랜섬웨어와 유포 실습

201411687 김교연
201215531 김형래
201411737 양준수
201311746 이찬우

목차

01

Ransomware?

a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

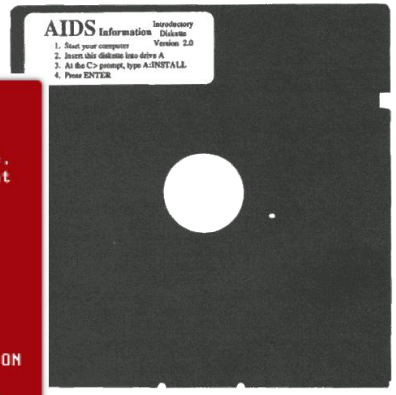
- Wikipedia

- 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류

- 사용자의 내부 파일을 암호화하여 금액 지불을 강요

- 최초의 랜섬웨어는 1989년 Joseph Popp이 작성한 AIDS

01



AIDS

AIDS, also known as Aids Info Disk or PC Cyborg Trojan, is a trojan horse that replaces the AUTOEXEC.BAT file, which would then be used by AIDS to count the number of times the computer has booted.

- Wikipedia

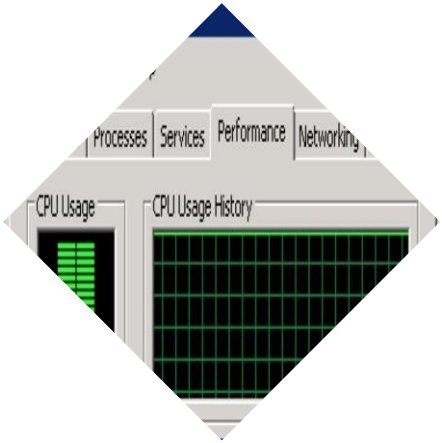
- 현재 기승을 부리는 Crypto 계열의 랜섬웨어는 2005년 처음 발견됐지만 AIDS는 1989년 등장

- 플로피 디스크를 통해 시스템 감염

- AIDS.trojan은 도스의 모든 파일명을 암호화해 시스템을 사용할 수 없게 만든 후 189달러를 파나마의 우편함으로 지불하면 복호화 키가 담긴 디스크를 받을 수 있었다.

