

# 471 Marketplace Intelligence

## KEY VALUE

Set watchers and alerts to ensure that you are notified as soon as any compromised credentials become available in the underground markets. A rapid response is essential in mitigating the business impact and actually reducing the value of stolen credentials in the marketplace.

The ability to track trends over time allows our clients to build up a masterview of how the markets behave over a certain time period. They can identify seasonality trends and even any causality so that they can prepare their defenses ahead of time.

Beyond being alerted about stolen cards and credentials, we offer the ability to further track the threat actors / merchants who sold the data to aid in determining how the cards or credentials were obtained and made their way into the marketplace. This allows proactive tracking of these actors and merchants to obtain early warning of future activity.

## Insights into underground marketplaces

Marketplace Intelligence is an essential tool for threat analysts. It offers unique insights into the most active and prolific underground marketplaces. 'Marketplaces' are underground websites intended for the sale of illicit goods but can be further categorized as markets and shops.

Underground markets allow many different sellers to sell a wide variety of illicit goods. Actors register as sellers on a market to start selling goods. A market can have listings for cards, credentials, drugs, weapons, and a host of other types of goods or services.

Underground shops allow one actor (the shop owner) or a limited group of actors (those invited by the actor running the shop) to sell a single type or a very limited set of types of goods: for instance, a card shop sells stolen credit or debit cards, whereas a credential shop only sells stolen credentials

Intel 471 Marketplace Intelligence delivers assets including:

1. **TITAN** exposes data from underground markets and shops
2. **Dashboards** highlight key marketplace metrics

Our Marketplace Intelligence customers can access details about the products for sale in the cyber underground, as well as research historical data, understand the activity, and set watchers to get notified when articles of interest are listed on one of the marketplaces.

## Purchasing access

Underground marketplaces are the most likely places that stolen cards and compromised credentials will surface. It is also where threat actors can purchase stolen digital assets relatively cheaply to facilitate some very expensive attacks.

Stolen data, such as cards and credentials, are easily obtained in the cyber underground and are often the starting point for further threats or attacks. Threat actors in possession of this critical information often look to compromise or damage a business to extort money.

471 Marketplace Intelligence illuminates the data being offered for sale in top tier marketplaces across the cyber underground. This capability alerts our customers when relevant items are being offered for sale and allows them to take protective measures to mitigate any impact that may follow from an attack.



This trend is gaining traction globally, with ransomware attacks increasing nearly **400%** between **2017** and **2021**

Statista, 2022



The expected cost to businesses is estimated to be **\$265 billion** by **2031**

## Prevention is better than cure

471 Marketplace Intelligence is a complete product offering. Collecting the stolen cards and compromised credentials is the initial response from most organizations, however the question needs to be, how did this happen? With our unique and inimitable product portfolio, we don't want to just inform our customers of an incident. We want to go beyond that and explain how this might have happened and what proactive steps they can take to reduce the possibility of it happening again. Our Malware and Adversary Intelligence is unparalleled in the industry and now, combined with Marketplace Intelligence, we have a more complete solution for dealing with and preventing financially motivated threat actors

## Why Intel 471?

Our experts operate across the globe, closely tracking sophisticated threat actors in the places they operate, speak their languages, and understand cultural references that expose and illuminate their underground activities. As a result, we can provide the most relevant and timely intelligence to our customers. Relevant intel refers to specific threats to your business or industry, and when CTI teams are often stretched to capacity, having the guidance on where to focus your team's finite resources is essential. The additional ability for organizations to understand and then implement necessary change is where the real value lies. We pride ourselves on helping organizations operationalize their intel so they are better protected against possible threats. As your organization and their CTI requirements grow, so too can our solution. Even for the most mature CTI teams, our intelligence will far exceed their most ambitious requirements.

For more information on 471 Marketplace Intelligence, visit [intel471.com](https://intel471.com)



[sales@intel471.com](mailto:sales@intel471.com)