Are you Protecting your Customers' Most Important Digital Asset?

As an MSP you are a trusted partner and advisor to your customers, providing a broad portfolio of services that can range from endpoint and server management to data backups, performance and capacity monitoring and software lifecycle management. **But are you helping your customers to protect their most valuable asset: their digital credentials?**

Digital credentials such as usernames and passwords are used by your customers to connect to critical business applications, as well as online services. Unfortunately, criminals know this — and that's why digital credentials are among the most valuable assets found on the Dark Web. The Dark Web is made up of digital communities that sit on top of the Internet, and while there are legitimate purposes to the Dark Web, it is estimated that over 50% of all sites on the Dark Web are used for criminal activities, including the disclosure and sale of digital credentials. Far too often, companies that have had their credentials compromised and sold on the Dark Web don't know it until they have been informed by law enforcement — but by then, it's too late.

Dark Web ID™ from ID Agent is the industry's first commercial solution to detect your customers' compromised credentials in real-time on the Dark Web. Using a proprietary technology, Dark Web ID vigilantly searches the most secretive corners of the Internet to find compromised credentials associated with your customers' employees, contractors and other personnel, and notifies you immediately when these critical assets are compromised, before they are used for identity theft, data breaches or other crimes.

Dark Web ID from ID Agent gives MSPs a critical tool to protect your customers' most valuable digital asset, and reduces their risk of being in the headlines due to a data breach. Dark Web ID provides a unique, fully-branded service that can be easily added to your solution portfolio with zero additional hardware or software, and helps you to drive additional revenue through add-on products and services that can protect credentials from reaching the Dark Web in the future. **Online criminals can hide from your customers — but they can't hide from Dark Web ID.**

idagent.com

PROTECT YOUR CLIENTS. GROW YOUR BUSINESS.

DARKWEB ID

How It Works

- Provides continuous searching, monitoring and reporting of your customers' digital credentials on the Dark Web.
- Supports hundreds of different sources, including criminal sites that sell credentials; open document repositories that post credentials publicly, Internet Relay Chat (IRC), and social media sites found only on the Dark Web.
- Establish specific domains or other unique identifiers to search, and Dark Web ID provides real-time and daily digest notification when matching data is found.

Why It's Important

- Compromised credentials are used to conduct further criminal activity, such as data breaches of sensitive corporate information, as well as identity theft of individual employees.
- Users often have the same password for multiple services, such as network logon, social media, online stores and other services, exponentially increasing the potential damage from a single compromised username and password.
- Customers have limited visibility into when their credentials are stolen; over 75% compromised credentials are reported to the victim organization by a third party, such as law enforcement.

Value for MSP Customers

- Delivers the same advanced credential monitoring capabilities used by Fortune 500 companies to organizations in the SMB and mid-market space.
- Connects to multiple Dark Web services including Tor, I2P and Freenet, to search for compromised credentials, without requiring customers to connect to these high-risk services directly.
- Proactive solution provides real-time awareness of compromised credentials before identity theft or data breaches occur.
- Lower price point and real-time discovery capabilities not available in competitive services.

Value for MSPs

In addition to the additional revenue stream Dark Web ID generates for MSPs, the platform provides multiple opportunities for fully-justified sales of additional value-add products and services to reduce customers' risk of compromised credentials:

- **Multi-Factor Authentication** - By requiring a second credential based on a physical token or phone-based SMS message, it's much less likely that a single username and password can be used to conduct a data breach or identity theft.
- **Data Loss Prevention** - DLP technologies can be used to detect when credentials are compromised at the source, inside your customers' networks.
- **Password Managers** - These tools make it easier for customers to use complex and varied passwords between different accounts, ensuring that one single compromised password can't be used across multiple sites and services.
- **Encryption** - Encryption tools can help reduce the likelihood of compromise of credentials by applying strong cryptography to credentials both in transit and at rest.
- **SIEM and Monitoring** - Log management and analysis tools such as SIEM can help to detect unusual network and user activity that can point to a potential compromise of credentials.

Dark Web ID provides MSPs with a unique opportunity to increase sales while securing their customers' most critical digital asset. Contact us today to find out more!

E: sales@idagent.com
idagent.com

DARKWEB ID