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

Cybercriminals Will Compromise Your Account Credentials

Every day news breaks of another major data breach, leaked personally identifiable information (PII), or malware campaign that pilfers usernames, passwords, and other sensitive data. It's now a foregone conclusion the credentials of your employees and customers, often through no fault of their own, will be compromised at some point or another. The same can be said of your key suppliers and vendors who are holding your customer data or providing business critical services. Compromised credentials, a highly sought-after commodity in the underground marketplace, are often an easy entry point into networks or the start of an account takeover (ATO) scenario that can leave your business reeling. Just sitting back and reacting to account anomalies, alerts, or even worse – a blog or news story – no longer is an effective way to manage the risk.

Unique and Comprehensive Data Set Complete with Context

Intel 471's automated collection systems and global "boots on the ground" Intel team constantly collects compromised credential data and produces unique intelligence. Our compromised credential database contains billions of credentials and tens of millions of other 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. This context is key as actors often combine many older releases into larger data sets and attempt to trade or sell them as well. This causes confusion and extra cycles to be spent tracking down stale data. Credential Intelligence allows you to differentiate between freshly compromised credentials and old repackaged data. While the news, blogs, and other vendors are sounding the alarm at the next billion-record data breach, you can rest easy knowing it's simply stale data repackaged and rereleased. Or you can act quickly when you are alerted to a fresh credential set when it hits the marketplace for the first time.

Benefits of Cybercrime Intelligence

Intel 471's complete coverage across the underground marketplace offers our clients the ability to be proactive by monitoring and mitigating the risk associated with compromised credentials as they hit the marketplace. 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.

sales@intel471.com