BSSi2

Innovations

Review Twice, Implement Once. Doing IT Right the First Time. • December 2017

Scott Bernstein, CPA
President

Nick Espinosa
CIO & Chief Security Fanatic

Are Your Digital Credentials for Sale on the Dark Web?

Digital credentials such as usernames and passwords connect you and your employees to critical business applications, as well as online services. Unfortunately, criminals know this — and that's why digital credentials are among the most valuable assets found on the Dark Web.

The Dark Web is made up of digital communities that sit on top of the Internet, and while there are legitimate purposes to the Dark Web, it is estimated that over 50% of all sites on the Dark Web are used for criminal activities, including the disclosure and sale of digital credentials. Far too often companies that have had their credentials compromised and sold on the Dark Web don't know it until they have been informed by law enforcement — but by then, it's too late.

BSSi2 Would Like to Announce a New Service: Dark Web Monitoring

Why It's Important

- Compromised credentials are used to conduct further criminal activity, such as data breaches of sensitive corporate information, as well as identity theft of individual employees.
- Users often have the same password for multiple services, such as network logon, social media, online stores and other services, exponentially increasing the potential damage from a single compromised username and password.
- Today, you have limited visibility into when your credentials are stolen; over 75% compromised credentials are reported to the victim organization by a third party, such as law enforcement.

Using a proprietary technology we vigilantly search the most secretive corners of the Internet to find compromised credentials associated with your company, contractors and other personnel, and notify you when these critical assets are compromised — before they can be used for identity theft, data breaches or other crimes.

The dark web is an ugly place. It's a tangle of hidden chat rooms, private websites, networks and technologies all driven by people seeking to steal your secrets. It's estimated that up to 80% of all hacks are credential based. So, if you are looking to protect your data and grow your business, we're a really good place to start.

We Go Into the Dark Web to Keep You Out of It

Our software monitors compromised credentials and alerts you of threats before they become risks. Our platform helps prevent data breaches, so you can focus on running your business. The dark web may be here to stay but we're making it brighter.

We Monitor

- Hidden Chat Rooms
- Private Websites
- Peer-to-peer networks
- IRC (internet replay chat) Channels
- Social Media Platforms
- Black Market Sites
- Over 640,000 Botnets

We Prevent

Attacks on networks may be inevitable, but they don't have to be destructive. Our proactive monitoring of stolen and compromised data alerts you when a threat is detected so you can respond immediately.

Start the new year off protected—contact us today for more information!

Cybercriminals Confess:

The Top 5 Tricks, Sneaky Schemes And Gimmicks They Use To Hack Your Computer Network

The contemporary world is rife with digital thieves. They're penetrating the complicated data structures of huge credit-monitoring companies like Equifax, scooping up the personal information of millions of people. They're releasing sensitive customer data to the public from discreet businesses like Ashley Madison. They're watching webcam feeds of our celebrities without them knowing; they're locking down the systems of public utilities like the German railway system; they're even managing to steal thousands of gigabytes of information directly from high-profile government entities like the CIA.

They're also targeting small businesses exactly like your own and extorting them for thousands and thousands of dollars.

When running a company, it's vital to have a dedicated security team, equipped with the most up-to-the-minute security technology, on your side to protect you from these malicious cyber threats. But it's not enough to leave it to somebody else. You also need to be informed. Here are five of the most common ways hackers infiltrate your network:

1) Phishing Scams

You receive an e-mail in your work inbox coming directly from a high-ranking employee with whom you've been working on a project. Inside is a link he needs you to click to access some "vital information," but when you click it, it rapidly installs a host of malware on the computer, spreads through the network and locks out everyone in the company.

Phishing scams are the oldest trick in a hacker's book – ever received one of those "Nigerian Prince" scams? – but they're still wildly successful. Not only that, but they're becoming increasingly more sophisticated. As Thomas Peters writes for "Newsweek," "The best messages look like they're trying to protect the company. One well-meaning system administrator even offered to post a PDF that could deliver malware on an internal server because it was called, 'How to avoid a phishing attack.'" How's that for irony?

2) Social Engineering

Social engineering is a type of "hacking" that uses real, well-intentioned people to carry out its schemes, rather than intricate lines of code.

This is especially effective for gathering sensitive information that can later be used in another type of attack – e-mail passwords used for phishing scams, for example. Maybe your IT guy receives a call from the "secretary" of one of your clients, pretending that they're experiencing problems with your service due to some firewall, a problem that your IT professional is more than happy to help out with. Before you know it, the caller knows the ins and outs of your entire security system, or lack thereof. Social engineers have been known to use phone company customer service departments, Facebook and other services to gather Social Security or credit card numbers, prepare for digital robbery and even change the passwords to your central data network security.

Continue on next page...

...continued from previous page

3) Password Hacking

You may think that your passwords are clever and complicated, filled with exclamation points and random numbers, but it's rarely enough. With information gathered carefully from social engineering or a simple check on your employees' social media accounts, hackers can easily use brute-force to figure out that your password is the name of the family dog, followed by your anniversary (for example). That's if they didn't already manage to steal your password through one of the techniques listed above.

