XARVIS

통합 딥다크웹 모니터링 솔루션

S2W

XARVIS

딥다크웹 종합 모니터링 솔루션

Xarvis는 뛰어난 성능의 딥다크웹 전문 검색엔진으로 서피스 웹은 물론 각종 히든 채널에서의 정보 수집을 도와줍니다.

사이버 범죄의 사각지대인 다크웹을 비롯한 다양한 은닉 채널 모니터링으로 방대한 양의 데이터를 수집합니다. 통합 웹모니터링을 이용해 특정 사건과 관련된 정보와 연관 범죄자에 대한 정보를 수집하고 데이터 정제 및 심층 분석을 통해 의미 있는 인텔리전스를 도출합니다.

Xarvis 핵심 서비스

통합 검색 엔진

딥다크웹, 텔레그램 등 숨겨진 채널의 데이터를 검색할 수 있습니다.

- 최신 딥다크웹 트렌드별 검색 가이드
- 다양한 필터 옵션 (언어, 이미지, 항목 등)

크로놀로지컬 웹 브라우저

휘발성 데이터를 캡쳐할 수 있도록 시간순으로 저장된 다크웹 콘텐츠를 제공합니다.

- 안전하고 직관적인 다크웹 브라우징
- 실시간으로 저장되는 데이터베이스로 삭제된 데이터도 열람 가능

실시간 딥다크웹 모니터링

딥다크웹 및 텔레그램에서 수집된 최신 콘텐츠와 데이터를 모니터링합니다.

- 맞춤형 키워드 모니터링
- 카드 정보 유출 모니터링
- 실시간 딥다크웹 위협 모니터링

멀티 도메인 교차 분석

흩어져있는 정보 조각들을 연결하고 관계도를 그려 인사이트 도출을 가능케합니다.

- 다양한 식별자 데이터베이스 (실시간 업데이트)
- 직관적으로 시각화된 그래프
- 페이지 리디렉션

유저 프로파일링 툴, ‘Darkspider’

잠재적 위협 그룹을 직관적으로 식별하는 다크웹 사용자 프로파일링 도구입니다.

- 주요 사이트의 사용자 규모 추이 모니터링
- 특정 유저의 활동 로그 추적 및 신규 게시물 업데이트

다크웹 뉴스 및 분석 리포트

다크웹 동향 파악에 도움을 주는 자체 제작 보고서를 제공합니다.

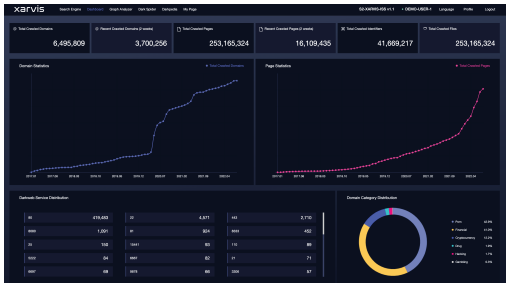
- 주간 딥다크웹 뉴스레터, ‘Darkpedia’
- 금융, 해킹 및 랜섬웨어 관련 뉴스 등
- 위협 요소 관련 통계적 데이터 제공

