최근 발전된 해킹 수법

-취약점을 이용한 해킹-

상명대학교 보안동아리 CodeCure

목 차

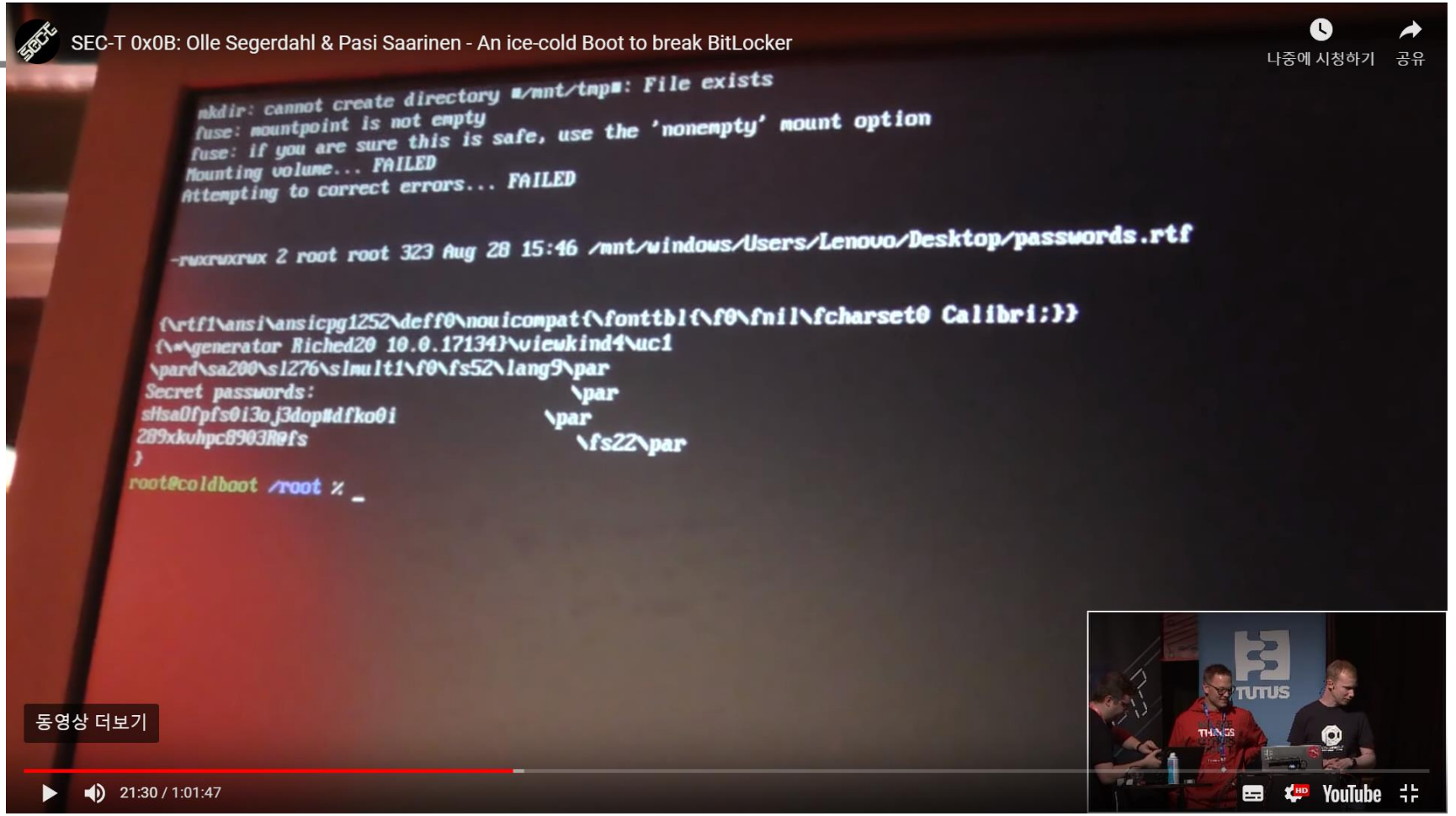
콜드부트 – 요약

- 2008년 부터 알려진 ‘콜드 부트 공격’이 업그레이드 되어 나타남
  - 콜드 부트 공격: 컴퓨터 종료 후 RAM에 잠시 남아있는 정보를 훔치는 공격
- 기존의 콜드 부트 공격은 TCG에서 개발한 안전 장치로 방어
  - TCG(Trusted Computing Group): 컴퓨팅 플랫폼의 표준을 개발하기 위한 산업 컨소시엄(협력단체)
  - 안전 장치: 장비 제대로 종료 되었는지 펌웨어가 확인, 제대로 종료 되지 않았다면 OS가 경고 전달

