



[2025.05.22]

- 최근 국내기업 주요 시스템에 BPFDoor 악성코드가 유포되어 4.26(토), 5.2(금), 5.4(일) 세 차례에 걸쳐 점검 방법 및 점검 도구를 포함한 보안권고문을 배포한 바 있습니다.
- 이에, 현재까지 해당 해킹사고에서 확인된 BPFDoor 악성코드를 자체 점검할 수 있도록 스크립트 형태의 점검 도구를 공유하오니 각급 기관에서는 전산망 점검 등 보안 조치에 활용하시기 바랍니다.

① 개 요

- BPFDoor 백도어는 리눅스 커널 영역에서 정상 프로세스로 위장하여 실행되며 네트워크 신호 모니터링을 통해 공격자 접속 확인 후 원격 명령을 수행합니다.
- 또한, 백도어에 명령을 전송하고 그 결과를 수신하는 컨트롤러 및 경유지에 접속하여 공격자의 지령을 송·수신하는 악성코드도 확인되어 점검 도구에 반영하였습니다.

② 주의 사항

- 첨부된 압축 파일(file.zip)에는 악성코드가 ↗. 실행 중일 때 탐지하는 '[BPFDoor_Process_Scan.sh](#)'와 ↘. 파일 형태로 저장 중일 때 탐지하는 '[BPFDoor_File_Scan.sh](#)'가 들어 있습니다.
- 해당 파일들은 쉘 스크립트로 제작되어 다양한 리눅스 환경과 상황을 고려하여 테스트 하였습니다. 다만, 실제 운영 환경에서 예상치 못한 결과가 발생할 수 있는데 이럴 때는 귀측의 환경에 맞도록 점검 도구의 소스코드를 검토하여 명령어 및 도구를 재사용하길 권고합니다.

③ 사용 방법

- 점검 도구 실행시 ①관리자 권한이 필요하며 ②'chmod 777 + 파일명' 명령을 통해 실행 가능한 형태로 변환후 사용합니다.

```
File Edit View Search Terminal Help
[test@localhost BPFDoor]$ su ①관리자 권한 획득
Password:
[root@localhost BPFDoor]# chmod 777 BPFDoor_Process_Scan.sh
[root@localhost BPFDoor]# chmod 777 BPFDoor_File_Scan.sh
②파일 실행 권한 획득
```

- ㄱ. (**BPFDoor_Process_Scan.sh**) Raw 패킷과 프로세스 검색을 통해 악성코드가 실행되는 것으로 의심되는 프로세스를 찾고 파일 내부에 저장된 BPFDoor의 주요 특징 비교를 통해 총 3가지 형태의 악성코드가 실행되고 있는지 확인합니다.

점검 방법	./BPFDoor_Process_Scan.sh => 서버에서 Terminal을 이용해 해당 파일 실행
실행결과(예시)	<p>정상</p> <pre>File Edit View Search Terminal Help [root@localhost BPFDoor]# ./BPFDoor_Process_Scan.sh [Scan Start] ① 파일 실행 ----- [Stage 0] Root Privilege Check OK!! [Stage 1] BPFDoor Check OK!! [Stage 2] BPFDoor Controller Check OK!! [Stage 3] BPFDoor Variant Check OK!! ***** [Total Result] ***** - Total Suspicious:0 - Total Malicious:0 ② 탐지 결과 이상 없음!! ----- [Scan Finish] [root@localhost BPFDoor]#</pre>

실행결과(예시)	탐지 <pre> File Edit View Search Terminal Help [root@localhost BPFDoor]\$./BPFDoor_Process_Scan.sh ① 파일 실행 [Scan Start] ----- [Stage 0] Root Privilege Check OK!! [Stage 1] BPFDoor Check [Malicious] PID: 58736 File: /home/test/test/file2 -> 악성코드 탐지 [Malicious] PID: 58728 File: /home/test/test/file1 -> 악성코드 탐지 [Stage 2] BPFDoor Controller Check [Malicious] PID: 58759 File: /home/test/test/file3 -> 악성코드 탐지 [Stage 3] BPFDoor Variant Check [Malicious] PID: 58775 File: /home/test/test/file4 -> 악성코드 탐지 ***** [Total Result] ***** - Total Suspicious:0 - Total Malicious:4 ② 악성코드 4개 탐지!!! -----</pre> <p>[Scan Finish]</p> <p>[root@localhost BPFDoor]\$ S■</p>
----------	---

└. (**BPFDoor_File_Scan.sh**) 시스템에 저장된 BPFDoor 악성코드를 찾아서 탐지합니다. 다만, 전체 폴더 검색 시 장시간 소요될 수 있으니 /dev, /var, /bin, /usr, /opt, /local, /share는 필수로 확인하시고 그 외는 각 기관의 환경에 따라 검색 대상을 선정하시면 됩니다.

점검 방법	./BPFDoor_File_Scan.sh '폴더명'=> 서버에서 Terminal을 이용해 폴더 지정 후 해당 파일 실행
실행결과(예시)	정상 <pre> File Edit View Search Terminal Help [root@localhost BPFDoor]# ./BPFDoor_File_Scan.sh /dev ① 파일 실행 + 폴더 지정 [Scan Start] ----- [Stage 0] Root Privilege Check OK!! [Stage 1] BPFDoor Check OK!! ***** [Total Result] ***** - Total Malicious:0 ② 탐지 결과 이상 없음!! -----</pre> <p>[Scan Finish]</p> <p>[root@localhost BPFDoor]# ■</p>

실행결과(예시)	탐지 <pre> File Edit View Search Terminal Help [root@localhost BPFDoor]# ./BPFDoor_File_Scan.sh /test [Scan Start] ----- [Stage 0] Root Privilege Check OK!! [Stage 1] BPFDoor Check /test/file1 -> 악성코드 탐지 /test/file2 -> 악성코드 탐지 /test/file3 -> 악성코드 탐지 /test/file4 -> 악성코드 탐지 ***** [Total Result] ***** - Total Malicious:4 ----- [Scan Finish] [root@localhost BPFDoor]# </pre>
----------	---

④ 조치 사항

- 각급 기관은 자체 점검 중에 문제가 발생하면 화면 캡쳐 및 설명과 함께 'analysis@ncsc.go.kr'로 메일을 보내주시고 문의사항은 '02-2210-8043'으로 하시면 됩니다. 그리고 각 기관별 점검 상황을 파악하고 있으니 이 권고문의 NCTI 게시물에 '조치 사항'을 업데이트해 주시기 바랍니다.