REVERSINGLABS

DATA SH EE T

A1000 멀웨어 분석 플랫폼

어드밴스드 멀웨어 헌팅, 식별 및 분석

A1000 멀웨어 분석 플랫폼은 하이 스피드 자동화 정적분석을 통해 어드밴스드 헌팅과 조사를 지원합니다. 파일 평판 서비스와 연동되어 70억개 이상의 파일(모든 파일형식 포함)에 대한 심층적 리치 콘텍스트와 위협 분류를 제공합니다.

A1000은 가시화, 자동화 워크플로우 연동 API, 멀웨어 검색 데이터베이스, 글로벌/로컬 YARA 규칙 매칭, 알람 구독 및 관리, 써트파티 샌드박스 도구 연동을 제공합니다.

A1000 주요기능

- **확정적 파일 분석** - 압축해제, 필터링, 내부 인디케이터 추출 및 밀리세컨드 내 위협레벨 할당.
- **광범위한 포맷 커버리지** - PE, ELF, MachO, Dex, .NET, Java, JS, 문서, 펌웨어, 비즈니스 애플리케이션 등 다양한 파일형식 지원
- **리치 콘텍스트 가시화** - 추후 액션을 위한 콘텍스트, 의도 및 심각도 확인
- **YARA 규칙 엔진 연동** - 사용자 지정 규칙 활용을 통한 신규 및 어드밴스드 멀웨어 탐지
- **비공개 파일 분석** - 파일은 공개적으로 공유되지 않아 고객사 사이트에서 유출불가
- **콘텐츠 저장소 중앙화** - 협업검색, 분석 및 헌팅을 위한 관심 대상의 파일 안전하게 저장
- **자동화된 워크플로우 연동** - 강력한 REST API 지원으로 기존의 워크플로우 및 프로세스와 연동 가능

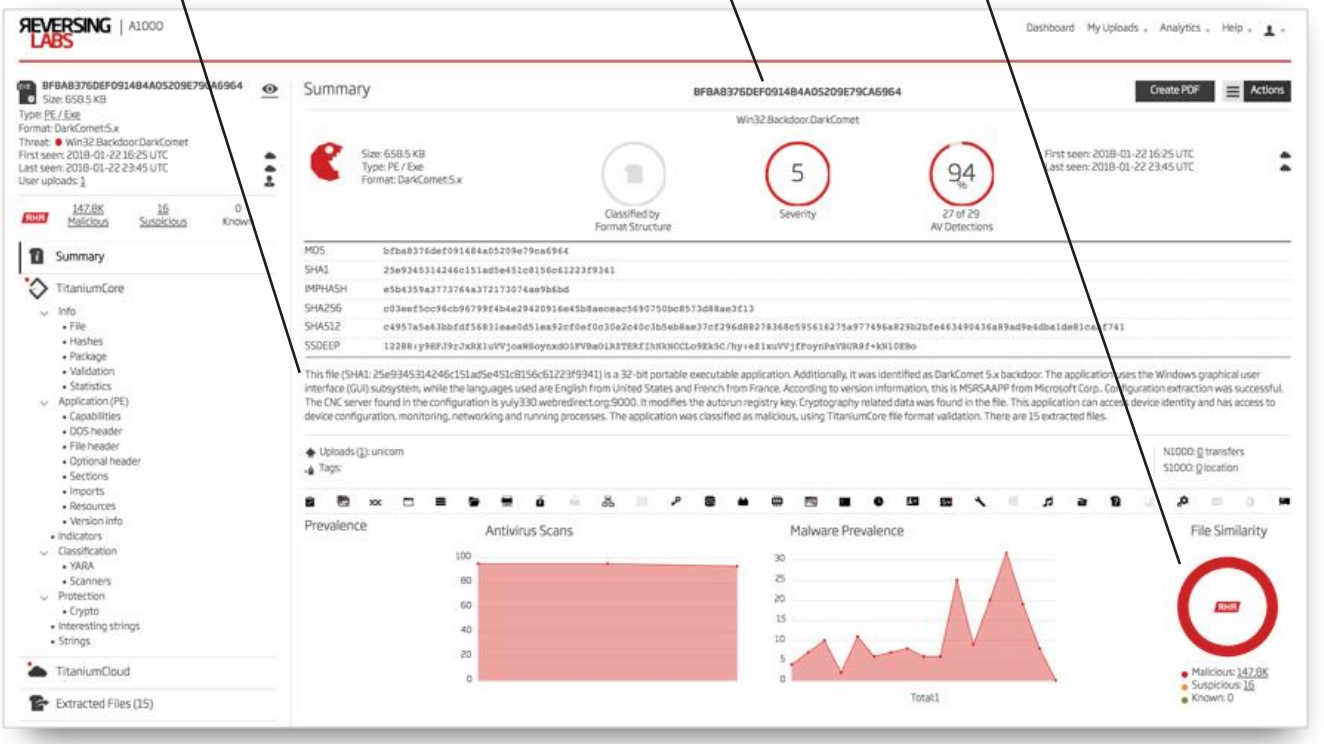
멀웨어 가시화

아래 보이는 예시는 A1000으로 검사한 파일 현황이며 분석가들의 관심분야를 집중 조명합니다.

