# (긴급) BPFDoor 점검도구 배포

[ 2025.5.2 ]

- 최근 이슈가 되고 있는 리눅스 악성코드 BPFDoor를 자체 점검할 수 있도록 점검도구를 배포하오니 활용하시기 바랍니다.

## 1. 개 요

- BPFDoor는 리눅스 커널 영역에서 실행되어 네트워크를 모니터링하다가 공격자의 특정 신호를 받아 원격 명령을 수행하는 방식으로 동작
- 이 같은 BPFDoor의 동작 방식을 고려, ❶네트워크 모니터링을 수행중인 프로세스를 식별하고 ❷해당 프로세스 관련 파일을 시스템 운영자에게 표출함으로써 시스템 운영자가 악성 여부를 확인할 수 있도록 도와주는 점검도구를 개발

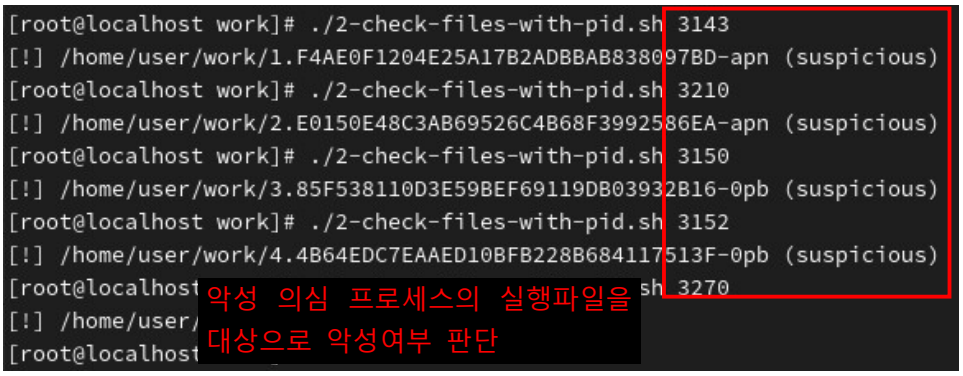
※ BPFDoor는 프로토콜·시그니처·매직패킷 처리방식 등을 기준으로 여러 종류로 구분할 수 있는데, 본 점검도구는 현재까지 파악된 5종에 대해 점검 가능

## 2. 사용 방법

1) 점검도구❶(1-check-network.sh)을 실행하면, 네트워크 상태 정보를 바탕으로 의심 프로세스를 식별하여 결과 출력

| | |
|---|---|
| 점검 방법 | **점검도구❶(1-check-network.sh) 실행** *root 권한 필요<br>※ (참고) '1-check-network.sh'는 아래 명령어로 구성(Oracle Linux 9.5 기준)<br>• **ss -apn \| grep -E ":1 \|:6 \|:17"**<br>> 비정상 로우(Low) 포트(1·6·17번) 탐지<br>• **ss -apn \| grep "ip:₩*" \| grep "UNCONN"**<br>> UNCONN 상태 Raw 소켓 탐지<br>• **ss –0pb \| grep -EB1 $((0x5293)) \| grep-EB1 $((0x7255))**<br>> 비정상 포트(0x5293→21139, 0x7255→29269) 사용 Raw 소켓·프로세스 탐지 |
| 실행 결과(예시) | [root@localhost work]# ./1-check-network.sh<br>[!] PID 3143 /usr/libexec/hald-addon-volume (suspicious)<br>[!] PID 3210 /usr/sbin/mcelog --daemon (suspicious)<br>[!] PID 3150 /usr/lib/systemd/systemd-machined (suspicious)<br>[!] PID 3152 /sbin/agetty --noclear tty1 linux (suspicious)<br>[!] PID 3270 /sbin/agetty --noclear tty1 linux (suspicious)<br>[root@localhost 자동으로 BPF Door 의심 프로세스 식별 |

