Have I been "pwned"?

Preamble

Firstly, "No, the title of this article does not contain a typo!" You will discover why in a moment. Second, in order to make sense of this article, I will do something that I never done before and try not to do – and that is, *I am going to have to get personal*. The reason for my doing this will *hopefully* be obvious. More specifically, a proper understanding of the content of this article is contingent on an understanding of "*moral philosophy*" – that is, "*the rational investigation of the truths and principles of conduct*".

Many, many years ago now, one of my mentors made mentioned of "*certain individuals on the Internet who feed on the naivety of the end user*". The whole problem here, at least as I see it, is that such naivety *should never, ever, be taken advantage of*. Sad to say, it is, and continues to be. This idea brings with it the use of the term "malicious" in reference to certain types of "software". More on this in a moment.

If anyone has watched any of the Fawlty Towers series, there is one particular episode where a somewhat disgruntled fellow confronts Mr. Fawlty saying, "*You know something! You are getting my dander up, you grotty little man!*" In all honestly, this is how I often *feel* about those who take advantage of others.

Introduction

To begin with, I am tired of those that would seem to have nothing better to do that to disrupt the lives of others. I am referring to software commonly referred to as "malicious software" – or "malware" for short. More specifically, I am referring to those individuals who intentionally develop such malware. Before continuing, a few terms need to be defined.

What is "Malware"?

Malware is simply a blanket term for any kind of computer software with malicious intent, with most online – or Internet-based threats, being some form of malware.

Hacker: Defined

A hacker is simply a person who gains illegal access to a computer system though the use of a "hack" – that is, "the altering of a computer program".

Script Kiddies: Defined

As odd as this may sound, there are actually individuals that are referred to as "ethical hackers". In the 1995 movie called "The Net", Angela Bennett, portrayed by Sandra Bullock – a systems analyst whose "job" it is to literally hack software to discover problems with that software. Such ethical hackers will refer to a certain group of hackers who hack for the sheer enjoyment of hacking as "script kiddies". My purpose in mentioning these hackers is that they are the ones who – *apparently*, are attributed with causing the most problems.

"Backdoor Virus": Defined

"*A backdoor virus is a program that enters a computer system without being detected and runs in the background to open ports, allowing third parties to control the computer clandestinely. These backdoor viruses can pass themselves off as legitimate programs. Backdoor viruses can compromise files and capture confidential information stored on the infected machine. They also allow hackers to run*

malicious software from the computer's Internet connection to launch other attacks. A backdoor virus is similar to a Trojan with the added threat that it exposes an infected system to unwanted remote access. Backdoor viruses first appeared as networked operating systems grew in popularity."[1]

"Phishing": Defined

The term "phishing" is defined as "*a scam by which an Internet user is duped – as by a deceptive e-mail message, into revealing personal or confidential information which the scammer can use illicitly.*"[2]

