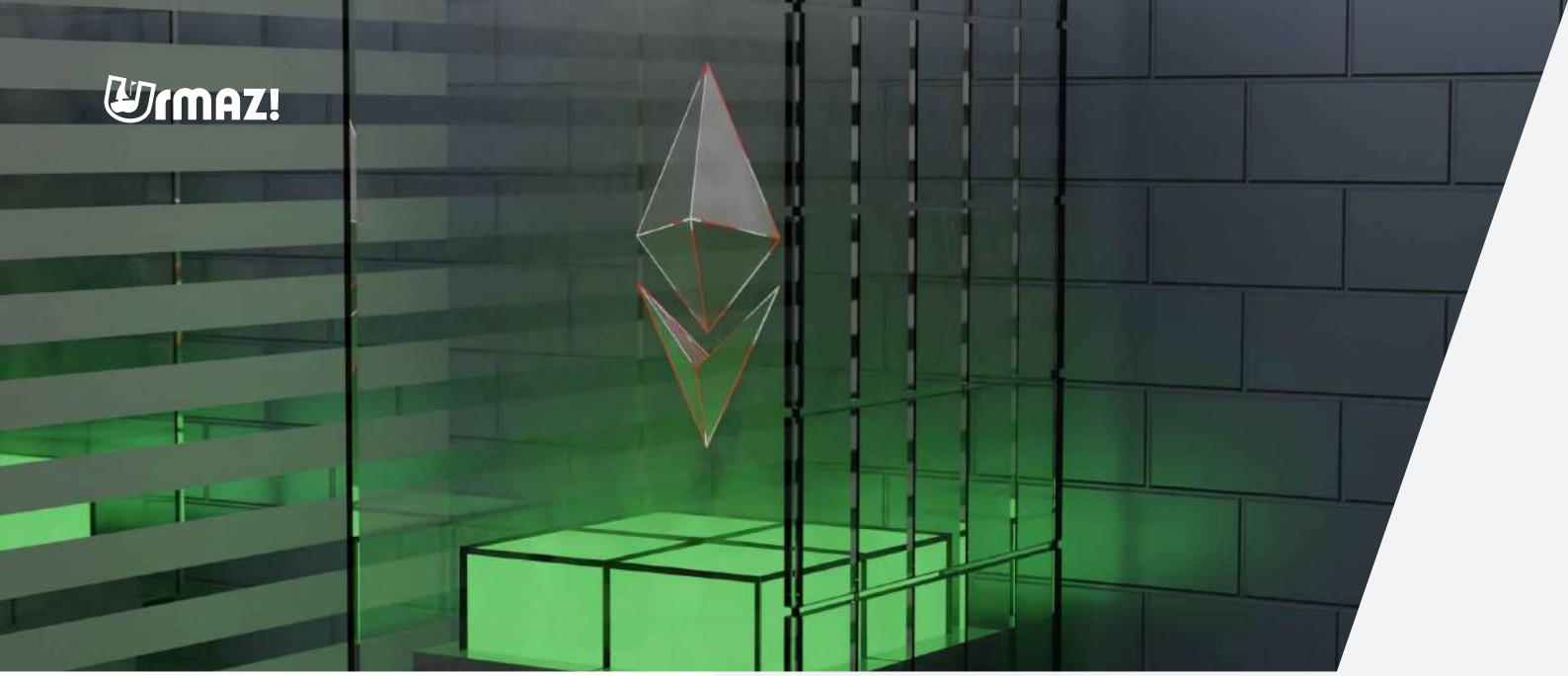

The Significant Benefits of Threat Intelligence Service

Increasing Number of Attacks

In 2022, the Internet Crime Complaint Center (IC3) — an establishment focused on fighting cybercrime— reported that total losses caused by cybercrime amounted to $27.6 billion. In the same report, the IC3 also highlighted the following:

7%

The number of cybercrime complaints filed with the IC3 increased by 7% in 2021. This is the fifth consecutive year that the number of complaints has increased.

24.3%

hishing was the most common type of cybercrime, accounting for 24.3% of all complaints.

15.4%

Ransomware attacks were also on the rise in 2021, accounting for 15.4% of all complaints.

