TREND MICRO

APT 보안 솔루션
Deep Discovery

한국트렌드마이크로
서울시 강남구 대치동 945-1
홍우빌딩 6층
(우 135-846)
TEL. 02-561-0990
FAX. 02-561-0660
www.trendmicro.co.kr

APT 보안 솔루션

Deep Discovery

Deep Discovery

APT(Advanced Persistent Threat, 지능형 지속위협)는 중요 정보 획득을 목적으로 지속적으로 특정 대상(정부, 금융기관 및 특정기업)에 공격을 수행하는 수법입니다. **Deep Discovery**는 기존의 백신이나 전통적인 보안솔루션을 우회하는 지능적인 공격에 선제적으로 대응하는 APT 보안 솔루션입니다.

- ☑ **Deep Discovery**는 네트워크 전반에 관한 통찰력 및 통제권을 제공하여, **APT** 공격과 타겟형 공격에 노출될 위험성을 줄여줍니다.
- ☑ **Deep Discovery**는 침투 위협을 실시간으로 감지하고 파악하여, 심층적인 분석과 정확한 정보를 제공함으로써 기업 데이터에 가해지는 공격을 탐지하고 파악하여 격리합니다.
- ☑ **Deep Discovery**의 검증된 접근 방식은 오탐이 적으며, 공격이 시작되는 시점에서 각 단계별로 악성 콘텐츠, 커뮤니케이션, 그리고 행동을 파악하여 최고의 탐지율과 방어율을 보여줍니다.
- ☑ **Deep Discovery**는 진화된 악성코드와 침투 공격자의 행동에 관한 탐지와 심층 예측 분석을 통하여 진화하는 컴퓨팅 환경에서 기업과 정부 기관에 새로운 수준의 가시성과 정보를 제공하여 **APT** 공격과 타겟형 공격에 대한 방어를 제공합니다.

APT 공격 및 타겟형 공격

- 제로데이 및 신종 악성코드
- 문서 취약점 악용 위협
- 공격자의 네트워크 행위
- 웹 위협(익스플로잇, 다운로드)
- 이메일 위협(피싱, 스피어 피싱)
- 봇, 트로이안 웜, 키로그 및 크라임웨어

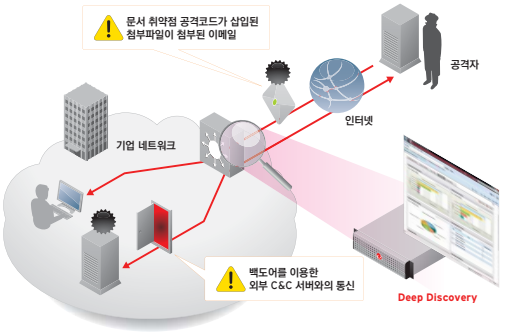
주요 이점

- 네트워크 가시성 확보 및 제어
- 포렌식 분석을 통한 상세 검증 및 분석으로 통찰력 제공
- 네트워크 레벨 공격 탐지 및 사용자 정의 기반 분석
- 사용자 정의 보안 업데이트
- 활용 가능한 분석 정보 수집 및 결과 제공

제품 구성

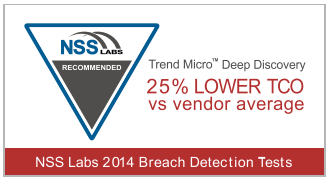
Deep Discovery는 **APT** 공격에 대응하기 위해 필요한 네트워크 가시화와 직관적인 로그 분석 기능을 제공합니다. 위협을 탐지하는 **Deep Discovery Inspector**와, 수집한 로그를 심층적으로 분석하고 위협을 차단하는 **Deep Discovery Advisor**로 구성됩니다.

- **Deep Discovery Inspector** : 네트워크 감시 및 실시간 분석, 리포트 제공으로 위협을 가시화하여 위협을 탐지합니다.
- **Deep Discovery Advisor** : 수집한 로그를 보다 심층적으로 분석하기 위해 각종 보안 제품과 연동할 수 있으며 분석 결과를 활용해 위협을 차단합니다.



