NIS NCSC

국내기업 주요 시스템 공격에 악용된 리눅스 악성코드 주의 권고

[2025.04.26]

- 최근 국내기업 주요 시스템에 리눅스 악성코드(백도어 기능)가 감염되어 전산망에 침투한 사실이 확인되었습니다.
- 이와 관련, 위협 정보 및 자체 감염 여부 확인 방법을 공유하오니 각급 기관에서는 전산망 점검 등 관련 보안 조치 바랍니다.

❶ 개 요

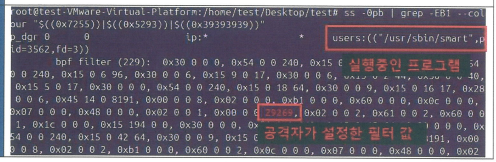
- 최근 국내기업 주요 시스템 커널 영역에서 실행되며 공격자의 신호 대기 후 원격 명령을 수행하는 리눅스 악성코드가 확인되었습니다.
  - 이와 관련, 아래와 같이 관련 정보를 공유하오니 기관 보안담당자는 감염 여부를 자체 점검하시어 추가 피해가 발생하지 않도록 유의하시기 바랍니다.

❷ 주요 침해지표

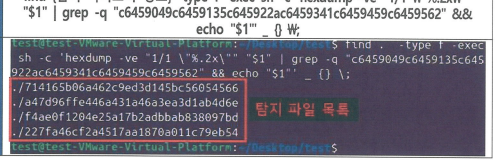
구분	내용	설명
악성코드 (MD5)	a47d96ffe446a431a46a3ea3d1ab4d6e	리버스 백도어 기능
	227fa46cf2a4517aa1870a011c79eb54	
	f4ae0f1204e25a17b2adbbab838097bd	
	714165b06a462c9ed3d145bc56054566	
경유지	165.232.174[.]130	탈취정보 저장용 (클라우드 업체 정상 서비스 IP)

❸ 주요 특징 및 자체 점검 방법

ㄱ. 악성코드는 공격자 접속 여부를 확인하기 위해 특정 패킷에서 '0x7255', '0x5293' ,'0x39393939' 값이 유입되는지 필터를 걸어 실시간으로 확인합니다. 이에, 리눅스 기본 명령어를 통한 해당 필터값을 확인합니다.

점검 방법	ss -0pb | grep -EB1 --colour "$((0x7255))\|$((0x5293))|$((0x39393939))"
실행결과(예시)	

ㄴ. 해당 악성코드에는 공통적으로 파일 내부에 'I5*AYbs@LdaWbs0' 문자열을 포함하고 있는데 단순 'strings' 명령으로는 찾을 수 없습니다. 이에, 아래와 같이 해당 문자열을 포함하고 있는 파일을 확인합니다.

점검 방법	find {검색 디렉토리 경로} -type f -exec sh -c 'hexdump -ve "1/1 ₩"%.2x₩"" "$1" | grep -q "c6459049c6459135c645922ac6459341c6459459c6459562" && echo "$1"' _ {} ₩;
실행결과(예시)	

ㄷ. 악성코드는 공격자가 전송한 명령에 따라 방화벽을 해제하고 특정 포트(42391~43391)를 오픈하고 대기하는 기능도 포함합니다. 이에, 해당 기능을 수행하고 있는지 확인합니다. (아래 점검 방법은 '42300~43399' 포트 대역 오픈 여부를 확인하는 기능이며, 이중 42391~43391 포트가 오픈되었다면 정밀 확인하시기 바랍니다.)

점검 방법	netstat -lpn | grep -E ':42[3-9][0-9]{2}|43[0-3][0-9]{2}'
실행결과(예시)	test@test-VMware-Virtual-Platform:~$ netstat -lpn | grep -E ':42[3-9][0-9]{2}|43[0-3][0-9]{2}' (Not all processes could be identified, non-owned process info will not be shown, you would have to be root to see it all.) tcp 0 0 127.0.0.1:4444 0.0.0.0:* LISTEN 7046/python3 열려 있는 포트

❹ 조치 사항

- 각급 기관 등은 자체 점검 후, 이상 징후가 확인되었을 경우 국가사이버안보센터(02-2210-8039, cert@ncsc.go.kr)로 신속 통보 바랍니다.