Is My Identity on the Dark Web?

Deep within the internet is a secretive place where criminals buy and sell your private data

by Doug Shadel with Neil Wertheimer , AARP Bulletin, September 2018 | Comments: 30

GREG REID, PROP STYLIST: BRIAN BYRNE/AARP

BRETT JOHNSON IS AN IMPOSING and charismatic ex-con whom the U.S. Secret Service once dubbed the “Original Internet Godfather.” His criminal masterstroke? Creating “Shadowcrew,” one of the first online forums where bad guys could safely buy guns, stolen credit cards, Social Security numbers and every drug imaginable. But Shadowcrew was shut down by federal agents in 2004, and for the next decade Brett was in and out of prison. At one point he went on a four-month run from the law, funded by roughly $500,000 he stole from ATMs. That landed him on the Secret Service’s “Most Wanted” list.

He’s the good guy of our story.

As is Blue London. Wiry, in his early 20s, with hair to his waist and an attitude to match, Blue recently pleaded guilty to crimes related to his role as a hacker for some of the biggest illegal sites on the internet. It was his first job and, with a looming prison sentence, it may be his last for a while. To protect him from reprisals, we agreed not to use his real name; he asked that we use “Blue London.”

Brett and Blue have seen the light. Today, both are willing to share in detail how the internet gets used by criminals to steal money from you. Brett, because it's his new job: He is now a consultant who helps law enforcement catch cybercriminals. Blue, because he wants to reduce his prison sentence.

Their coming forward is timely. Massive data breaches get big headlines, but many more occur with little fanfare. In 2017, there were 829 data breaches in the United States, exposing over 2 billion individual records, says Paul Stephens of the Privacy Rights Clearinghouse. Identity fraud — defined as using personal identifying information to steal money from victims — is at an all-time high, with 16.7 million Americans losing nearly $17 billion in 2017, according to Javelin Strategy & Research. Brett and Blue know why these numbers keep growing because they contributed to it. And truth is, it was pretty easy.

The two recently gave me a tutorial on how criminals go about stealing people's identities and turning that data into money. The class took place mostly in the "dark web," a secretive place on the internet where crooks and scammers buy and sell their wares under the protective blanket of anonymity. Here's what I discovered.

A Descent Into the Dark Web

Think of the internet as an ocean. At the top is the "surface web" and its familiar occupants like Google, CNN, Amazon, Yahoo and thousands of other public websites. The surface web is where the vast majority of people spend their internet time. All is public, all is searchable, and all is (mostly) friendly.

Go a little deeper, where the sunlight begins to fade away, and there is the "deep web." It is much larger than the surface web but can only be accessed by individuals who have logins for the databases and websites here. Most of the activity is perfectly legal; it's just not as easy for everyday folk like us to see. Some of the biggest sites here include the databases for NASA, the U.S. National Oceanic and Atmospheric Administration, the U.S. Patent Office and private databases like LexisNexis and Westlaw. Traditional search engines can't find these pages because they aren't indexed like pages on the surface web; you need to know your destination and have an authorized password to get in.

Descend even further, to where there is no light and far fewer denizens, and there is the dark web (also called the "darknet"), a part of the deep web that is accessible only to those who use software called TOR, which stands for The Onion Router. Ironically, TOR software was developed by the U.S. Navy in the 1990s as a way to allow intelligence agents operating overseas to communicate anonymously with their colleagues here in the U.S. It was released as free, open software to the public in 2003, though government dollars continued to support its upkeep and growth.

The Onion Router got its name because all transmissions through it are anonymous: Messages are sent to multiple servers around the world to disguise the sender — kind of like layers of an onion. Search for information using TOR, and it takes several seconds to load, because your request travels tens of thousands of miles between all those servers before coming back to you. It's perfect for preserving anonymity for political dissidents, journalists, spies and — as it turns out — criminals. TOR is free and available to anyone who wishes to download the appropriate software onto his or her computer.

Criminals have flocked to the dark web because it allows the buying and selling of illicit goods with total anonymity. The TOR browser hides users' IP addresses, and transactions are usually conducted in a cryptocurrency like bitcoin to make them untraceable.

