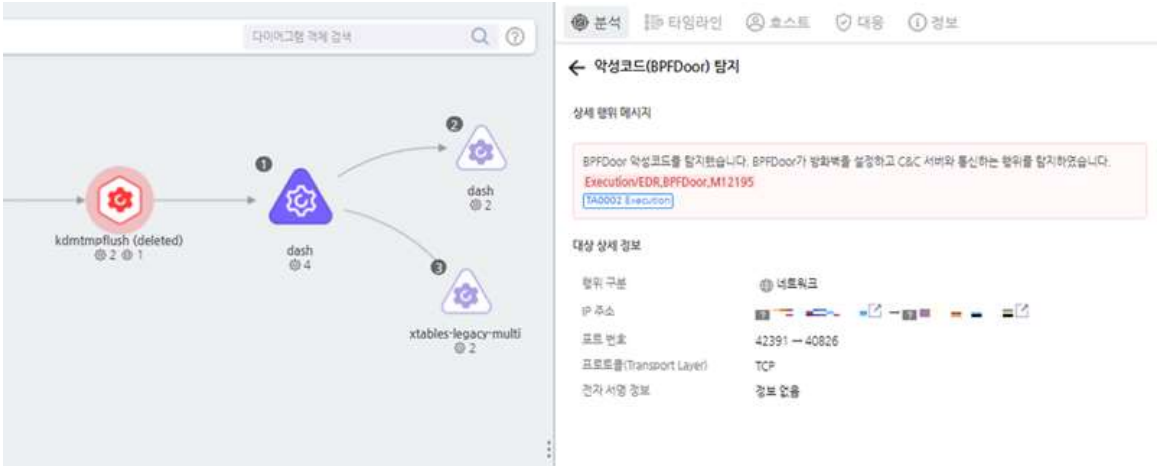
BPFDoor 악성코드, 차세대 보안 모델로 극복하기

지난 4월, 국내 통신사의 다수 고객 유심 정보가 외부 공격에 의해 유출되는 사고가 발생했다. 본 사건은 통신사의 리눅스 기반 서버에 침입한 해커가 BPFDoor 계열 악성코드를 설치해 벌어진 것으로 알려졌다.

안랩은 지난해 10월, 자사 EDR 솔루션인 AhnLab EDR을 활용해 통신사 공격에 활용된 악성코드와 유사한 BPFDoor 계열 악성코드를 탐지해 분석 내용을 공개했다. 통신사 공격에 사용된 BPFDoor는 당시 탐지했던 악성코드와 몇 가지 차이점이 있지만 주요 기능들은 대부분 동일하다.



[그림 1] AhnLab EDR로 탐지한 BPFDoor 악성코드 - 2024년 10월

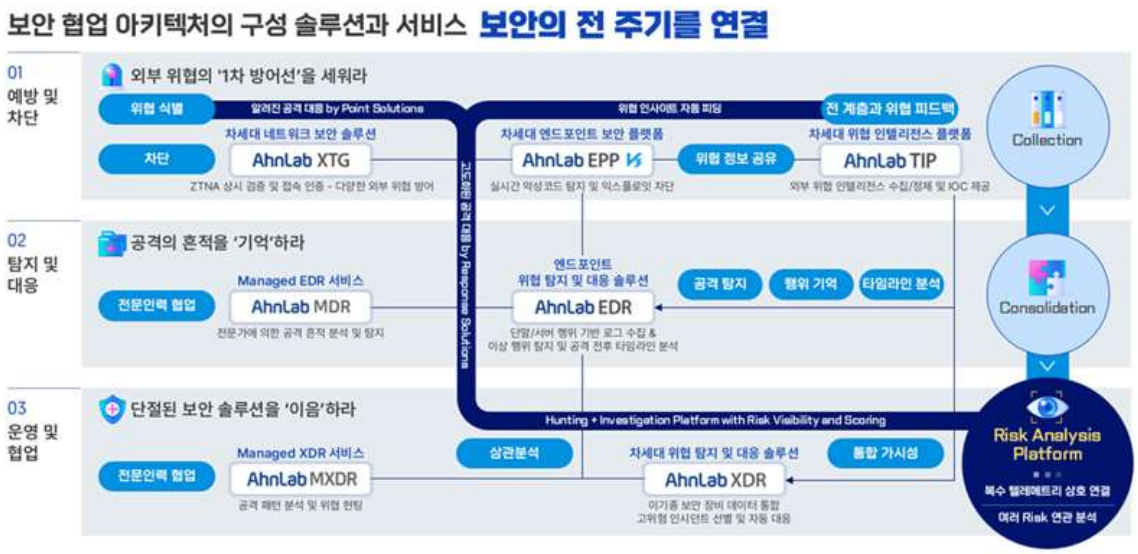
AhnLab EDR 외에도 안랩은 샌드박스 솔루션 AhnLab MDS의 동적 분석 역량을 활용해 악성코드와 관련 행위 및 악성 패킷에 대응한다. 리눅스 서버 백신 V3 Net for Linux와 네트워크 보안 솔루션 AhnLab XTG 및 AhnLab AIPS, 클라우드 워크로드 보안 플랫폼 AhnLab CPP의 Host IPS에는 탐지 시그니처를 적용해 BPFDoor를 사전 차단할 수 있도록 지원해오고 있다. 위협 인텔리전스 플랫폼 AhnLab TIP는 BPFDoor와 관련된 위협 정보를 빠르게 공유한다.

제품명	탐지 대상	역할
AhnLab EDR	공격 관련 모든 이벤트	- 방화벽 설정 변경, 포트 리다이렉트 등 행위 탐지 - 보안 솔루션 우회 행위 탐지 - 컨텍스트 분석을 통한 공격 캠페인 이해
V3 Net for Linux Server	알려진 악성코드	- 서버 유입 악성코드의 시그니처 기반 탐지 및 치료
AhnLab XTG	알려진 악성 패킷	- 시그니처 기반 '매직 패킷' 차단 (방화벽의 IPS 기능)
AhnLab AIPS	알려진 악성 패킷	- 시그니처 기반 '매직 패킷' 차단

AhnLab TIP	공격 관련 모든 위협정보	- 악성코드 최신 동향 및 IoC 정보를 보안 운영에 적용
AhnLab MDS	알려진 악성코드 및 악성 패킷 공격 관련 이벤트	- 유입 악성코드 시그니처 기반 탐지 및 치료 - 시그니처 기반 '매직 패킷' 차단 - 방화벽 설정 변경, 포트 리다이렉트, 우회 행위 등 탐지 (동적 분석)
AhnLab CPP(Host IPS)	알려진 악성 패킷	- 시그니처 기반 '매직 패킷' 차단

[표] 안랩 솔루션의 BPFDoor 악성코드 대응 내용

더 나아가, 안랩은 고객들이 중장기적으로 BPFDoor와 같은 고도화된 공격으로부터 조직을 효과적으로 보호할 수 있도록 ▲예방 및 차단 ▲탐지 및 대응 ▲운영 및 협업까지 사이버 보안 사이클을 아우르는 솔루션-서비스 연계 보안 모델을 제시하고 있다.



[그림 2] 안랩 차세대 보안 모델 아키텍처

이번 케이스스터디에서는 BPFDoor 악성코드의 특징과 안랩의 대응 현황 및 자사 차세대 보안 모델을 활용한 보안 방안을 소개한다.

▶BPFDoor와 안랩 차세대 보안 모델 케이스스터디 다운로드

콘텐츠마케팅팀

신재만 과장