

금융회사 침해사고 분석

2023.02.08

안소희 책임 연구원
천호진 선임 연구원

K-CTI 2023

2023 대한민국 사이버위협·침해사고대응 인텔리전스 컨퍼런스



ENKI

CONTENTS.

01 개요

- 무슨 발표를 하는걸까?

02 침해사고 요약

- 초동 분석
- DB 함수와 테이블 & 트리거
- 악성코드 패킷
- 디스크 덤프

03 악성 코드

- 인포스틸러
- 루트킷
- 백도어

04 마치며

- 공격 그룹
- 공격 특징
- 악성코드 특징
- 탐지 방안



01

개요

개요

이런 이슈와 관련 있는 내용입니다

■ Syslogk

- 작년 6월 syslogk로 명명된 루트킷 등장(avast)
- 매직 패킷을 이용하여 백도어(rekoobe)를 실행 시킴
- 오픈소스 Adore-Ng를 수정하여 사용
- **디렉토리, 네트워크, 프로세스 등 은닉에 특화**

개요

이런 이슈와 관련 있는 내용입니다

■ But

- 엔키는 금융 회사 침해사고 조사를 통해 해당 악성코드를 확인한 전적이 존재
- 본 발표에서는 당시 확인된 악성코드들과 악성코드 채증 과정에 대해 설명
- 나아가 해당 악성코드를 탐지할 수 있는 방안에 대해 소개



02

침해사고 요약

침해사고 요약

초동 분석

■ 그리고 아무 것도 없었다

- 처음에는 “수상한 흔적”을 찾기 위해 라이브 환경에서 서버 전수 조사 진행.
- 침해사고 분석 시 확인하는 기본적인 로그들을 확인하였으나 이상 없음.
- 비정상적인 파일 확인, 히스토리, 시스템 파일 변조 유무, 서비스, 프로세스, 시스템 로그 등

침해사고 요약

DB 함수와 테이블 & 트리거

■ DB 서버에서 발견된 수상한 흔적

- 임의의 테이블과 트리거(Trigger)에 대한 정보를 전달받음
- 임의의 테이블에 고객 정보가 저장되고 있는 상황
- DB함수는 코드가 암호화 되어있는 상태

침해사고 요약

악성코드 패킷

■ SMTP패킷과 악성코드

- SMTP 통신과 상관없는 서버에서 발견된 SMTP 패킷
- 암호화되어있어서 무슨 내용이 오고 가는지 확인 불가 상태
- 하지만?

