수집DB를 활용한 악성코드 관리

1. 수집 DB란?

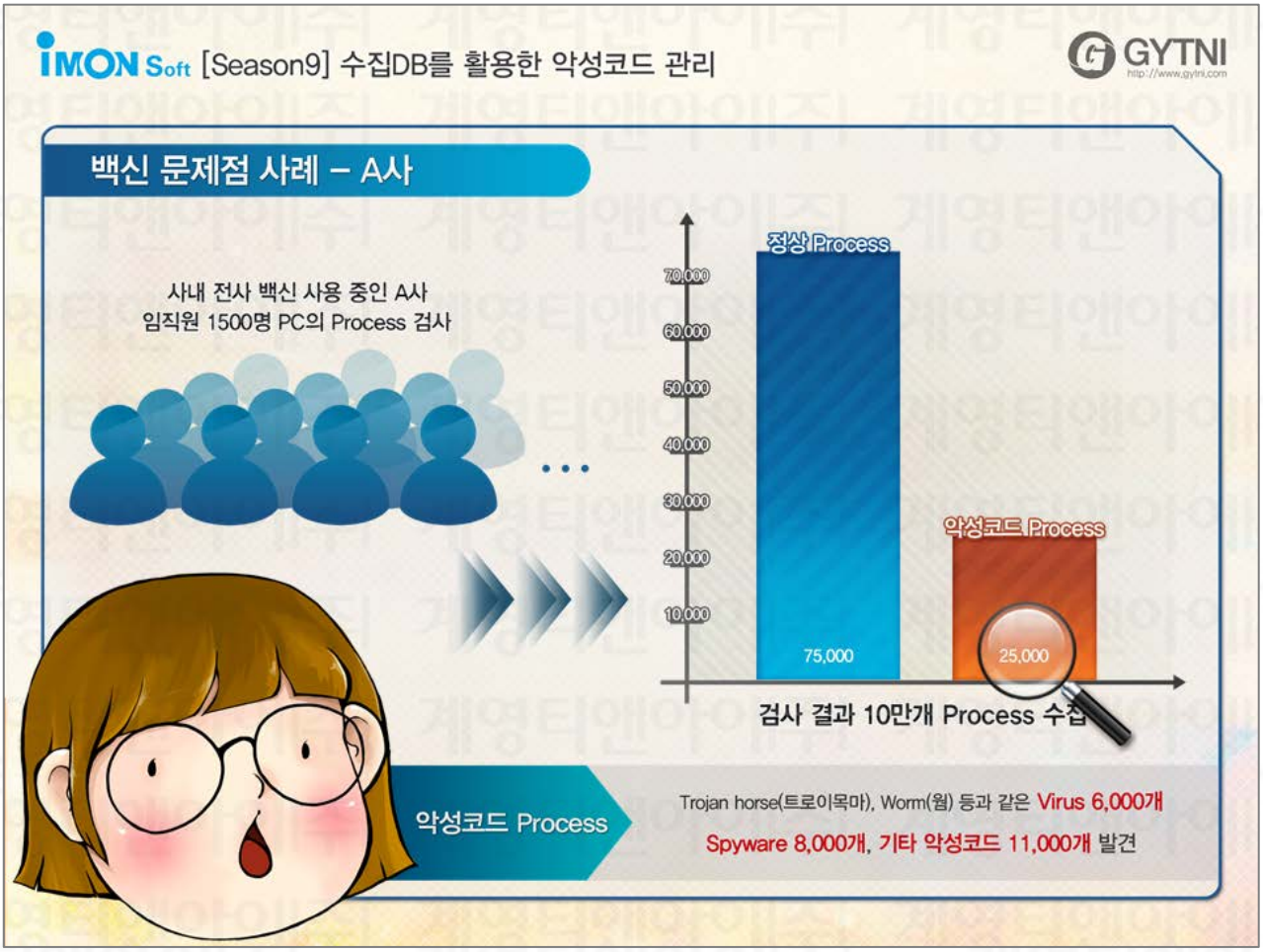
2. 기존 백신의 악성코드 관리 문제점

3. 수집DB를 활용한 악성코드 관리 (DB: 데이터의 집합 또는 데이터 공유를 위한 서비스)

