PSI IP-Intrusion Service Database

Exposing cyber-crime and sharing information across the academic community
Why do we need an IP Intrusion Database?

The growing impact of cyber-crime is evidenced by the number of recent headlines mentioning the problem:

- The Washington Post – *Research firm releases new details on alleged Iranian hacking campaign targeting 300 universities* – March 2018
- The Scholarly Kitchen – *FBI indicts nine Iranians in a massive scheme to target academic credentials and steal content* – March 2018
- Harvard Business Review – *You can’t secure 100% of your data 100% of the time* – Dec 2017
- The Times – *University secrets are stolen by cybergangs* – Sept 2017
- Science Magazine - *Sci-Hub’s cache of pirated papers is so big, subscription journals are doomed, data analyst suggests* – July 2017
Intrusions – the cost to publishers

License negotiations impacted as libraries no longer “need” to pay for content. Small publishers face non renewal and less chance of new licenses.

Skewing of usage metrics - libraries that are hacked will see spikes in usage, while others will see less usage where patrons are using e.g. Sci-Hub

Validity of content could be compromised (paper could have been corrected and/or updated). Is the latest version reaching researchers?

Publishers are spending significant amounts of time fighting court battles with “whack a mole” results

Publishing industry facing negative press due to blocks and libraries having been constantly shut down
Intrusions – the cost to libraries

- Skewed usage metrics: increased usage may result in increased cost to library
- Hardware costs: computers analysed for virus removal or even replaced
- IT system are slowed e.g. by dictionary attacks and/or phishing
- Personal data can get into the wrong hands – possible GDPR penalties
- Staffing costs – library staff and IT staff
- Credentials can be used on other sites increasing the possibility of identity fraud
- Loss of access to electronic resources
- Validity of content could be compromised (paper could be corrected and/or updated)
- Even OA usage metrics are impacted
What is the PSI Intrusion Database?

PSI’s **IP Intrusion Database** is a new tool that helps both publishers and libraries by preventing intrusions of their secure IT systems.

With the IP intrusion service the academic research community can work together to fight against hackers, spammers, password crackers, scrapers and, most importantly, it will combat piracy and spear-phishing attacks.

This new service also helps protect publishers’ copyrighted content, universities’ intellectual property, and researchers’ personal data and identities.

The **PSI IP Intrusion Database** exposes cyber-crime across the academic research community, with the added benefit of reducing service interruptions from blocks that arise from these malicious threats.
How does it work?

Step 1: Ingestion and storage of IP Addresses

- IP Address Ingestion
- Step 6: Complete the circle
- Publishers
- Libraries

Step 2: Data Upgrade

- IANA
- + Timestamps
- + Responsible ISP & RIR
- + Threat Reporter
- + IP owner
- + Associated IPs
- + Registration details, inc. company name and contact details

Step 3: Data Authentication

- PSI IP Intrusion Service Database
- Step 2: Data Upgrade
- Step 6: Complete the circle
- Publishers
- Libraries
- The IP addresses are authenticated against theIPregistry.org which is used as a white list to avoid access interruptions for active customers.

Step 4: Filter by customer requirements

- Results
- Risk Rating
- The Whitelist (Legitimate Customers)
  - * ORG ID
  - * Standard Name
- The Blacklist
  - Filtered by ISP
  - Date
  - Category
  - Outcome
  - RIR

Step 5: Results reporting

- Step 4: Filter by customer requirements
- Step 2: Data Upgrade
- Step 6: Complete the circle
- Results

Step 6: Complete the circle

- Step 2: Data Upgrade
- Step 3: Data Authentication
- Publishers
- Libraries
- Results
- Risk Rating

66% ISPs

The Whitelist

The Blacklist

filtered by:

ISP, Date, Category, RIR
What does this mean?

**PSI IP Intrusion Database** allows publishers and libraries to share detailed information about intrusions so they can protect themselves from future threats.

Each day users of the service receive details of the latest intrusions across the industry allowing them to block the attacks at source.

The “white list” of verified institutional data is used to alert publishers that attacks are being made via a legitimate organisation, allowing them to treat these intrusions differently.

Libraries are alerted about breaches in real time. They will investigate the source IP of the intrusion and share these details, so that other libraries and institutions can block cyber-attacks from the source before they even happen.
An award-worthy service

The IP-Intrusion database offers significant value to the scholarly community.

Every intrusion reported within the database will provide the academic community with an opportunity to fight back.

This is a truly collaborative approach to fighting cyber-crime that will give the industry an opportunity to think ahead and try to stay one step ahead of the cyber-criminals.

The PSI IP Intrusion Database offers the academic research community a unique opportunity to work together to fight all forms of cyber-crime.