2ND QUARTER NEWSLETTER 2018

PCS TechNEWS

Happy Summer!

Pittsburgh Computer Solutions 451 Valleybrook Road Suite 200 McMurray, PA 15317 724-942-1337

8 Ways Hackers Monetize Stolen Data

by Steve Zurier

Hackers are craftier than ever, pilfering PII (Personally identifiable information) piecemeal so bad actors can combine data to set up schemes to defraud medical practices, steal military secrets and hijack R&D (Research and Development—refers to innovative activities undertaken by corporations or governments in developing new services or products, or improving existing services or products) product information.

Create a Repository of the Stolen Data

Hackers start by taking an inventory of what was stolen. They will look through the stolen data files for the victim's authentication credentials, personal information such as names, addresses and phone numbers, as well as financial information such as credit card details. Much of this information can be used for future attacks or sold off for more money.

Sell the Personal Information

Once an inventory is created, hackers will package up and sell personal information such as names, addresses, phone numbers, and email addresses. They are typically sold in bulk, mainly to maximize profit. The more recent the records are, the more valuable they are on the black market.

Target Data That's Worth the Most Money

Once the baseline personal information is accounted for, hackers will then comb through the list of authentication credentials and look for potentially lucrative accounts. Government and military addresses are very valuable, as well as company email addresses and passwords for large corporations. Users are notoriously bad at selecting passwords. Many people often reuse their passwords, which lets hackers use credentials for military or corporate accounts to target other companies or other accounts owned by the original victims. In one noted example, Dropbox was breached in 2012 using credentials stolen during the LinkedIn data breach of earlier that year. This type of attack is very common. Attackers will decide what will make the most money. They may plan such a hack themselves, or they may sell the credentials to others on the dark web for a higher price.

Continued on page 2

Continued from Page 1

8 Ways Hackers Monetize Stolen Data

Sell Credit Card Information

Financial information such as credit card numbers are typically packaged by hackers and sold in bundles. A criminal with the right contacts on the black market could easily buy credit card information in groups of ten or a hundred. Usually a "broker" buys the card information, then sells them to a "carder", who goes through a series of phoney purchases to avoid detection. First the "carders" use a stolen credit card to buy gift cards to stores or to Amazon.com. They then use those gift cards to buy physical items. The carder may then sell the electronics through legitimate channels like eBay, or through an underground website on the dark web. According to McAfee (Cyber Security Solutions), a credit card with a CVV2 code on the back is worth between $5 and $8, but if it also has the bank's ID number, it could go for $15 online. If the stolen information has the victim's complete information, that could go for up to $30.

Offload Remaining Stolen Data in Bulk

After several months, the hacker will bundle up authentication credentials and sell them in bulk at a discounted price on the dark web. By now, most of the credentials are worthless since the company has most likely discovered the breach and taken steps to fix it. For example, a database containing the entire LinkedIn credentials dump from several years ago is still available, but are for the most part of little value.

Receive Refunds on Phony Tax Returns

Criminal organizations will take stolen identities and file fraudulent tax returns, seeking to receive tax rebates from both state goverment treasuries and the IRS. In most cases, they piecemeal the data sets, often stealing names, addresses, social security numbers and other financial information seperately. But once they have enough data they then file the fraudulent return. While the IRS reports that total fraud losses dropped 14% last year, fraudsters still stole $783 million last year.

Open Fake Medical Practice and File Fraudulant Claims

This has become a growing problem, especially with Medicare where the federal government estimates that rougly 10% of the money spent on the program is lost to fraud and waste. Trustwave (Information security company that helps businesses fight cybercrime, protect data and reduce security risk) reported this year that one medical record from a single individual fetches $250 on the black market. Because of the millions of dollars that can be made on the black market, criminals set up fraudulent medical practices and submit false claims based on stolen information. They will also prey on the elderly or most any other citizen. It's easy to send bills for small amounts that people assume they need to pay. Incremental payments of $26 here and $56 there add up and don't take a lot of work on the part of the criminal.