APT 공격에 대한 완벽한 라이프사이클 제공

APT 탐지율 1위! NSS Labs 정보 유출 진단 테스트에서 최고점 획득

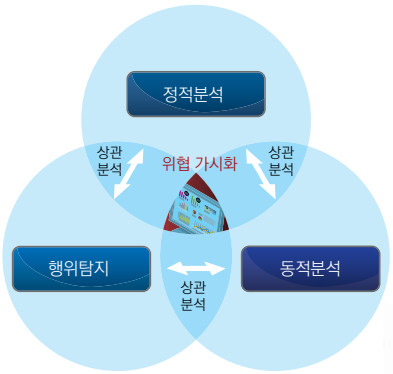


- **침해 탐지율 부문 최고 점수(99.1%)** : 테스트 제품 중 최고 수준
- 오탐률 제로 : 정상 파일을 오탐하는 것에 대한 테스트에서 오탐률 제로
- 낮은 TCO : 테스트한 전체 제품의 평균보다도 25% 이상 저렴

Deep Discovery Inspector

Deep Discovery Inspector는 위협 탐지 장비로, 100여 가지의 애플리케이션 프로토콜을 지원하며 정적분석, 동적분석, 행위탐지라는 3가지 방법을 사용하여 위협을 다각도에서 모니터링 및 탐지합니다. 폭넓은 애플리케이션 프로토콜에 있어서 3가지 방법으로 찾아낸 로그 정보를 상관 분석함으로써 전체 트래픽 상황을 시각화하고 조직 내부에 잠재된 위협을 탐지합니다.

정적분석, 동적분석, 행위탐지를 상관분석하여 가시화



메일, 웹을 포함해 100가지 이상의 애플리케이션 프로토콜을 지원

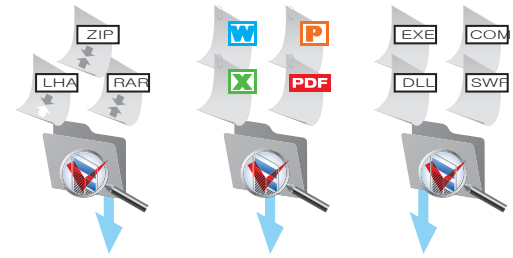
탐지 방법

정적분석

- **파일 구조 분석으로 의심 파일을 탐지**
  조직 네트워크에서는 PDF, 워드를 비롯한 수많은 형식의 파일이 사용되며 다양한 압축 형식이나 아카이브 형식이 이용되기도 합니다. 정적분석은 트렌드마이크로가 25년간 축적해온 다양한 파일 형식에 대한 대응력을 기반으로 한 새로운 분석 기술로 APT 공격을 탐지합니다.

- **위협 탐지 엔진(ATSE, Advanced Threat Scanning Engine)**
  Deep Discovery Inspector의 위협 탐지 엔진은 APT 공격에 최적화되어 있습니다. Document Exploit Engine을 통해 PDF, 오피스 파일 등의 취약점을 탐지합니다. 한글 파일(hwp)을 비롯해 수많은 파일 형식을 지원하고 있으며, 문서 취약점 공격 코드를 탐지합니다. 또한 자동 실행되는 압축파일(packer)도 탐지하는 IntelliTrap 기능도 제공합니다.

