랜섬웨어 Hidden Tear 분석하기 (클라이언트, 서버)

2021년 12월 22일

남수만

한동대학교
HANDONG GLOBAL UNIVERSITY

남수만

㈜두두아이티 연구소장

서울여자대학교 정보보학학과 겸임교수

인천재능대학교 인공지능컴퓨터과 강사

파일 3개 다운로드

강의 사전조사

http://naver.me/Gp9ch9Lq

강의 목표

1. 사이버 공격의 트렌드를 알자!

2. 최근 유행하는 랜섬웨어 공격 원리를 파악하자!
   - 특히, 첫 번째 랜섬웨어인 Hidden Tear을 통해 원리 파악

3. 파악된 원리를 통해 **랜섬웨어를 완벽하게 대응**하자!

제48조(정보통신망 침해행위 등의 금지)

1. 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.

   → **다른 사람의 계정 정보(인증 정보)를 사용해 시스템에 로그인하는 행위**

2. 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하여서는 아니 된다.

   → **인증 시스템을 공격해 인증을 우회하는 행위**
   (SQL 주입 등으로 웹 사이트 로그인을 우회하는 등)

3. 누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하여서는 아니 된다.

   → **네트워크를 통해 다른 시스템에 공격을 실시해 해당 시스템을 장악하는 행위**

제48조에 따른 벌칙

제72조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 **3년 이하의 징역 또는 3천만원 이하의 벌금**에 처한다.

1. 제48조제1항을 위반하여 정보통신망에 침입한 자

제71조(벌칙) 다은 각 호의 어느 하나에 해당하는 자는 **5년 이하의 징역 또는 5천만원 이하의 벌금**에 처한다.

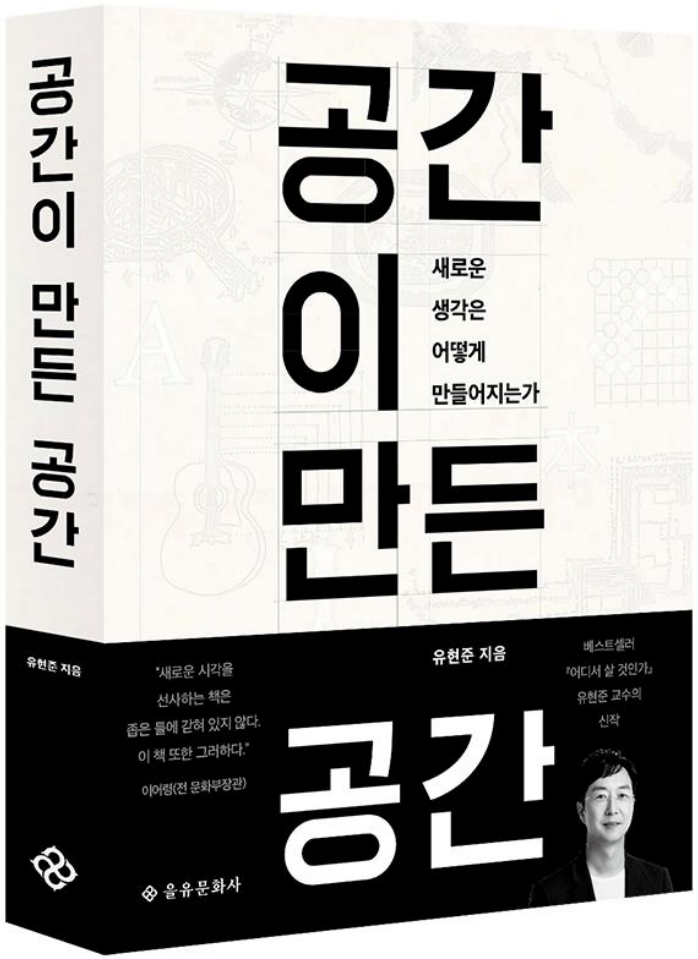
9. 제48조제2항을 위반하여 악성프로그램을 전달 또는 유포한 자
10. 제 48조제3항을 위반하여 정보통신망에 장애가 발생하게 한 자

청주대학교 CHEONGJU UNIVERSITY

정보보안의 필요성

네트워크를 통한 연결성 확대

네트워크의 어려움



541쪽

기술은 눈에 보이지 않게 **숨겨**지는 방향으로 발전한다.

