Title A: Dark Web Monitoring: Have Your Users Been Hacked and Not Know It?

Subtitle A: Cyberattacks and data breaches are not instantaneous – you can catch user data on the dark web.

Title B: Dark Web Monitoring Lets You Catch Compromised User Credentials Before Hackers Attack

Subtitle B: Use advanced monitoring to catch user data in unauthorized places on the dark web.

Title C: Dark Web Monitoring: The Last Line of Defense for Compromised User Credentials

Subtitle C: Find out when your user credentials end up on dark web marketplaces – and act fast!

https://pixabay.com/illustrations/deep-web-dark-web-darkness-binary-1106648/

Data breaches don't happen overnight.

In fact, the average data breach can take weeks or months to perpetrate. A great deal of time can pass

from the first moment an unauthorized user gains access to your network and the moment your IT team becomes aware of the problem.

Often, the initial perpetrators are not the ones who actually carry out the cyberattack themselves. In 2016, a hacker named Peace obtained 117 million LinkedIn credentials from another group of hackers and offered to sell them on the Dark Web. The initial data breach occurred in 2012, and many users were left unaware until the Dark Web sale started making headlines.

If Your Passwords Are On the Dark Web, It's Not Too Late To Act

Having your confidential user data on sale on an illegal Dark Web marketplace might seem like a hopeless place to be, but there is still time to act. As long as your users still have access to their accounts, changing their passwords and enabling dual-factor authentication will stop unauthorized users in their tracks.

This can be challenging if you have hundreds, thousands, or millions of compromised login credentials to update, but it can be done. In fact, depending on where your organization does business, failure to notify users and try to help them mitigate the damage might be against the law. If you can catch user credentials for sale on the dark web and act quickly enough to strengthen those credentials before a hacker strikes, you may be able to mitigate the worst part of the data breach and significantly reduce damages.

Doing this requires being able to automatically scour Dark Web marketplaces for data that correlates to the platforms and services you use. This is the promise that advanced Dark Web monitoring makes.

How Dark Web Monitoring Works

There are few barriers to entry into the cybercrime industry. Any appropriately equipped user can access the Dark Web – which means that security professionals can obtain data on Dark Web marketplace transactions the same way hackers do.

In many cases, in order to catch a cybercriminal, you have to think like a cybercriminal. This is part of what makes Certified Ethical Hackers such valuable additions to any cybersecurity workforce. It is also what empowers organizations to use Dark Web monitoring as a final line of defense against costly, reputation-damaging data breaches.

Dark Web monitoring services work developing and deploying automated systems to check for user-specific information on the most popular Dark Web marketplaces. As soon as one of your user's account information becomes available through one of these marketplaces, the monitoring services alert your IT team so you can update the stolen user credentials quickly.

This can mean the difference between dealing with an unmitigated data disaster and being able to demonstrate to users that their data is safe with you.

Dark Web Monitoring Is Part of a Holistic Security Framework

Just over half of all organizational data breach victims only learn they have been attacked because an outsider tells them. In most cases, law enforcement is the one responsible for alerting the organization. They immediately launch an investigation and tie up organizational resources while compelling the organization to announce the data breach to its users.

Data breaches are typically contained sooner and more effectively if the organization detects the breach on its own. This is only possible if the staff conducts routine vulnerability assessments, invests in Dark Web monitoring, and conducts penetration testing as part of a multi-tiered cybersecurity framework.

Penetration testing is another tool in the Certified Ethical Hacker's toolkit. This is essentially a controlled form of internal auditing where a security professional takes on the role of a hacker in order to search for and exploit vulnerabilities in the company's network, then reports on their findings.

Professional password management is yet another pillar of excellent cybersecurity. Instead of leaving users to come up with their own passwords, security-oriented organizations implement password-changing policies using automated password generators that can prevent accounts from being compromised even after hackers crack them.

Dark Web monitoring, penetration testing, and password management form three parts of an advanced, holistic security approach that protects organizations against sophisticated threats. There is no such thing as the "perfect" security solution – only increasingly reliable ways to discourage cyberattackers from

claiming your organization as their next victim. With the right approach, you can save your business even after hackers successfully steal data from your users.

Sources:

https://www.vice.com/en_us/article/78kk4z/another-day-another-hack-117-million-linkedin-emails-and-password

https://www.csoonline.com/article/3239144/2fa-explained-how-to-enable-it-and-how-it-works.html

https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html