How big is the dark web? No one knows exactly. But consider AlphaBay, a site on the dark web that was taken down in July 2017 by the FBI. At its peak, AlphaBay had over 200,000 users and was taking in between $600,000 and $800,000 a day. The site's founder, Alexandre Cazes, was arrested; eight days later he was found dead in his jail cell from an apparent suicide.

While most of the illegal traffic on AlphaBay was drug related, there was also a huge volume of so-called digital goods sold. The FBI estimated that when AlphaBay was busted, it had listings for 4,488 stolen personal IDs, 28,800 stolen credit card numbers and 3,586 hacking tools. Attorney General Jeff Sessions called the bust "the largest darknet marketplace takedown in history."

A Rich Marketplace

But there are plenty of other inhabitants of the dark web eager to fill the space that AlphaBay vacated. Brett and Blue showed me several dark web sites that were selling a range of stolen digital goods: high-end credit card numbers, logins and passwords, individual credit reports and what is known as a "fullz" — a complete package of everything needed to commit identity theft: Social Security number, date of birth, mother's maiden name, address, phone numbers, driver's license number and more.

Blue told me that on the dark web sites he worked for, fullz were by far the most viewed and purchased items among the digital goods for sale. A fullz can sell for $20 to $130 depending on the victim's age and credit score, as well as the breadth of information provided. The fullz profiles most in demand, our experts said, belong to older people.

Data also gets sold piecemeal. Brett asked me my wife's name and, within a few moments, found her Social Security number, available for all of $2.99. The website he found it on claimed to have over 170 million Social Security numbers and dates of birth for sale.

Surprised? Don't be. A recent study found that Social Security numbers comprised 35 percent of data breaches in 2017, surpassing credit cards (30 percent) as the top personal information compromised.

Much of that data goes up for sale shortly after it has been stolen. Lillian Ablon is an information scientist for the Rand Corp. who recently testified before Congress about the monetization of stolen personal information. She described four kinds of internet bad guys: state-sponsored hackers who steal data or attack computer systems for political reasons; "hacktivists" who often do it just for fun, to prove themselves or to forward a personal agenda; cyberterrorists seeking to create fear and chaos; and cybercriminals like Brett and Blue who do it for the money.

Of these, cybercriminals are the most likely to dump their stolen information on the dark web. As Ablon told the U.S. House Subcommittee on Terrorism and Illicit Finance earlier this year, "Immediately after a large breach, batches of credit cards get released in the cybercrime black markets." When thousands of credit card numbers or logins and ID numbers flood the market, the bloated supply drives down prices, allowing criminals to purchase our information more cheaply.

Blue observed this phenomenon firsthand. “I actually felt sorry for some scammers who had invested a lot in stolen information, only to have a huge data breach flood the market and deflate prices,” he told me. Ablon noted that savvy crooks have learned to release stolen data in batches to avoid forcing prices too low.

Brett could not show me what digital goods look like on the dark web because that would require breaking the law. But he did show me a site where one hacker was quitting the business. Like a drug dealer who quits and gives his remaining stash to a couple of lucky neighborhood teenagers, this individual had freely posted 47 fullz profiles on a dark web site Brett was investigating. The ages of these identity fraud targets ranged from a 36-year-old from Sitka, Alaska, to an 85-year-old retired engineer from Arizona. The average age was 52. Each profile had at least eight separate pieces of information, among them: address, email address, home and work phone numbers, date of birth, Social Security number, mother’s maiden name, credit card numbers, bank account numbers, even their computer’s IP address — all for anyone to see and use however they chose.

A Perennial Victim

I decided to try to contact some of these 47 people to warn them that their personal information had been posted online and to find out if any of them had ever been victimized by identity fraud. After getting several disconnected numbers, I reached Joan Adams, a 51-year-old Army veteran living in the Southwest. When I told Joan (not her real name, to protect her from further scams) what a crook had posted on the internet, there was a long pause, then a deep sigh. “I’m not surprised,” she replied.

