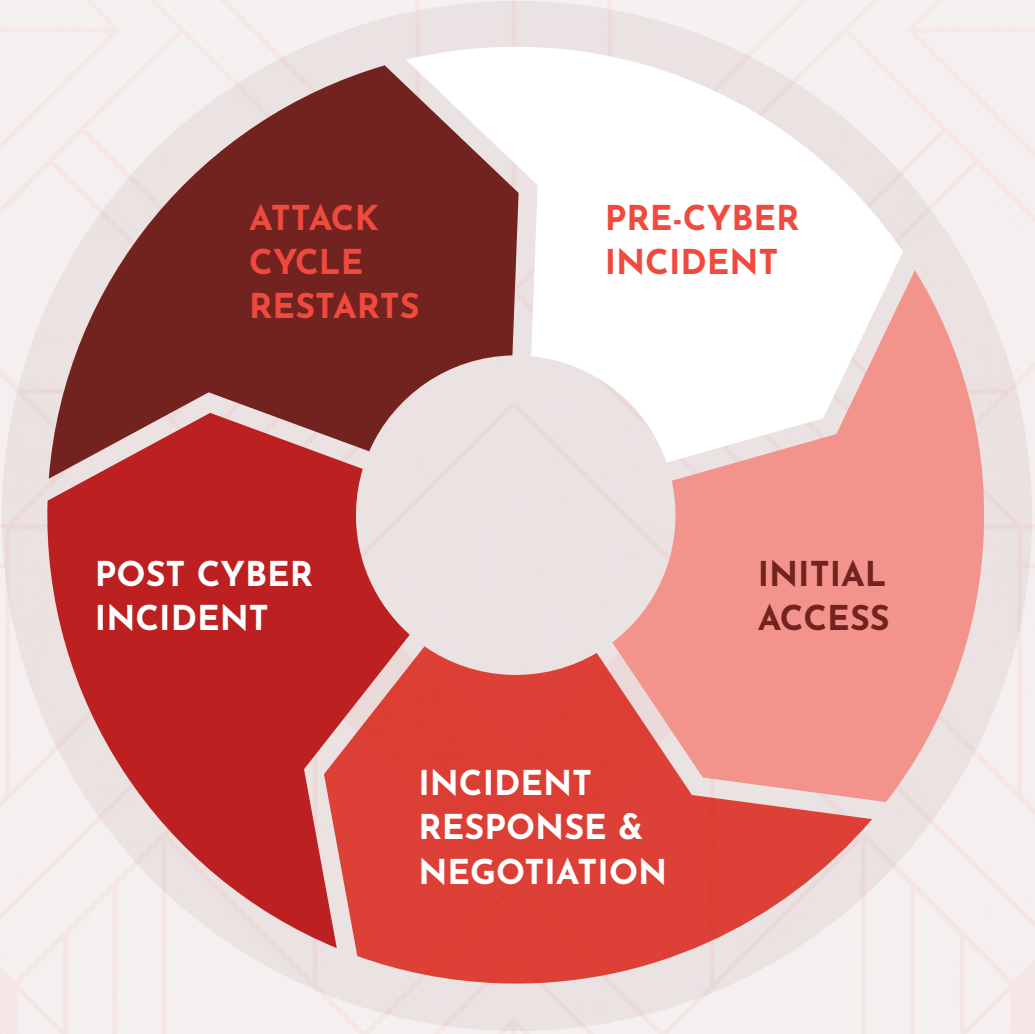
DARKOWL

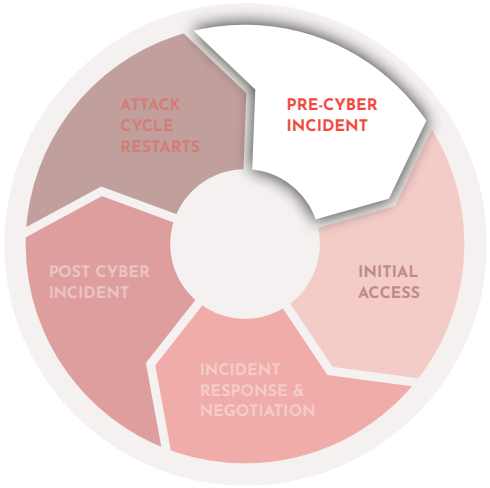
DARKNET RANSOMWARE THREAT SIGNAL & DATA FLOW

Research from DarkOwl into ransomware attacks key stages

July, 2022

MANY RANSOMWARE ATTACKS ARE COMPRISED OF KEY STAGES THAT, WHEN VIEWED ON A LARGER SCALE, FORM A PICTURE THAT REPRESENTS A CYCLICAL RANSOMWARE ECOSYSTEM THAT FEEDS VARIOUS INDUSTRIES IN THE DARKNET.