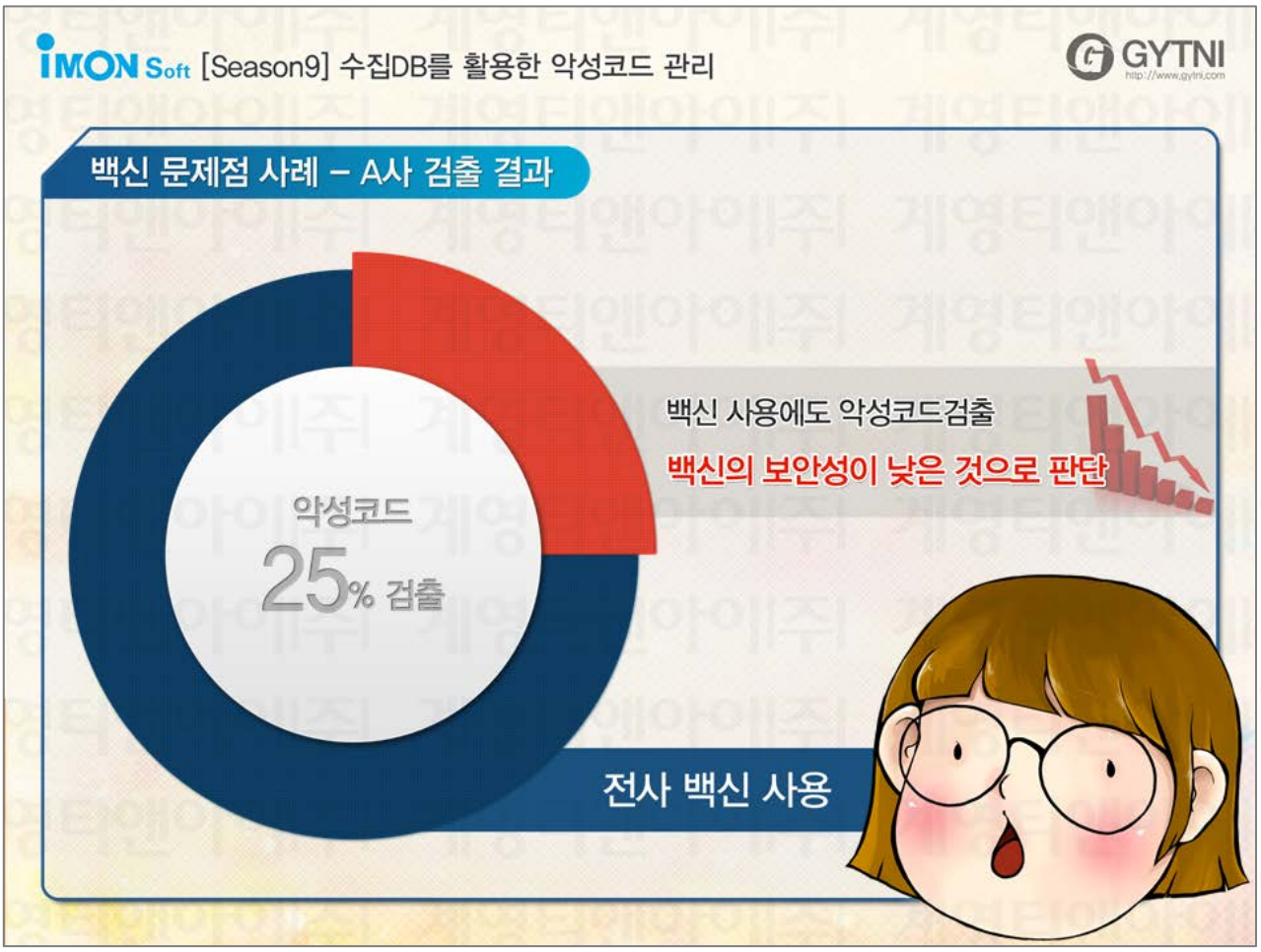
1. 수집DB란?

