471 Credential Intelligence

KEY VALUE

- Proactively monitor, alert, and mitigate the risk associated with compromised credentials via API, WebUI, or third-party integration
- Protect your employee accounts from account takeover (ATO), thus reducing the risk posed to your business
- Know when executives or other key personnel have compromised credentials available to cybercriminals
- Monitor for exposure to your key third-party suppliers and vendors to receive a data-driven assessment of the risk they pose
- Protect your customers and bottom line from fraud related to criminal takeover of their online accounts
- Obtain unique visibility and data collected from the underground marketplace where cybercriminals operate
- Easily pivot into Intel 471's other intelligence offerings for context to deconflict old data from fresh data quickly
- Leverage a feature-rich monitoring and alerting system and consume notifications via our Titan WebUI, API, email, or third-party integrations

How Safe Are Your Account Credentials?

Everyday news breaks of another major data breach including leaked personally identifiable information (PII), or a malware campaign that pilfers usernames, passwords, and other sensitive data. It seems inevitable that the credentials of your employees and customers will be compromised by breaches to your organization or to your key suppliers holding your sensitive business data. Compromised credentials are a highly sought-after and valuable commodity in the underground marketplace, as these are often an easy entry point into networks or the start of an account takeover (ATO) scenario that can leave your business reeling.

Unique, Comprehensive and Relevant

Intel 471's automated collection systems and global research team constantly collect compromised credential data and produce unique intelligence. Our database contains billions of credentials and tens of millions of unique data points that provide valuable context. Linking and pivoting across credential releases and into our intelligence knowledge base is as simple as a click. Additionally, relevance is key as actors often combine many older releases into larger data sets and attempt to trade or sell them as well. 471 Credential Intelligence allows you to differentiate between newly compromised credentials and older repackaged data. Identifying the most relevant threats empowers your finite resources to put an effective and targeted response into play.

Benefits of Credential Intelligence

Intel 471's comprehensive coverage across the underground marketplace offers our clients the ability to be proactive, monitoring and mitigating the risk associated with compromised credentials as they hit the marketplace. 471 Credential Intelligence satisfies four core-use cases associated with compromised credentials:

- ***Employees***: Know when your employee accounts have been compromised and stop ATO and other types of malicious activity
- ***VIPs***: Proactively monitor and protect accounts of executives and key personnel before those key accounts are used as a launching point
- ***Customers***: Alert your own customers to malware infections associated with their online accounts using your services
- ***Third-party relationships***: Know when your third-party vendors and suppliers have exposure that, by extension, introduces unnecessary risk to your business

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.

sales@intel471.com