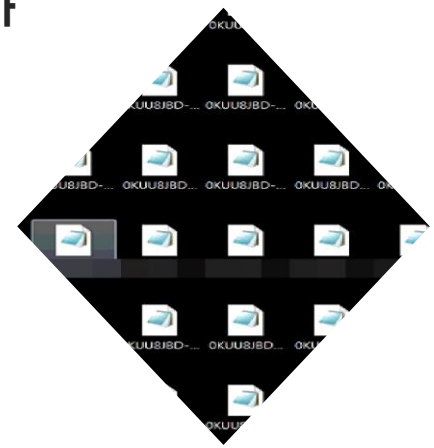
01 대표적인 감염 증상

주요 시스템 파일
열기 불가



CPU와 램
사용량이 급격히
증가

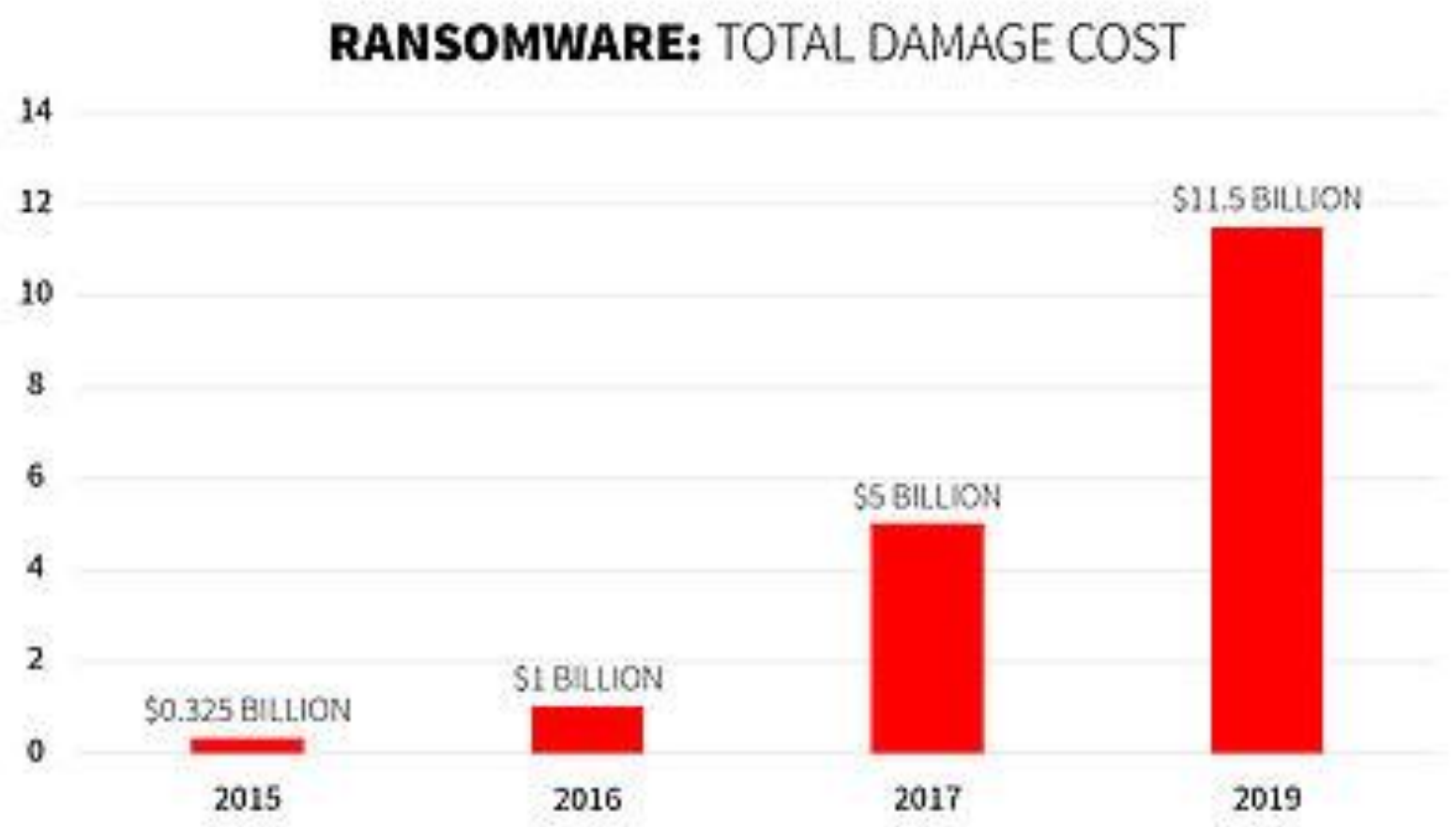
백신 프로그램 강제
종료/중지/오류
등이 지속적으로
발생



파일들의 확장자가
변경

윈도우 복원 시점
제거

01 랜섬 웨어 피해 예상 비용



2019년 현재 세계적으로 약 11.5조 달러 규모의 피해가 예상됨

02

구현 (1)

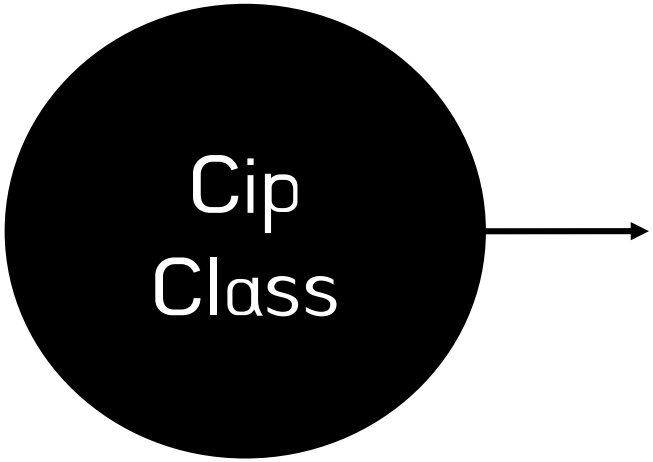
랜섬에어 감염 -> 사용자 파일 암호화 및 복호화

- Filesearch Class
  코드 내 목록에 있는 확장자 파일 -> 암호화 및 원본 파일명 저장
  (하위 디렉토리와 그 디렉토리 파일들 찾아 리스트로 반환)

- 복호화는 아까 찾은 리스트에서 암호화된 파일 이름이 저장되어 있다면 원본으로 복호화

02 구현 (2)

- 복호화 조건은 감염 컴퓨터 바탕화면에 경고 메시지가 있으면 복호화

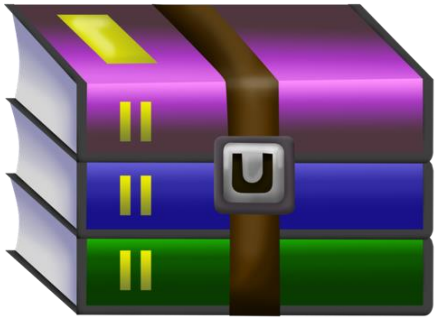


- 키를 생성하고 리스트로 받은 파일들 암호화 시키는 클래스
- 암호화 방식은 AES/ECB
- RSA를 사용하지 않은 이유는 다량의 파일을 암호화 시키기에는 속도가 너무 느리기 때문에 상대적으로 빠른 속도의 AES 방식 차용

