



The Underground Economy of Data Breaches

The Underground Economy of Data Breaches

While the vast majority of business owners think of a data breach as a single event, the truth is that a breach never just stops there.

Additionally, a data breach is more than just a virus or malware that impacts your networks performance or taps into your outdated desktop files.

In reality, data breaches can result in hackers gaining access to much more serious assets, including bank accounts, credit cards and even your identity. To illustrate the point further, take a breach in a database that stores electronic health records (EHRs). These could contain obviously sensitive data such as date of birth, social security number and maiden name. While valuable enough on its own, this information may also be used to access sites that are under stricter protection. For example, If your banking site security question asks the name of the first bone you broke, a hacker who already had your login and password information could then complete the process of unauthorized access by filling in the blank with information stolen from your EHR.

In addition to stealing data directly, an entire underground economy has built up around data breaches. Hackers steal and then resell sensitive information, creating an online black market where information is the currency of choice.

This online criminal economy has proven difficult to shut down, for a number of reasons:

- Since it's virtual, there aren't any headquarters or definitive leaders that can be directly targeted by law enforcement.
- The online nature of this underground element means hackers are incredibly adaptable and versatile, using a number of sophisticated maneuvering tactics to avoid tracking.

- The income potential keeps the underground economy thriving, and that's not likely to change anytime soon.

At the same time, there have been some notable successes in this battle as well:

- The arrest of Aleksandr Andreevich Panin, who developed and distributed SpyEye malware, a virus that ultimately infected over 1.4 million computers in the U.S. alone.
- The shut-down of the Citadel botnets, a network responsible for distributing Citadel malware, as Microsoft's Digital Crimes Unit worked in partnership with the FBI in one of the most aggressive anti-cybercrime operations to date.

Perhaps most importantly, the continued development of increasingly sophisticated software and a renewed focus on securing data, particularly with regards to health records, is creating a more hostile environment for hackers to gain any footing in the first place.

The History of the Underground Economy

So how did something as evolved and insidious as black-market data trading ever take root? Not surprisingly, the exact origins of the "botnet" are tricky to pin down. While viruses, malware and hackers have developed in direct correlation with technological advances, it was around the turn of the Millennium when cybercrime seemed to take on a more organized approach.

- Sub7 and Pretty Park utilized Internet relay chat (IRC) channels to troll for malicious commands, launching a new standard for creativity among hackers.

These days, social media networks like Twitter and Facebook serve as surrogate platforms from which hackers can command and control infrastructure.

- By 2002, open-source malware with high levels of functionality, like Agobot, began to emerge, along with the concept of staged attacks: the first breach installs a backdoor vulnerability, then the next attack leverages this access into disabling any antivirus and blocking access to security updates.
- Key logging and data mining were the next evolution of malware, along with a new bot family that used encryption algorithms and compression to avoid detection.

At around the same time, hackers realized that P2P networks presented a huge potential for decentralizing operations, removing the vulnerabilities of IRC command and control centers, not to mention opening up all the new possibilities inherent in Web 2.0.

These days, social media networks like Twitter and Facebook serve as surrogate platforms from which hackers can command and control infrastructure. Additionally, the per-card fees that once commanded a hefty payoff for cybercriminals have been dwarfed by the benefits of harvesting and reselling data instead—not necessarily account data, but personal data such as social security numbers and birthdays. Even access to social media accounts themselves has become a hot commodity.

Evolving Adaptations

In short, the underground economy has evolved to meet the needs of a shifting criminal market while at the same time manipulating the ever-changing vulnerabilities that are made possible through new tech, the most recent apps and other innovations in software development. Through all of this, cybercriminals have only become more organized and smarter about evading detection. This can be done by stacking proxies, routing commands through social media and other obfuscating platforms and never sticking with one strategy for very long.

There have been a number of highly publicized data breaches, the most recent of which was that sustained by Target right at the peak of the holiday shopping season in 2013. This example only serves as a reminder that even the most trusted merchants may themselves fall victim to the unpleasant realities of these virtual threats.

What does the future hold for cybercrime? The rise and fall of Bitcoin shows just how popular the concept of anonymous currency can be, and cybercriminals will only continue to zero in on the perceived potential that new technological advances present.

Of course, law enforcement—both domestic and overseas—continues working diligently to stave off these attacks, pinpoint their origins and educate enterprises as well as individuals on the best steps to take to protect their data. Microsoft's Digital Crimes Unit mentioned above is only one example of the proactive strategy that forward-thinking companies are adopting, and the vast majority of techs and start-ups are following suit.



Reselling to the Highest Bidder

It wasn't that long ago that "hacking" meant stealing a credit card number or finding a way into a bank account. However, with so many online financial services operating under heavy encryption, cybercriminals have realized that the true value lies not in breaking in, but in figuring out a way to unlock the deadbolt instead. This mindset has led to the stealing and reselling of information instead of just account data.

Many of the sites used for these transactions are actually open to the public, confirming once again that it's far easier to tap into the criminal element than many of us realize. After an initial vetting, members of these forum boards and websites can bid on their chosen item, just like a virtual, criminal auction house.

Stolen data is incredibly valuable, especially as financial institutions and even simple ecommerce sites ramp up their online security measures. Account numbers can be resold directly, while credentials mined from other data can then be leveraged against those accounts or others for unfettered access.

For example, a hacker armed with basic information such as your full name, date and place of birth, social security number and name of your spouse can then more easily infer your password to certain websites: a combination of birthday, last name and anniversary, perhaps? Or the birthdates of your children? What hackers lack in firsthand knowledge, they can make up for with skills and perseverance... and buying your data helps them connect all the dots. In many cases, this information can sell for even more than actual account numbers.

While law enforcement efforts are encouraging, the end user is ultimately responsible for his or her own account protection.

Tips for Protection

While law enforcement efforts are encouraging, the end user is ultimately responsible for his or her own account protection. There are a number of tips for online and/or account safety that are strongly recommended on a personal level:

- Always use smart password practices
 - Never share passwords and usernames across multiple sites
 - Combine lowercase and uppercase letters, along with numbers and special characters
 - Don't use personal data (birthday, anniversary, etc.) as part of your password




- Consider two-step password verification, in which the user must enter a key from a secondary device, such as a smartphone, to gain account access.
- Regularly monitor all your accounts in order to catch any usage anomalies early, like unauthorized charges or access from an unrecognized device.
- Practice safe email and browsing habits
 - Don't open emails or download email attachments from unknown senders.
 - Avoid sites with expired security certificates
 - Only make online purchases from trusted vendors using encrypted payment processing

At the enterprise level, a few more steps should be included:

- Update your company's policies regularly. For example, what sites can be accessed from work computers? Who has access to sensitive data? Are access logs in place?

- Perform regular risk analyses so any potential vulnerability can be identified and mitigated.
- Implement a remediation plan by looking for an outside data breach solution.
 - Incorporate a continuous monitoring system that tracks Protected Health Information (PHI)
 - Identify events such as loss of records
 - Maintain compliance with HIPAA, HITECH and the 2013 Final Omnibus Rule

By taking steps at the personal and enterprise level to protect yourself and your business, and calling on outside expertise as needed for a higher level of defense, you can minimize the chances that any of your data can be accessed, purchased or resold in the underground cybercriminal market.



If you would like to learn more about
how iBridge can help you with
your data security,
please contact us.

info@ibridgellc.com
503.906.3930

Follow us!

