NIS NCSC

[긴급] 국내기업 주요 시스템 공격에 악용된 리눅스 악성코드 주의 권고(2차)

[2025.05.04]

- 최근 국내기업 주요 시스템에 리눅스 악성코드(백도어 기능)가 유포되어 4.26(토) 점검 방법을 포함한 보안권고문을 배포한바 있습니다.
- 악성코드 8종이 추가 발견되었는데, 그중 2종이 기존 보안권고문으로 탐지되지 않아 추가 확인 방법을 공유하오니 각급기관에서는 전산망 점검 등 보안조치 바랍니다.

❶ 개 요

- 최근 국내기업 주요 시스템 커널 영역에서 실행되며 공격자의 신호 대기 후 원격 명령을 수행하는 리눅스 악성코드가 확인되었습니다.
  - 4.26 각급기관이 감염여부를 자체점검토록 확인방법을 공유하였는데 이번에 기존 점검 방법으로는 확인이 곤란한 악성코드가 입수되었기에 추가 확인방법을 알려드립니다.

❷ 주요 침해지표

연번	구분	내용	설명
1	악성코드 (MD5)	3c54d788de1bf6bd2e7bc7af39270540	'BPFDoor 백도어' 기존(4.26) 보안권고문으로 탐지 가능
2		fbe4d008a79f09c2d46b0bcb1ba926b3	
3		c2415a464ce17d54b01fc91805f68967	
4		aba893ffb1179b2a0530fe4f0daf94da	
5		e2c2f1a1fbd66b4973c0373200130676	
6		dc3361ce344917da20f1b8cb4ae0b31d	

연번	구분	내용	설명
7	악성코드 (MD5)	5f6f79d276a2d84e74047358be4f7ee1	'BPFDoor 컨트롤러'
8		0bcd4f14e7d8a3dc908b5c17183269a4	신규 탐지방법 적용 필요

❸ 주요 특징 및 자체 점검 방법

- BPFDoor 컨트롤러는 'abrtd' 프로세스 이름으로 자신을 실행하므로 해당 프로세스 명이 실제 동작 중인지 확인하고 해당 파일의 실제 위치를 파악합니다. (해당 경로에 저장된 파일이 귀측에서 사용 중인 정상 프로그램인 경우 신고는 불필요하며, 악의적인 동작으로 의심되는 경우는 아래로 신고 바랍니다.)

점검 방법	ㄱ. ps -ef | grep "abrtd" => 확인되는 경우, ㄴ. 진행 ㄴ. ls -l /proc/(의심 프로세스 PID)/exe
실행결과(예시)	ㄱ [root@localhost test]# ps -ef | grep "abrtd" root 4471 2851 0 20:54 pts/1 00:00:00 /usr/sbin/abrtd root 의심 PID 4500 2523 0 20:55 pts/0 00:00:00 grep --color=auto abrtd
	ㄴ [root@localhost test]# ls -l /proc/4471/exe lrwxrwxrwx. 1 root root 0 5월 3 20:55 /proc/4471/exe ->
/home/test/5f6f79d276a2d84e74047358be4f7ee1 파일 경로

* ❸번 점검 방법은 BPFDoor 컨트롤러가 실제 동작 중일 경우 탐지되므로, 미실행일 경우를 대비하여 上記 표 연번 7~8번에 있는 MD5값 검색도 추가 진행하시기 바랍니다.

❹ 조치 사항

- 각급 기관 등은 자체 점검 중 '점검 방법' 관련 문의는 국가사이버안보센터(02-2210-8043), '이상 징후'가 확인되었을 경우 '02-2210-8039, cert@ncsc.go.kr' 으로 신속 통보 바랍니다.