- 기업 및 기관의 임직원 PC내 존재하는 Process 수집 정보
- Hash값/제어판명/저작권사 등 수집

2. 기존 백신의 악성코드 관리 문제점

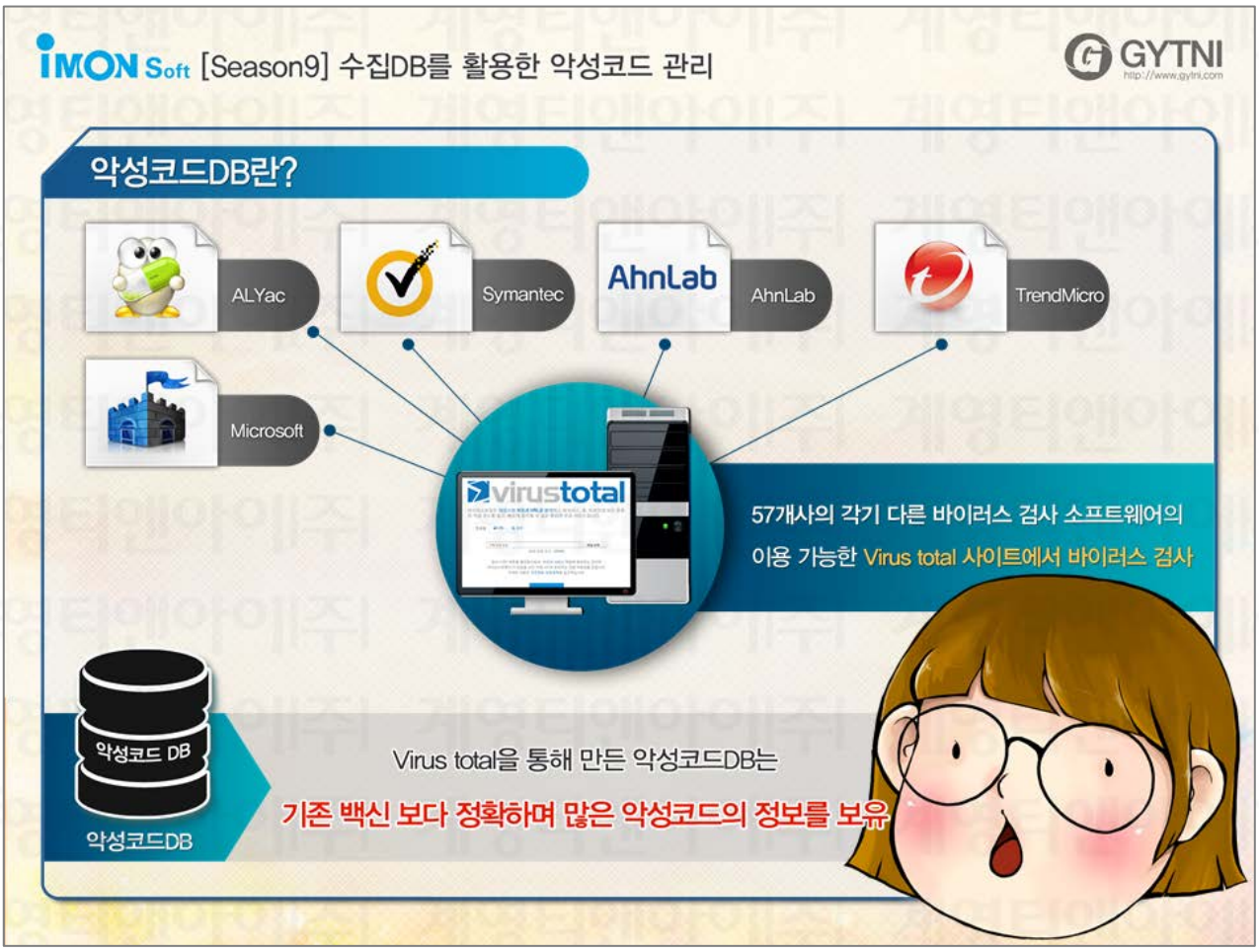


- 문제점: 백신 기업마다 가지고 있는 차단 항목이 한정되어 있어 항목 외 악성코드는 차단되지 않으며 지속적으로 생성되는 신종/변종 악성코드 현황 파악이 느려 악성코드로 인한 피해 가능성 多
- 사례: 사내 전사 백신을 사용 중인 A사의 임직원 1500명 PC Process를 검사해본 결과 10만개 Process 중 25000개의 Process에서 악성코드 발견
  - ▶ 25000개 중 6000개의 Trojan horse(트로이목마), Worm(웜) 등과 같은 Virus와 8000개의 Spyware, 11000개의 기타 악성코드 존재



- A사 문제: 사내 전사 백신이 설치되어 있지만 전체 Process 중 25%에 해당되는 Process에서 악성코드가 검출돼 백신의 보안성이 낮은 것으로 판단되며 이러한 상황이 지속될 경우 존재하는 악성코드로 인한 피해 가능성 증가

3. 수집DB를 활용한 악성코드 관리 (DB: 데이터의 집합 또는 데이터 공유를 위한 서비스)



- 57가지의 바이러스 검사 소프트웨어를 이용할 수 있는 사이트인 Virus total에서 바이러스 검사를 통해 만든 악성코드 DB는 기존 백신보다 정확하며 많은 악성코드의 정보를 보유
- 프로세스 수집현황(수집DB)을 악성코드 DB와 비교
  : 수집현황(수집DB)과 악성코드DB 현황을 비교하여 일치 Process를 검출
  검출된 Process를 Virus, Spyware, 기타 악성코드로 분류
- 기업 및 기관에서는 악성코드DB와 비교해 검출된 정보 확인 가능하며 지속적인 삭제관리 필요

수집 DB 를 활용한 악성코드 관리 대본

안녕하세요! 모니입니다~
