

# BPF도어 공격 위협정보 및 대응 방법 안내

<'25.04.30(수), 의료정보보호센터>

## □ 개요

- 최근 국내기업 주요 시스템을 대상으로 해킹 공격하는 사례가 확인되어 위협 정보 공유
- BPF도어<sup>1)</sup> 악성코드를 이용한 백도어<sup>2)</sup> 공격 주의 필요

## □ 주요 내용

- (상세 내용) 알 수 없는 경로에 아래 4개의 악성코드를 설치하고 공격 IP로 통신
  - 대상 시스템 : 리눅스 서버
  - 공격 IP : 165.232.174[.]130
  - 악성코드 해시값 및 파일정보

악성코드 명	size	해시값
hpsasmrld	2,265KB	(SHA256) c7f693f7f85b01a8c0e561bd369845f40bff423b0743c7aa0f4c323d9133b5d4
		(MD5) a47d96ffe446a431a46a3ea3d1ab4d6e
smartadm	2,067KB	(SHA256) 3f6f108db37d18519f47c5e4182e5e33cc795564f286ae770aa03372133d15c4
		(MD5) 227fa46cf2a4517aa1870a011c79eb54
hald-addon-volume	2,071KB	(SHA256) 95fd8a70c4b18a9a669fec6eb82dac0ba6a9236ac42a5ecde270330b66f51595
		(MD5) f4ae0f1204e25a17b2adbbab838097bd
dbus-srv-bin.txt	34KB	(SHA256) aa779e83ff5271d3f2d270eaed16751a109eb722fca61465d86317e03bbf49e4
		(MD5) 714165b06a462c9ed3d145bc56054566

- 1) Berkeley Packet Filer Door로 평소에는 통신하지 않으나 특정 패킷이 들어오면 프로세스가 활성화 되어 아웃바운드 통신 포트를 개방함. 공격자는 해당 모듈을 통해 명령어를 수행하고 정보를 탈취함
- 2) 컴퓨터 시스템이나 네트워크의 보안을 우회하여 접근할 수 있게 해주는 비밀 통로 또는 숨겨진 방법을 의미

## □ 대응 방법

- 상기 위협정보를 참고하여 자체적으로 보안점검\* 후, 침입 흔적 및 침해사고가 확인되면 의료정보보호센터나 보호나라를 통해 침해사고 즉시 신고

\* 보안점검 방법은 [붙임] 자체 보안점검 방법 참조

### ○ 침해사고 발생 시 아래 절차를 통해 침해사고 신고

- 침해사고 시스템이 진료 정보를 보유하고 있는 경우  
의료정보보호센터(<https://www.hisc.or.kr>) > 침해사고 신고 > 사고 신고
- 침해사고 시스템이 진료 정보를 보유하고 있지 않은 경우  
보호나라(<https://www.boho.or.kr>) > 침해사고 신고 > 신고하기

### ○ 악성코드 감염예방을 위한 아래 수칙 등 준수

- 운영체제 및 사용 프로그램 최신버전으로 유지
- 백신프로그램 설치 및 최신버전으로 유지, 주기적 업데이트 실행
- 백신프로그램 실시간 탐지 활성화 및 주기적 검사 실행
- 출처가 불분명한 파일 다운로드 및 실행 금지
- 정품 소프트웨어 사용 및 불필요한 프로그램 사용 지양

## □ 기타 권고사항

- 의료기관에서 운영중인 시스템 중, 개인의 민감정보, 사생활, 자산 등에 대한 정보를 열람, 발급 할수 있도록 제공하고 있는 시스템의 경우 휴대폰 본인확인 인증 외에 모바일 신분증, 전자서명(공동·금융인증서, 간편인증) 등 보다 안전한 수단으로 인증 절차 추가

## □ 기타

### ○ (출처)

- <https://www.krcert.or.kr/kr/bbs/view.do?searchCnd=&bbsId=B0000133&searchWrd=&menuNo=205020&pageIndex=1&categoryCode=&nttId=71726>

