DECIPHERING TERMS: The “Dark Web”

-AND WHY IS IT BAD IF MY CREDENTIALS LIVE THERE?

What is the “Dark Web”?

We’re all aware of what the internet is, and most people have ‘some’ knowledge of the risks that being ‘online’ poses.
However, whilst many have heard of terms such as “Deep Web” or “Dark Web”, very few actually understand what they mean.

One could write many pages about the topic, but it is perhaps sufficient to understand that 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.

The Dark Web “marketplace”

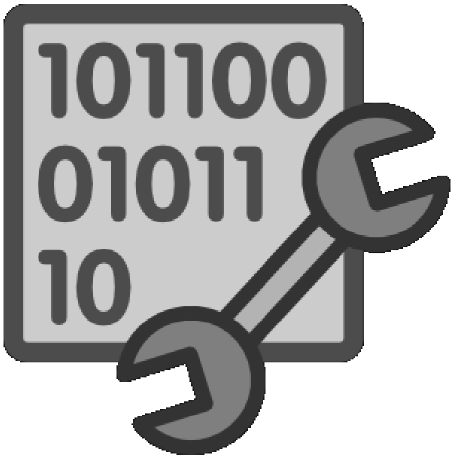
It is this criminal and ‘underground’ portion of internet that contains a marketplace for all kinds of dangerous products including but not limited to:

- ‘bot nets’ for hire consisting of (sometimes) thousands of compromised devices (including your average home router/modem) that can be used in coordination to carry out denial of service (DoS) attacks, brute-force password cracking, or other CREDENTIAL gathering activities.

- Hacking ‘tools’ sold to any who wish to use them – such as internet address scanning, vulnerable device detection, port scanners, traffic ‘sniffers’ and internet packet intercept & analysis etc – often used for capturing plain-text passwords (CREDENTIALS) transmitted by you, over the web.

- Malware program code that can be bought and implanted into websites, or ‘app’ ads, or other ‘seemingly’ useful apps that you can download for free on the internet to your PC or mobile device – but actually give remote control to hackers or sends them your keystrokes so that they may learn your CREDENTIALS.

The Dark Web “marketplace” <continued>



- Phishing email campaign templates, or even ‘phishing as a service’, designed to trick others into typing their CREDENTIALS into fake versions of banking login screens or other trusted online forms.

- Access to compromised servers or devices, using compromised CREDENTIALS

- YOUR CREDENTIALS – login names, email addresses, passwords, and personal details about you including addresses, phone numbers, places of work and more.

How do you know if your credentials are compromised on the Dark Web?

It is perhaps obvious why the Dark Web is not a good place for your CREDENTIALS to be available for sale. The security of your data, intellectual property, privacy and safety is perhaps proportionate to the integrity of your online ID and CREDENTIALS.

But how would you know if your CREDENTIALS have been exposed on the Dark Web?

It is important to keep in mind that your credentials only have marketable value if they are current. This infers two things:

1. It is in a hacker’s best interests to keep you blissfully unaware that your details are compromised, because not ‘tipping you off’ is key to retaining that value. It is unlikely that you know you have been compromised or how it occurred.

2. Regular changes of passwords AND utilization of a 2nd factor for securing your systems can reduce the value of harvested CREDENTIALS to zero.

Nonetheless, knowing “IF” your CREDENTIALS have been compromised, “WHICH” ones were leaked, “WHEN” the compromise occurred and “HOW” you became exposed is invaluable in the self-education process and necessary to help in re-securing your online identity and preventing future breaches.