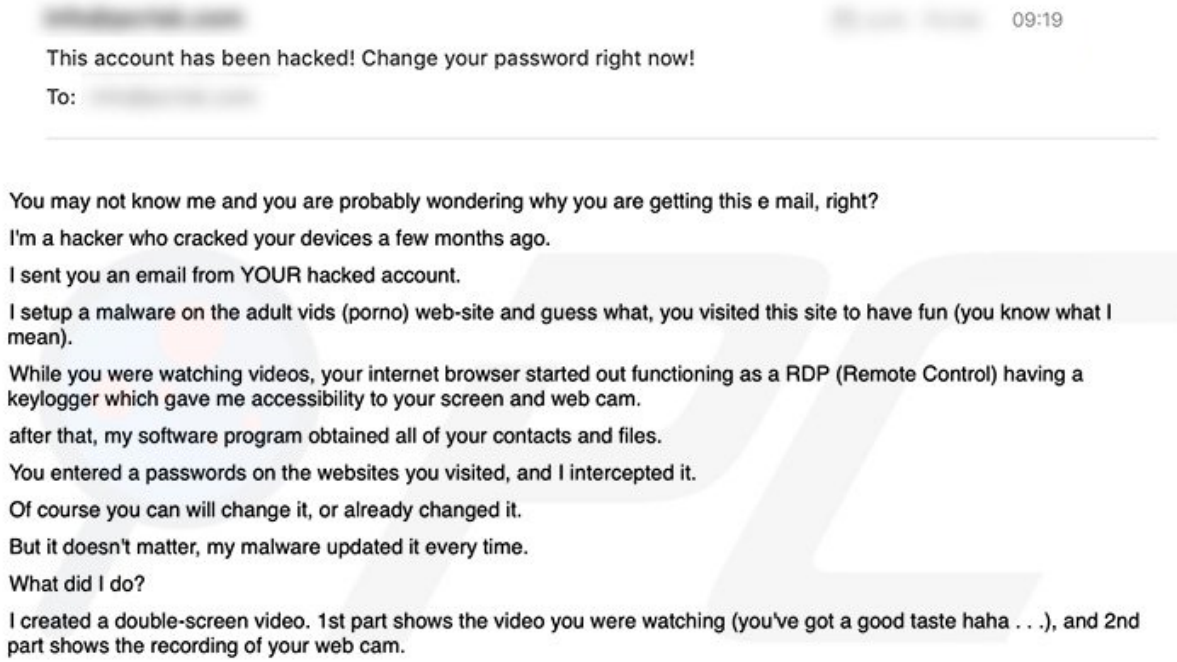
"pwnd": Defined

The origin of the term "pwnd" is uncertain. However, the use of the term may likely be attributed to the slang use of "owned" – and which has an equivalent meaning. Interestingly, *pwned* might owe its etymological genesis as the result of a simple keyboard error in which the letter "p" was mistyped for the letter "o" – as both letters are indeed adjacent to each other.

If the term "pwnage" is used as a noun, it would then refer to the experience of being – or causing someone to be, defeated badly, or failing profoundly. This latter usage originated with the online game "Warcraft" – where a map designer misspelled the term "owned." When a computer beat a player, it was supposed to say, so-and-so "*has been owned*." Instead, the computer now said, so-and-so "*has been pwned*." Lastly because the term *pwn* is primarily used in written form, it has no single generally accepted pronunciation.

"pwnd": Usage, Email Scam

The most common form of "being pwnd" is via a "phishing scam". For example, the following is a sample of a "phishing scam":



09:19

This account has been hacked! Change your password right now!

To:

You may not know me and you are probably wondering why you are getting this e mail, right?

I'm a hacker who cracked your devices a few months ago.

I sent you an email from YOUR hacked account.

I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean).

While you were watching videos, your internet browser started out functioning as a RDP (Remote Control) having a keylogger which gave me accessibility to your screen and web cam.

after that, my software program obtained all of your contacts and files.

You entered a passwords on the websites you visited, and I intercepted it.

Of course you can will change it, or already changed it.

But it doesn't matter, my malware updated it every time.

What did I do?

I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

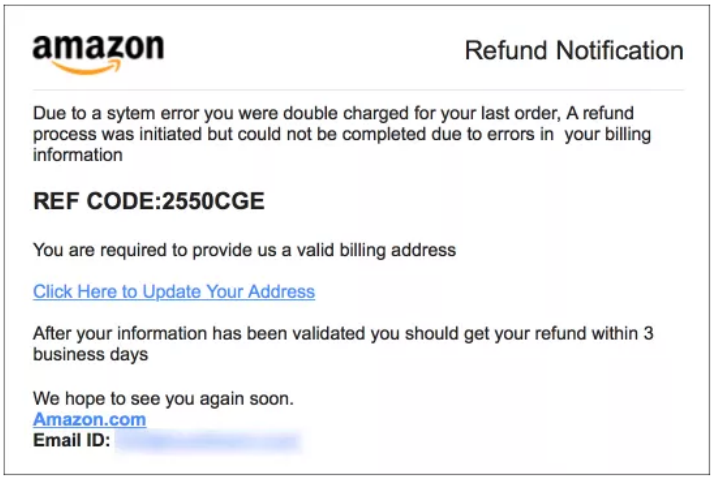
What is particularly *disconcerting* about this particular scam is that the sender purports to have knowledge of the user's password and email – which are shown to be very similar to the user's actual password and email!