다양한 파일의 구조를 분석하는 정적분석

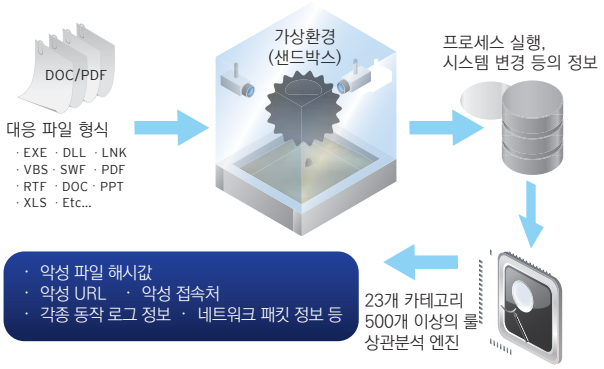


많은 압축 형식, 아카이브 형식, 파일 형식을 지원하여 패턴 및 휴리스틱 룰뿐만 아니라 문서 취약점 공격 코드를 파일 구조에서 탐지하여 의심스러운 파일을 찾아냅니다.

동적분석

- **샌드박스로 의심파일을 분석**
  정적분석과 행위탐지로 발견된 의심파일을 샌드박스라는 가상환경에서 실행시켜보고 그 움직임을 통해 위험도를 평가하는 것이 동적분석인 Virtual Analysis입니다. 커스터마이징이 가능한 이 샌드박스에서는 한국어 OS 및 각종 애플리케이션 등을 선택할 수 있고 실제 조직의 IT 환경을 구성해 볼 수 있어 위협이 미치는 환경이나 범위를 상세하게 조사할 수 있습니다.

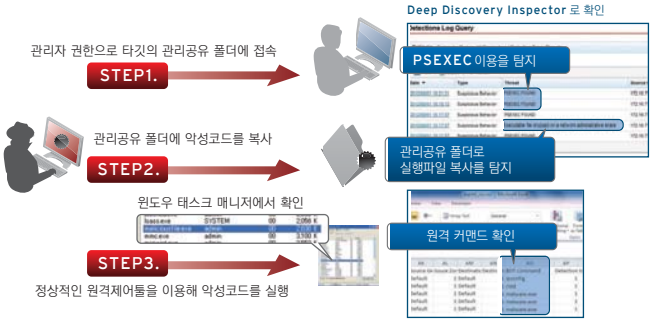
동적분석(Virtual Analysis)의 의심파일 분석 방법



행위탐지

- **알아차리기 어려운 위협을 파악**
  네트워크에 잠재되어 있는 위협을 파악하기 위해 샘플 분석 내용 및 실제로 공격 당한 사용자 환경에 대응하면서 얻은 지식 등을 바탕으로 한 행위탐지를 실시합니다. 예를 들면 정상적인 시스템 관리 툴이 악용되었을 경우 네트워크 상의 행위 자체는 올바른 것으로 간주되지만 접속한 PC가 IT 부서가 아니라면 올바른 접근이라고 볼 수 없을 것입니다. 이처럼 기업의 업무나 운용 프로세스를 참조하여 판별하기 어려운 위협도 탐지할 수 있습니다.

정상적인 툴을 악용한 알아차리기 어려운 공격도 탐지



Deep Discovery Advisor

Deep Discovery Advisor는 Deep Discovery Inspector를 비롯해 트렌드마이크로의 메시징 보안 제품과 연동하여 확장성 있는 고도의 가상 분석 기능을 이용한 대책을 제공합니다. 가상 분석 결과 및 각 제품에서 수집된 이벤트 로그를 유연성 높은 인터페이스를 통해 심층적, 다각적으로 분석할 수 있습니다. 사용자 환경에 따른 분석 및 리포팅, 통지 기능을 통해 APT 공격에 대한 기업의 분석력과 대응력을 강화할 수 있습니다. 또한 Deep Discovery Advisor는 5대까지 Cluster 구성이 가능하여 샌드박스 성능 확장에 대한 높은 유연성을 제공합니다.