침해사고 요약

디스크 덤프

■ 드러난 실체

- 루트킷 악성코드 확인
- **초동 분석 때는 왜 안 보였을까?**

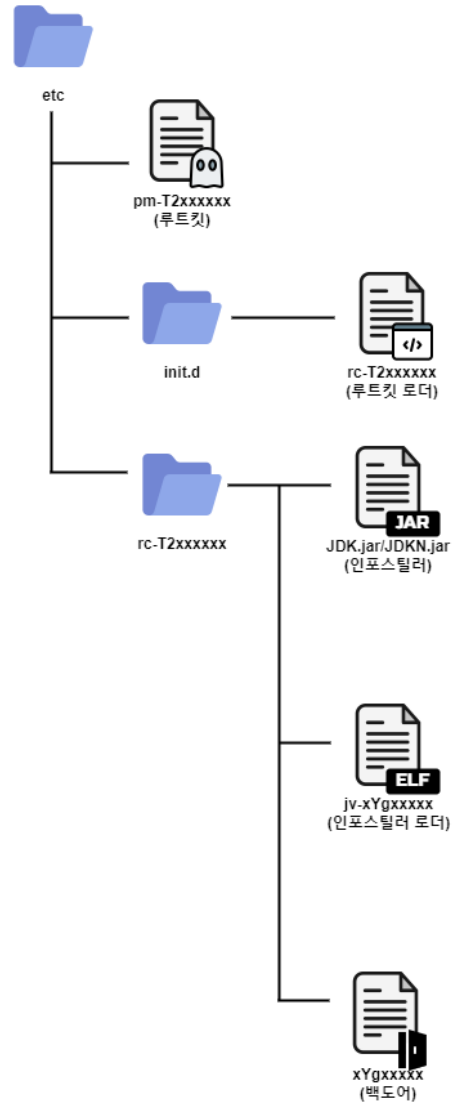


03

악성코드

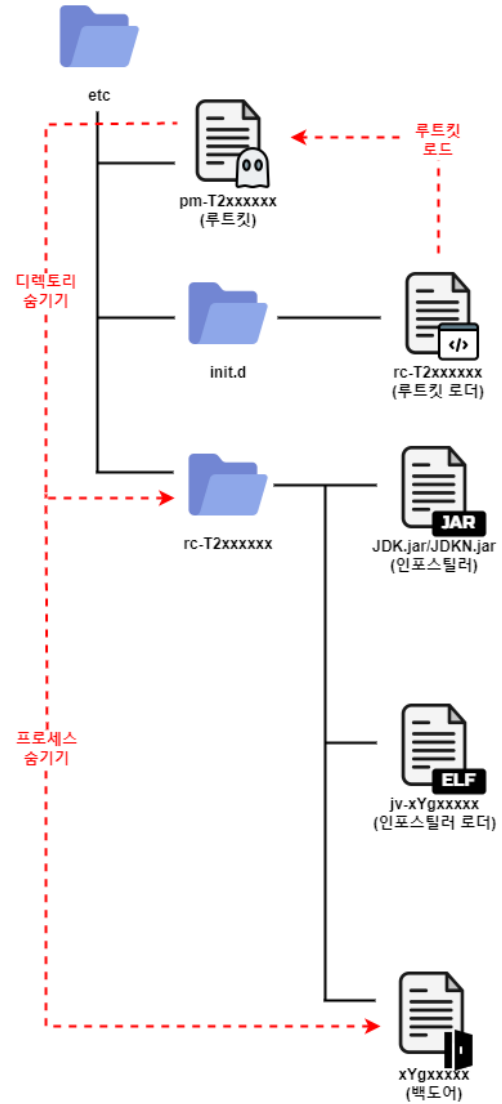
악성코드

전체 구성



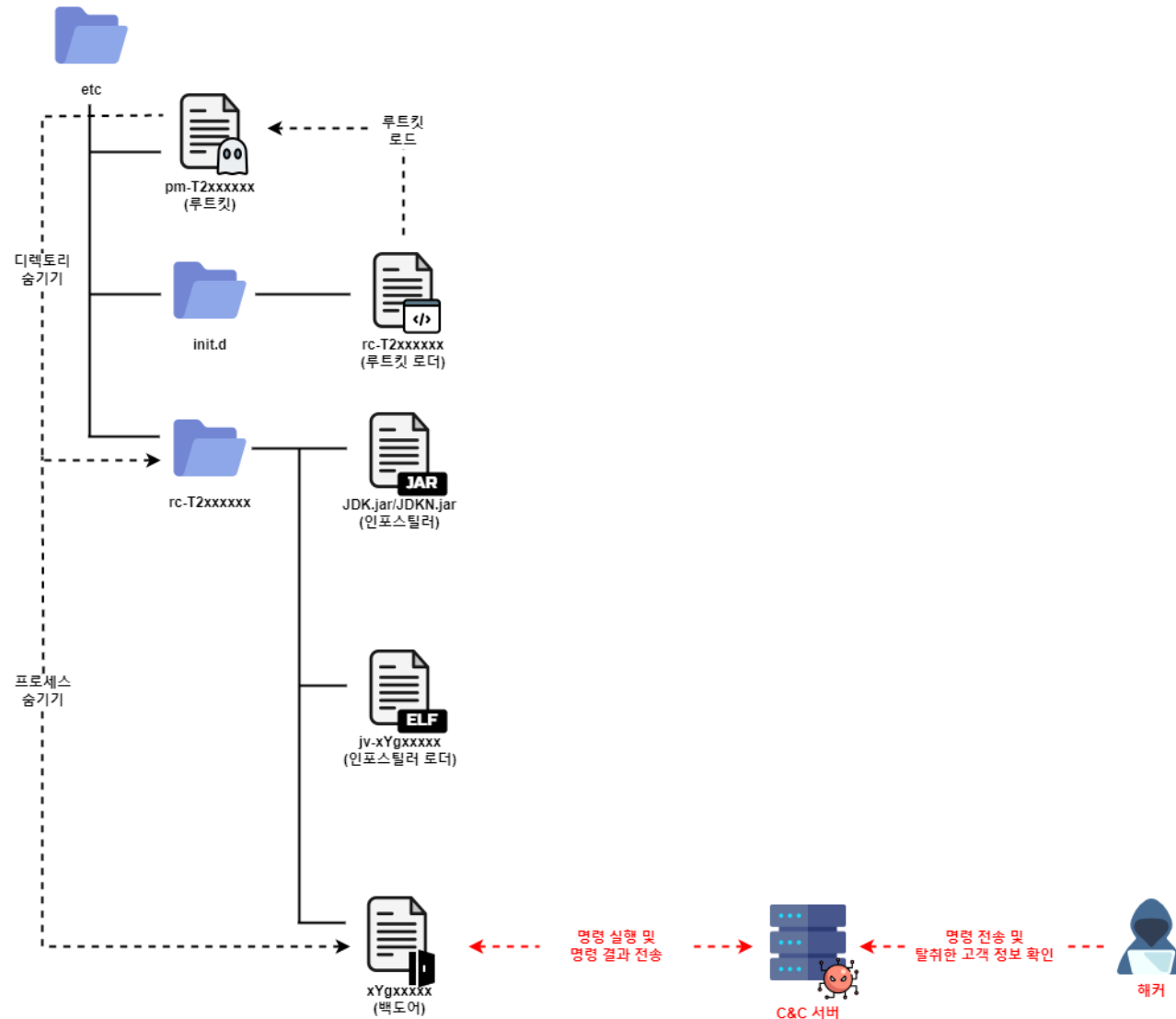
악성코드

전체 구성



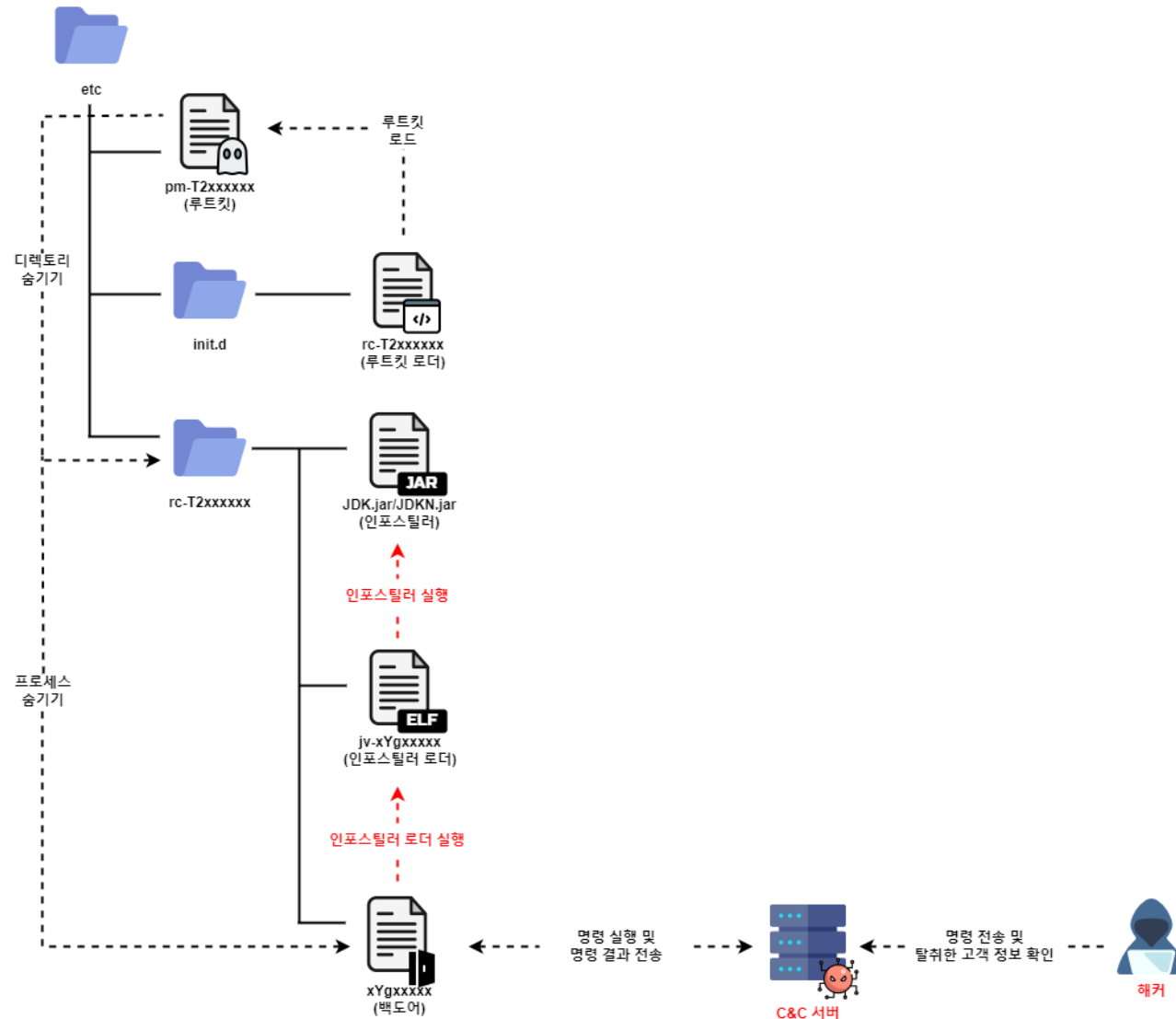
악성코드

전체 구성



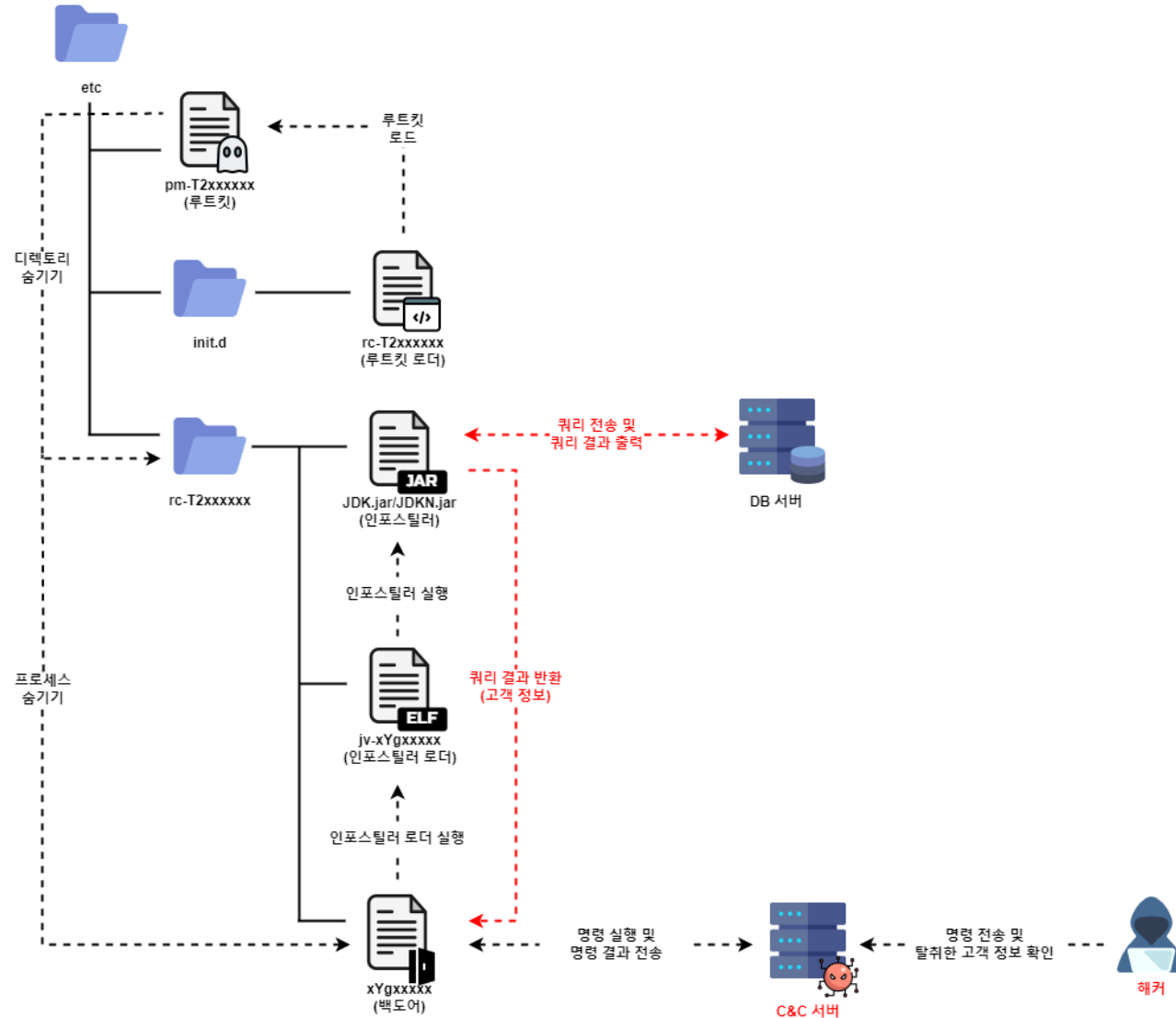
악성코드

전체 구성





악성코드










전체 구성



악성코드