사이버 공격 == 공성전

참고: https://www.youtube.com/watch?v=g3rRqvMvbYE

안시성

창(공격)과 방패(보안시스템)

운동, 게임, 전쟁: **창 < 방패, 방패 < 창**

- 변수: 시간과 자원 제약

정보보안: **방패 < 창**

- 자원 무한

패들렛(생각 공유)

https://padlet.com/wisespace/vimmjvrafdmwyemu

청주대학교
CHEONGJU UNIVERSITY

역사의 중요성

역사(과거)의 트렌드를 알면,
미래 트렌드가 보인다.

1999년 이전

통신 방법: 컴퓨터 모뎀 (모뎀 통신 속도: 56kbit/s)

인터넷 화면(예: 네이버)

1998년 12월 네이버 메인 페이지 모습

2017년 네이버 메인 페이지 모습

인터넷 역사

ADSL 등장(**1999년 4월 1일**; 하나로통신(SK브로드밴드))

- Asymmetric digital subscriber line(비동기식 디지털 가입자 회선)
- 장점: 가격 정액제
- 전송 데이터 (모뎀 통신 속도: 56kbit/s)
  - 다운스트림시 1.5Mbps
  - 업스트림시 384 Kbps

VDSL(2002년부터 상용화; KT)

- 서비스 속도는 10Mbps로 최대 2Mbps 속도

메가패스(2003년; KT)

- 초고속 인터넷

인터넷 사용자(2003년 8월말 기준)

초고속 인터넷 총 가입자(총 11,259,480명)

- 1위 KT: 의 48.8%인 5,492,237명
- 2위 하나로 통신: 26.4%인 2,972,129명
- 3위 두루넷: 11.5%인 1,289,839명

전 국민의 4명 중 1명이 초고속 인터넷 사용자

- 가입자 수는 가구 수 기준이 아님(보통 3~4명 당 1가구)

