Computers and Technology

The Most Dangerous Threat to Your Staff and Business Survival

By Anthony Mckenzie

Being involved with technology solutions professionals see things that could be a real threat to you, your staff or even your business; while the internet can be seen as a wonderful tool (cloud based communications and solutions for example) and all of the other great achievements that the internet has created there is a far darker side to it all; of that there is no doubt and it can be a real threat.

And factually you have in your business nowhere to run or nowhere to hide; sooner or later it becomes a high odd's bet that employee, you or your company will suffer and in severe cases the effects could even close your company overnight.

Don't believe this? Read on where examples of actual major threats are shown below. Not worried? You should be!

It's so dangerous that Deloitte opened a cyber threat hunting service!

But on an everyday level to ordinary SME's just like your business there really is no amount of anti virus this or anti malware that available that is really going to help; the examples below show you exactly why; things these days have moved on exponentially to levels that you may not believe, but some are revealed that are actual examples highlighting just how bad these threats have become. There will be casualties no doubt but you don't want to be one of them!

Email has been a driving force that has moved forward communications between every aspect of business that anyone could imagine, from sales, customers, support, management, publicity and many more important areas; but it's obvious that the underlying technology of email servers are flawed and because it's now a worldwide transport for communications that's hard to fix; these communications channels have to be compatible with every other email server in the world and that creates massive inherent vulnerabilities.

In almost every town, city or country, government bodies are working towards combating fraud and other nasty things from many areas, but email is one of the most widely abused platforms there is because of the ease of abuse by non-experts. And if you're not an expert it does not take long to learn how to be one!

One organisation in the UK is Action Fraud operated by the police and while they handle other areas of fraud, email scams are very high on their list.

But here's where things start to get nasty. Since the advent of cryptocurrency worldwide fraud has increased exponentially. And in the USA SEC Rejects Bitcoin Exchange Traded Fund because they are very concerned about investor losses in Bitcoin.

However, this article is specific; Bitcoin is being used fraudulently and in both of the cases shown below Bitcoin is clearly involved in the transportation of monies to the perpetrators of these illegal demands on you, your staff or even your business. It's no joke and anyone ignoring these really bad potential harms to

their organisation will sooner or later come unstuck in maybe a really big way. The results could be catastrophic.

The first example shown below included personal details of the recipient that have been removed for security reasons. But this email (that passed every check through a company's infrastructure) is threatening the life of an employee and should never be ignored.

Note that Bitcoin and email addresses are edited for security purposes throughout this article.

HERE IS EXAMPLE ONE VERBATIM:

"From: kristin*********

Sent: ******

To: *********

Subject: How to save themself

Read this *warn* carefully, since it can be the last in your life.

People are by nature envious. Given the fact of successful development of your business, people (your contestant) paid me 30,000 Pound Sterling for your head on a stick.

It's not the first time I've done this kind of work, but I'm already tired of these envious bastards and your life will be the last one I'll take or will not do, it's up to you.

Under normal circumstances, I would just do the work for which I was paid without going into the details, but I'm going to get away from it and go on a long-awaited vacation.

You have 2 versions for deciding this problem.

Adopt my proposal or refuse.

You pay me 5 thousand GBP for safe your life and you receive all the information about the customer with whom you apply to the police and thus you save your life and the lives of your relatives.

The second option is you ignore my proposal and turn to the police, but by the same token you will only postpone your judgment day, even if I can not do the work, then somebody else will do it, not within a week and say in a month or half a year, but order for your head will be fulfilled sooner or later.

Thus, you will be afraid of every rustle, walk around looking and thinking that you are being persecuted.

If you want such a life, your choice, but if I were you, I would think very well.

Tickets to England have been taken for July **, and you have exactly 3 days to transfer money to an anonymous account bitcoin 1QJNjRmon3iD3RwdjaGomFLHs25B******.

I can check the last time receipt of money before the flight to you, on the **th

In the event of receiving a reward, I will not come to take your life, but will also pass all the information about your customer (Let the bastards get what they deserve) and you can protect yourself, otherwise you know the consequences.

The well-being of the future life depends on your choice.