콜드부트 – 요약

- 핀란드의 연구원들은 TCG의 보안 프로그램을 무력화 시킬 수 있는 방법 발견

- 작은 장비를 플래시 메모리 칩에 연결하여 OS 경고 제거, 비휘발성 메모리 칩을 다시 작성하여 외부 장치로부터 부팅 가능하게 만듦


SEC-T 0x0B: Olle Segerdahl & Pasi Saarinen - An ice-cold Boot to break BitLocker
나중에 시청하기
공유
mkdir: cannot create directory ‘/mnt/tmp’: File exists
fuse: mountpoint is not empty
fuse: if you are sure this is safe, use the ‘nonempty’ mount option
Mounting volume... FAILED
Attempting to correct errors... FAILED
-rwxrwxrwx 2 root root 323 Aug 28 15:46 /mnt/windows/Users/Lenovo/Desktop/passwords.rtf
{\rtf1\ansi\ansicpg1252\deff0\nouicompat{\fonttbl{\f0\fnil\fcharset0 Calibri;}}
{*\generator Riched20 10.0.17134}\viewkind4\uc1
\pard\sa200\sl276\slmult1\f0\fs52\lang9\par
Secret passwords: \par
sHsaOfpfs0i3oj3dop#dfko0i \par
289xkvhpc8903R@fs \fs22\par
}
root@coldboot /root % _
동영상 더보기
21:30 / 1:01:47
YouTube

콜드부트 – 용어

- 콜드 부트: 전원 버튼 사용하여 컴퓨터를 켜거나, 사용 도중 전원을 껐다 키는 것
- 펌웨어: 시스템의 효율을 높이기 위해 ROM에 넣은 기본적인 프로그램
- 플래시 메모리: 전원이 꺼져도 저장된 정보가 지워지지 않는 메모리. 비휘발성 메모리의 일종
- 비휘발성 메모리: 전원을 꺼도 메모리 내용이 지워지지 않는 메모리

.hwp의 취약점 - 요약

- 부동산 협회를 사칭한 라자루스가 HWP형태의 악성파일 유포
  - 라자루스: 북한의 해커 단체
- HWP를 악용해 한글 구조 내부 PS파일에 셸코드를 포함, 16바이트 XOR키로 셸코드를 복호화
- 셸코드가 실행되면 특정 주소에서 파일을 다운로드, 명령제어 서버에 접속을 시도

.hwp의 취약점 - 용어

- 셸코드(ShellCode) : 명령셸을 시작시켜 공격자가 영향 준 컴퓨터 제어 가능
  - 명령셸 : 명령을 해석하여 실행하는 프로그램
- 복호화 : 암호문을 평문으로 변환
- 명령제어(C&C) 서버 : DDOS 공격을 명령 내리는 서버

.docx 기능의 취약점 - 요약

- 보안 업체(Cymulate)의 전문가들이 발견
- 워드의 영상 엠베드 기능으로 실행
  - 엠베드 기능: 영상 이미지 뒤에 HTML스크립트를 생성
- HTML 코드를 편집하여 멀웨어로 연결 가능

.docx 기능의 취약점 - 요약

- 피해자가 문서를 열어야 하므로 피싱 공격이 가장 실제적인 공격 시나리오
- MS오피스의 디폴트 설정 상 엠베드 된 영상 코드를 실행할 때 사용자의 허락을 다시 구하지 않기 때문에 사용자가 문서를 열자마자 공격 성공
- MS오피스 2016 및 그 이하 버전 모두 피해 가능
- 마이크로소프트는 이를 오류라 여기지 않아 패치 없을 예정

.docx 기능의 취약점- 용어

- HTML : 문서의 글자 크기, 글자색, 글자모양, 그래픽, 문서이동(하이퍼링크) 등을 정의하는 명령어
- 멀웨어: 시스템을 해하기 위해 설계된 소프트웨어
- 피싱 공격: 사용자를 현혹하여 파일을 열도록 함
- 디폴트: 사용자가 별도의 명령을 내리지 않았을 때, 시스템이 미리 정해진 값이나 조건을 자동 적용

감사합니다!