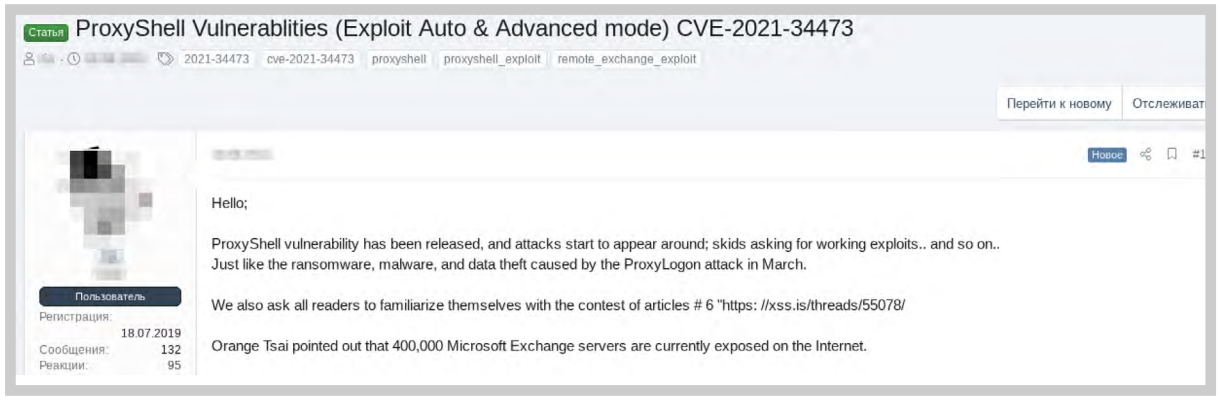




PRE-CYBER INCIDENT

ALL RANSOMWARE ATTACKS ARE COMPRISED OF KEY STAGES THAT, WHEN VIEWED ON A LARGER SCALE, FORM A PICTURE THAT REPRESENTS A CYCLICAL RANSOMWARE ECOSYSTEM.

46% of victims face multiple ransomware incidents



KEY MILESTONES: RECONNAISSANCE & THREAT ACTOR COLLABORATION

During this phase, threat actors gather data to define targets and initial access attack vectors. This information is compiled from a variety of sources, including the darknet, paste sites or via OSINT tools like Shodan.

While compiling the targets data, ransomware groups will also assemble OSINT and darknet data to prepare social engineering tactics, which are sometimes successfully deployed to gain access to the victim's network. They will also research available CVE data for potential use during the initial access phase.

DATA GATHERED DURING RECONNAISSANCE:

Common data that is gathered by the ransomware groups about their next includes:

- **Email addresses**
- **Network domains & subdomains**
- **Developer keys & server tokens**
- **Server OS data**

As well as other information from data leaks, including organization authentication data. This is also when discussions occur regarding applicable CVE's effectiveness against different hardware endpoints, network devices, or software architectures.