S2W

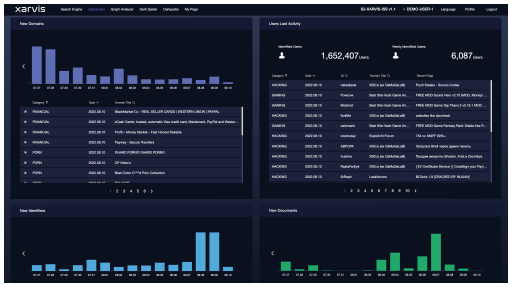
Xarvis 주요 기능

대시보드

- 수집된 다크웹 데이터 현황
- 주요 다크웹 관련 위협 정보 및 콘텐츠
- 데이터 맵



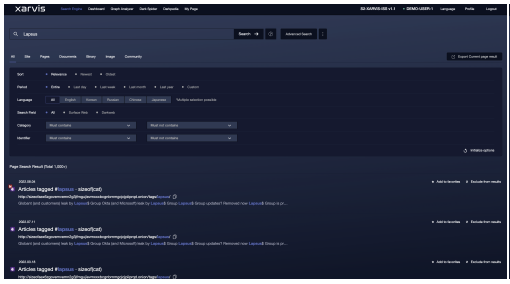
▲ 메인 대시보드



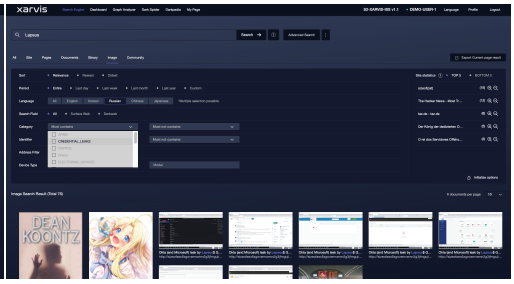
▲ 다크웹 트렌드

검색 엔진

- 일반/상세 검색 기능
- 다양한 필터 옵션
- 현재 페이지 검색 결과 추출
- 게시물 원본 페이지로 리디렉션



▲ 검색 엔진

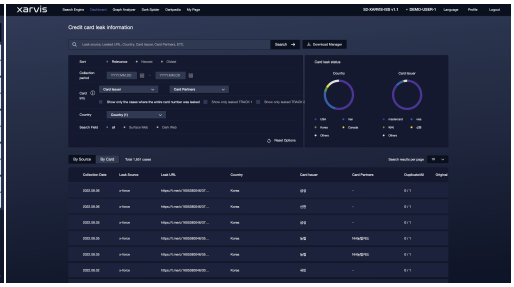


▲ 상세 검색 필터

맞춤형 모니터링

- 고객 맞춤 키워드 모니터링
- 카드 정보 유출 모니터링
- 관심 분야 모니터링

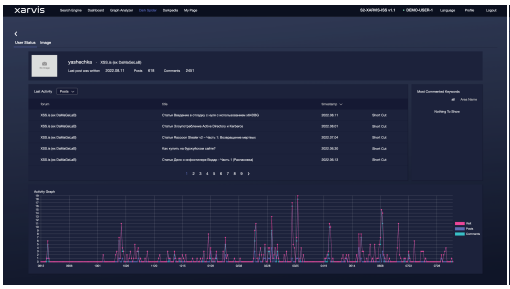
▲ 사용자 지정 키워드 모니터링



▲ 카드 유출 정보 모니터링

분석 툴

- 다크웹 유저 프로파일링 툴, ‘Darkspider’
- 멀티 도메인 교차 분석
- 다크웹, 서피스 웹 정보 분석

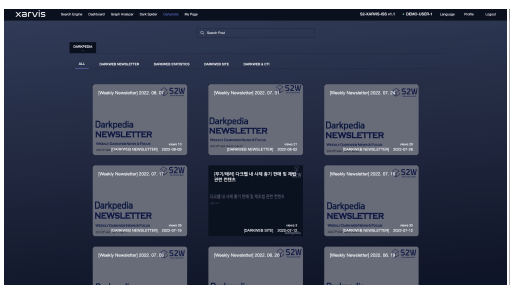


▲ 다크웹 유저 프로파일링 툴, ‘Darkspider’

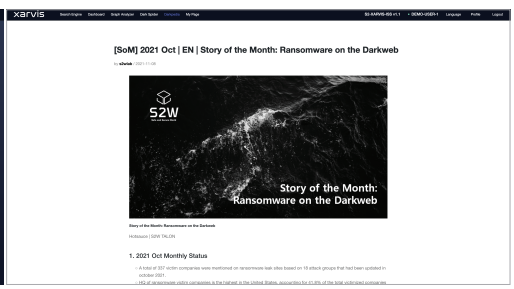
▲ 그래프 분석

인텔리전스 보고서

- 주간 다크웹 뉴스레터, ‘Darkpedia’
- 고객 전용 분석 보고서
- 고객 요청 시 신속한 보고서 제공



▲ Darkpedia



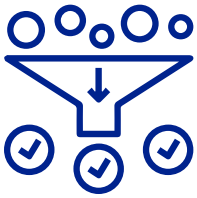
▲ 보고서

S2W

Xarvis의 차별점

자동화된 웹 페이지 카테고리 분류

딥러닝 기술을 이용해 수집된 모든 다크웹 콘텐츠를 10개의 주제로 자동 분류합니다. 수집한 불법/위협 콘텐츠들을 해킹, 마약, 음란물, 무기, 금융 등 불법/위협 등의 카테고리로 신속하게 분류해 필요에 따라 데이터를 효율적으로 활용할 수 있습니다.