이번 시간에는 수집 DB를 활용한 악성코드 관리에 대해 배워볼게요~

먼저 수집DB란 무엇일까요?

기업 및 기관의 임직원 PC에서 한번이라도 실행되었던 프로그램의 정보 값을 수집한 것을 수집DB라고 합니다.

수집DB를 활용해 악성코드를 관리하는 이유는 불법 S/W, 프리웨어 등을 설치 시 사용자 모르게 설치되는 악성코드를 차단해야 하는데 기존 백신은 백신 기업 마다 가지고 있는 차단 항목이 한정되어 있어 항목 외 악성코드는 차단되지 않습니다.

또한 지속적으로 생성되는 신종/변종 악성코드 현황 파악이 느려 신종/변종 악성코드로 인한 피해 가능성이 존재합니다.

사례로 사내 전사 백신을 사용 중인 A사의 임직원 1500명 PC의 Process를 검사해본 결과
10만개 Process 중 25000개의 Process에서 악성코드가 발견되었습니다.
25000개 중 6000개에서 트로이목마, 웜 등과 같은 Virus와, 8000개의 Spyware 그리고 11000개의 기타 악성코드가 발견되었습니다.

A사는 전사 백신이 설치되어 있는데도 불구하고 전체 Process 중 25%에 해당되는 악성코드가 검출된 결과로 보아 사용 중인 백신의 보안성이 낮은 것으로 판단할 수 있습니다.

이러한 상황이 지속될 경우 PC내 존재하는 악성코드로 인한 피해 가능성이 높습니다.

수집DB를 활용해 악성코드를 관리하는 방법으로 수집DB와 악성코드DB를 비교합니다.

57개사의 각기 다른 바이러스 검사 소프트웨어를 이용할 수 있는 Virus total 사이트에서 바이러스 검사를 통해 만든 악성코드DB는 기존 백신 보다 정확하며 많은 악성코드의 정보를 보유하고 있습니다.

이러한 악성코드DB와 수집DB를 비교해 일치하는 Process를 검출합니다.

검출된 Process는 Virus, Spyware, 기타 악성코드로 분류합니다.

기업 및 기관에서는 검출된 정보를 확인할 수 있으며 지속적인 삭제 관리를 통해 악성코드를 관리해야 합니다.