4) Fault Injection

Sophisticated hackers can scan your businesses' network or software source code for weak points. Once they're located, they can surgically attempt to crash the system through snippets of code they splice in expressly for that purpose. Different commands can do different things, whether they want to deliver a devastating virus, redirect links on your website to malicious malware or steal and erase vast swathes of information.

5) USB-based Malware

At the last conference you attended, someone probably handed out free branded USB sticks to keep their business top-of-mind. Hackers will sometimes covertly slip a bunch of infected USB sticks into a company's stash. The instant somebody tries to use one, their computer is taken over by ransomware.

So What Can I Do About It?

It's a scary world out there, with virtually everyone left vulnerable to digital attack. Knowing the strategies hackers deploy is half the battle. But, frankly, these techniques are constantly changing; it's impossible to keep up by yourself.

That's why it's so important to utilize only the most up-to-date security solutions when protecting your business. Hackers move fast. You and your security technology need to stay one step ahead.

Survive the Holidays as a Small-Business Owner

Every small business owner knows how tricky the holidays can be. Either you can choose to shut down and risk losing your clients, or you miss out on a much-needed break and valuable time spent with your friends and family.

To survive, it's vital that you get more organized than ever before, scheduling everything from dinners with friends to shopping trips for gifts.

Program downtime directly into your schedule and communicate constantly with your clients. If they're aware of when you're available and not, they're less likely to abandon your service.

The Lighter Side….

What happens when kids' letters arrive at the North Pole? Does Kringle and Co. sell the data to online marketers? We read the fine print on Santa's website:

- Santa's Privacy Policy: At Santa's Workshop, your privacy is important to us. What follows is an explanation of how we collect and safeguard your personal information.
- Why Do We Need This Information? Santa Claus requires your information in order to compile his annual list of who is Naughty and who is Nice and to ensure accuracy when he checks it twice. Your information is also used in connection with delivering the kinds of goods and services you've come to expect from Santa, including but not limited to toys, games, good cheer, merriment, Christmas spirit, seasonal joy, and holly jollyness.
- What Information Do We Collect? We obtain information from the unsolicited letters sent to Santa by children all over the world listing specific items they would like to receive for Christmas. Often these letters convey additional information, such as which of their siblings are doodyheads. The letters also provide another important piece of information—fingerprints. We run these through databases maintained by the FBI, CIA, NSA, Interpol, MI6, and the Mossad. If we find a match, it goes straight on the Naughty List. We also harvest a saliva sample from the flap of the envelope in which the letter arrives in order to establish a baseline genetic identity for each correspondent. This is used to determine if there might be an inherent predisposition for naughtiness.
- What Do We Do with the Information We Collect? Sharing is one of the joys of Christmas. For this reason, we share your personal information with unaffiliated third parties: the Easter Bunny, the Tooth Fairy, and Hanukkah Harry.

—Laurence Hughes, from McSweeney's Internet Tendency

December 2017

35 Aztec Court
South Barrington,
IL 60010

(312) 752-4679

www.bssi2.com

Shiny New Gadget of the Month

E-mail Signature Rescue

The business world runs on e-mail. According to LifeWire, around 269 billion e-mails are sent around the world each and every day. But for every e-mail sent, millions go unread, and those that do are often found wanting. How, in the midst of all that noise, can you possibly get your own work e-mails to stand out?

Enter E-mail Signature Rescue (emailsignaturerescue.com), a business dedicated to creating custom, professional e-mail signature templates for all kinds of companies and teams. Using their proprietary software, it's easy to build a robust and beautiful HTML e-mail signature template that will make your e-mails pop. Signatures may seem small, but they can go a long way toward convincing a recipient that you mean business.

BSSI2 is Hiring!

BSSi2 is looking for another technician!

This person needs to be proficient with Windows and preferably have a passion for security. And above all else, they must have a demeanor and work ethic that would make them someone you would want servicing your IT needs — someone who embodies our core values. If you know of a candidate send them our way!

Honesty, Integrity, and Respect Above All Else

Honesty, Integrity, and Respect are traits we live and breathe at BSSi2. These values form the foundation on which we perform work, treat others, and conduct ourselves. Without these, trust is lost.

Removing Obstacles

Obstacles slow down progress and efficiency—we do our best to remove them from yours and our daily work. BSSi2 is constantly looking at new ways, as well as reviewing time-tested processes, to make everyday tasks easier for everyone.

Continuously Improving

Technology is one of the fastest growing and changing industries, with new or improved inventions emerging daily. We strive to stay on top of ever changing technology by keeping tabs on industry leaders, testing new products and training. We do this so that you don't have to. Our aim is to continuously improve your customer service experience, not just the technology we implement and support.

Positive, Profitable Environment

We believe that a positive atmosphere will lead to a profitable future, not just for BSSi2 but for our customers and employee as well. We cannot succeed without you, so we'll work hard to make your business grow and profit.

No Assholes Allowed

Have you encountered an arrogant, rude, or obnoxious IT person who makes you dread every interaction? You won't at BSSi2. We don't hire assholes, so you don't have to deal with one. We want our customers to enjoy every interaction with our employees. And truthfully, we want to enjoy working with our fellow coworkers too.

(847) 551-4626 | sbernstein@bssi2.com