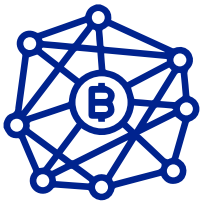


음란 콘텐츠 필터링

이미지와 텍스트 분석을 기반으로 다크웹에서 수많은 음란물을 자동으로 감지합니다. 사용자가 원치 않는 부적절한 콘텐츠에 노출되는 것을 방지하기 위한 사전 필터링 시스템입니다.

자동 식별자 수집

다크웹, Telegram, Wicker, Discord 등 모니터링 채널에 언급되는 식별자를 자동으로 추출합니다. 메신저의 이메일 주소, 가상 자산 주소 및 ID를 포함한 다양한 식별자들을 수집합니다. 이는 개인 신상 파악, 비공개 채널 식별 및 다크웹 포럼내 다양한 도메인 교차 분석 등에 도움을 줍니다.

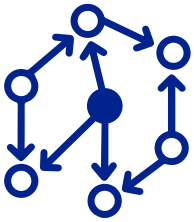


블록체인 주소 분석

블록체인 거래 주소를 수집해 다크웹과 서피스 웹을 포함한 통합 웹상 데이터를 교차 매칭합니다. 비트코인 주소를 사용하여 가상 자산의 흐름에 대한 단서를 제공하고 주소 소유자를 추적하는 데 도움이 되는 실마리를 제공합니다. 또한 다크웹에 있는 자산의 예상 가치 추적에 도움이 됩니다.

안전한 다크웹 브라우징

S2W는 다크웹 원본 콘텐츠를 제공을 위해 다크웹 내 실제 데이터를 수집해 자체 데이터베이스에 저장합니다. 저장된 데이터는 크로놀로지컬 브라우저로 제공되며, 이를 통해 휘발성 다크웹 데이터를 안전하게 보존합니다. 따라서 사용자는 실제 다크웹에 나타나는 원본 데이터를 보다 안전하고 빠르게 또, 직관적으로 볼 수 있습니다.



통합 데이터 분석

흩어져 있는 데이터를 수집해 시각적 관계 그래프를 구성하고 관계 분석을 수행할 수 있습니다. 위협 행위자와 관련 데이터 간의 관계 파악에 도움을 줍니다. 이는 결과적으로 실효적인 인텔리전스를 도출하고 추적 경로 확장을 가능하게 합니다.

S2W

S2W는 사이버 위협, 브랜드/디지털 어뷰징 및 가상 자산을 위한 인텔리전스 솔루션을 제공합니다.

데이터 중심의 초연결 사회에서 최적의 문제 해결 방법을 도출하고, 외부 위협으로부터 조직을 보호하고 기업 브랜드 가치 향상을 위한 맞춤형 솔루션을 제안합니다.

S2W는 빅 데이터 분석, 머신 러닝, 딥 러닝 등 다양한 기술을 활용해 위협 인텔리전스, 디지털 어뷰징 인텔리전스, 가상 자산 인텔리전스 솔루션을 제공합니다.

INTERPOL · SAMSUNG ELECTRONICS · HYUNDAI · KIA · KOREAN AIR · coupang · KOREAN NATIONAL POLICE AGENCY

NAVER · Korea Investment & Securities Co., Ltd. · SK shieldus · SK telecom · kt · LG U+ · Swit · 우아한형제들

Klaytn kakao · kakaopay · BUNJANG · BALAAN · WOORI CARD · BNK Busan Bank · SEMES

KISA · NSR 국가보안기술연구소 · Humanizing Genomics macrogen · HYUNDAI BNGSTEEL · MARIOMALL · FINANCIAL SECURITY INSTITUTE · R.O.K. CYBER COMMAND 국군사이버사령부

HYUNDAI ENGINEERING & CONSTRUCTION · HYUNDAI STEEL · HYUNDAI WIA · HYUNDAI AutoEver · HYUNDAI MOBIS · HYUNDAI TRANSYS · HYUNDAI GLOVIS

발표

Cybercriminal Minds
An investigative study of cryptocurrency abuses in the Dark Web (NDSS 2019)

Doppelgangers on the Dark Web
A large-scale Assessment on phishing Hidden Web Services (WWW 2019)

OPERATION NEWTON
HI KIMSUKY? DID AN APPLE(SEED) REALLY FALL ON NEWTON'S HEAD? (Virus Bulletin 2021)