It turns out that Joan has been a victim of identity theft on and off for 17 years. “It started in 2000 right after I got out of the military,” she began. “I was just raising my kids, working hard, paying my bills and thought everything was fine. Then I started getting these delinquency notices saying I was past due on accounts I never knew I had.” Someone had stolen her identity and opened multiple accounts in her name.

So Joan, a mortgage underwriter and no stranger to paperwork, took action. She froze her credit and placed alerts on all her bank and credit card accounts. This shut down the criminal activity. Or so she thought. After several years without credit problems, she let down her guard and removed the credit freeze on her account. Sure enough, it happened again. More bogus accounts, multiple hits on her credit file and endless collection agency calls about debts she had not incurred. So once again, she froze her credit, put alerts on all her accounts and signed up for an ID theft monitoring service. And it’s a good thing she did. “I’m not kidding, I was getting eight to 10 alerts a day saying people were trying to use my Social Security number to open new accounts. It was very stressful.”

Eventually, Joan received a letter from the U.S. Department of Justice telling her they had just arrested a notorious identity thief and that her name was among those of his victims. In fact, the Justice Department told Joan her information had been bought and sold so many times that she needed to change her Social Security number — which she did.

As it turns out, most of the information on Joan’s fullz that got posted by the retiring hacker was outdated. But even knowing that, she is taking active steps to protect herself. Like most of us, Joan will have to watch her digital identity like a hawk from now on.

Illegal data merchants use many of the same marketing and customer-service tools that legitimate sites use on the surface web; it’s a sales business, after all, even if the product is illegal. One example: Dark web site sellers encourage customer feedback ratings so that prospective buyers can evaluate the criminal's reputation for delivering the illegal stolen identities as described. Brett showed me the web page of a scammer named "Hackyboy" who had a customer rating of 299 positive reviews and 18 complaints — pretty good. This essentially means that 299 of his customers have reported that he delivered precisely the stolen credit information he said he would deliver. This same scammer said he had 1,500 positive reviews across about eight different dark web sites.

Blue also described listings for what are known as "calling services." These are offered to fraudsters who are in the process of taking over someone's financial accounts. A calling service will contact the target victim's banks, credit card companies or identity-theft monitoring companies pretending to be the person and arranging to have their email and phone number changed. If these companies later suspect inappropriate activity, their calls and emails to the person will then go to the calling center, which will cover for the crook. Calling centers are often located in an overseas country. (Many scammers, it turns out, are uncomfortable making or taking such calls because of the risks; it's safer to have out-of-country professionals do it for you.) Once the victim's contact info is changed, the scammer can open new accounts, max out old accounts, even take out new loans in the victim's name without the victim ever knowing.

After many hours with Brett and Blue, I came to realize that while the dark web has its legal usages, it also contains a massive collection of auction sites for criminals, fueled by data breaches that pump millions of new records of personal information into this underground market each year. Which may be why Alexandre Cazes, the founder of AlphaBay, had said his goal was to make it "the largest eBay-style underworld marketplace."

Don't Fall for a Dark Web Protection Scam

You're probably seen or heard the ads by now: "Good guy" businesses offering to "scan the dark web" for your name and data to make sure you're not vulnerable to identity theft. Use if you wish, but know that the majority of personal data on the dark web is hidden behind paywalls in carefully guarded websites run by savvy criminals. General scans may catch the occasional situation in which personal information is posted, but they won't tell you if your information is behind a paywall that only a crook with the URL can access.

I next asked Brett and Blue how they would use this vast supply of stolen information to make money. They agreed the starting point was identifying a good victim, and that usually begins with their age.

"Seniors are prime targets because they are more likely to have money and better credit," Brett said. Blue agreed: "The stolen profiles of seniors are the easiest to acquire and are the least likely to become compromised, because most seniors don't check their accounts."

A new AARP survey confirms that last point: Only 1 in 3 individuals over 65 have online access to all of their bank accounts for monitoring purposes, greatly reducing their ability to check for illegal activity.

Once a target is identified, the next step is to build out a complete profile. Let's say the scammer starts with a basic profile that includes name, address, Social Security number and date of birth, which he bought on the dark web. From there, he would go to one of the many background-check websites on the surface web and find out as much as he can about the person.