PRIMARY AREAS WHERE A PRE-CYBER INCIDENT TAKES PLACE

Paste Sites

RaaS Official Darknet Blog

Raas Darknet Chat Server / TOX

Forums' Marketplaces

Darknet Classifieds & Markets

Other OSINT Resources

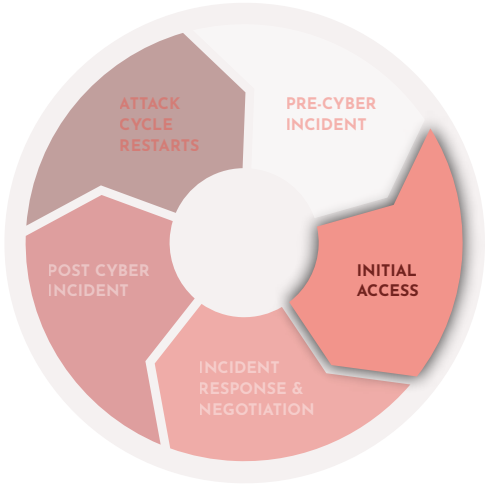
Telegram

Forum Chatter

Public News Media Outlets

Social Media

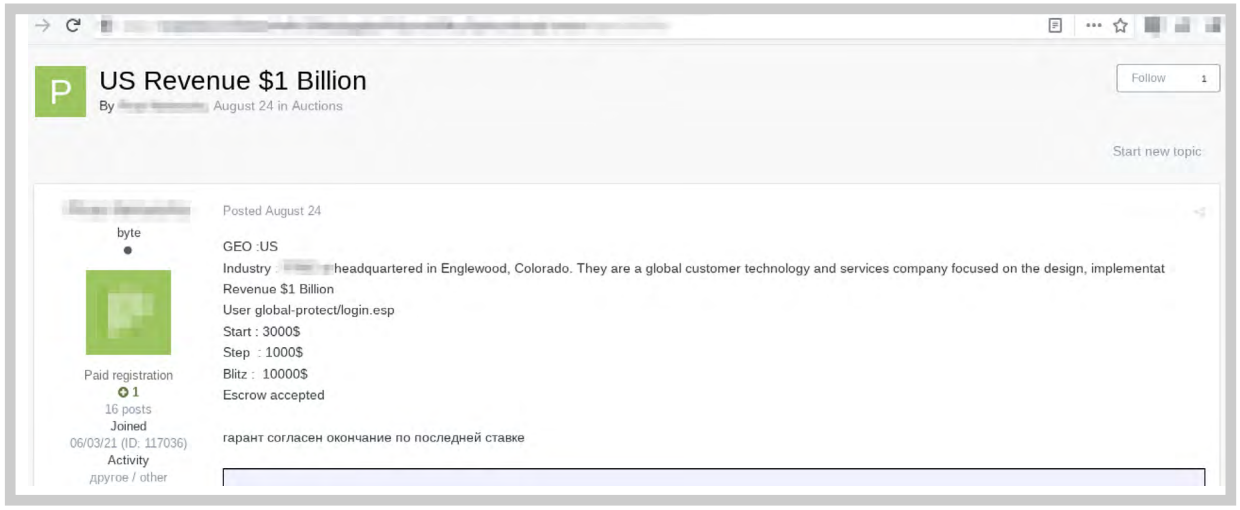
3rd Party Repositories



INITIAL ACCESS

ALL RANSOMWARE ATTACKS ARE COMPRISED OF KEY STAGES THAT, WHEN VIEWED ON A LARGER SCALE, FORM A PICTURE THAT REPRESENTS A CYCLICAL RANSOMWARE ECOSYSTEM.

In 2021, 67% of the offers on the darknet for access to corporate networks costs $5,000 USD or less.



KEY MILESTONES: ATTACK CAMPAIGN LAUNCHED

DarkOwl has observed pre-cyber reconnaissance and initial access fulfilled by underground initial access brokers (IABs) who offer the access along with other telemetry about the victim for sale on marketplaces inside darknet discussion forums. Corporate details are discovered using other OSINT resources.

Many of these offers include detail such as:

- **Initial access cost**
- **Victim's estimated revenue (if company)**
- **Associated industry information**
- **Number of employees**
- **Number of systems (or devices) in the victim network**