Shedding New Light on the Language of the Dark Web
(NAACL 2022)

특허권

암호화폐 거래 분석 방법 및 시스템

지식 그래프를 활용한 사이버 보안 제공 방법과 장치 그리고 프로그램

암호화폐 거래 분석 방법과 장치

다중 도메인에서 데이터를 수집하는 방법과 장치

S2W

info@s2w.inc | +82 70 5066 5277 | www.s2w.inc

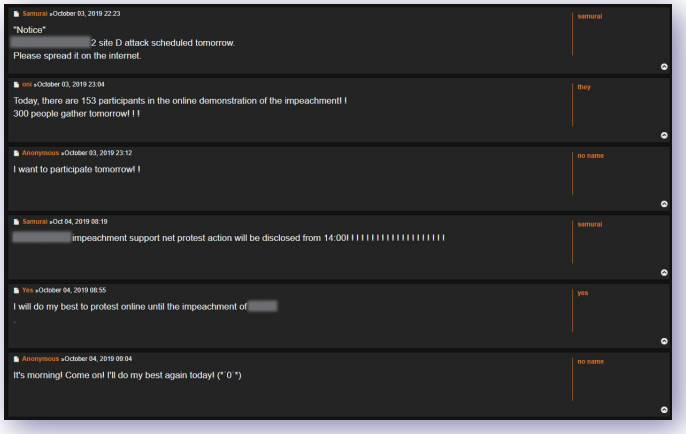
XARVIS

활용 사례

Xarvis는 뛰어난 성능의 딥다크웹 전문 검색엔진으로 서피스 웹은 물론 각종 히든 채널에서의 정보 탐색을 도와줍니다. 통합 웹 모니터링을 통해 사용자가 특정 사건 및 범죄자와 관련된 정보를 수집할 수 있고, 데이터 정제 및 심층 분석을 통해 의미 있는 인텔리전스 도출이 가능합니다. 현재 많은 수의 S2W의 고객이 Xarvis로 깊이있는 다크웹 인텔리전스를 얻고 활용하고 있습니다.

특정 정당 타겟 사이버 테러 사전 탐지

다크웹 모니터링



Xarvis를 활용하면 다크웹상의 잠재적 위협에 대한 모니터링이 수월해집니다. 관심 키워드를 등록하여 관련 콘텐츠가 업데이트 될 때마다 알림을 받을 수도 있습니다. 이 케이스는 S2W의 한 분석가가 Xarvis의 다크웹 모니터링 시스템을 통해 특정 정당을 타깃으로 한 DDos 공격에 대한 징조를 발견했던 케이스입니다.

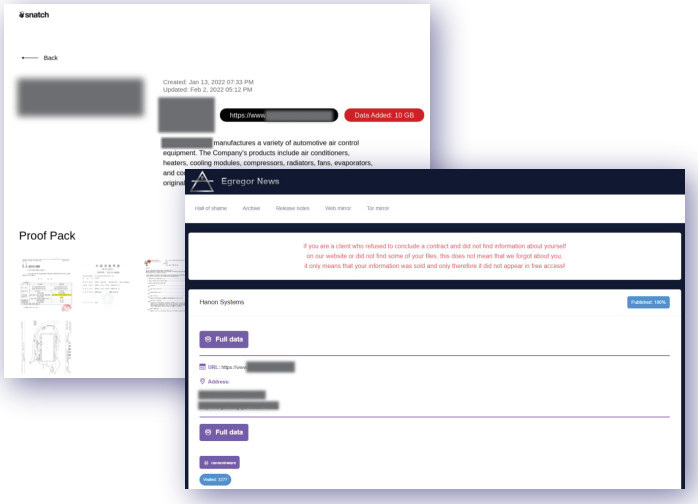
S2W의 분석가가 해당 국가를 타겟하는 사이버 공격 모집 게시물을 포착했을때, 테러 모의 상황을 지속적으로 추적하기 위해 Xarvis 모니터링 시스템에 관련 키워드를 등록했습니다. 그리고 해당 게시물에서 작성자의 움직임을 주시하기 위해 그의 다크웹 유저 ID를 비롯한 이메일 주소 등의 식별자 데이터를 수집했습니다.

그 결과 실제로 S2W는 동일한 사용자가 동일한 정당을 타겟으로 하는 두 번째 DDos 공격을 예고하는 게시물을 포착했고, 실제로 그가 예고한 날짜에 공격이 발생했습니다.