해킹 및 침해사고와 정책

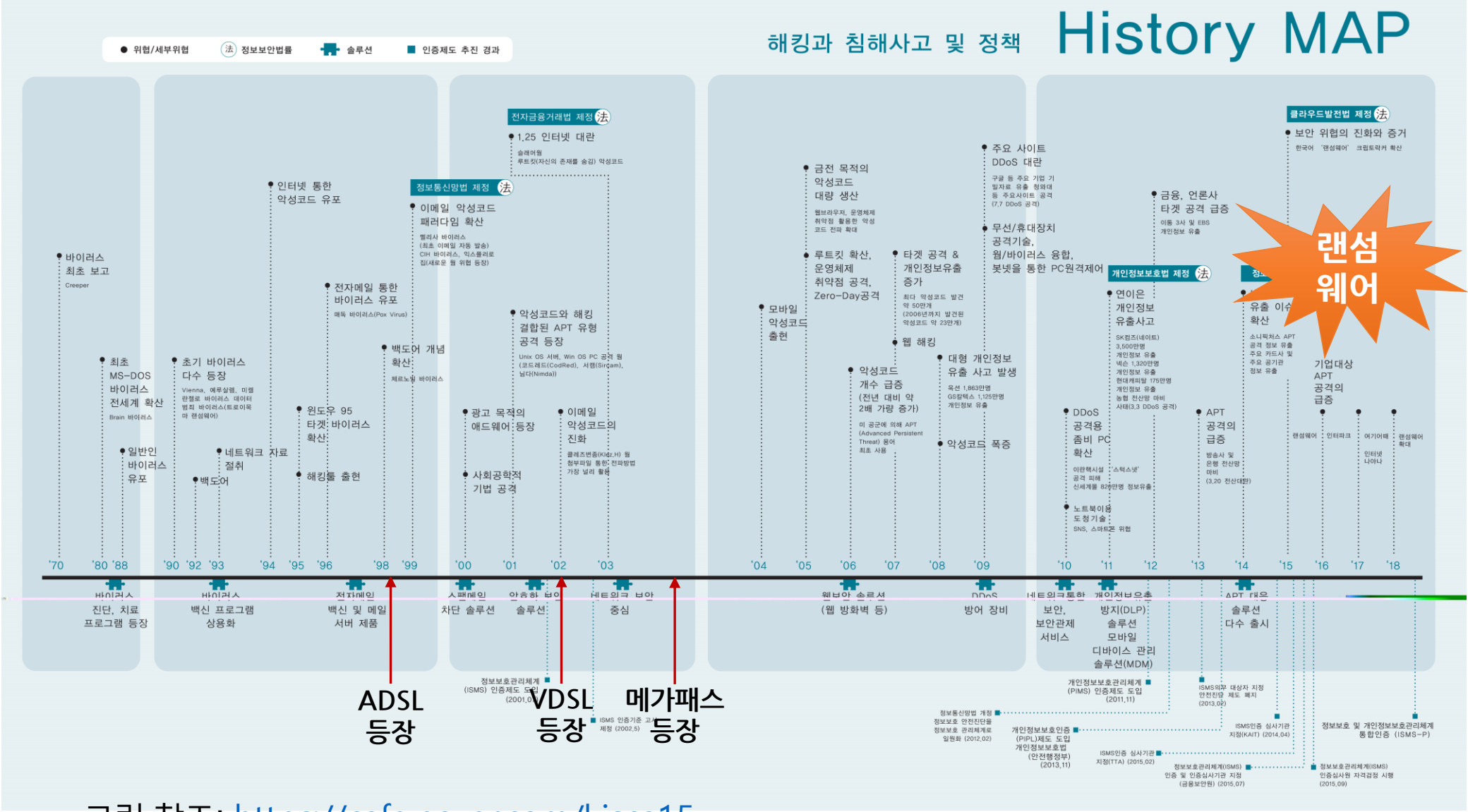


그림 참조: https://cafe.naver.com/kisca15

랜섬웨어 공격 특징 및 추세

랜섬웨어(Ransom) 공격 특징 및 추세

■ 개요

- 악성코드를 설치하고, 사용자 파일을 모두 암호화 시켜 인질로 잡고, 금전을 요구하는 공격
- 공격기법 : 파일암호형(CrytoWall 등), 화면잠금형(Winlocker 등), MBR파괴형(Petya 등)

■ 최근 동향 및 추세

- 10종(2015년) ⇒ 60종(2018년)으로 6배 증가, 피해금액 및 상담건수 증가

구분	2015년	2016년	2017년	2018년
접수건수	2,678	3,255	4,475	4,283
피해자	53,000	130,000	260,000	285,000
피해금액	1,090억원	3,000억원	7,000억원	1조 500억원

칠레 국영은행, 랜섬웨어로 1400만달러 피해

칠레 국영은행이 랜섬웨어 공격을 받아 **약 1400만달러(약 165억원)** 규모 피해를 입었다. 이로 인해 은행 전 지점이 폐쇄됐으며 국가 컴퓨터 보안사고대응팀(CSIRT)이 보안 경보를 발령했다. … 랜섬웨어에 감염된 뒤 전 지점을 폐쇄하고 시스템 복구와 조사에 착수했다. … 감염된 컴퓨터는 약 1만2000대로 집계됐다.

공격자가 사고를 틈타 직접 탈취한 금액은 약 1300만달러(약 150억원)로 나타났다. 시스템 복구 비용 등을 포함하면 총 피해액은 약 1400만달러로 추정된다.

현지 언론에 따르면 이번 공격 배후는 북한 정찰총국 산하 해킹조직 '라자루스'와 '비글보이즈'로 추정된다.