How is information obtained?

The first question to ask is, "Has this information *actually been obtained*?" If, the answer is "Yes", then it is possible that such information was stolen from a compromised Web-site such as Yahoo and Facebook – as these Web-site breaches are quite common. This being said, there are as many varied ways to hack as there are hackers.

How does this type of hack occur?

Though the actual methods of "intrusion" are varied, the principle is not – *and which is simply based on "trust"*. In particular, the hacker attempts to trick the user into opening an email attachment – such as an invoice, a fake bill, and so on. These attachments may come in the form of Microsoft Office documents – such Word, Excel, or other such files. And though more difficult to achieve today, a *hack* may come in the form of an attached image – such as "jpegs". More specifically, the hacker attempts to trick the user into selecting what is referred to as a "**hyperlink**"


amazon

Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

You are required to provide us a valid billing address

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
Amazon.com
Email ID:

The text, "Click Here to Update Your Address" is a hyperlink. Once selected, the link will then do whatever that link has been assigned to do. And once selected – there is really *not* a whole lot that can be done to stop it.

What to do?

What is very important for you to remember here is with regards to the "sender" of an email. In particular:

1. Unknown sender: If you do not know the sender, then do not open the email – simply delete that message.
2. Known sender #1: If you do know the sender, but they have never sent you an attachment before, then do not open that message. Rather, you should contact the sender – asking them to verify the purpose of sending you the attachment in the first place.
3. Known sender #2: If you do know the sender, and they have sent attachments previously, then you can *assume* that the attachments are legitimate – and therefore, safe.
4. Known sender #3: If you do know the sender, and they have sent attachments previously, but there is something that just does not look right, then do not open the attachment. At this point, you may want to contact the sender to verify any and all changes that you have just witnessed.

It is imperative to understand that once the attachment has been opened – you have said "*Yes*" to whatever is contained within that attachment. As a real-world example, let us say that someone gives you a magazine with an enclosed envelope. You then open the envelope and out pours some form of gelatinous substance akin to "Jello".

With a computer attachment then, once opened, these attachments may download and install what are referred to as *high-risk viruses*. These viruses often cause subsequent problems relating to privacy and Internet browsing safety. These viruses may also record sensitive data, such as banking details, passwords, logins, and so on. Some of these viruses might even open "backdoors" – thus causing more infections, such as *ransom ware-type* viruses. A computer thus infected, may lead to privacy issues, data loss, or even financial loss.

Cell Phones

As I do not own or use a cell phone – a cell phone is often not on my list of things to mention. However, even a cursory glance on the Internet leaves no doubt whatsoever those devices are one, if not the primary source of hacks. For example, most folks have a single email address – and which is often used on multiple devices, such as a cell phone and a laptop computer. Now, if a hacker were to hack an actual email address – this means that any device that uses that email address will share the same hack. Also, cell phones are used "everywhere" – in particular, using public Wi-Fi networks, such as Starbuck's, McDonalds, Tim Horton's and a plethora of others.

- Note: I have a laptop computer that I use at times and will use public Wi-Fi networks when needed. However, I never keep anything important on the laptop – storing my important data on a secured thumb drive as I would never trust working with personal or sensitive data in a public environment without appropriate protection.

On-Line Storage

Now a word or two about on-line storage. "Online data storage refers to the practice of storing electronic data with a third party service accessed via the Internet. It is an alternative to traditional local storage (such as disk or tape drives) and portable storage (such as optical media or flash drives). It can also be called "hosted storage," "Internet storage" or "cloud storage."[3]

Most devices, such as cell phones, tablets and laptop computers, have available what is referred to as "internal storage" – that is, the means of being able to store data on that device itself. However these same devices can store data "on the Internet" using on-line services such as *One Drive* and *Google Drive* for PC's, and *iCloud* for MAC's. It is even possible to be using both internal and on-line storage concurrently.