이와 같은 방법으로 Xarvis는 지정된 키워드와 다크웹 사용자를 지속적으로 모니터링하고 추적함으로써 잠재 위협에 대비할 수 있게 도와줍니다.

통합 다크웹 검색 엔진을 활용한 랜섬웨어 공격 추적

다크웹 검색



Xarvis 다크웹 탐지 시스템이 한 자동차 회사의 데이터가 유출된 것을 감지한 사례입니다. S2W는 Xarvis 검색 엔진과 다크웹 크로놀로지컬(Chronological) 브라우징 기능을 통해 1년 전 다른 다크웹 랜섬웨어 그룹인 Eggregor가 해당 기업의 내부 데이터를 유출했던 사실을 발견했습니다.

과거 유출 데이터와 새로이 유출된 문서를 교차 대조하고 유출 상황을 분석한 결과 두 공격 방식이 유사한 패턴을 보이는 것으로 나타났습니다. S2W는 회사의 사이버 보안 시스템의 취약점이 해결되지 않아 내부 자산과 계정 정보 중 일부가 여전히 외부에 노출되고 있을거라 의심했습니다. 그리고 Xarvis 검색 엔진을 통해 확인 결과인 실제로 회사의 핵심 자산이 과거와 동일하게 외부 서버에 노출되고 있다는 사실을 확인했습니다.

이러한 방식으로 Xarvis는 사건의 내용을 시간순으로 파악하고, 상세한 정보 수집을 통해 효과적인 대응책을 마련할 수 있도록 합니다. 이는 기업 및 기관이 사이버 보안 현황을 파악하고 상황에 따라 효율적으로 대응할 수 있게 도와줍니다.

S2W

약물 재배 다크웹 유저 신상 파악

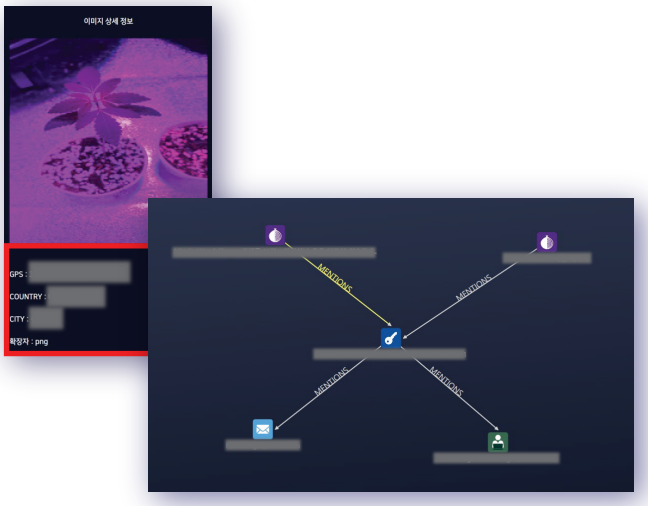
다크웹 유저 프로파일링/교차분석

약물 관련 콘텐츠 모니터링 중 Xarvis는 한 다크웹 유저가 약물을 재배하는 다크웹 게시물을 감지했습니다. Xarvis의 이미지 분석 기능으로 포스트에 첨부된 이미지를 이용하여 유저의 거주 지역을 식별했습니다.

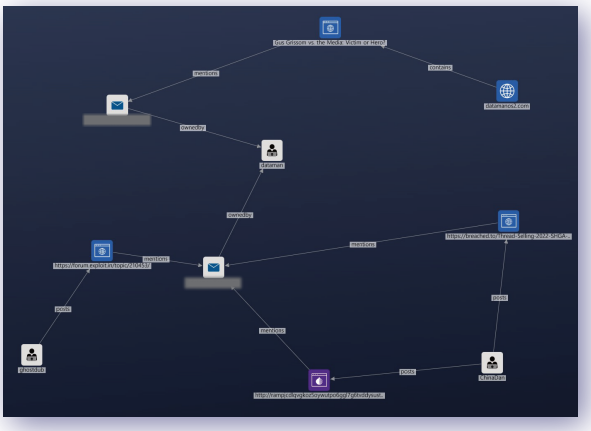
해당 게시물의 분석을 통해 유저의 식별자를 획득하고, 이를 활용해 다크웹에서 과거 마약 관련 게시물 및 활동 내용을 확인하였습니다. 교차 분석 결과에 따르면 해당 유저는 마지막 게시물을 올리기 한 달 전에 마약 거래 암시장에서 활동한 것으로 드러났습니다.