Sell Intellectual Property (IP)

Companies in the industrialized world spend millions of dollars every year on research and development, money that developing nations in the Middle East, Eastern Europe and Asia don't have. It was bad enough when hackers stole emails, social security numbers and salary data on more than 50,000 Sony employees a few years ago, but it escalated to another level when unreleased movies, important IP ("Intellectual Property" is a category of property that includes intangible creations of the human intellect, and primarily encompasses copyrights, patents, and trademarks) to Sony, was stolen. The stolen IP issue has been in the news of late as President Trump has forged a trade war with China over the multi-billion dollar US trade deficit with China as well as the People's Republic policy of stealing IP from US companies. The United States Trade Representative recently reported that IP theft by the Chinese alone costs US businesses at least $50 billion annually. Most of these hacks are sophisticated actions sanctioned by nation-states and have grabbed the attention of the federal government. Other more garden-variety hackers also sell stolen data piecemeal. Stolen emails, for example, can lead more sophisticated hacking organizations to IP theft that would interest developing nations.

"Helpful sites from your friendly team at PCS"

We search the web so you don't have to!

LastPass ••• | https://www.lastpass.com/password-generator

Get Total Password Peace-of-Mind

Instantly create a secure, random password.

Passwords are a real security threat. Over 80% of hacking-related breaches are due to weak or stolen passwords, a recent report shows. So if you want to safeguard your personal info and assets, creating secure passwords is a big first step. And that's where the LastPass Password Generator can help. Impossible-to-crack passwords are complex with multipletypes of characters (numbers, letters, and symbols). Making passwords different for each website or app also helps defend against hacking. This password generator tool runs locally on your Windows, Mac or Linux computer, as well as your iOS or Android device. The passwords you generate are never sent across the web.

The Best password tips from the pros

1. Always use a unique password for each account you create. The danger with reusing passwords is that as soon as one site has a security issue, it's very easy for hackers to try the same username and password combination on other websites.
2. Don't use any personally identifiable information in your passwords. Names, birthdays, and street addresses may be easy to remember but they're also easily found online and should always be avoided in passwords to ensure the greatest strength.
3. Make sure your passwords are at least 12 characters long and contain letters, numbers, and special characters. Some people prefer to generate passwords which are 14 to 20 characters in length.
4. If you're creating a master password that you'll need to remember, try using phrases or lyrics from your favorite movie or song. Just add random characters, but don't replace them in easy patterns.
5. Use a password manager like LastPass to save your passwords. LastPass keeps your information protected from attacks or snooping.
6. Avoid weak, commonly used passwords like asd123, or password1, or Temp!. Some examples of a strong password include: S&2x4S12nLS1*, JANa@sx312&s$, 49915w5$oYmH.
7. Avoid using personal information for your security questions, instead, use LastPass to generate another "password" and store it as the answer to these questions. The reason? Some of this information, like the name of the street you grew up on or your mother's maiden name, is easily found by hackers and can be used in a brute-force attack to gain access to your accounts.
8. Avoid using similar passwords that change only a single word or character. This practice weakens your account security across multiple sites.
9. Change your passwords when you have reason to, such as after you've shared them with someone, after a website has had a breach, or if it's been over a year since you last rotated it.
10. You should never share your passwords via email or text message. The secure way to share is with a tool like LastPass that gives you the ability to share a hidden password and even revoke access when the time comes.

Office 365 Training Center

Work smarter and get more out of your Office apps by training on the software applications you need and use the most.

Quick Starts

Get up and running quickly with the basic info you need to be productive right away. Learn what's possible with Word, Excel, PowerPoint and more!

Save time with Office tips & tricks

- Create personalized signatures for your email messages that include text, images, your electronic business card, a logo, or even an image of your handwritten signature. You can set it up so that signatures can be added automatically to all outgoing messages, or you can choose which messages include a signature.
- Add energy and action to your PowerPoint presentation by inserting an online video. Because the video is on a web site, rather than actually in your presentation, you must be connected to the Internet in order for the video to play successfully.
- Add a heading in a Word document. Headings make text stand out and help people scan your document. Simplest way to add a heading is with heading styles. Using heading styles mean you can also quickly build a table of contents, reorganize your document, and reformat its design without having to manually change each heading's text. Best tip, write out your whole document first, then head over to styles and choose from the many selections.

Get up to speed in no time with these popular guides for all of the apps you know and love. Click on the link below to get started.

https://support.office.com/en-us/office-training-center