

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's New

Interested in a FREE Dark Web scan for your company? Contact us today! The FREE offer is good for the first 5 companies who contact us right away! Not one of the first 5 companies? No problem! You can get the Dark Web scan for your company for just \$29. Call the office right away at 701-364-2718 or email info@imsnetworking.com for more information!



Are Your Company's Digital Credentials For Sale On The 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.

Dark Web ID

How does Dark Web ID help protect

my organization?

The 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

June 2018



This monthly publication provided courtesy of Rick Johnston, President of Information Management Systems

"Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere"

Want to Lock-in your IT Costs for the Next **THREE** Years? Sign up for IMS Total Care Services **TODAY!**

threats that are specific to our client's environments. We monitor the Dark Web and the criminal hacker underground for exposure of our clients' credentials to malicious individuals.

Data source locations & descriptions: where do they find the 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

Dark Web Statistics:

- 80% of hacking-related breaches leveraged either stolen passwords and/or weak or guessable passwords
- 85% of all business with <100 employees have been hacked, and *most don't even know*
- 4.2 BILLION email account credentials and 85 MILLION stolen PII records (drivers license, SSN, DOB, etc.) for sale on the Dark Web
- Global costs of a data breaches will reach \$2.1 TRILLION by 2019
- 73.18% of US Population with at least 1 compromised credential found within the Dark Web: (237,736,346)
- 18.6% of US Population with a compromised social security number found within the Dark Web: (60,441,444)
- 76% of people will use the same password for most, if not all, websites

We can help! We now offer Dark Web ID—a threat monitoring tool that provides

24/7/365 monitoring for signs a company's exposed and compromised email credentials. The platform's engine scours millions of sources including:

- Botnets
- Criminal chat rooms
- Peer-to-peer networks
- Malicious websites and blogs
- Bulletin boards
- Illegal black market sites
- And other private public forums—all to ensure we know as soon as compromise occurs.

With Dark Web ID we can persistently shine a spotlight on the darkest corners of the Dark Web, and know when any email with your domain extension ends up with credentials available:

- Email address
- Password
- Date of birth
- Social security number
- Home address
- Drivers license number

Now we have the intelligence to take action, before compromise becomes a catastrophe. Interested in a FREE Dark Web scan for your company? Contact us today! The FREE offer is good for the first 5 companies who contact us right away! Not one of the first 5 companies? No problem! You can get the Dark Web scan for your company for just \$29. You can call the office at 701-364-2718 or email info@imsnetworking.com for more information.



Shiny New Gadget Of The Month:



Watch What You Eat With LinkSquare

Everywhere we go, most of us use vision to navigate our world. Whether our mouth begins to water at the sight of a tasty dish or our brow furrows at the sight of a shady-looking dollar bill, our eyes are one of our primary means of connection to the world around us. But, just by looking, can you tell whether that delicious-looking food is as high quality as it seems? Or be absolutely sure that the dollar is real?

Enter LinkSquare, the pocket-sized spectrometer that enables us to gaze deeper into the objects around us. After you scan an object with the device, it uses machine learning to analyze the properties of all sorts of items, including the freshness of food, the authenticity of money or gold, the identification of stray medications and a huge variety of other potential applications. If you're interested in purchasing this wildly futuristic technology, it'll cost about \$300. Learn more at LinkSquare.io.

Vega Stealer Malware Goes After Your Saved Credentials

There's a new security threat to be worried about, and security professionals are warning that it could be very bad indeed. The new malware is known as the "Vega Stealer," and is currently being used in a relatively simplistic phishing campaign designed to harvest financial data that has been saved in both Google Chrome and Firefox browsers. Unfortunately, based on an analysis of the code, it could be a much more serious threat.

Vega Stealer isn't 100 percent original work, but rather, is a variant of another nasty bit of malware known as "August Stealer." Built on the .NET framework, it's designed to ferret out and steal cryptocurrency wallets, passwords, cookies, saved credit cards, and more.

