InformationAge
Insights and analysis for IT leaders
Posted by Ben Rossi on 8 July 2015

The ripple effect of identity theft: what happens to my data once it's stolen?

What do hackers do with the data they have stolen? And more importantly, how can organisations prevent it from happening in the first place?

As a society, we hear about data breaches all the time, but we rarely hear about what happens to the stolen data afterwards.

We may not think much of losing one username and password combo or having to cancel a credit card, but each piece of data doesn't just disappear. It gets collected and combined into the tool of choice for today's fraudsters – one that's so difficult to overcome that organisations have had to rebuild how they do internet security.


'Data thieves sell this information to aggregators, who cross-reference and compile full identities - called "fullz" on the data black market'

Data privacy is dead

Since 2005, more than 675 million data records have been involved in data breaches in the U.S. alone, according to the Identity Theft Resource Center. These records include incredibly personal data such as a person's Social Security number, name, address, phone number, credit card number, name of local bank branch and so on.

Data thieves sell this information to aggregators, who cross-reference and compile full identities – called "fullz" on the data black market. This increases the value and usefulness of the stolen data, which may have been gathered from multiple data breaches.

With this level of information, fraudsters can create new bank accounts or take out loans under an actual person's name. These actions cannot be traced back to the fraudster and can cause problems for the fraud victim for years down the road.

In a recent New York Times article, a reporter details how a recent healthcare data breach exposed his child to identity theft that could hinder her for the rest of her life, because her Social Security number was stolen.

Bad news travels fast

A recent report found that it took just 12 days for the account information of 1,500 "employees" to travel from California to 22 countries and five continents. In the first few days, the information was viewed over 200 times and in 12 days over 1,000 times.

Fortunately, in this case, these accounts were fake – created and then intentionally leaked in order to determine the speed at which compromised data travels. This is especially disturbing when you consider it takes an average of 205 days for most corporations to detect a breach has taken place.

The experiment didn't just show how quickly stolen information gets circulated. It determined that the false information was being tested for validity too. Had the fake data actually been real accounts, fraud attempts would already be underway.

It's the ripple effect. Small data breaches look on the surface to be minor losses of data but they expand out across the digital waters faster than ever before, converging into a wave of personal information so detailed that undoing the damage is next to impossible.

Rise of the account takeover

What can you do with all of that stolen information? Depends on how much of it is amassed. There is a hierarchy of value on the dark web for stolen data. Stolen credit cards can cost mere cents and are labour-intensive and low return for fraudsters.

It takes many attempts for a fraud scheme to work as cards are tested and cycled through. With so many data breaches last year, credit card numbers flooded the black market, lowering their value.

Fullz sell for $5 a piece, but require a more in-depth and risky scam to be fully utilised. Working user accounts with a payment method attached, an easy-grab scam with lucrative results, go for a mere $27 each and can translate into hundreds to thousands of dollars in stolen money and merchandise.

As a result, account takeover is growing quickly in the fraud world. NuData Security monitors more than 18 billion user interactions across the Internet annually and has seen 112% year-over-year increases in account takeover (ATO) attacks.

In ATOs, fraudsters attempt to hijack valid user accounts instead of creating new accounts with stolen credit cards. ATOs can be automated, including scripted attacks, or can be done with small teams of human operators posing as account holders.

Helping out the scammers are middlemen who play a key role in testing the login credentials before they are used again to commit actual fraud.

Based on behavioural analysis, there are on average three high-risk logins for every high-risk checkout. The first login is to verify if the account works. The second time is to gain intelligence, and the third time is when the fraudster attempts to commit actual fraud.

The transaction is no longer the point of focus for fraud – it is the login. This shift creates an imperative to look at the login and account creation – rather than the transaction – in order to stop fraud before it happens.

In a sea of available data, account takeover pirates have their pick of digital credentials. Organisations must not only secure their own data but also be ever vigilant against people using stolen data on their websites as well.

By protecting the login pages of their websites, organisations cut fraudsters off at the source. They stop them from being able to take control of the account in the first place.

How can companies protect login pages from data thieves? Most merchants look for a username and password match. Some use device ID or check for password resets. But the newer, more sophisticated criminals are skilled at bypassing these mechanisms.

Full packages of user information – full identities – are prevalent and cheap. If an organisation is not confident it can separate account testers and fraudsters from legitimate users, the real question it needs to ask is, "Do I understand my user in enough detail?"

Rather than a simple checklist, behavioural analytics focuses on observed characteristics of who the user is, not just who they tell you they are. User behaviour analytics are aimed at observing and understanding how the user behaves, in an effort to answer bigger questions. Observing user behaviour in detail enables the best chance of beating fraud.

Fraud detection

A recent research note from Gartner indicates that perimeter-focused security isn't keeping malicious actors out when it comes to enterprise security controls.

Merchants are beginning to realise they can no longer rely on basic data validation measures anymore, because when it comes to account takeover, all of the data may be compromised and will be correct regardless of who logs in – legitimate user or imposter.

Instead, the key is to look at the behaviour at login and connect it to checkout. Behavioural analytics digs under the surface of matching usernames and passwords to truly understand user behaviour.

These behaviour patterns reveal details that fraudsters can't hide despite their best efforts. As ATO schemes gain prominence, fraud detection and prevention efforts need to be focused on behaviour.

Sourced from Ryan Wilk, ***NuData Security***