨 섀도 복사본 파일을 분석해주는 Shadow Explorer 프로그램을 이용해 원본 데이터 추출에 성공하였으며, seed 전수조사를 통해 암호키를 재현할 수 있음을 제시하였고 PoC 코드 구현을 통해 검증하였다. 또한, 메모리 분석을 통해 암호키와 IV가 메모리에 남아있음을 확인하였다. 이를 통해 5ss5c와 Immuni 랜섬웨어에 피해를 입은 PC나 서버의 복구에 도움을 줄 수 있을 것으로 예상한다. 또한, 동작 과정이 유사한 랜섬웨어 유포 시 복호화 가능성 분석의 기반 데이터로 사용할 수 있을 것으로 판단한다.

감사의 글

본 논문은 2020년도 과학기술정보통신부(암호이용활성화)의 재원으로 한국인터넷진흥원의 지원을 받아 수행된 연구사업임

참고문헌

[1] Maeil Business, Ransomware Attacks focused on Companies [Internet]. Available: https://www.mk.co.kr/news/it/view/2020/09/906950/
[2] Maeil Business, No. 1 ransomware damage [Internet]. Available: https://www.mk.co.kr/opinion/editorial/view/2020/02/130217/
[3] Dailysecu, Continuing Ransomware Damage [Internet]. Available: https://www.dailysecu.com/news/articleView.html?idxno=113925
[4] Dongascience, Ransomware attack kills female patient in German hospital [Internet]. Available: http://dongascience.donga.com/news.php?idx=39930
[5] Donga, Confidential Leakage [Internet]. Available: https://www.donga.com/news/Economy/article/all/20200910/102867665/1
[6] ANY.RUN [Internet]. Available: https://any.run/
[7] Boannews, Appearing 5ss5c Ransomware [Internet]. Available: https://www.boannews.com/media/view.asp?idx=85821
[8] TACHYON ISARC, Ransomware trends in May [Internet]. Available: https://isarc.tachyonlab.com/3108
[9] ESTsecurity, Appearing immuni Ransomware [Internet]. Available: https://blog.alyac.co.kr/3019
[10] ShadowExplorer [Internet]. Available: https://www.shadowexplorer.com/

신수민(Sumin Shin)

2020년 2월 : 국민대학교 정보보안암호수학과 졸업

2020년 3월~현 재 : 국민대학교 금융정보보안학과 석사과정
※관심분야 : 디지털 포렌식, 정보보호

김소람(Soram Kim)

2016년 2월 : 국민대학교 수학과 졸업
2018년 2월 : 국민대학교 금융정보보안학과 석사

2018년 3월~현 재 : 국민대학교 금융정보보안학과 박사과정
※관심분야 : 디지털 포렌식, 정보보호

윤병철(Byungchul Youn)

2019년 2월 : 국민대학교 수학과 졸업

2019년 9월~현 재 : 국민대학교 금융정보보안학과 석사과정
※관심분야 : 디지털 포렌식, 정보보호

허욱(Uk Hur)

2019년 2월 : 건국대학교 신소재공학과 졸업

2019년 3월~현 재 : 국민대학교 금융정보보안학과 석사과정
※관심분야 : 디지털 포렌식, 정보보호

김대운(Daeun Kim)

2015년 2월: 전남대학교 컴퓨터공학과 졸업
2017년 2월: 전남대학교 정보보안협동과정 석사

2017년 3월~현 재 : 한국인터넷진흥원(KISA)
※관심분야 : 악성코드, 디지털 포렌식, 빅데이터 분석

김기문(Kimoon Kim)

2017년 2월 : 고려대학교 정보보호대학원(공학석사)

2011년~현 재 : 한국인터넷진흥원(KISA) 책임연구원
※관심분야 : 정보보호, 암호 알고리즘

김종성(Jongsung Kim)

2000년 8월/2002년 8월 : 고려대학교 수학 학사/이학석사
2006년 11월 : K.U.Leuven, ESAT/SCD-COSIC 정보보호 공학박사
2007년 2월 : 고려대학교 정보보호대학원 공학박사
2007년 3월 ~ 2009년 8월 : 고려대학교 정보보호기술연구센터 연구교수
2009년 9월 ~ 2013년 2월 : 경남대학교 e-비즈니스학과 조교수
2013년 3월 ~ 2017년 2월 : 국민대학교 수학과 부교수
2013년 3월 ~ 2020년 8월 : 국민대학교 일반대학원 금융정보보안학과 부교수
2017년 3월 ~ 2020년 8월 : 국민대학교 정보보안암호수학과 부교수

2020년 9월~현 재 : 국민대학교 정보보안암호수학과/일반대학원 금융정보보안학과 교수
※관심분야 : 정보보호, 암호 알고리즘, 디지털 포렌식