기능 및 특징

제품 연동

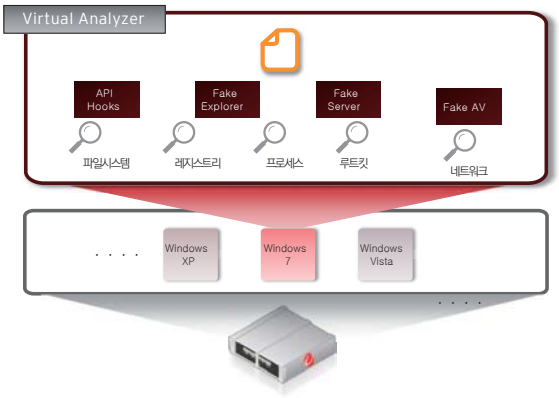
- **위협 대응력 강화**
  Deep Discovery Inspector 및 트렌드마이크로 메시징 보안 제품의 위협 탐지 엔진(ATSE)으로 탐지된 악성파일을 Deep Discovery Advisor의 고도의 가상 분석 기능을 통해 분석하여 리스크가 높은 샘플을 차단합니다.

위협 분석

- **커스텀 샌드박스로 의심파일을 분석 - 사용자 정의 샌드박스 환경 구성**
  각 제품에서 발견된 의심파일을 Deep Discovery Advisor의 커스텀 샌드박스 가상 환경에서 실행시켜 그 움직임에 따라 위험도를 평가하는 것이 가상 분석 기능입니다. 커스텀 샌드박스는 실제 조직 내의 IT 환경을 그대로 구성해 볼 수 있기 때문에 위협이 가져오는 영향이나 리스크 범위를 상세하게 조사할 수 있습니다.

- **커스텀 샌드박스**
  - 여러 OS 이미지 활용
  - 고속 실행
  - 안티VM 탐지
  - 실행파일, 문서, URL 분석

- **라이브 모니터링**
  - 커널 모드에서 각종 후킹
  - 네트워크 플로우 분석
  - 이벤트 상관 분석



Threat Intelligence Center

- **주체적이고 직관적으로 위협을 파악**
  Deep Discovery Advisor는 탐지한 위협에 대해 직관적인 조작을 통해 주체적이고 직관적으로 심층 분석이 가능합니다.

- **직관적인 필터링이 가능한 Investigation**
  특정 기간의 위협 동향을 꺾은선 그래프로 시각화하여 확인할 수 있습니다.
  카테고리별로 정리된 위협 리스트에서 항목을 마우스 우클릭하여 직관적으로 로그를 필터링하면서 심층 분석을 실시할 수 있습니다.

- **악성 통신을 판별하는 C&C 콜백 이벤트**
  APT 공격의 특징적인 활동인 C&C 서버 통신의 탐지 로그를 트렌드마이크로 보안 제품에서 취득하여 의심스러운 통신의 발생 상황을 알려줍니다.

- **접속 호스트 및 수신 파일의 관련성을 조사하는 Impact Analysis**
  대상 오브젝트(ex 호스트)를 중심으로 다른 오브젝트(ex 사내외 접속 호스트, 수신 파일, C&C 서버 등)와의 관련성을 거미줄 차트로 표시합니다.

- **동적분석 결과를 드릴다운**
  샌드박스 분석 결과에 대해 관련 파일이나 특이한 특징 등 상세정보를 드릴다운 할 수 있습니다.

- **분석 방법을 저장하여 리포트 및 알람에 활용**
  사용자가 커스터마이징한 분석 조건은 Investigation Baskets에 저장할 수 있습니다. 분석 조건을 활용해 리포트나 알람을 용이하게 생성할 수 있습니다.

- **통합 운영 리포트**
  트렌드마이크로 형식의 리포트를 제공합니다. 영향이 있는 호스트, 액티브 C&C 서버 리스트 등이 통합 정리되어 있습니다.

보안 업데이트 서버

위협 분석에서 분석된 의심스러운 파일 및 통신 로그에서 추출한 IP주소나 URL을 위험성이 높은 출처 정보로서 Deep Discovery Advisor의 '커스텀 CCCA 데이터베이스'에 등록합니다. 그 후 C&C 서버 정보를 당사의 엔드포인트 제품이나 서버 보호 제품, 메일/웹 게이트웨이용 제품에 피드백합니다.