Think of these background sites as Googling yourself on steroids. I paid a small fee, submitted my name and received a 92-page report containing all of my current and previous addresses, phone numbers, social media sites and email addresses. The site also provided descriptions of my family members and neighbors and details about property past and present that I have owned — including mortgage documents and amounts. It's all legal; the information is pulled from public documents. Nonetheless, seeing my history for sale to any stranger who wants it was a chilling experience.

Brett would also study the personal info that you put on social media sites like Facebook or LinkedIn. If you haven't altered the privacy settings to restrict who can see such information, guys like Brett and Blue can easily harvest your data for criminal purposes. Yet the AARP survey found that only 39 percent of people over 65 had ever changed the privacy settings on their Facebook accounts.

You might wonder why scammers need so much personal information about us to commit fraud. Brett points out that a primary defense employed by the credit bureaus and others to protect our credit files is something called "knowledge-based authentication" (KBA) questions. These are questions that supposedly only you know, like your mother's maiden name or the name of your high school mascot. While KBAs create a roadblock for many scammers, enterprising cybercriminals who know how to successfully mine the data-rich environment on the surface and dark web can often come up with the answers.

Armed with all this data and personal history, the assault starts. People like Brett and Blue can infiltrate the victims' credit bureau files; change their contact phone numbers and emails; take over their bank or investment accounts; create new credit card accounts; and even take out personal loans. Depending on how much the victim has done to defend against such attacks, he or she may not even know the assault is happening until months later, when the damage is done and the scammer long gone.

A Reality Check

Believe it or not, there can be a happy ending to this story. Despite the undeniable reality that there are more data breaches — and more fraud victims — than ever before, the fact remains that in 2017, only 6.6 percent of the adult population of the U.S. was victimized by identity fraud. That means that 93.4 percent of us were not victimized. And there are things each of us can do to greatly reduce the chances of victimization.

First, take the attitude that we are all in a post-prevention world. Simply assume all of your information is already out there on the internet in some form. We can sit around worrying about this, or we can take action to make it harder for criminals to exploit our data for material gain. As it turns out, there are powerful things you can do to make sure that stolen data can't be used to defraud you.

Cybersecurity experts and former hackers agree on the three steps you should take to stay safe: freeze your credit, closely monitor all accounts, and use a password manager. I fully subscribe to this advice and have taken all of these steps. But don't take my word for it. Joan Adams, the former ID theft victim, is also a big believer. "I have tried it both ways. When I didn't freeze my credit and monitor my accounts, ID thieves attacked me and my family relentlessly. Once I took these steps and got ID theft monitoring, the victimization stopped. It's as simple as that."

Law enforcement is doing more to stop this type of criminal activity, said Lillian Ablon of the Rand Corp. But they have a daunting challenge. "The cops work 9 to 5; cybercriminals work 24/7 to steal information," she said. "It's a cat-and-mouse game. As soon as law enforcement has figured out one little trick, the cybercriminals then switch tactics."

But we also know that cybercriminals follow the path of least resistance. So if we put up any resistance at all, the Brett Johnsons and Blue Londons of the world will likely avoid us like the plague.

“Even though personal information is everywhere, if you just do one or two things to create roadblocks for the scammers, people like me will probably move on,” said Brett. “There are plenty of other marks out there who do nothing.”

Protect Your Identity With These Actions Steps

Freeze your credit

“The number one piece of advice is to place a security freeze on all your accounts with the three major credit reporting agencies,” says Paul Stephens of the Privacy Rights Clearinghouse. The reason: It is the best way to stop ID thieves from opening new accounts in your name. Yet an AARP study found that just 14 percent of adults have ever done this.

Monitor your accounts

Register for online access to every financial account you have (bank accounts, credit cards, 401(k)s and so on). Then check each one weekly. Also consider setting up alerts on your major accounts so that any time there is activity, you are sent a text message. Most companies will do this for free and allow you to set a dollar threshold.

Use a password manager

These digital services store all your passwords in a secure online vault, so you'll never lose a password again. The software generates complex, hard-to-hack passwords for each of your accounts; and often will notify you of data breaches at companies you have accounts with. That allows you to quickly change the password for that account, protecting your information.