Deep/Dark web data analysis solution

XARVIS

S2W

XARVIS

Deep/dark web data collection and analysis tool

Xarvis is an outstanding search engine for the deep/dark web, which helps you comprehensively grasp all of the information on the surface web and hidden channels.

It collects vast amounts of data through monitoring various hidden channels, including the dark web, which has become a blind spot for cybercrime. Through integrated web monitoring, it allows users to collect pieces of information related to a particular case and that criminals involved, and it derives meaningful intelligence through data refinement and in-depth analysis.

Xarvis Core Service

Integrated Search Engine

Able to search data and contents on hidden channels, including deep/dark web and Telegram.

- Search guide by latest deep/dark web trend
- Various filter option (i.e. language, content type, category, etc.)

Chronological Web Browser

Provides chronologically saved dark web pages, which allow the user to capture volatile data.

- Secure and intuitive
- Able to capture the deleted data in chronological browser

Real-time Deep/Dark web Monitoring

Monitors latest contents and data collected from deep/dark web and Telegram.

- Customized keyword monitoring
- Card leak monitoring
- Real time deep/dark web threat monitoring

Multi Domain Cross Analysis

Enables to derive in-depth insights by connecting scattered individual information.

- Database of various identifier (real time update)
- Intuitively visualized graph
- Page redirection

User Profiling Tool, 'Darkspider'

Dark web user profiling tool to identify potential threat actors intuitively.

- Track user size trend by major site
- Activity log tracking and update on new posts of designated users

Analysis Report

Original analysis reports are provided to help identify dark web trends.

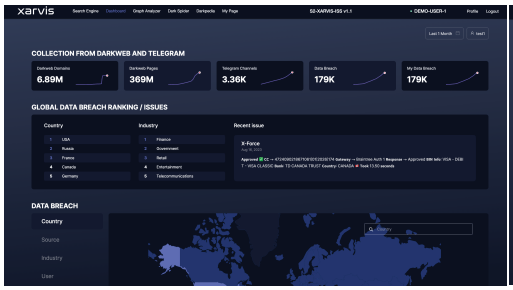
- Weekly deep/dark web newsletter, Darkpedia
- Threat news on financial/ hacking/ransomware
- Statistical data on threat factor

S2W

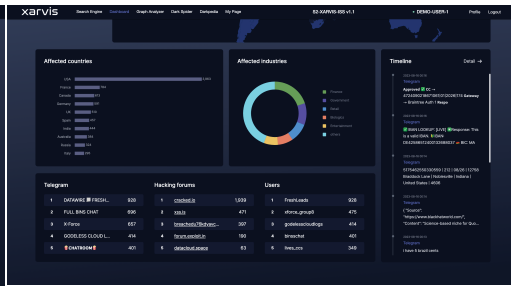
Xarvis Key Features

Dashboard

- Collected dark web data statistics
- Data breach trend by country
- Data breach trend by industry
- Recent Issue



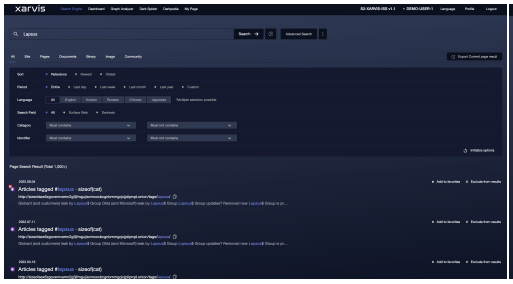
▲ Main Dashboard



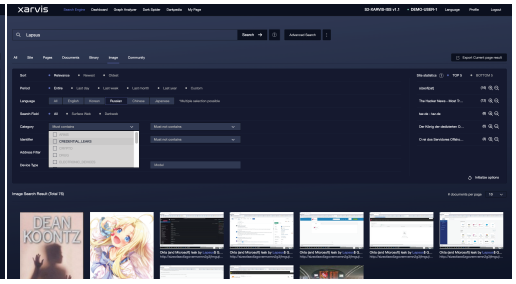
▲ Dark web trend

Search Engine

- General/advanced search
- Multiple filter options
- Export the search results of the current page
- Link to original post



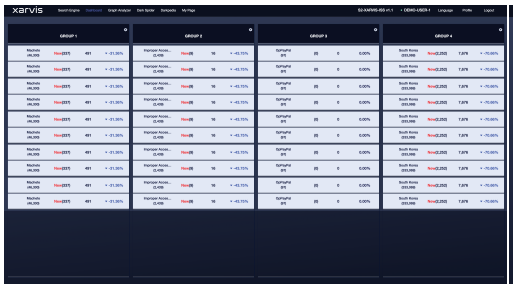
▲ Search engine



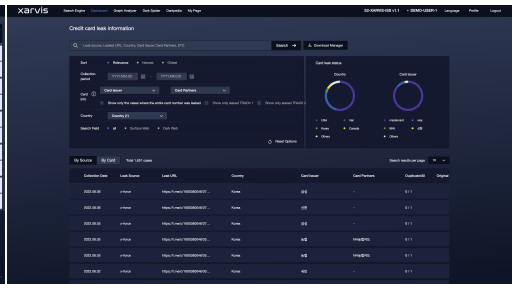
▲ Advanced search options

Customized Monitoring

- Customer designated keywords monitoring
- Card leak monitoring
- Monitor contents in categories of interest