출처: 전자신문, https://m.etnews.com/20200916000079, **2020년 9월 16일**

국내 이랜드 랜섬웨어 피해

2020년 11월 22일. 국내 대기업 이랜드 그룹 사내 네트워크에서 랜섬웨어 감염이 발생, 오프라인 매장 시스템이 중단되는 사고가 발생했다.
사고 여파는 컸다. 일요일이었던 22일. 이랜드 그룹 계열사 뉴코아 아울렛, 2001 아울렛 등 그룹이 운영하는 **점포 48곳 가운데 23곳이 영업을 중단**했다.
출처 : 세이프타임즈(http://www.safetimes.co.kr)

지난 22일 이랜드그룹 서버를 공격한 해커 쪽은 회사에 "**4000만달러(약 444억원) 상당의 비트코인을 지불**하지 않으면 이번 공격으로 확보한 고객 카드정보 200만건을 공개하겠다"고 협박한 것으로 알려졌다.
랜섬웨어는 사용자 컴퓨터의 데이터를 암호화한 뒤 이를 풀어주는 대가로 돈을 요구하는 악성코드다.

출처 :
https://www.hani.co.kr/arti/economy/consumer/971860.html

이랜드 공격 랜섬웨어는 '클롭'…"공격 경로 조사중"(1/2)

최근 이랜드 그룹의 사내 네트워크 시스템을 마비시켜 강남 NC백화점 등 일부 매장 영업 활동에 차질을 일으킨 랜섬웨어는 '**클롭**'이라는 분석이 제기됐다.

23일 이스트시큐리티 등 보안업계는 지난 22일 새벽 이랜드 그룹의 서버·시스템을 감염시킨 랜섬웨어 종류를 클롭으로 추정하고 있다. 현재 서울지방경찰청과 한국인터넷진흥원(KISA) 등이 조사를 진행 중인 건으로 정확한 사건 경위는 최소 2~3일 뒤 나올 것으로 보인다.

앞서 랜섬웨어에 감염된 이랜드 측은 확산을 막기 위해 네트워크를 차단하면서 일부 판매관리시스템(POS) 단말기 등 작동을 중단한 바 있다. 이 때문에 일부 점포는 긴급 휴점에 돌입했다.

참고: 아이뉴스24, http://www.inews24.com/view/1319834, 2020년 11월 23일

이랜드 공격 랜섬웨어는 '클롭'…"공격 경로 조사중"(1/2)

클롭은 최근 기승을 부려온 랜섬웨어로 주로 **워드(.doc), 엑셀(.xls) 등 파일에 첨부돼 이메일로 유포**된다. 만약 사용자가 해당 악성 문서를 열면 PC 내 데이터 일부가 암호화돼 데이터가 잠긴다. 그간 일각에서는 러시아 해킹 조직을 클롭 공격의 배후로 지목해왔다.

우리은행 사칭 '랜섬웨어' 주의보(1/2)

