DarkTracer 제품소개서

Version 2020

NSHC SECURITY

DarkTracer 다크트레이서

다크웹 위협정보 수집·검색 솔루션 <다크트레이서>는 다크웹(ToR) 상의 도메인 내 서비스 정보 및 웹 콘텐츠를 수집하여 사용자가 위협정보를 검색·모니터링할 수 있게 하는 솔루션입니다.

다크웹에서 발견된 다양한 정보[이메일, 문서/이미지 등 파일, 암호화폐 지갑주소(비트코인/이더리움), 전화번호, 아이디, 실제 근원지 IP정보, 일반 인터넷 웹정보, 다양한 고유 식별 정보 등]을 추출하여 사용자가 다크웹에 노출된 위협정보를 쉽게 검색할 수 있게 제공합니다.

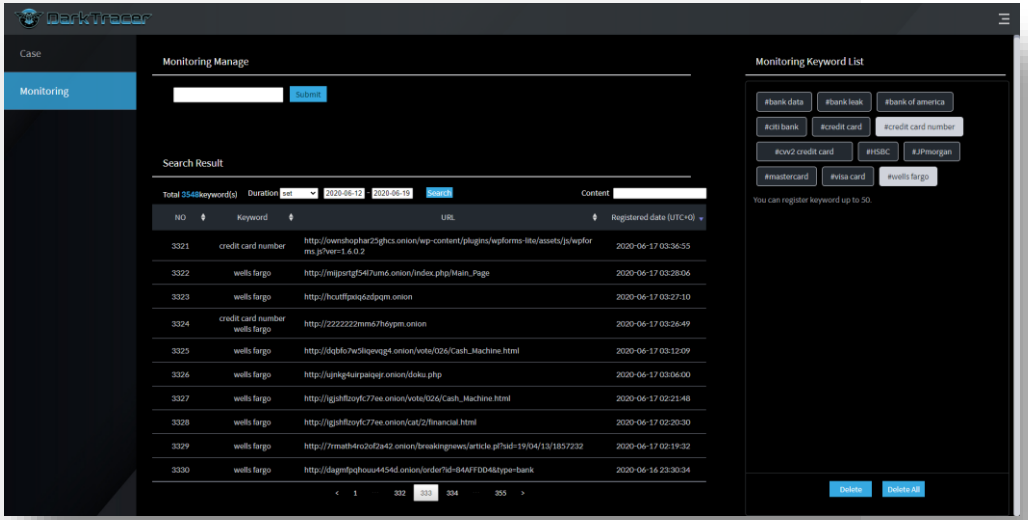
주요 기능

검색 인텔리전스 & 프로파일링

약 155억여 개의 다크웹 데이터를 대상으로 키워드 검색 및 20여 가지 지시어 기반 검색을 지원합니다.

검색 키워드, 위협정보를 기점으로 관련 데이터를 검색하며, 주요 정보를 그래프 캔버스에 저장하여 프로파일링 케이스를 작성할 수 있습니다.

주요 기능



키워드 모니터링

관심 키워드를 등록하여 키워드가 발견된 최신 다크 웹 데이터를 모니터링할 수 있습니다.

관심 키워드가 포함된 웹URL이 조회되며 링크를 클릭하여 URL 상세정보와 실제 웹브라우저 상의 화면을 지원합니다.

DarkTracer를 이용하여..

1 다크웹 내 키워드 검색과 위협정보 검색을 통해 정보 유출여부를 확인할 수 있으며 불법 정보 유통 동향을 조사할 수 있습니다.

2 키워드 및 위협정보를 기점으로 관련 식별정보를 검색·수집하여 프로파일링 분석을 수행할 수 있습니다.

3 다크웹 내 유출 / 침해 사고(개인정보 유출, 기밀문서 유출, 사이버공격 도모) 징후 탐지 모니터링을 수행할 수 있습니다.

“위험을 사전대응하고 보안수준을 향상할 수 있습니다.”

지원 기능

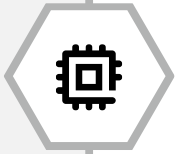
다크웹 데이터 수집

- ToR 등 다크넷 상 유통되는 위협정보 수집
- 총 150억 여 개의 위협정보 보유
- 전체 Onion 도메인 98만 여 개 및 Alive Onion 도메인 24만여 개 보유

프로파일링 정보 분석

- 웹데이터 내 다양한 위협식별정보 분석 추출
- 네트워크 정보: 도메인, URL, IP 등
- 유출정보: 이메일, ID, 전화번호, 지갑주소 등
- 파일정보: 문서, 이미지, 실행파일, 기타파일 등

검색 인텔리전스



- 수집 데이터 대상 키워드 검색 지원
- 프로파일링 지시자 검색을 통한 옵션검색 지원
- 카테고리 별 검색결과 도출

지원 기능

프로파일링 케이스

- 검색 키워드, 위협정보를 보관하여 정보를 캔버스에 보관 및 프로파일링 케이스 작성 가능
- 보관한 정보 간의 관계 그래프를 도출
- 프로파일링 정보 및 그래프를 케이스로 저장

그래프 추적 인터페이스

- 사용자가 저장한 정보를 노드로 표현하여 노드 간 연계성을 그래프화
- 방사형 / 계층형 등 정보 간 관계를 추적할 수 있는 다양한 형태의 그래프 지원

키워드 모니터링

- 특정 키워드를 등록하여 키워드가 발견된 최신 다크웹 데이터 모니터링 기능
- 키워드가 발견된 다크웹 URL 조회
- 최대 50개 키워드 지원 및 키워드 관리 기능

웹페이지 실제화면

- 편리한 웹데이터 확인을 위해 웹 URL 상세정보 외 텍스트 화면, 웹브라우저 화면 지원
- 웹데이터의 변경 히스토리, 해시값, HTML 소스 등 제공

제품 규격

규격명	값	구독형	
네트워크	HTTPS	계정수	3계정 제공
용도 및 기능	다크웹 위협정보 수집검색 솔루션	구축형	
운영체계	Windows, Linux, Unix	소프트웨어 종류	대용량분산 / 통합검색엔진
인터넷 웹브라우저	Edge, Chrome, Safari, FireFox	중앙처리장치(CPU) 규격	Xeon
옵션 / 기타	다양한 검색 옵션 기능 제공	하드디스크(HDD) 용량	100TB
사용자 범위	개인 / 기업 / 기관	하드디스크(HDD) 여유공간	제한없음

Current Updates_ver 2.7

No	Title	Description
1	IOC 카테고리 확장	I2P, 신용카드, SNS(페이스북, 트위터), 메신저(텔레그램, 디스코드, 라인) 단축URL 등 추가 분류
2	구글 스타일 검색 UI	키워드 검색 시, 키워드가 포함된 URL 내용을 표시
3	CL 기능 추가	Credential Lookout(유출계정 조회 솔루션) 기능 지원 *별도 구매
4	CDS 기능 추가	Compromised Data Set(유출계정 조회 솔루션): 기능 지원 *별도 구매
5	HTML Viewer 개선	상세정보 내 'Data from'의 HTML Viewer 지원
6	시간순 정렬	URL/도메인 카테고리의 시간순 정렬
7	GPS 정보 지원	GPS 카테고리 지원
8	유출정보 검색 지원	이메일, 이메일파일, 오디오파일, 패스워드, 설계도 등 유출정보 수집 및 검색 지원
9	수집 범위 확장	다크웹 종류 중 I2P 수집범위 확장