SonMax Consultants Inc.
24 Manor Drive
Marlboro, NJ 07746
E: sales@sonmax.com
T: +1 732.591.1512
F: +1 732.591.5424
www.sonmax.com

Can you really scan the dark web?

As new breaches are announced, the latest being the 2016 breach at Uber, more and more people are worrying about the integrity and security of their personally identifiable information ("PII"), Payment Card Information data ("PCI") and protected health information ("PHI"). A number of firms, including Experian, have been talking about free and paid services that scan the dark web to see if your PII, PCI and/or PHI data have been compromised and appear on the dark web.

Naturally, there's been pushback on the web about the reliability, security and effectiveness of the dark web scan services. So here are some facts, not fear uncertainty and doubt ("FUD") to help you decide how to best address the issue:

1. There are approximately 1.2 Septillion internet address combinations potentially out on the dark web (that's 1.2×10^{24} combinations). It is impossible to scan every single combination, in a timely manner, to see if your data is captured in all of these possible locations.
2. That said, there are many well-known aggregate sites – known as "bazaars", that act as a clearing house for PII, PCI and PHI data. Sites such as ***Joker's Stash***, a dark web credit card theft bazaar, is well-known. Other sites, include:
    a. AERO Market
    b. Berlusconi Market
    c. CGMC
    d. Dream Market
    e. Libertas Market
    f. RsClub Market
    g. Sourcery Market
    h. The Majestic Garden
    i. Tochka
    j. Wall Street Market

SonMax Consultants Inc.
24 Manor Drive
Marlboro, NJ 07746
E: sales@sonmax.com
T: +1 732.591.1512
F: +1 732.591.5424
www.sonmax.com

All of which are up and running right now, despite the takedown earlier this year of AlphaBay, and Hansa (two of the largest Dark Web bazaars) by Interpol and US law enforcement.

So, what can you do? First, if you're looking for a dark web scanning service or tool, ask some basic questions:

1. Does the service/tool include scanning the above sites?
2. Does the service/tool include scanning the sites that have been taken over by the authorities?
3. Does the service/tool provider have written evidence to support their coverage?

If you decide to go with one of these tools or services, understand that they will limit their scans to the most well-known and heavily trafficked areas of the dark web. If they come back negative, it does **not** mean you are safe and you should plan on repeating the scan on a regular basis, as data moves constantly. If the scan or tools shows that your PII, PCI or PHI data is on the dark web then you have to take steps to mitigate potential damage to your credit and secure against additional identity/information theft. Below are some common-sense steps that are critically important.

First, change passwords! Go to every site where you have passwords and immediately change them to something new. Don't change single characters, change it so the new one cannot be easily guessed. Then change your security questions so that it will be harder to fake out the web-site. Then consider purchasing a password logging application/tool. There are several available for smartphones that are safe and reliable. This will help you manage the scores of web-based accounts that have to be changed.

Then go deeper – if you think your social security number was compromised, you can advise the credit agencies of the risk, and credit lock your accounts. If it's severe, you can work with the government to get a new SS# issued. But beware, so much of our lives are tightly integrated with our SS#; all financial services, credit services, government issued ID, school records, utility company records, auto loans, mortgages, taxes, SSI benefits, etc. It is an enormous task to get every single entity changed over.

If your passport number or driver's license number has been compromised, immediately contact the government issuing authority and work with them to get the old number cancelled and flagged and have new credentials issued. Government agencies tend to be very supportive of that sort of proactive effort.

Ultimately, it is about being vigilant. Monitor your credit activity closely with alerts from banking and credit agencies. Be diligent in reviewing all banking and credit card activity for suspicious transactions and credit agency changes.

Knowledge and awareness are your best defense!
Please follow me on twitter: @stevewertheim