DARKWEB ID

FREQUENTLY ASKED QUESTIONS

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 DARK WEB ID 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. Dark Web ID 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?

Dark Web ID 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. DOESN'T 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.

IDENTIFIED METHOD USED TO CAPTURE/ STEAL DATA: HOW WAS THE DATA STOLEN OR COMPROMISED?

- Tested: the compromised data was tested to determine if it is live/active;
- Sample: the compromised data was posted to prove its validity;
- Keylogged or Phished: the compromised data was entered into a fictitious website or extracted through software designed to steal PII;
- 3rd Party Breach: the compromised data was exposed as part of a company's internal data breach or on a 3rd party Website;
- Accidental Exposure: the compromised data was accidentally shared on a Web, social media, or Peer-to-Peer site;
- Malicious / Doxed: the compromised data was intentionally broadcast to expose PII.

WHAT DOES PASSWORD CRITERIA MEAN?

Password Criteria is designed to allow you or your clients to identify what their on-network password criteria is in order to put a higher alert status on credential exposures that may meet these criteria. It allows you to enter minimum lengths, number of letters, numbers, special characters and capital letters.

WHAT DOES IT MEAN WHEN A PASSWORD HAS A LONG SERIES OF RANDOM NUMBERS AND LETTERS?

This means the password was published as “hashed” (still encrypted). Hundreds of encryption dictionaries are readily available on the Web, and it’s not uncommon for these passwords to be “cracked” or decrypted and available on multiple 3rd party websites.

I SEE FAKE EMAILS (FALSE POSITIVES). WHY IS THIS IMPORTANT?

Fake email accounts are routinely created by employees as a “throw away” when wanting to gain access to a system or piece of data. However, fake email accounts are frequently created to facilitate well-crafted social engineering and/or phishing attacks. Often, the identification of fake email accounts indicates that an organization has been targeted by individuals or groups in the past.

THE PASSWORD IDENTIFIED DOES NOT MEET OUR NETWORK CRITERIA. WHY SHOULD WE CARE ABOUT THIS?

Employees often recycle passwords throughout their work and personal networks. If your internal requirement is to have a capital letter and special character, it’s common practice for employees to use a password they are familiar with, and add a capital letter and exclamation mark. (Example: Exposed Password: cowboys, Variation: Cowboys!, Cowboys1, Cowboys!1, and so on.) Knowing this, hackers will run scripts using metasploit frameworks (hacking and pentesting tools) to “brute force” their way into an unsuspecting system.

I’M SEEING MULTIPLE USERS WITH THE SAME PASSWORD BEING EXPOSED ON THE SAME DAY, WHAT DOES THAT MEAN?”

In most cases, someone is testing a password against a series of users to gain access.

WHAT IS THE DIFFERENCE BETWEEN A PRIVILEGED USER AND STANDARD USER?

The Standard User does NOT have access to view passwords.

CAN I TRACK PERSONAL EMAIL ACCOUNTS FOR COMPROMISES?

We allow for up to 5 personal email addresses per organization to be tracked, in addition to all emails on the company domain.

ANY “BEST PRACTICES” FOR INDIVIDUAL USERS OR CORPORATE IT ON FREQUENCY OF PASSWORD CHANGE OR ACTUALLY CHANGING YOUR PERSONAL OR PROFESSIONAL EMAIL?

Please refer to the National Institute of Standards and Technology’s (NIST) Special Publication 800-63B Digital Identity. A link to SP800-63B can be found here: https://pages.nist.gov/800-63-3/sp800-63b.html

IS IT SAFE TO SAY CLOUD STORAGE IS A SERIOUS CONCERN FOR DATA BREACH? WITH MOST OF OUR SOFTWARE TOOLS MOVING TO CLOUD HOSTING, DOES THIS CREATE MORE RISK FOR MY COMPANY'S IP?

There can be as much risk to your data within a Cloud environment as there is when it resides locally within your own servers. When researching Cloud providers and data centers, make sure you understand their compliance and certification with the security standards and protocols that impact your industry. CSO Online maintains a thorough list of security laws, regulations and guidelines by type: http://www. csoonline.com/article/2126072/compliance/ compliance-the-security-laws-regulations-andguidelines-directory.html

IF YOUR PERSONAL DATA IS FOUND ON THE DARK WEB, CAN IT BE REMOVED?

Once the data is posted for sale within the Dark Web, it is quickly copied and distributed (re-sold or traded) to a large number of cyber criminals, within a short period of time. It is generally implausible to remove data that has been disseminated within the Dark Web. Individuals whose PII has been discovered on the Dark Web are encouraged to enroll in an identity and credit monitoring service immediately. http://www. idagent.com/identity-theft-protection-2/ be used for exploit.

ARE THERE ANY SPECIAL CREDENTIALS NEEDED TO INVESTIGATE THE DARK WEB?

You do not need special permission to access the deep or Dark Web. However, accessing the deep or Dark Web requires the use of a "TOR" browser and should only be done using a VPN/ 10042017
encrypted tunnel. In general, we advise against attempting to access the Dark Web.