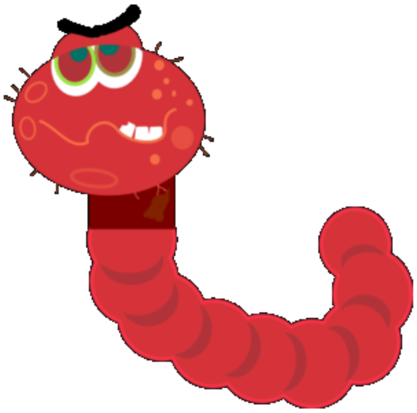
Recovery from Credential leakage on the “Dark Web”

Whilst it is quite impossible for you to remove your identity from the Dark Web (i.e. once exposed it is likely that your details were rapidly copied and traded), it is possible for you to immediately take action to minimize damage and mitigate future risk.

STEP 1: IDENTIFY

- ✓ **First understand WHICH of your online ID’s have been exposed, WHEN & HOW. It is a service that we can assist you with FREE of charge. If you learn that your CREDENTIALS have been compromised, then we can further assist you with the remaining steps :**

STEP 2: RECTIFY



- ✓ **Immediately rectify any existing compromises through password changes, (from safe devices!) at all identifiable entry points that use those credentials**

- ✓ **Most importantly, rectify the cause – be it due to malware or infection or virus or an unpatched vulnerability of your software/operating system – or even hardware (yes hardware flaws – eg in CPU – refer ‘spectre’ and ‘meltdown’ vulnerabilities present in older hardware!)**

STEP 3: QUANTIFY

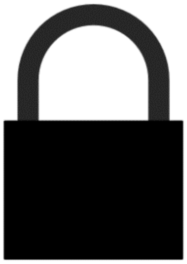
- ✓ **Assessment of whether it is likely that confidential data has been leaked as a result, determine the scale and impact, and whether credentials have been used to create other access points**

STEP 4: NOTIFY

- ✓ **Depending on the outcomes of the ‘QUANTIFY’ stage, it may be necessary for you to notify your insurance company (in order to alert them to potential future claims). The insurer may wish to engage a specialist to correctly notify other parties that may have been affected by the breach. It may also be a requirement under law to publicly disclose that a breach has occurred.**

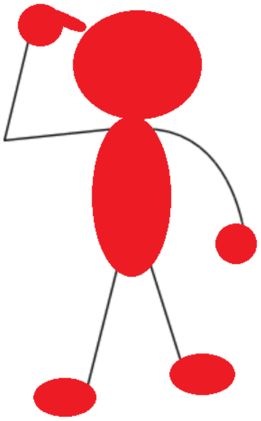
STEP 5: SECURE

- ✓ **re-securing resources that may have been compromised by removing unauthorized entry points, implementing safeguards to increase security (eg VPN, 2-factor authentication, regular malware detection and or managed system patching / update regime**



Recovery from Credential leakage on the “Dark Web” <continued>

STEP 6: LEARN



- ✓ Learn from the process, understand how leakage occurs, change behaviors. We offer a service whereby you (and your team) can be educated about how breaches occur and that changed behaviours can dramatically lessen the risk of data compromise for your business.

STEP 7: MONITOR

- ✓ Regular audits of password change policies, top-up training and assessment for your team, monthly Dark-Web scans to validate that your credentials are being kept secure

Can I remove my personal data from the Dark Web?

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 identity or credentials has been discovered on the Dark Web are encouraged to enroll in an identity and credential monitoring service immediately. You can call us for more details on 1800 505 767, or email us at: info@accountable-it.com.au

How can I secure my data from cyber criminals? Are good passwords enough?

Internet security is increasingly becoming a specialist area, and cyber-crime is on the increase. A good password is simply inadequate nowadays. It is advisable to engage an IT Professional that is well-versed in cyber security if you value the security of your corporate data. However, everybody can reduce their online risk by following these top 5 suggestions:

- ✓ Use complex & unique passwords.
- ✓ Wherever possible, use a 2nd factor to protect all of your digital assets
- ✓ Keep computers and mobile devices up-to-date with patches
- ✓ Use a VPN to encrypt all internet-based traffic
- ✓ Think before you click & beware of free ‘anything’ online

@ccountable
IT GROUP
smart . business . partner.

www.accountable-it.com.au