Think about your life, you family.

on all will of Allah"

END OF EMAIL MESSAGE ONE

The above email is unedited except for recipients details and Bitcoin account numbers. It can be clearly seen in this email that there is a threat on the life of the recipient. While some recipients would simply brush this type of email off, others become extremely concerned; it's easy to see exactly why. Indeed some recipients will go and pay the demanded money and not think twice. Imagine that a key employee received this email and they completely believed its contents? The resultant downfall of the employee could be extreme. This email threatens the recipients life and mentions their family etc.

Notice that the spelling is incorrect for English on this example (undisclosed but its in the content) and somehow the writer suggests that the email is the 'will of Allah'. Probably not. But the user identified the recipient was in 'England' likely from the email address so the recipient could believe some of the contents.

The above email passed numerous checks throughout the receiving companies infrastructure. Now it's easy to see if you are tech savvy, but most email users are not. And if you're a small SME then things could happen that could literally create very serious effects on your business even though the email targeted an employee. But if you're not tech savvy and a company owner, would you believe the above? and send money? Many will have and that 'feeds' the criminals for millions of pounds or in this case $US.

Bitcoin in the above example is used because ***Bitcoin CANNOT be traced to the ultimate recipient of the payment***. This is a major flaw in crypto currency and one reason (irrespective of some suggesting it's an easy way to make money) you really should have nothing to do with it. Criminals use Bitcoin all the time.

As suggested, you just might not believe the above email if you received it, but there is no doubt that you might well believe the next example because it has information in it that is only known by you!

HERE IS EXAMPLE TWO VERBATIM:

From: "Gloriana Feany"

To: **********

Date: *********

Subject: (HERE WAS THE USERS NAME AND THEIR PASSWORD)

I know ****** is your password. Lets get right to the purpose. You may not know me and you are most likely thinking why you are getting this email? Nobody has paid me to check you.

actually, I actually setup a malware on the X videos (porn material) web site and you know what, you visited this site to have fun (you know what I mean). While you were viewing videos, your web browser initiated operating as a RDP that has a key logger which gave me access to your display and webcam. Immediately after that, my software program gathered every one of your contacts from your Messenger, social networks, and emailaccount. And then I created a video. First part displays the video you were watching (you've got a fine taste hehe), and 2nd part displays the recording of your web camera, yea it is u.

There are two different possibilities. Let us take a look at each one of these options in details:

1st alternative is to skip this message. In this case, I most certainly will send your very own video clip to all your your contacts and visualize concerning the humiliation you will see. Moreover if you happen to be in a committed relationship, how it will affect?

Next choice should be to give me $3000. We are going to call it a donation. In this scenario, I most certainly will quickly remove your videotape. You will continue your way of life like this never took place and you will never hear back again from me.

You will make the payment through Bitcoin (if you do not know this, search for "how to buy bitcoin" in Google search engine).

BTC Address: 18PvdmxemjDkNxHF3p3Fu9wkaAZ********

[CASE sensitive, copy & paste it]

In case you are thinking about going to the law enforcement officials, very well, this e-mail can not be traced back to me. I have covered my actions. I am also not trying to charge you a lot, I simply want to be rewarded. I've a unique pixel in this e-mail, and at this moment I know that you have read through this email message. You have one day in order to pay. If I don't get the BitCoins, I will certainly send your video to all of your contacts including family members, colleagues, etc. Having said that, if I receive the payment, I'll erase the recording right away. If you really want evidence, reply Yup! then I will send out your video to your 7 friends. This is the non-negotiable offer, and thus please do not waste my personal time & yours by responding to this e mail.

END OF EXAMPLE TWO EMAIL:

This is an entirely different threat. The recipient picked this email up because of a multitude of reasons that were simply incorrect and not representative of their actions on the internet; however, the stated password was about 80% shown (and it would be reasonable to assume the perpetrator knew the rest of the password). This could be seen by many as a factual document and it's credibility is created in the recipients mind by the inclusion of the password in to the threat.

Imagine owning a SME business that might indeed be a larger business, the threat demanded much more money and the recipient had viewed what was suggested in the email? People do. It could be seen as likely or at;east a possibility that the recipient might well pay the money to the perpetrator through Bitcoin. And again Bitcoin rears its ugly head.

Again in this second email instance shown the email passed all checks and tests in the company where the email was received. So these are real threats to individuals or business.