2) '1)항'에서 식별된 프로세스의 PID를 참조하여 점검도구❷(2-check-files-with-pid.sh)를 실행하면, 해당 프로세스에 연결된 바이너리를 대상으로 패턴 매칭 결과 출력

| | |
|---|---|
| **점검 방법** | **의심 PID를 매개변수로, 점검도구❷(2-check-files-with-pid.sh) 실행** *root 권한 필요<br>※ (참고) '2-check-files-with-pid.sh'는 아래 명령어로 구성(Oracle Linux 9.5 기준)<br>• **xxd –p <의심파일> \| tr –d '₩n' \| grep –o "55720000"**<br>• **xxd –p <의심파일> \| tr –d '₩n' \| grep –o "93520000"**<br>> 의심 파일 내에서 BPFDoor 시그니처(55720000 • 93520000) 탐지 |
| **실행 결과(예시)** |  |

## 3. 주의 사항

- 위 점검도구는 다양한 리눅스 버전을 고려하여 개발되었으나, 실제 운용 환경에서 오탐•미작동 가능성도 있으므로, 각급기관 담당자께서는 점검도구의 소스코드를 검토하여 기관 시스템 환경에 적합한지 확인 후 활용(필요시 수정 가능)

## 4. 적용 가능한 리눅스 배포판 목록

| 배포판 | 버전 | 출시일자 |
|---|---|---|
| SUSE Linux Enterprise Server | 15 SP6 | 2024-06-01 |
| | 15 SP5 | 2023-06-01 |
| | 15 SP4 | 2022-06-01 |
| | 15 SP3 | 2021-06-01 |
| | 15 SP2 | 2020-07-01 |
| | 15 SP1 | 2019-06-01 |
| | 15 | 2018-07-01 |
| | 12 SP5 | 2019-12-01 |
| | 12 SP4 | 2018-12-01 |
| | 12 SP3 | 2017-08-01 |
| | 12 SP2 | 2016-11-01 |
| | 12 SP1 | 2015-12-01 |
| | 12 | 2014-11-01 |

| 배포판 | 버전 | 출시일자 |
|---|---|---|
| CentOS(Stream) | 10 | 2024-12-12 |
| | 9 | 2021-12-03 |
| | 8 | 2019-09-24 |
| | 7 | 2014-07-07 |
| Ubuntu | 24.04 | 2024-04-25 |
| | 22.04 | 2022-04-21 |
| | 20.04 | 2020-04-23 |
| | 18.04 | 2018-04-27 |
| | 16.04 | 2016-04-21 |
| | 14.04 | 2014-04-17 |
| RedHatEnterprise Linux | 9.5 | 2024-11-13 |
| | 8.1 | 2019-07-24 |
| | 7.9 | 2020-05-20 |
| | 7.7 | 2019-06-05 |
| | 7.5 | 2018-01-24 |
| | 7.4 | 2017-05-23 |
| | 7.3 | 2016-08-25 |
| | 7.2 | 2015-08-31 |
| | 7.1 | 2015-03-03 |
| | 7.0 | 2013-12-11 |
| Oracle Linux | 9.5 | 2024-11-19 |
| | 9.3 | 2023-11-15 |
| | 8.8 | 2023-05-24 |
| | 7.7 | 2019-08-15 |
| | 7.3 | 2016-11-10 |
| | 7.2 | 2015-11-25 |
| | 7.0 | 2014-07-23 |

## 5. 조치 사항

- 각급 기관 등은 자체 점검 후, 이상 징후가 확인되었을 경우 국가사이버안보센터(cert@ncsc.go.kr)로 통보 바랍니다.

## ※ 참고사이트


1. https://trendmicro.com/en_us/research/25/d/bpfdoor-hidden-controller.html
2. https://asec.ahnlab.com/ko/83742
3. https://s2w.medium.com/detailed-analysis-of-bpfdoor-targeting-south-korean-company-328171880a98


. 끝.