PRIMARY SOURCE AREAS WHERE THIS PHASE OCCURS

Paste Sites

RaaS Official Darknet Blog

Raas Darknet Chat Server / TOX

Forums' Marketplaces

Darknet Classifieds & Markets

Other OSINT Resources

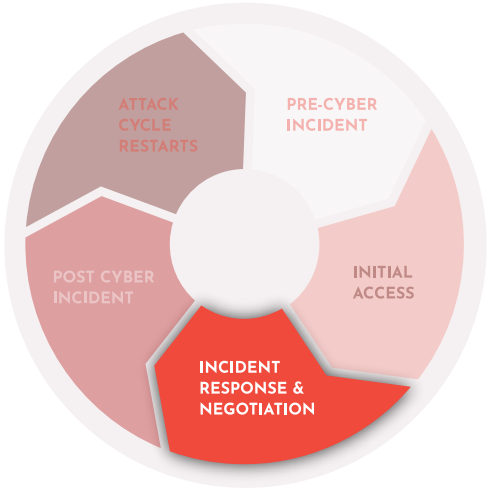
Telegram

Forum Chatter

Public News Media Outlets

Social Media

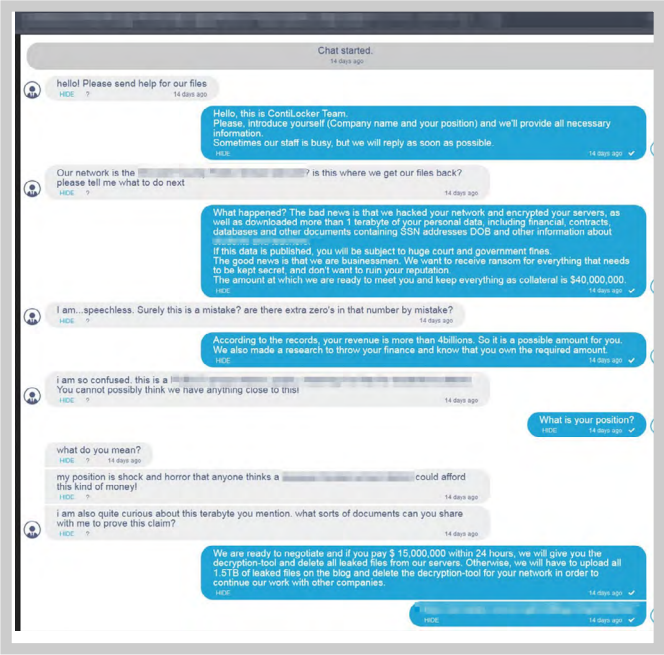
3rd Party Repositories

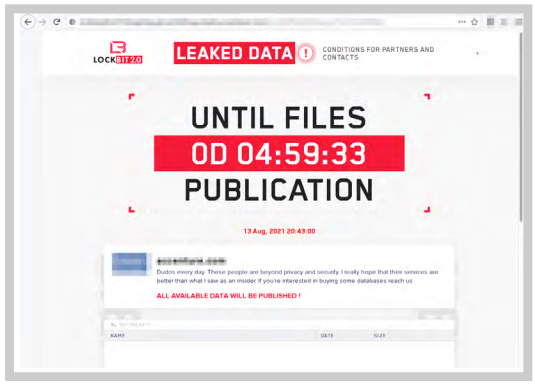


INCIDENT RESPONSE AND NEGOTIATIONS

ALL RANSOMWARE ATTACKS ARE COMPRISED OF KEY STAGES THAT, WHEN VIEWED ON A LARGER SCALE, FORM A PICTURE THAT REPRESENTS A CYCLICAL RANSOMWARE ECOSYSTEM.

The average ransomware threat actor 'dwell time' – time between initial access to encryption – is 15 days.





KEY MILESTONES: EXFILTRATION, ENCRYPTION, AND ANNOUNCEMENT

Once the ransomware actors have either cultivated or procured access to the victim network, they infiltrate and exfiltrate prior to encryption and extortion. Often, encryption is the first indication of compromise the victim experiences. The RaaS gang will then simultaneously post an announcement on their darknet blog and/or news sites to reveal who their victim is and proof that they have stolen critical data. At this point, victim/threat actor negotiations take place regarding any demands of ransom payments.

The announcements typically include a publication date and specified warnings toward their target. Victim launches incident response.