02 구현 (3)

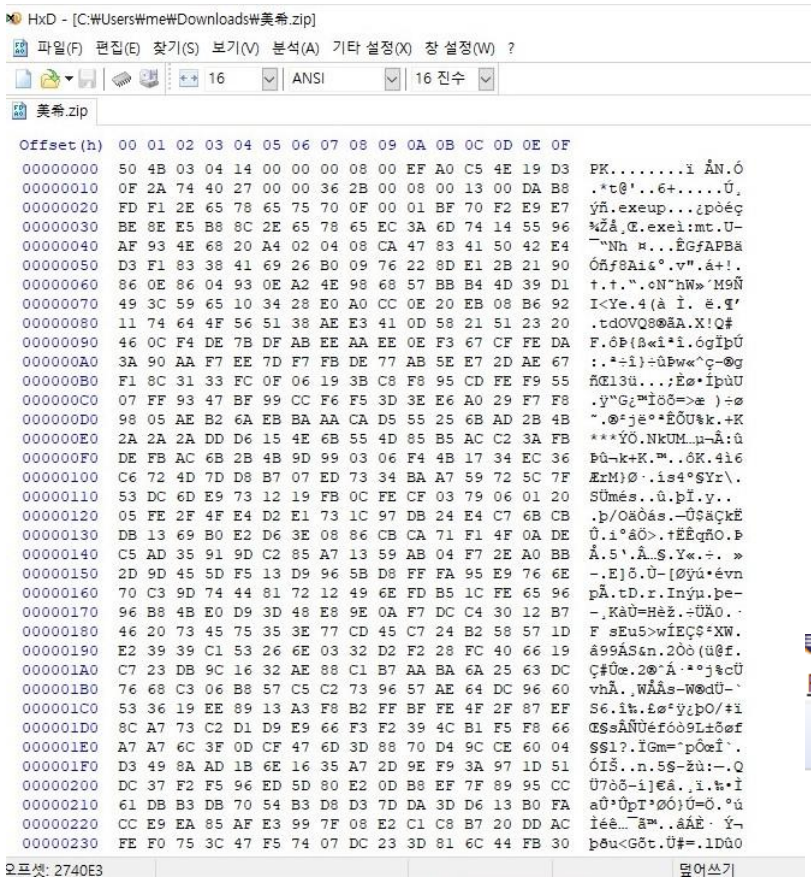
- 구현물은 이미지 파일로 위장되며 이미지 파일이 열릴 경우 키 생성과 동시에 감염