크리티컬 상세사항, 탐지결과 및 멀웨어가 취하는 액션 요약본 제공
예) CNC SERVER

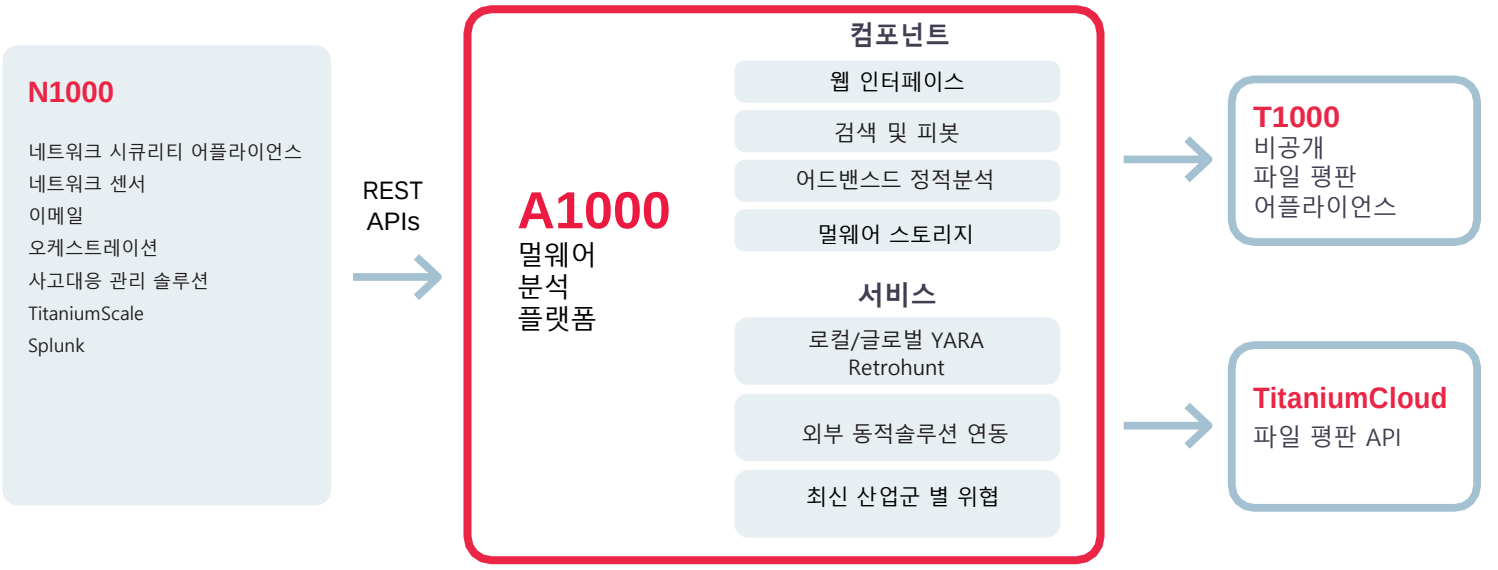
보안 분석이 필요한 크리티컬한 기록 정보가 목록화된 리포트 통합

탐지를 통해 분류된 기능적 유사 변종 목록화 및 악성 샘플의 피봇 활성화



A1000 멀웨와 헌팅 및 분석

A1000은 심층적 파일 분석의 주요 워크벤치로서, 위협 인텔리전스, 분석, 헌팅팀의 조사와 대응 활동을 가속화합니다. 멀웨어 계열은 기술과 난독화에 의해 시간이 지남에 따라 멀웨어와 멀웨어 상태의 변화를 평가합니다. TitaniumCloud 연동은 70억개 이상의 굿웨어와 멀웨어 파일을 검색하고 비공개 분석대상 파일 업로드를 지원합니다.



A1000 기능

멀웨어 분석 및 조사 연동

- 분석엔진은 하이 스피드 정적분석으로 파일 압축해제, 내부 인디케이터 추출, 및 위협레벨 할당을 수행
- 연동 데이터베이스는 탐지결과의 안전한 보관과 위협 인디케이터를 통한 샘플서치를 지원
- 크리티컬 정보를 신속하게 이해할 수 있는 가시화 GUI

자동화 정적 파일 분석

- 밀리세컨드 내 파일 처리
- 알려진 멀웨어에 기능적 유사성 평가
- 사용자 지정 YARA 규칙 구축 및 디플로이
- 300개 이상의 아카이브, 인스톨러, 패커, 컴프레서 압축해제
- 3500 개 이상의 파일형식 식별
- 3000 이상의 위협 인디케이터 추출

비공개 콘텐츠 저장소

- 악성 및 의심스러운 파일의 안전한 스토리지 제공
- 내장 검색 데이터베이스 내 파일 콘텍스트 저장
- 안전한 비공개 샘플 공유/기록 분석 지원

구독 및 관리 알림

- 최대 6개의 이메일 알람공지 구독

광범위한 검색 & 어드밴스드 헌팅

- 해시, 임프해시, 파일명, 태그 검색
- 기능 유사성 기반의 파일 검색 및 다운로드
- 매칭 및 헌팅을 위한 사용자 지정 YARA 규칙 지원

TitaniumCloud 파일 평판 서비스 연동

- 70억 개 굿웨어/멀웨어의 위협 인텔리전스와 평판 데이터의 포괄적이고 큐레이팅 된 소스 엑세스
- GUI를 통한 샘플 업로드/다운로드
- YARA 규칙 검색 지원

어드밴스드 헌팅 옵션

- 고급검색
- 엑티브 YARA 및 레트로 YARA

연동 지원

- REST API를 통한 자동화된 분석 워크플로우 지원
- Cuckoo와 Joe Sandbox 직접 연동

배포

- 하드웨어, VMDK, 클라우드 기반 어플라이언스

REVERSINGLABS

Korea Sales: 02.538.9225
briankim@reversinglabs.co.kr