Frequently Asked Questions
Dark Web

What is the Dark Web?

The Dark Web is a hidden universe contained within the "Deep Web"- a sub-layer of the Internet that is hidden from conventional search engines. Search engines like Google, BING and Yahoo only search .04% of the indexed or "surface" Internet. The other 99.96% of the Web consists of databases, private academic and government networks, and the Dark Web. The Dark Web is estimated at 550 times larger than the surface Web and growing. Because you can operate anonymously, the Dark Web holds a wealth of stolen data and illegal activity.

How Does RadiusBridge Dark Web Scanning Help Protect My Organization?

Our service is designed to help both public and private sector organizations detect and mitigate cyber threats that leverage stolen email addresses and passwords. RadiusBridge Dark Web Scanning leverages a combination of human and artificial intelligence that scours botnets, criminal chat rooms, blogs, Websites and bulletin boards, Peer to Peer networks, forums, private networks, and other black-market sites 24/7, 365 days a year to identify stolen credentials and other personally identifiable information (PII).

How are the Stolen or Exposed Credentials Found on the Dark Web?

RadiusBridge Dark Web Scanning focuses on cyber threats that are specific to our clients' environments. We monitor the Dark Web and the criminal hacker underground for exposure of our clients' credentials to malicious individuals. We accomplish this by looking specifically for our clients' top level email domains. When a credential is identified, we harvest it. While we harvest data from typical hacker sites like Pastebin, a lot of our data originates from sites that require credibility or a membership within the hacker community to enter. To that end, we monitor over 500 distinct Internet relay chatroom (IRC) channels, 600,000 private Websites, 600 twitter feeds, and execute 10,000 refined queries daily.

Does the Identification of My Organization's Exposed Credentials Mean We Are Being Targeted by Hackers?

While we can't say definitively that the data we've discovered has already been used to exploit your organization, the fact that we are able to identify this data should be very concerning. Organizations should consult their internal or external IT and/or security teams to determine if they have suffered a cyber incident or data breach.

Data Source Locations & Descriptions: Where Do We Find Data?

Dark Web Chatroom: compromised data discovered in a hidden IRC
Hacking Site: compromised data exposed on a hacked Website or data dump site
Hidden Theft Forum: compromised data published within a hacking forum or community
P2P File Leak: compromised data leaked from a Peer-to-Peer file sharing program or network
Social Media Post: compromised data posted on a social media platform
C2 Server/Malware: compromised data harvested through botnets or on a command and control (C2) server

Some of this Data is Old and Includes Employees that are no Longer Working for Us. Does this Mean We are Not at Risk?

While employees may have moved on from your organization, their company issued credentials can still be active and valid within the 3rd party systems they used while employed. In many cases, the 3rd party systems or databases that have been compromised have been in existence for 10+ years holding millions of "zombie" accounts that can be used to exploit an organization. Discovery of credentials from legacy employees should be a good reminder to confirm you've shut down any active internal and 3rd party accounts that could be used for exploit.

RADIUSBRIDGE®

Know your data. Control your data. Grow your business.