PRIMARY SOURCE AREAS WHERE THIS PHASE OCCURS

Paste Sites

RaaS Official Darknet Blog

RaaS Darknet Chat Server / TOX

Forums' Marketplaces

Darknet Classifieds & Markets

Other OSINT Resources

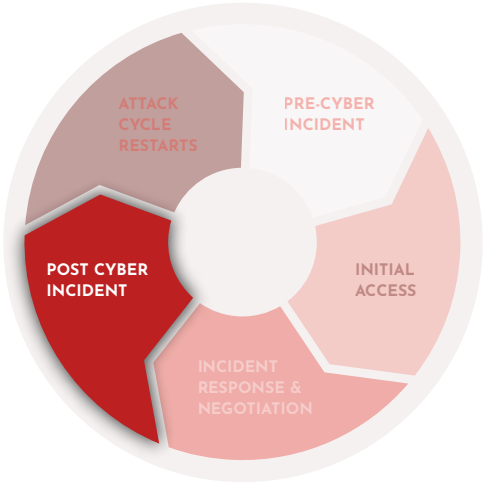
Telegram

Forum Chatter

Public News Media Outlets

Social Media

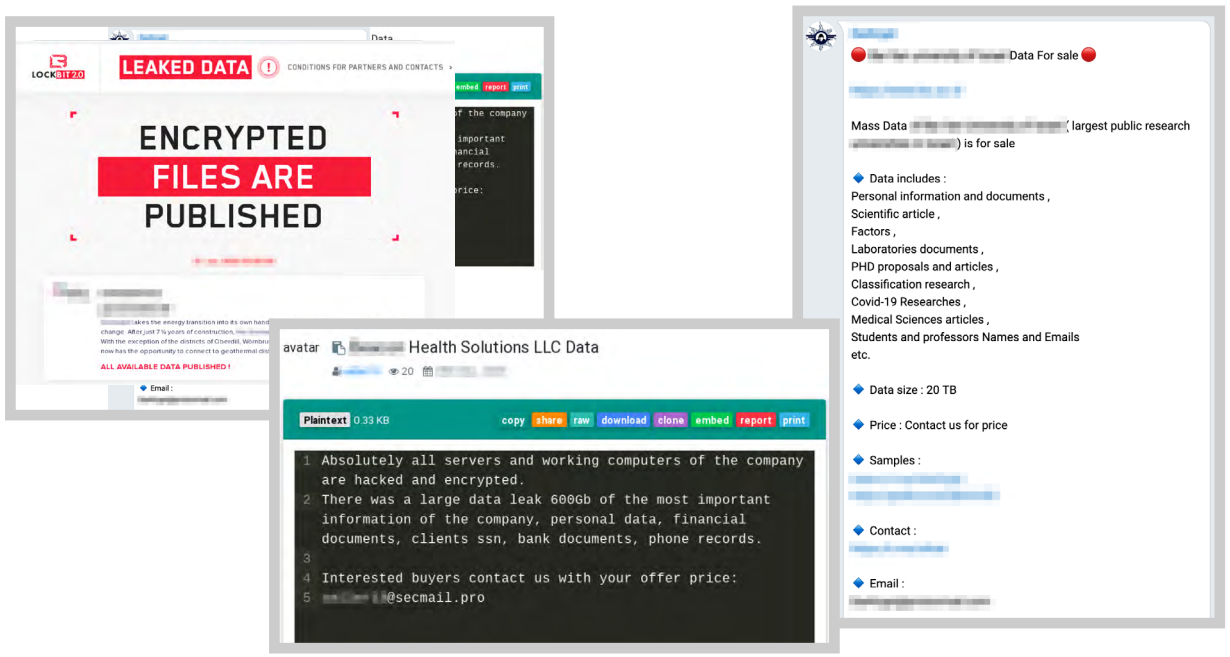
3rd Party Repositories



POST-CYBER INCIDENT

ALL RANSOMWARE ATTACKS ARE COMPRISED OF KEY STAGES THAT, WHEN VIEWED ON A LARGER SCALE, FORM A PICTURE THAT REPRESENTS A CYCLICAL RANSOMWARE ECOSYSTEM.

In 2021, the average extortion ransom demand for $100M companies reached $220,298 USD; an increase of 43% from 2020.



KEY MILESTONES: SHAMING & DATA SHARING

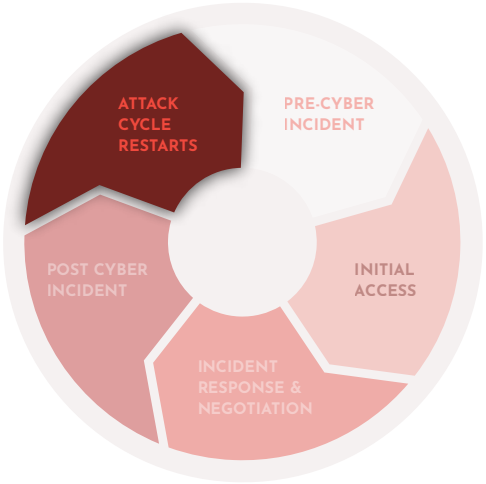
Depending on the ransomware group and victim, events from this phase case vary considerably. For example, if a victim has not paid their ransom, the threat actor group may begin auctioning off the victims data to the highest bidder. Even if the victims have paid their ransom, the attackers may still parse apart the stole information and distribute the victim's data for purchase, analysis, and potential future exploitation.

Data is hosted directly on the RaaS darknet blog or on a 3rd party data repository, where other threat actors download and circulate the archives extensively across the darknet and social media.