루트킷

 **greatyao** fix for 3.16 522c80a on Dec 30, 2015  11 commits

 .gitignore	Initial commit	8 years ago
 LICENSE	Initial commit	8 years ago
 Makefile	* tested on ubuntu 10.04(x86), 12.04(x64) and 13.04(x86)	8 years ago
 README.md	Initial commit	8 years ago
 adore-ng.c	fix for 3.16	7 years ago
 adore-ng.h	add port 9099	8 years ago
 ava.c	instead execve of execvp	8 years ago
 libinvisible.c	* tested on ubuntu 10.04(x86), 12.04(x64) and 13.04(x86)	8 years ago
 libinvisible.h	* tested on ubuntu 10.04(x86), 12.04(x64) and 13.04(x86)	8 years ago

README.md

adore-ng

linux rootkit adapted for 2.6 and 3.x



악성코드

루트킷

```
__int64 __fastcall proc_init(__int64 a1)
{
    __fentry__(a1);
    proc_file = proc_create_data("syslogk", 0LL, 0LL, &proc_fops, 0LL);
    return proc_file == 0 ? 0xFFFFFFFF4 : 0;
}
```



04

마치며

마치며

공격 특징

■ 정교하고 다양한 자원 활용

- 고객 정보 탈취만을 위한 악성코드를 자체 제작
- 공개되어 있는 코드를 활용해 공수 최소화
 - 공격 그룹 추적에 어려움 존재
- 해커가 원하는 때에만 악성코드 실행
- 루트킷을 이용한 악성코드 은닉
- 외부 서버를 시작으로 내부 서버까지 정밀 공격 수행



주식회사 엔키 (Enki Co., Ltd)
경기도 성남시 수정구 고등로 3, 411호
(현대지식산업센터 성남고등)
Mail. info@enki.co.kr
Tel. 031-722-1337 Fax. 031-722-1338