- exe 파일을 png 형태의 이미지 파일로 위장하는 것은 압축 프로그램 winrar의 취약점을 이용

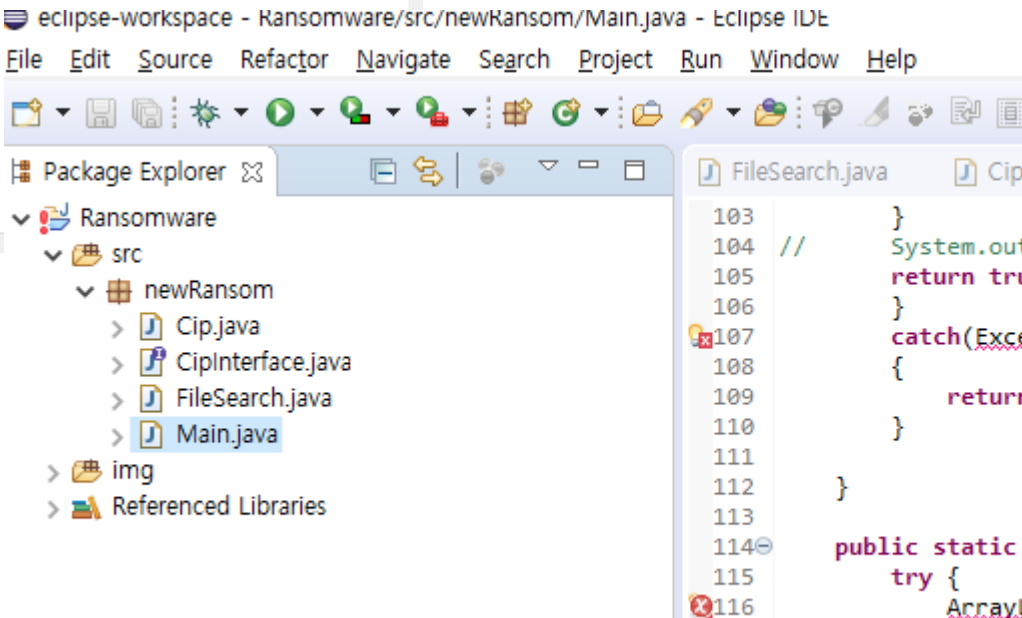


- winrar 구버전에는 취약점이 존재하며 폴더를 압축한 후 바이너리 코드를 수정하면 exe가 정상적으로 존재하지만 png 파일 같은 이미지로 위장 가능

02 구현 (4)



랜섬웨어를 헥스
에디터로 오픈한 모습

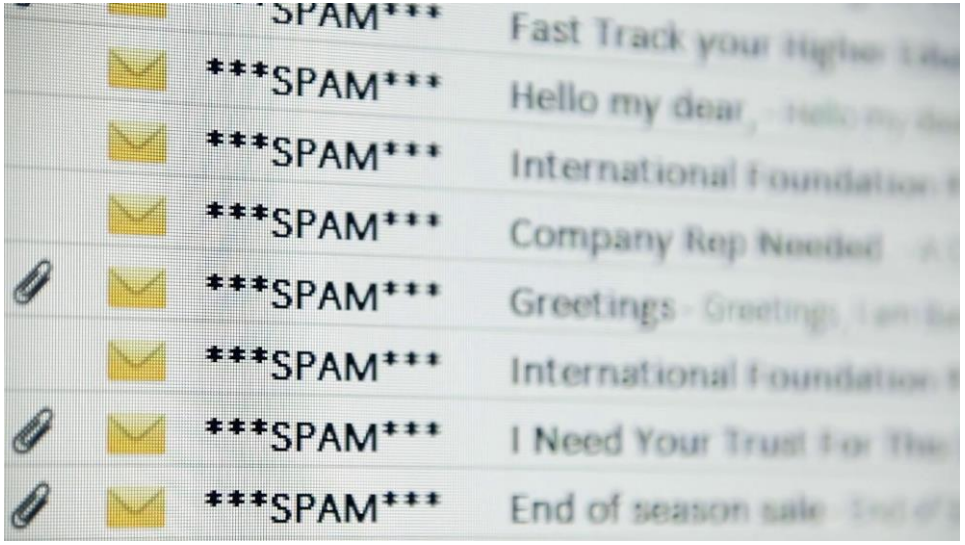


개발한 랜섬웨어
클래스 구조

03 유포 경로 (1)

신뢰할 수 없는 사이트

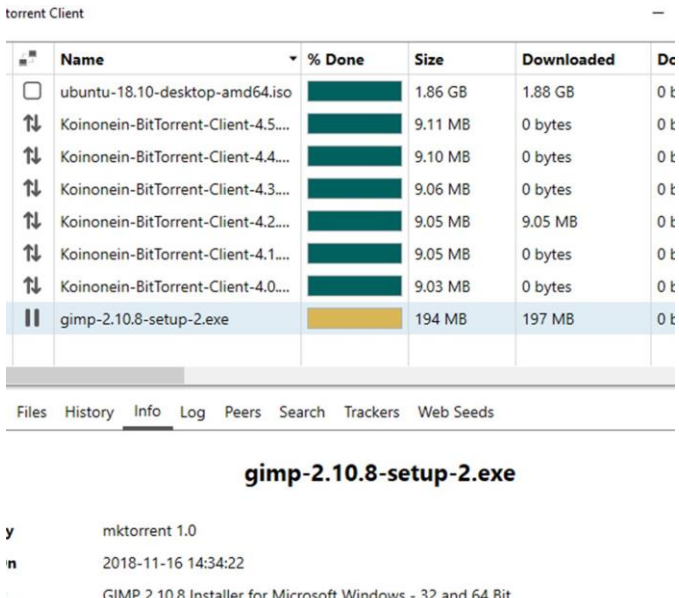
스팸 메일



03 유포 경로 (2)