The point in all of this is that if you do happen to use on-line storage and if a hacker hacks your on-line storage, and that on-line storage just happens to be accessed using another device then that device could be potentially be affected as well.

The Residual Effects

What is both disconcerting and frustrating however is with regards to *the residual effects* of a thus-infected computer. More specifically, what took just a few seconds to "let in" – may now take hours to rectify with the costs being of both a monetary and incommodious nature.

"Yours truly, Concerned"

In 2008, I wrote an article entitled, "Safe Surfing" and which contains a simple principle for how to use the Internet and which I taught to my seven children during a home-school lesson back in 1996. As mentioned in that article, "*Before you go to that web site, you should be asking yourself this question:*

'Where is it that I am about to go?' Knowing where you are going can alleviate many potential problems down the road. Very simply, the results of my search can take me down one of three avenues:

- *A filtered site*
- *A non-filtered site*
- *A dark site*

We all should want to go to the first location and try avoiding the second and third. So what is the difference?"

- Note: The entire article can be found on the "Articles Page" of the Customer First Computing Web site.

Interestingly, as a direct result of the members of my family being made aware of theses three different types of Web sites has eliminated the necessity for me in having to repair their computers. This is particularly significant in that being "family", would of necessity, *negate* my charging them for these services. All-in-all, having knowledge of such information has been a "win-win" situation for us all!

However, I am still concerned! Though I do make my living servicing computers, I would rather not to have to do so as a direct result of an *honest* error on the part of a client. To me, this manner of earning a living would be, in a word, *unethical*.

About Passwords

One final point – and this is with regards to passwords. When *push-comes-to-shove*, passwords are all important. For some rather pertinent information please see "Password Do's and Don'ts"[4] – with a link provide in "Sources" at then end of this article. Whatever you do, make any and all passwords a long as is possible – *as length is the one of the keys to generating a good and secure password*. Here are some highlights from that article:

Some do's…

Create unique passwords that that use a combination of words, numbers, symbols, and both upper-case and lower-case letters.

…and some do not's…

1. Do not use easily guessed passwords, such as "password" or "user."
2. Do not choose passwords based upon details that may not be as confidential as you would expect, such as your birth date, your SIN, or phone number, or names of family members.
3. Do not use words that can be found in the dictionary.
4. Avoid using simple adjacent keyboard combinations such as "qwerty", "asdzxc" and "123456".
5. Avoid using the same password at multiple Web sites.
6. Never use the password that you have used for your email account at any online site.

…and for sure, some do not's…

Whatever you do, do not store your list of passwords on your computer in plain text.

- I suggest storing this information on a thumb drive, which is then removed for security.

An example

If I *were* to use my name and birthdate, Dell Krauchi, 1954 – which is *not recommended* by-the-way, here are a few suggestions just for the sake of interest:

Do not's	Do's	Note
dellkrauchi1954	DellKrauchi1954	Not recommended, uses my real name
dellk1954	DellK1954	Not recommended, uses my real name

19dellkrauchi54	19DellKrauchi54	Not recommended, uses my real name
dellkrauchi1954	d3!1Kr8u3h!54	Notice that this password looks similar to my name

Here are two really good passwords:

humTdumt$@t0nAwa11	Humpty Dumpty sat on a wall
L37sH@vEsumfUN!;-)	Let's have some fun!

The Resolve...

Sadly, there is only one solution available to us all – and that solution is simply, "*proactive education*". By proactive education, I simply mean "*to learn the 'good' so that when the 'bad' appears, I will be able to recognize it*". I do hope that this makes sense. This is the premise behind "Safe Surfing" – knowing what a filtered Web-site looks like will help me in recognizing what the other two types of Web-sites look like.

I do sincerely hope that you find this article of some practicable use to you. Thank you for your time and interest to the above.

Sincerely,

Dell Krauchi

Sources

[1] www.reference.com/technology/backdoor-virus-bb044d8db32eb9d1
[2] www.merriam-webster.com/dictionary/phishing
[3] www.webopedia.com/TERM/O/online_data_storage.html
[4] https://krebsonsecurity.com/password-dos-and-donts/