News media sources report on the incident and shareholder impact.

PRIMARY AREAS WHERE A PRE-CYBER INCIDENT TAKES PLACE

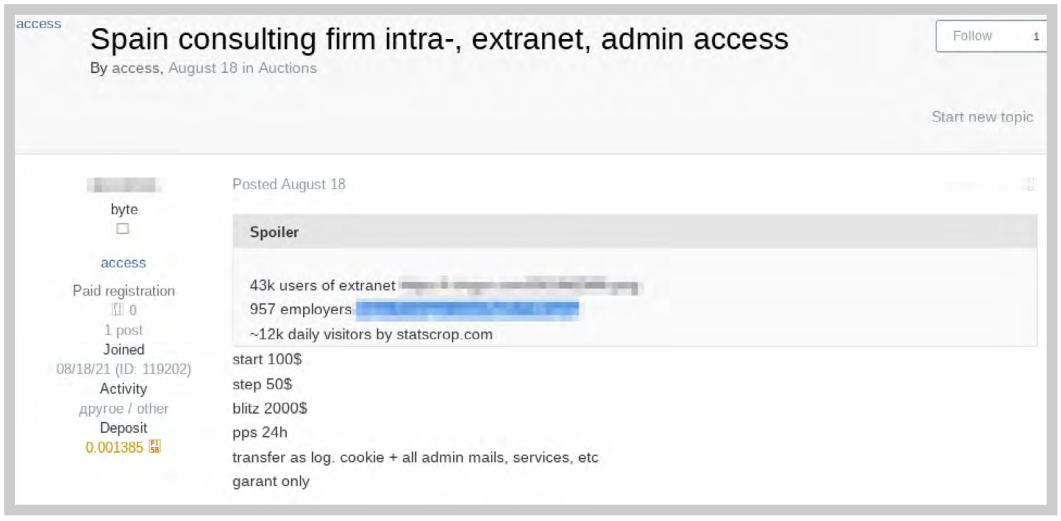
- Paste Sites
- RaaS Official Darknet Blog
- RaaS Darknet Chat Server / TOX
- Forums' Marketplaces
- Darknet Classifieds & Markets
- **Other OSINT Resources**
- Telegram
- Forum Chatter
- Public News Media Outlets
- Social Media
- 3rd Party Repositories



ATTACK CYCLE RESTARTS

ALL RANSOMWARE ATTACKS ARE COMPRISED OF KEY STAGES THAT, WHEN VIEWED ON A LARGER SCALE, FORM A PICTURE THAT REPRESENTS A CYCLICAL RANSOMWARE ECOSYSTEM.

Ransomware cost organizations around the world $20 billion USD in 2021.



KEY MILESTONE: SUBSEQUENT CAMPAIGNS AGAINST COMPANY, VENDORS & SUPPLIERS

As the exfiltrated data continues to circulate in all the corners of the surface, deep, and darknet, the compromised data from the initial target is exploited by a broader threat actor audience. It is often used to identify new victims – such as the suppliers or partners of the target company. Discussions on darknet forums regarding applicable new 0-days and the effectiveness of CVE's aid in identifying a new victim. Once one has been chosen, network surveillance, attack preparation and campaign coordination may take place weeks or months in advance.

In 2021, 37% of all businesses & organizations were hit with ransomware & sensitive information leaked on the darknet.

PRIMARY SOURCES AREAS WHERE THIS PHASE OCCURS

Paste Sites

RaaS Official Darknet Blog

RaaS Darknet Chat Server / TOX

Forums' Marketplaces

Darknet Classifieds & Markets

Other OSINT Resources

Telegram

Forum Chatter

Public News Media Outlets

Social Media

3rd Party Repositories

DARKOWL

ABOUT DARKOWL

DarkOwl uses machine learning to automatically, continuously, and anonymously collect, index and rank darknet, deep web, and high-risk surface net data that allows for simplicity in searching. Our platform collects and stores data in near realtime, allowing darknet sites that frequently change location and availability, be queried in a safe and secure manner without having to access the darknet itself.

For streamlined insight into ransomware group activity, check out our new product **Ransomware API >>**

DARKOWL DATA SOURCES

Tor, I2P, ZeroNet, authenticated forums, darknet marketplaces, IRC, high-risk paste sites, encrypted chat services, and open FTP servers.