### ○ (연락처) 의료정보보호센터

- email : [cert@hisac.or.kr](mailto:cert@hisac.or.kr) - Tel : 02-6360-6280

## 자체 보안점검 방법

- ❶ 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 -t   grep -EB1 --colour "\$((0x7255)) \$((0x5293)) \$((0x39393939))"
실행결과 (예시)	<pre> root@test-VMware-Virtual-Platform:/home/test/Desktop/test# ss -t   grep -EB1 --colour "\$((0x7255)) \$((0x5293)) \$((0x39393939))" State     Recv-Q    Send-Q     Local Address:Port      Peer Address:Port  Process tcp        0      0      *          *          *          *          users:(("/usr/sbin/smart",p id=3562,fd=3)) bpf filter (229):  0x30 0 0 0, 0x54 0 0 240, 0x15 0 0 0, 실행중인 프로그램 54 0 0 240, 0x15 0 6 96, 0x30 0 0 6, 0x15 9 0 17, 0x30 0 0 6, 0x15 0 2 24, 0x30 0 0 40, 0x15 5 0 17, 0x30 0 0 0, 0x54 0 0 240, 0x15 0 18 64, 0x30 0 0 9, 0x15 0 16 17, 0x28 0 0 6, 0x45 14 0 8191, 0x00 0 0 8, 0x02 0 0 8, 0x0b1 0 0 0, 0x60 0 0 0, 0x0c 0 0 0, 0x07 0 0, 0x48 0 0 0, 0x02 0 0 1, 0x00 0 0 0, 29269, 0x02 0 0 2, 0x61 0 0 2, 0x60 0 0 1, 0x1c 0 0 0, 0x15 194 0 0, 0x30 0 0 0, 0x15 0 0 0, 0x15 0 0 0, 0x15 0 0 0, 0x 54 0 0 240, 0x15 0 42 64, 0x30 0 0 9, 0x15 0 0 0, 0x15 0 0 0, 0x15 0 0 0, 191, 0x00 0 0 8, 0x02 0 0 2, 0xb1 0 0 0, 0x60 0 0 2, 0x0c 0 0 0, 0x07 0 0 0, 0x48 0 0 0, 0x02 </pre>

- ② 해당 악성코드는 공통적으로 파일 내부에 '15\*AYbs@LdaWbs0' 문자열을 포함하고 있는데 단순 'strings' 명령으로는 찾을 수 없습니다. 이에, 아래와 같이 해당 문자열을 포함하고 있는지 파일을 확인합니다.

<p><b>점검 방법</b></p>	<pre>find 검색 디렉토리 경로 -type f -exec sh -c 'hexdump -ve "1/1" "%.2x" "" "\$1"   grep -q "c6459049c6459135c645922ac6459341c6459459c6459562" &amp;&amp; echo "\$1" _ ;</pre>
<p><b>실행결과 (예시)</b></p>	<pre>test@test-VMware-Virtual-Platform:~/Desktop/test\$ find . -type f -exec sh -c 'hexdump -ve "1/1" "%.2x\\"" "\$1"   grep -q "c6459049c6459135c645 922ac6459341c6459459c6459562" &amp;&amp; echo "\$1" _ {} \;</pre> <div style="border: 2px solid red; padding: 5px; display: inline-block;"> <pre>./714165b06a462c9ed3d145bc56054566 ./a47d96ffe446a431a46a3ea3d1ab4d6e ./f4ae0f1204e25a17b2adbbab838097bd ./227fa46cf2a4517aa1870a011c79eb54</pre> </div> <p><b>탐지 파일 목록</b></p> <pre>test@test-VMware-Virtual-Platform:~/Desktop/test\$</pre>

- ③ 악성코드는 공격자가 전송한 명령에 따라 OS 방화벽을 해제하고 특정 포트 (42391~43391)를 개방한 후, 대기하는 기능도 포함합니다. 이에, 해당 기능을 수행하고 있는지 확인합니다.

(아래 점검 방법은 '42300~43399' 포트 대역 개방 여부를 확인하는 기능이며,  
이 중 42391~43391 포트가 개방되어 있다면 정밀 확인하시기 바랍니다.)

점검 방법	netstat -lpn   grep -E ':42[3-9][0-9] 2  43[0-3][0-9] 2 '
실행결과 (예시)	<pre> test@test-VMware-Virtual-Platform: ~/Desktop/test/test2/22027575120\$ 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 0.0.0.0:4243 0.0.0.0:*        LISTEN      7046/python3 </pre> <p style="text-align: center;">열려 있는 포트</p>