보안 – 악성코드 분석

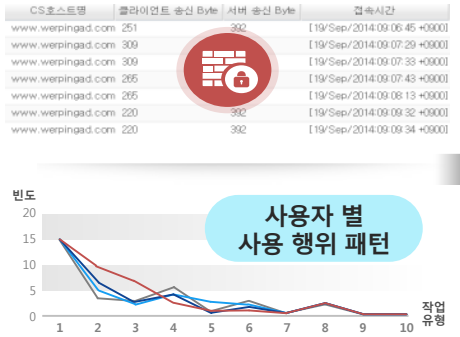
사업적 가치

- **고도화되는 악성코드 공격 APT(Advanced Persistent Threat) 해킹수법 대응을 위해 기존 룰베이스, 시그니처 방식에서 Analytics를 활용한 악성코드 분석모델 개발**
  - 대용량 보안 데이터를 시각화하여 해킹 의심 PC/HOST의 패턴을 쉽게 파악 가능 및 분석시간 단축
- **임직원 문서 사용패턴을 분석하여 정보유출(개인정보) 징후탐지모델 개발**

활용 기술

- **보안 로그데이터 분석을 통한 해킹 의심PC 탐지 모델 개발**
- **개인 정보유출 의심사용자 탐지모델 개발**

보안 Log



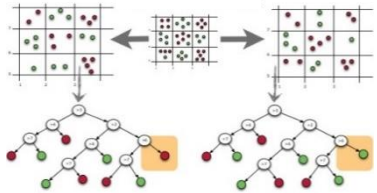
특성인자 추출

해킹의심PC 모델 추출인자

- 데이터 전송량
- 접속 간격/주기
- User-Agent 특이점
- 문서 첨부 및 수정
- :

해킹의심PC 탐지 모델

Random Forest



SNA 시각화