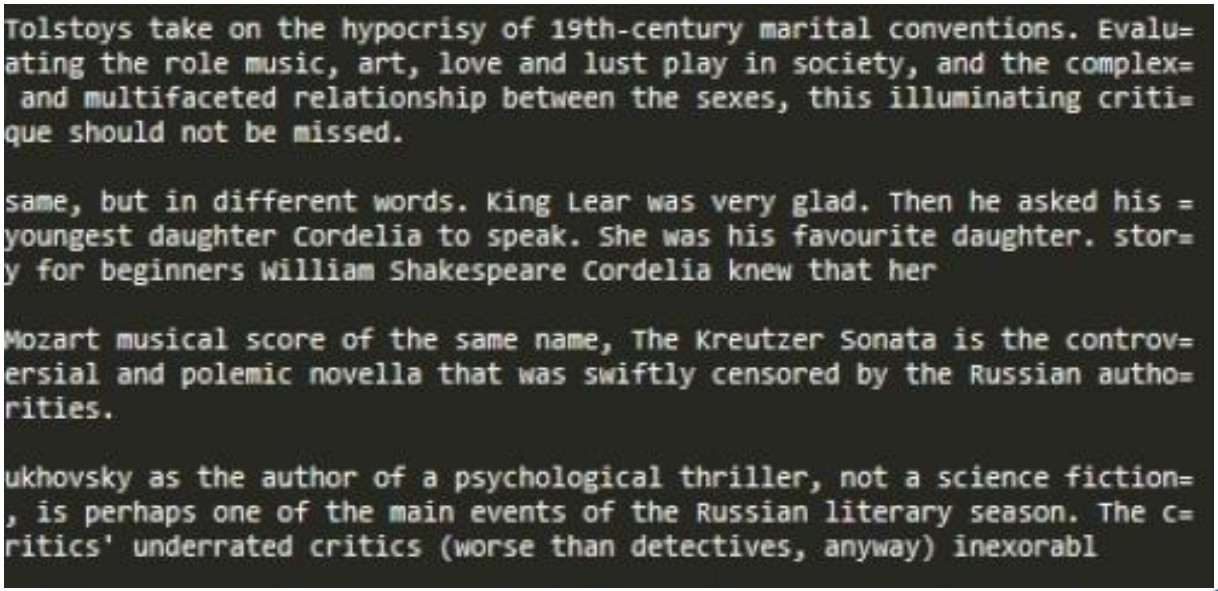
우리은행을 사칭한 이메일로 랜섬웨어 악성코드가 유포되고 있다. 27일 국내 보안업체 이스트시큐리티에 따르면 지난 23일부터 우리은행을 사칭한 악성 이메일 공격이 발견됐다. 메일 발신자명은 '**Woori Financial Departments**'를 사용했으며, 메일 제목은 '지불 정지. 우리은행'이었다. 첨부한 압축 파일 역시 '우리_은행'이라는 이름을 썼다.

참고: 아이뉴스24, http://www.inews24.com/view/1204493, 2019년 8월 27일

우리은행 사칭 '랜섬웨어' 주의보(2/2)

압축 파일을 해제하면 '결제정보_세부정보가 잘못 입력되었습니다'라는 이름으로 마이크로소프트(MS) 워드 문서 파일을 가장한 실행(exe) 파일이 나타난다.

클릭할 경우 '**소디노키비(Sodinokibi)**' 랜섬웨어에 감염된다. 해당 메일을 '**텍스트뷰어**' 프로그램으로 열람하면 러시아의 대문호 **'톨스토이'에 관한 소개 내용을 확인**할 수 있다는 것도 특이점이다.



Hidden Tear

Hidden Tear is the first open-source ransomware trojan that targets computers running Microsoft Windows[1] The original sample was posted in August 2015 to **GitHub**.

When Hidden Tear is activated, it encrypts certain types of files using a symmetric **AES** algorithm, then sends the symmetric key to the malware's control servers.

AES(Advanced Encryption Standard)

대표적인 대칭키 알고리즘(DES 대체용)

- 암호화키 == 복호화키

가변 길이의 블록과 키 사용

	Key kength (Nk words)	Block length (Nb words)	Number of Rounds
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

< Key-Block-Round Combinations >

(절차) Hidden Tear 설치

1. **사전 준비**
2. **실행** [초급과정]
    - Hidden Tear 실행
3. **Hidden Tear 구축** [중/고급과정]
4. 배포
    - 이번 시간은 제외(악성코드 배포 참고)

실습내용

https://www.notion.so/wisespace/Hidden-Tear-0bd223bcc8b34238a3f436c16c06bedd

VMware Windows 10 Password: **techfin**

Hidden Tear 구성요소

구성요소: 피해PC, 웹서버

랜섬웨어 솔루션

- 파일 버전 관리 → 백업 서버 공격

다른 랜섬웨어

Jasmin Ransomware (Hidden Tear와 유사)
https://github.com/codesiddhant/Jasmin-Ransomware

RAASNet (Python 기반)
https://github.com/leonv024/RAASNet

Closing

(옛날) 바다 **해적** == (현대) 사이버 **해커**

기본기를 통한 역량 강화

사이버보안 전문가!!!


32%
23%
INTRUSION DETECTED
SECURITY BREACH
HACKING DETECTED
47%
74%
56%
18%
67%