그리고 Xarvis의 다크웹 유저 프로파일링 도구인 Darkspider를 사용하여 다크웹 사이트 방문 이력, 게시물, 게시 시간 등 과거 다크웹 활동을 조회했습니다. 그 결과 해당 유저가 다른 나라를 방문하여 그곳에서 약을 구입했던 사실을 확인했습니다.

이 케이스에서 Xarvis는 해당 다크웹 유저가 지속적으로 마약을 구매해 사용하고 있으며 자체적으로 마약을 재배하는 범죄를 저지르고 있다는 정황증거를 제공했습니다. 특히 Darkpsider는 특정 다크웹 유저를 모니터링하고 그의 활동 패턴, 게시물 상태 등을 빠르게 파악하는데 결정적인 역할을 했습니다.



멀티 도메인 교차 분석



휘발성 강한 다크웹 데이터 보존으로 위협 행위자 추적

사이버 위법 행위 및 사건이 발생할 경우 Xarvis는 관련 식별자를 수집하고 수집된 여러 데이터를 교차 분석할 수 있습니다.

2022년, 유명 해킹 포럼인 Breached에 중국 데이터베이스가 포함된 게시글을 통해 수십만 명의 중국인 개인 정보와 범죄 기록이 공개됐습니다. 해당 게시물을 작성한 사용자 "ChinaDan"은 해당 데이터를 약 180만 달러에 판매하고 게시물 삭제 후 잠적하였습니다.

S2W는 Xarvis의 크로놀로지컬 브라우저를 사용하여 "ChinaDan" 유저 이름과 관련된 정보를 이미 삭제된 데이터까지 포함하여 검색한 결과 작성자의 이메일 주소를 획득했습니다. 해당 이메일 주소를 사용하여 서피스 웹 블로그 게시물을 찾을 수 있었고, 해당 유저의 다른 사용자 계정과 이메일 주소도 발견하게 됐습니다. 이후 오픈 서비스를 통해 해당 블로그의 IP 주소가 미국에 위치한 사실을 확인하였습니다.

위협 그룹 관련 유의미한 정보를 얻기 위해 Xarvis는 다양한 채널에서 최대한 많은 데이터를 수집합니다. 그리고 수집된 식별자를 활용하여 더 확장된 범위에서 새로운 정보를 얻습니다. 이를 통해 웹상의 다른 공간에 유저가 남긴 흔적들과 교차 분석이 가능하고 결과적으로 신원을 식별할 수 있게 합니다.

글로벌 이슈 모니터링, 코로나19 관련 다크웹 사이버 범죄

다크웹 모니터링

Xarvis는 다크웹에서 이슈가 되고 있는 글로벌 이슈들을 모니터링합니다. 이는 글로벌 이슈에 대한 사이버 범죄자들의 행동 패턴과 변화를 파악하고 선제적으로 대응을 가능하게 합니다.

코로나19가 전세계를 강타한 이후로 코로나 바이러스와 관련된 콘텐츠가 다크웹에도 업로드되기 시작했습니다. 초창기 게시물은 주로 코로나19 위키 등 바이러스에 대한 정보를 교환하는 데 그쳤으나, 시간이 지날수록 바이러스를 악용하여 금전적으로 이득을 취하는 범죄 관련 게시물이 증가했습니다.

Xarvis는 유명한 다크웹 포럼 DeepPaste에서 코로나19 관련 게시물에서 정보를 탐지하고 수집했습니다. 코로나19 확진자의 혈액, 타액 판매 게시글이 올라오고, 코로나 19 감염 혈액, 혈장 판매 사이트가 오픈됐습니다. Xarvis는 코로나19 바이러스 판매 사이트 관련 정보를 모니터링하고 수집했습니다.

이와 같이 Xarvis는 특정 주제를 집중적으로 모니터링하고 유저의 전반적인 행동 패턴과 다크웹상 해당 주제의 동향 파악에에도 용이하게 활용됩니다.

*DeepPaste: 불법 거래에 특화된 유명 다크웹 플랫폼.

COVID-19 관련 다크웹 사이버 범죄 양상의 변화

www.s2w.inc | info@s2w.inc | +82 70 5066 5277
경기도 성남시 분당구 판교역로 192번길 12, 판교미래에셋센터 3층