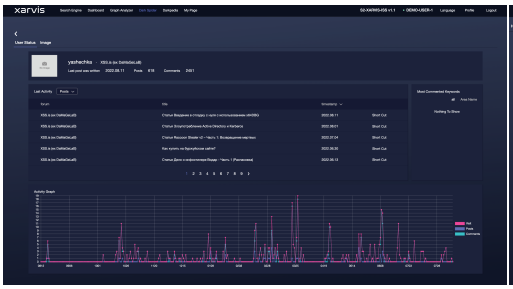
▲ Customer tailored keyword monitoring



▲ Credit card leak monitoring

Analysis Tools

- Dark web user profiling tool, ‘Darkspider’
- Multi-domain cross-analysis
- Dark web, surface web contents analysis

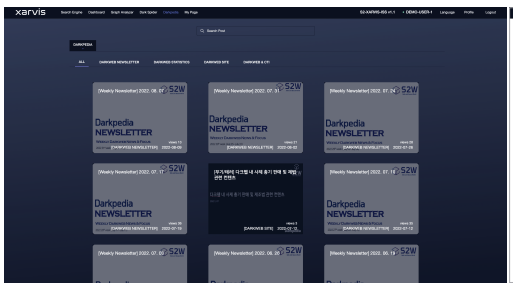


▲ Dark web user profiling tool ‘Darkspider’

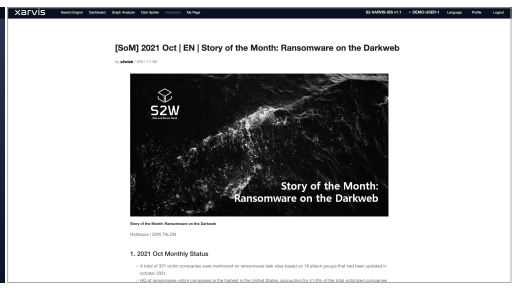
▲ Graph Analyzer

Intelligence Reports

- Weekly dark web newsletter, ‘Darkpedia’
- Exclusive analysis report
- Lightning report upon client request



▲ Darkpedia



▲ Report

S2W

DarkBERT

The very first Dark web specialized AI language model

Why is a specialized AI language model for the dark web needed?

01 **Crime Detection and Prevention**

The dark web is a place where illegal activities frequently occur, and a specialized AI language model for the dark web can help in understanding and analyzing the language and communication used on the dark web. This can be a valuable tool for detecting and preventing such activities.

02 **Investigation and Inquiry**

Law enforcement and judicial institutions need to investigate crimes on the dark web and collect relevant information. An AI model that comprehends dark web languages can support the investigative process and aid in tracking down criminals.

Dark web data collection and analysis process

1 Data Collection

2 Data Filtering

3 Text Preprocessing

4 DarkBERT Pretraining

5 Evaluation & Use Case

How DarkBERT is used in Xarvis?

DarkBERT is utilized for extracting core threat information in Xarvis.

Dark web activity classification

It classifies collected data into 10 categories, including drugs, gambling, crypto, hacking, etc.

Ransomware leak site detection

It is possible to determine whether the given dark web site is a ransomware leak site or general hacking site.

Noteworthy thread detection

It is possible to determine whether the given post within the hacking forum is an important post.

Threat keyword inference

For example, in a sentence where a drug name is mentioned and it is masked, it can determine that the masked word is related to drugs.

S2W

About S2W

S2W provides intelligence solutions for cyber threats, brand/digital abuse, and virtual assets.

In a data-oriented hyperconnected society, we derive optimal problem-solving methods and propose customized solutions to protect organizations from external threats and realize corporate brand value.

S2W utilizes various big data analysis, machine learning, deep learning, and other technologies to provide Threat Intelligence, Digital Abuse Intelligence, and Virtual Asset Intelligence solutions.

Publications

DarkBERT
A Language Model forthe Dark Side of the Internet (ACL 2023)

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

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

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

Patents

Methods and systems for analyzing cryptocurrency transactions

Methods, devices and computer programs for providing cybersecurity using knowledge graphs

Methods and devices for analyzing cryptocurrency transactions

Methods and devices for collecting data in multi-domain

info@s2w.inc | +82 70 7008 5278 | www.s2w.inc