SNS

광고 배너



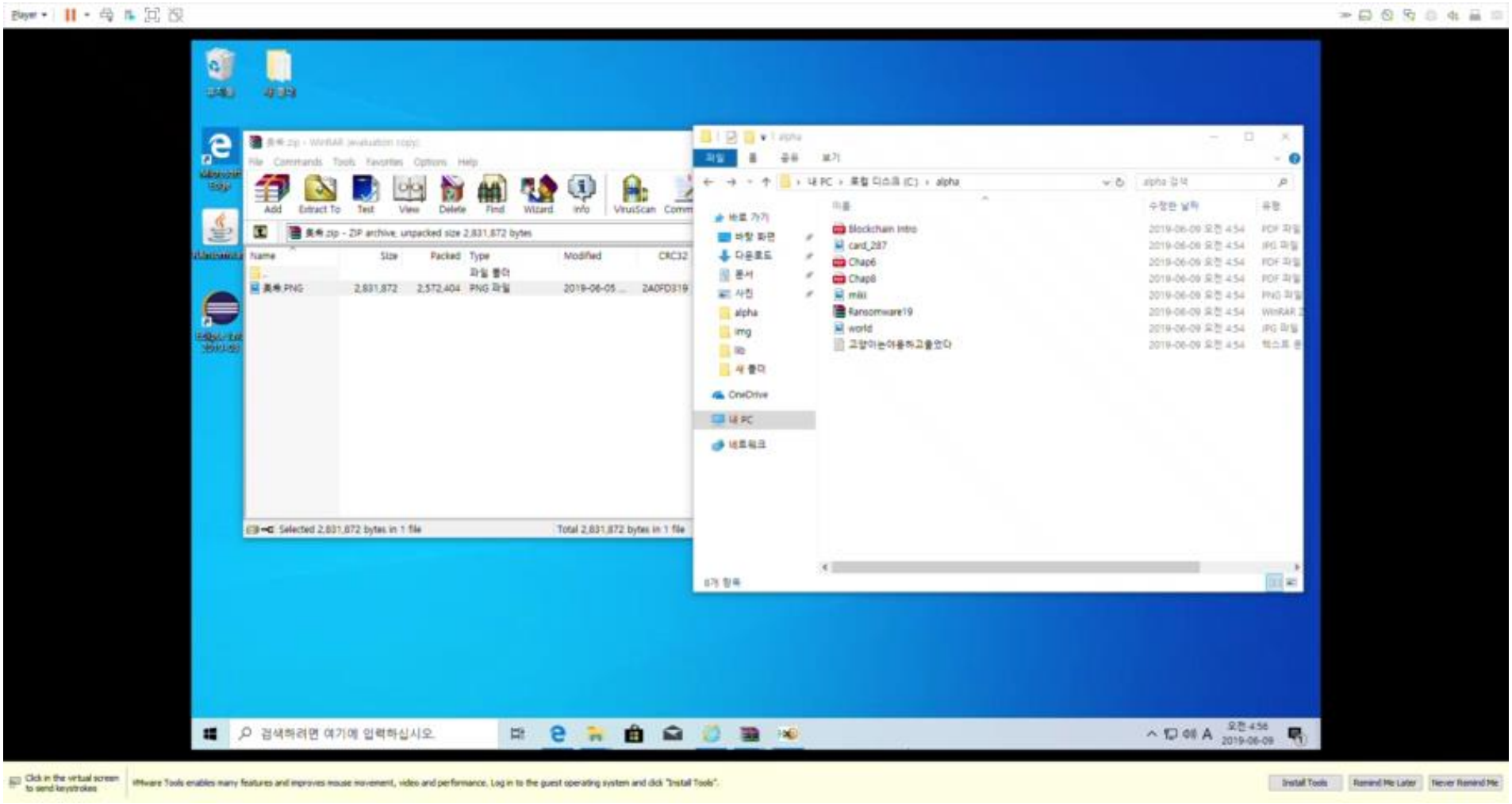
P2P

03 프로젝트에서의 유포 방식

exe를 PNG 이미지
파일로 위장

사용자에게 보여질
위장된 파일의 이미지

03 실제 구현물의 동작


Add
Extract To
Test
View
Delete
Find
Wizard
Info
VirusScan
Name
Size
Packed
Type
Modified
CRC32
Selected 2,831,872 bytes in 1 file
Total 2,831,872 bytes in 1 file
Blockchain Intro
card_287
Chap6
Chap8
miki
Ransomware19
world
OneDrive
내 PC
네트워크
검색하려면 여기에 입력하십시오.
Install Tools
Remind Me Later
Never Remind Me

04 정리

- 악의적으로 유포되는 악성코드들은 프로그램 업데이트만 주기적으로 해도 대개 감염되는 것을 예방할 수 있다.

- 용도에 따라 암호화 방식별로 다른 속도 차이를 고려해야 한다.

- 악성코드 자체의 개발은 의외로 어렵지 않으며 유포가 관건이다.


감사합니다