TechXplore

Buying and selling hacked passwords—how does it work?

June 22 2016, by Thomas Holt, Michigan State University

Credit: AI-generated image (disclaimer)

Data breaches are a regular part of the cyberthreat landscape. They generate a great deal of media attention, both because the quantity of information stolen is often large, and because so much of it is data people would prefer remained private. Dozens of high-profile breaches over the last few years have targeted national retailers, health care providers and even databases of the federal government, getting Social Security numbers, fingerprints and even background-check results. Though breaches affecting consumer data have become commonplace, there are other resources that, when targeted, lead to major security concerns. Recently, a hacker claimed to be selling over 32 million Twitter usernames and passwords on an underground marketplace.

But what happens after a breach? What does an attacker do with the information collected? And who wants it, anyway? My research, and various studies from other computer and social scientists, demonstrates that stolen data is usually sold by hackers to others in underground markets online. Sellers typically use their technical prowess to collect desirable information, or work on behalf of hackers as a front man to offer information. Buyers want to use stolen information to its maximum financial advantage, including buying goods with stolen credit card numbers or engaging in money transfers to directly acquire cash. In the case of social media account data, buyers could hold people's internet accounts for ransom, use the data to craft more targeted attacks on victims, or as fake followers that pad legitimate accounts' reputations.

Because of the clandestine nature of the online black market, the total number of completed sales of stolen information is hard to quantify. Most sellers advertise their data and services in web forums that operate like any other online retailer like Amazon, where buyers and sellers rate each other and the quality of their products – personal information – being sold. Recently, my colleagues and I estimated the income of data buyers and sellers using online feedback posted after sales were completed. We examined feedback on transactions involving credit and debit card information, some of which also included the three-digit Card Verification Value on the back of a physical card.

We found that data sellers in 320 transactions may have earned between US$1 million and $2 million. Similarly, buyers in 141 of these transactions earned an estimated $1.7 million and $3.4 million through the use of the information they purchased. These massive profits are likely a key reason these data breaches continue. There is a clear demand for personal information that can be used to facilitate cybercrime, and a robust supply of sources.

Getting to the market

Clandestine data markets are, it turns out, very similar to legal online markets like eBay and Amazon, and shopping sites run by legitimate retail companies. They differ in the ways the markets are advertised or hidden from the general public, the technical proficiency of the operators, and the ways that payments are sent and received.

Most of these markets operate on the so-called "open" web, on sites accessible like most websites, with conventional web browser software like Chrome or Firefox. They sell sell credit and debit card account numbers, as well as other forms of data including medical information.

A small but emerging number of markets operate on another portion of the internet called the "dark web." These sites are only accessible by using specialized encryption software and browser protocols that hide the location of users who participate in these sites, such as the free Tor service. It is unclear how many of these dark markets exist, though it is possible Tor-based services will become more common as other underground markets use this platform.

Connecting buyers and sellers

Data sellers post information about what type of data they have, how much of it, pricing, the best way for a prospective buyer to contact them and their preferred method of payment. Sellers accept online payments through various electronic mechanisms, including Web Money, Yandex and Bitcoin. Some sellers even accept real-world payments via Western Union and MoneyGram, but they often charge additional fees to cover the costs of using intermediaries to transfer and receive hard currency internationally.

Most negotiations for data take place via either online chat or an email account designated by the seller. Once buyer and seller agree on a deal, the buyer pays the seller up front and must then await delivery of product. It takes between a few hours to a few days for a seller to release the data sold.

Reviewing the transaction

If a buyer makes a deal but the seller never sends the data, or what arrives includes inactive or inaccurate information, the buyer will not sue for breach of contract or call the FBI to complain he got ripped off. The illegal nature of the transaction renders the buyer largely powerless to use traditional means of dispute resolution.

To rebalance this power, social forces come into play, maximizing rewards for both buyers and sellers and minimizing the risk of loss. As in systems from eBay to Lyft, buyers and sellers in many underground markets can publicly review each other's adherence to a negotiated deal. The parties operate anonymously, but have usernames that stay the same from transaction to transaction, building up their reputations in the marketplace over time. Posting reviews and feedback about purchase and sale experiences promotes trust and makes the marketplace more transparent. Feedback shows all users who operates according to community norms, whose behavior is worrisome, and which new users might not yet know all the rules.

This ability to post and review feedback presents an interesting avenue for market disruption. If all sellers within a market were to be flooded with negative and positive feedback, buyers would have trouble figuring out who is trustworthy. Some computer scientists have suggested that approach could disrupt the data market without the need for arrests and traditional law enforcement methods. More research into how to curtail the market for stolen data could investigate this and other potential strategies.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation

Citation: Buying and selling hacked passwords—how does it work? (2016, June 22) retrieved 26 April 2024 from https://techxplore.com/news/2016-06-hacked-passwordshow.html