If your computer is infected, and you're using Firefox, Vega Stealer will specifically target the files "key3.db" and "key4.db," along with "cookies.sqlite" and "logins.json," which store a variety of keys and passwords.

In addition to that though, it can also take screen captures of your PC and scan for, and steal any file with the following extensions:

- .pdf
- .xlsx
- .xrft
- .docx
- .doc

Of course, it would be a trivial matter for the owners of the malware to expand this list even further.

As mentioned, the current campaign isn't terribly sophisticated, relying on emails bearing titles like "Online Store Developer Required." The emails being sent contain a poisoned file called "brief.doc" which contains macros designed to install the malware.

If the recipient clicks on the word doc, it will install a file named "ljoyoxu.pkzip" in that user's "Music" directory, and then automatically executes the file so it can begin harvesting.

Researchers from Proofpoint, who found the malware strain had this to say:

"The document macro utilized in this campaign is a commodity macro that we believe is for sale and used by multiple actors, including the threat actor spreading Emotet banking Trojan. However, the URL pattern from which the macro retrieves the payload are the same as those used by an actor we are tracking who distributes the Ursnif banking Trojan, which often downloads secondary payloads such as Nymaim, Gootkit, or IcedID. As a result, we attribute this campaign to the same actor with medium confidence."

Be on your guard.



For more information about this article, go here: <https://www.imsnetworking.com/2018/05/28/vega-stealer-malware-goes->

Bits & Bytes

■ **How To Quickly And Easily Make Your Business More Profitable**

Early in any small business, it's extremely difficult to turn a profit. Even after you gain a little traction, it's easy to get caught up in the never-ending details. This means you have no time left for the things that will actually increase your revenue. But there are a few things you can do right now to raise your bottom line.

Perhaps the most important action item on your list should be to calculate the exact costs of your business. In order to know where you're starting, you need to look beyond general expenses and pinpoint just how much your activities are worth to the company. Then you can start cutting out tasks that are measurably low in value, automating them wherever possible. If you can do that for both you and your team, you have a great place from which to start. *SmallBizTrends.com, March 26, 2018.*

■ **Top Ways To Stay Secure In The Social-Media World**

Social media allows millions of people to reconnect and stay up-to-date with family members, friends, acquaintances and even

former in-laws. But as social media reshapes the way we communicate with one another, it's important to keep a couple of things in mind to protect yourself and your data.

Remember that there's no "delete" button on the Internet. Even if something seems temporary, a simple screenshot or check through the archives can make it permanent. Even if you keep your social media completely private, relationships change, and what was private yesterday may suddenly become public record. The question you need to ask is whether you'll be comfortable in 10 years with what you're posting today.

In the same vein, if you post in online forums or on message boards, consider using a pseudonym. Never share names of real businesses, clients, friends or family. If a bank manager wouldn't allow a picture of all the money in the vault to be shared on the web, you shouldn't allow a picture containing confidential, financial, legal or other protected documents and items to be shared either. A good social-media policy in the office now can save headaches down the road.

■ **Apps That Make Our Lives Easier, All Under \$10**

With new apps flooding the market every day, it can be difficult to pick out the ones that will assist you instead of just inspiring buyer's remorse. But there are dozens of apps that, despite their miniscule price tag, can have a small but lasting impact on your day-to-day.

Take Dark Sky (\$4) for example. An up-to-the-minute accurate forecasting app that will break down weather information for exactly where you are at any given moment, down to when the expected rain or snowstorm will start and stop.

You can also check out Notability (\$9.99), which Business Insider calls "one of the best things to ever happen to note-taking." The app allows you to mark up PDFs and photos, take voice recordings, and a number of other functions, with everything stored in the cloud.

Those young people mentioned above who have trouble keeping more than one password might appreciate 1Password (Free), a dedicated place to guard all your passwords behind one difficult-to-hack password. *BusinessInsider.com 10/26/2017*