While the reported figures already paint a bleak picture, it is important to note that these figures only represent the tip of the iceberg. The World Economic Forum (WEF) has noted that a significant proportion of cybercrime goes undetected. The actual number of victims may be significantly higher.

Stopping Threats at The Source

Almost all cybercrime require connecting to malicious domains. Threat actors need users to initiate an online connection (e.g., click a link, visit a webpage, or download a file) to start the attack chain. Early on, knowing which domains were malicious became critical to threat intelligence, and soon experts started classifying domains into broad groups:

1 **Known malicious domains**
These are domains that have been identified as being associated with malicious activity. Since the late 1990s, online communities have been compiling a list of known malicious domains. This has led to the creation of DNS blacklists, which was originally created to address the growing problem of spam email in the late 1990s.

2 **Suspicious domains**
These are domains that have not yet been identified as malicious, but exhibit some characteristics associated with malicious domains. It is advised to keep in contact with security professionals to gain more information if these domains eventually turn out to be malicious.

3 **New domains**
These are domains that have recently been registered. New domains are often used by attackers because they are less likely to be blocked by security software.

As cybercrime became more complex, classification methods evolved. However, the fundamental principle remained the same: collecting information about known threats to help protect against them.

SF-WP-30714

16F, No. 80, Sec. 1, Zhongxiao W. Rd.,Zhongzheng Dist., Taipei City 100007, Taiwan (R.O.C.)
www.urmazi.com

Threat Categories Help Avoid Risks

Over time, having a large and ever-growing database of malicious domains can get difficult to maintain. URMAZI then opted to group related threats into specific categories for better management. Using categories confers a number of benefits:

- **Categories are the fastest way to block large lists of undesirable domains.**
- Grouping domains into categories enables admins to provide users with information about why a particular website was blocked. This improves the transparency of the filtering system and makes it more user-friendly.
- Using categories make it easier to track and analyze trends. Collected information can then be used to develop new strategies or technologies that are more resilient to future attacks.
- Categories provide a level of control over the filtering system. A granular filtering system gives administrators more flexibility in selecting websites to block or allow.

Overall, categories allow customers to simplify the management of content that is deemed acceptable or inappropriate for their organization.

Gain Benefits via Subscription Services

Since cybercrime grows exponentially every year, it is highly recommended to invest in a service that is always up to date on the latest threats. iSafer offers a constantly updated list of categories. On iSafer's **[Go-Start Subscription]**, the 3 most critical categories are already included:

01 Botnet

02 Phishing

03 Scam

These categories offer strong protection against the most common attacks, and is available on all subscription levels. Additionally, this protection works at the DNS level, meaning it is not dependent on apps and will work across all operating systems and data providers.

For enterprises that perform extensive data analysis and threat investigations, iSafer also provides an additional 55 categories via its **[PLUS Subscription]** which includes Ransomware, Crypto, Shorter URL, Very New Domain and business related intelligences. These categories catalog millions of malicious domains, with more being added daily protecting your business operation and brand reputation.

This feature is part of iSafer's evolving Threat Intelligence service. The service is committed in keeping threat data in all iSafer installations accurate and up-to-date:

- Updated automatically in the background
- Kept current by a dedicated team which monitors the latest attacks
- Available 24 hours a day, 7 days a week
- Uses machine learning to identify possible malicious domains
- Detects recently created domains, IP addresses and URLs

Moreover, organizations can further enhance the protection provided by iSafer via the creation of prevention strategies through rigorous study of previous attacks, comprehensive knowledge of the current infrastructure, and implementation of programs that ensure everyone's threat knowledge is kept up-to-date. Through awareness and research, risks can be minimized.

In summary, having a comprehensive and well-maintained knowledge of threats is critical to protecting your business from the ever increasing wave of cybercrime. iSafer offers a Threat Intelligence service that is not only kept up-to-date, but also organized into categories that allow for easy management, analysis, and investigation, with even more categories available via subscription. With your knowledge and iSafer's Threat Intelligence, you can rest assure that you, your brand, and your digital assets are kept safe from attacks.

SF-WP-30714

16F, No. 80, Sec. 1, Zhongxiao W. Rd., Zhongzheng Dist., Taipei City 100007, Taiwan (R.O.C.)
www.urmazi.com