But consider this; how did the perpetrator get the recipients password? (it was an old password but nevertheless was mostly valid). The perpetrator suggested key logging on a site known for pornographic video and images. But that is most likely not where the perp got the details from.

When reading about companies like Facebook, TalkTalk, Dixons Carphone Warehouse, Equifax, Adobe, AOL, Apple, AT&T, British Airways, Mastercard and Visa, Compass Bank, Dominos Pizza, DVLA UK, Dropbox, Kmart, Hewlett Packard, eBay, Experian, Trump Hotels, Gmail, Vodaphone, Walmart, Morgan Stanley, NHS, Ofcom, SnapChat, Adidas, Macys, Sony Pictures (and the list goes on) is it really no wonder that most personal details of importance (even financially) of individuals and businesses are all over the internet. There is a Wikipedia about these breaches of data that is extremely concerning reading as these breaches involve all kinds of information that will no doubt be available to buy on the internet. With the incredible reductions in share prices at Facebook maybe that might be the start of a mass exodus from those sort of 'social media' sites; but of course Facebook is merely one of the very long list of companies that have let you down through not protecting your data properly as the list above clearly demonstrates.

Its easy to see why GDPR has become law and countries will continue to pass GDPR legislation accordingly. Thank all of the companies mentioned above and many more for allowing this ridiculous situation that could be the start of the downfall of the internet as it is known today.

But is it time to go back and retrospectively fine each and every company involved in the dispersal of personal details? Are those companies any less 'guilty' now? It seems for many companies that the only thing they understand is when they are faced with very large fines; and even the fines might be irrelevant to organisations like Facebook and Google because large fines seem to be 'petty cash' to some of those companies. But shere price reduction wakes them up.

If anyone is concerned about a 'key logger' from the above email example getting your information Kaspersky latest offering of internet security includes software that stops key loggers from logging your information as you type.

A third example of fraud covered in this article relates to a company that received an email pro-forma invoice to pay from one of its regular suppliers. One day the finance department received a pro-forma invoice that needed to be paid immediately. The email address and the invoice itself looked entirely

unremarkable. The sending company advised the finance department that they had recently changed banks and that the new details were on the invoice attached. Finance paid the £60,000+ ($US 80,000) invoice.

The only problem was, that the invoice was completely fraudulent, the email address did read correctly unless you looked close (instead of *wonderful*.com it was *wonderfull*.com (just made up example to illustrate the methodology used) and the recipient in the finance department saw and read what they were used to seeing. The real question is, how did the perpetrators get all that information about what an invoice should be like, the real suppliers details, etc., their website and email addresses and more; it's food for thought and make no mistake it can be so easy to allow one of these scams through your business; the chances are pretty high and the consequences could be dire and even bankrupt your business if taken to the extreme.

There is no doubt that the underlying email systems are no longer fit for purpose in general and have not been for some time. Notice that in the first example the scammer sent mail from 'mail.bg' and the second one (even more concerning) was from 'outlook.com'. While the sending email addresses can be 'replaced' with any email address upon examination those two shown emails seemed to be real; indeed one of the perps even used Google to advise how to use Bitcoin for payment. But there are multiples of very large companies that every day offer a service but allow their email servers and systems to send out such threatening emails to users. Maybe it's time to pressure these organisations (outlook.com, gmail.com and there are multiples of others) to actually filter their emails properly as well as the sendersbefore these sort of threats go out and create serious harm that these sort of messages could easily do.

Of course there are millions of other examples of fraud through an outdated abused email system (and other related internet technologies) that could be shown here, but the aim of this article is to educate readers so that they don't fall foul to these sort of appalling scams.

One company, Network Systems has seen many of these sort of internet related issues and offers a cybercrime service to SME's to help to create a safe environment for empolyees and business as they work on the internet today.

Hopefully this article will at least make the reader think very hard about how they are going to ensure protection of employees and their company and if nothing else that is a wothwhile objective. Using specialist companies will always help more than by just trying to put solutions in place created by someone without experience in this area and could actually save your company.

Anthony Mckenzie is the managing director of a company involved with technology solutions for a number of business sectors and also an international reviewer of technology products for vertical sectors of business.

Article Source: http://EzineArticles.com/expert/Anthony_Mckenzie/2574739