미국 통신·IT기업,
아시아 통신기업·정부기관 공격
리눅스 기반 BPFDoor 악성코드

(1) BPFDoor는
유닉스·리눅스 기반의 백도어 악성코드로
강력한 은닉기능이 특징이며
APT공격에 주로 사용됨.

(2) 해당 악성코드는
중국 해킹그룹인 레드멘션(Red Menshen)에서
활용하고 있으며 미국 통신·IT기업,
아시아 통신기업·정부기관을 공격한 악성코드로 알려짐.

(3) 일반적인 **서버 안티바이러스 · EDR 솔루션으로**
검출 및 격리할 수 있음.

(4) 그러나 운영서버는 **서버 안정성 문제**로
서버 안티바이러스 솔루션 설치율이 낮음.

1. BPFDoor 악성코드 특징

(1) 외부와의 통신 시 특정한
‘리슨 포트(Listen Port)’를 생성하지 않음.
리눅스 운영체제의 패킷 필터 기능 (BPF)을 활용하여
특정 조건의 네트워크 패킷만 골라내므로,
포트스캔 작업에 의해 검출되지 않음.

(2) 실행 시 은폐를 위해 **정상적인**
‘리눅스 시스템 데몬 이름’을 무작위로 선택하여 **사용**함.
시스템 관리자에게는 정상적인 시스템 데몬으로 인식되어
악성코드 구분이 어렵도록 위장함.

(3) **메모리 기반 파일시스템** 상에서 활동하며,
실행 후 자가삭제를 통해 디스크 내 흔적을 제거함.

(4) 외부명령 수신 및 전송 시
RC4 스트림 암호화 알고리즘을 사용함.
네트워크 기반 탐지 솔루션 우회수단으로 활용됨.

2. 프로세스 흐름

위장·은폐 메커니즘

실행위치	메모리 기반 파일 시스템 상에서 실행.
파일명 변경	실제 커널 유틸리티와 유사한 이름을 사용하여 정상 파일처럼 위장.
프로세스명 변경	일반적 리눅스 시스템 데몬 이름 10개 중 무작위로 1개 선택하여 변경.
자가삭제	실행 후에는 자가삭제를 통해 디스크 흔적 최소화.
분리	프로세스명 분리 및 데몬화. 정상 데몬처럼 백그라운드에서 동작.
RC4 기반 통신 암호화	RC4로 암호화된 데이터는 랜덤한 바이트열처럼 보이기 때문에 네트워크 기반 탐지 솔루션을 우회할 수 있음.

2. 프로세스 흐름

통신 메커니즘

BPF 설정	특정 조건을 만족시키는 패킷만 선택하도록 구성. 리슨 포트 생성 없음.
매직 패킷	매직 바이트(magic bytes)와 공격정보(공격자IP, 포트,명령어)가 포함된 특정 패킷에만 반응하며 해당 명령에 따라 악성행위 수행 • ‘socket’ 명령어: 호스트/서버내 방화벽 허용 룰셋 작업 수행 • ‘justforfun’ 명령어: 리버스쉘 환경 구성하여 공격자에게 제공 • 명령어 없음: 해당서버에 BPFDoor가 설치되어 있음을 알려주는 패킷을 공격자에게 전송

매직 패킷 (Magic Packet)

BPFDoor 악성코드가 감염된 서버를 제어할 명령어가 포함된 패킷.
명령어 앞에 매직 바이트(특정문자열:magic bytes)가 포함되어 있음.

3. 대응방안

(1) **리눅스 시스템에 등록된 BPF 필터**에서
의심스러운 BPF 프로그램을 식별하고
필터에서 **등록 해제**

(2) **서버 안티바이러스 솔루션**(Server-i AV 등)을 통한
스케쥴 **검사를 수행**하여
주기적으로 악성코드를 탐지 및 제거

(3) **리눅스 시스템**의 최신 **보안 업데이트** 설치

(4) 불필요한 **인터넷 아웃바운드 통신차단**

BPFDoor 악성코드에 관한 상세내용을 원하실 경우,
소만사 악성코드 분석센터에서 직접 테스트하고 분석한
'악성코드 분석리포트'를 보내 드립니다.

신청방법 : privacy@somansa.com으로 자료요청
또는 영업담당자에게 직접 문의

SOMANSA

4. 참고자료

[소만사 악성코드 분석리포트]
미국 통신·IT기업, 아시아 통신기업·정부기관 공격
BPFDoor 악성코드 분석 보고서
(상세 내용은 소만사 영업담당자에게 직접 문의)

BPFDoor's Hidden Controller Used Against Asia, Middle East Targets
https://www.trendmicro.com/en_us/research/25/d/bpfdoor-hidden-controller.html

PwC Cyber Threats 2021: A Year in Retrospect
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf

Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications
https://www.congress.gov/crs-product/IF12798

A step-by-step BPFDoorc ompromise
https://www.countercraftsec.com/blog/a-step-by-step-bpfdoor-compromise/

* BPF (Berkeley Packet Filter)

(1) 버클리 패킷 필터(BPF)는
운영체제 커널 수준에서
네트워크 패킷을 필터링하고
캡처할 수 있도록 지원하는 메커니즘.

(2) 사용자 공간 프로그램은
필터 조건을 정의해 원하는 패킷만 수신할 수 있음.
이를 통해 **시스템 성능과 분석 효율성**을 높일 수 있음.

(3) **리눅스를 포함한**
대부분의 유닉스 계열 시스템에서 사용되며,
이를 확장한 **eBPF는**
보안 정책 적용, 커널 트레이싱 등
다양한 용도로 활용되고 있음