Why Hackers Love Small Businesses

Broadcast: January 23, 2007
[On WSRadio.com]

Anita Campbell: Research shows that 72 percent of small business owners believe that hackers do not want to bother with our small networks. Now, most of us small business owners believe that hackers only want what larger companies and financial institutions have to offer. Well, nothing could be further from the truth.

Today's guest, Thomas Raef, founder of e-Based Security, has over two decades of providing IT solutions to small businesses in the Chicago area. He is with us to explain why you and your Web operations are on the radar screen of hackers. He's also going to share ways that you can regain that comfort level of feeling secure again.

Well I hope so! Welcome to the show, Tom.

Thomas Raef: Thank you, Anita.

Anita Campbell: Everyone assumes they're safe online, if they've installed a firewall and anti-virus software on their systems. Why is it that you say we are not safe, even though we've done that?

Thomas Raef: Well, first of all I'd like to thank you for having me on your show. The reason why we're not safe is that people understand how your anti-virus software works. Those are the two main levels of protection small businesses have -- anti-virus and firewall. But anti-virus signatures are based on information that's found by people submitting infected files.

First, a number of companies have to find an infected file, submit it to their anti-virus company. The anti-virus company analyzes it, produces a signature, and then pushes that signature out. Sometimes this happens quickly, depending on how widespread the virus is released, other times it could take a couple of days. During that time, you're totally unprotected, so that's the fallacy of anti-virus software.

Your firewall is designed to primarily protect you from attacks coming in, but even those are mostly poorly configured and a lot of times once the hacker takes control of your system, their traffic is going outbound, and your firewall does very little to stop that.

Anita Campbell: Tom, what is it that hackers want from us?

Thomas Raef: They want control of your systems. They make money by being able to send spam from your systems. They put keyboard loggers on your system. A keyboard logger will record the keystrokes that type on your keyboard and send it to them.

Do you pay your bills online? Do you log into your bank account online? All that information is stored into a file and then sent to them. They make money off of selling that, or they use it themselves to drain your account.

Anita Campbell: You mentioned, as the first thing, that one of the things they do is that they send spam out from your system. Now, why would they need another computer to send spam out? I assume they could send it from their own systems, right?

Thomas Raef: Well, they could, but then they get caught, and their location gets published around as a source of spam; it gets blocked by everybody. So what they do -- it's one of the primary reasons that they like to take over controls of systems -- is that they send spam out from your system. They may send … some of these hackers will control networks of 50,000 to 100,000 systems. They send a little bit of spam from each one, and the spam gets out. By the time it gets caught and reported, they've already moved on to another group of PCs.

Anita Campbell: How do know if your PC is one of the ones that have been captured this way? Is there some sort of a telltale sign? Or is it that it's happening and you don't even know about it?

Thomas Raef: Typically, the end user isn't even going to know about it.

It used to be that they would hack, and it was all for malicious fun. They would open up your CD drive door or they'd play some loud, obnoxious sound out of your computer speakers. When their motivation turned to one of profit, one of making money -- that's their source of income -- they now want all their activity to be very stealth.

So you may not even know it, but a couple of telltale signs is, if your system starts running slow. Now that's not a dead giveaway, but if your system is running slow then you have to check the activity on your system. Is there something happening? Do you see your drive light going on while you're sitting there doing nothing?

There are some other telltale signs that you can check to see if there is any activity coming from your system. You need to really be aware of the activity, the drive light, and the speed of your system. Some things like that are pretty good indications that you may have somebody on your system.

Anita Campbell: Well you mentioned that these hackers might have, I think you said, 150,000 computer systems actually running?

Thomas Raef: Yes.

Anita Campbell: I mean, that sounds very organized. Tell us a little bit more about what they're doing and how they're working.

Thomas Raef: Well, basically, when they hack into a computer, that's what they want. They want control of it so that they can use it for a lot of their activities. One of the things they like to do is they like to steal credit card information. So a lot of times, they'll take control of your system, copy software down, like I said before, its like a keyboard logger, so it'll record all your keystrokes and send that information to them.

I've been, even in the last three weeks, through some diligent searching online, I found a number of online forums where these people just brazenly advertise how many credit cards they have available for sale. They even give some of them away to people to prove how valid the cards are. People come back on these forums and they post reviews. "I used six out of seven cards and each one was good for $2,000." They'll publish this information and then that stolen credit card vendor gets a high rating and people know that they can trust them, so it's very organized.

There's software that these people can download if they just have a credit card number. People have gone to the trouble of putting together large databases of personal information, so you plug in a credit card number and it will tell you what bank issued it, the ABA, the routing number for that bank, the bank's location, the bank phone number, a lot of times it has the owner's name and address. You know, this kind of information is available online and easily obtainable by the cyber-criminals.

Anita Campbell: Where are these people located? Are they offshore; are they in the United States, or both? This is like something out of a novel!

Thomas Raef: Right. It really is. It scares me. Obviously, being a security professional I have to dive into some of these areas. It scares me when I look at this information and it's just screen after screen of this stuff.

I used to think a lot of these people were based offshore. There are a number of them that are based here in the United States. When they start naming stores that they've been to with these stolen credit cards, you can kind of get a feel of that. And you can tell also by the language that they use in these forums. I mean, it's very clear English and so, you have to believe that some of these people are here in the States.

The majority of them -- these websites that host these forums where people openly display their wares of stolen information -- those websites are hosted over in like Eastern block countries.

Anita Campbell: Well, now let me stop you for one second and phrase a question here. You mentioned that you did some online searching and you managed to find these forums where people are out in the open. Why doesn't the government actually shut them down?

Thomas Raef: Well, because the websites are hosted in locations that really don't participate with the U.S. government. A lot of it is Eastern block countries and their laws aren't as strict as ours. We don't really have any way of stopping them.

The government tries as hard as they can to come out with laws. You know there is the Can Spam Act --- and that has pushed a lot of spammers offshore in "illegitimate operations." I'm not talking about sending spam from someone's system unknowingly, but you know there used to be people in Florida and all over the United States that actually had spam operations.

Anita Campbell: We are going to take a short break. I want you to come back. We've got a lot more with Tom Raef. We're going to get into specific tips that Tom is going to be giving us about how you can protect your systems from these organized hacking gangs. So come right back. I'm Anita Campbell.

(Radio Break)

Anita Campbell: Hi. We're here with Tom Raef, founder of www.ebasedsecurity.com, a provider of unified threat management systems for small businesses. We're talking about why hackers love small businesses. Tom I'd like to go back to something that you mentioned early on. You said that we might notice our systems being slow, for example.

That might be a tip-off that one of these gangs has somehow infiltrated our system, taking control of it. Well, let's say that I'm online and I notice my computer suddenly becomes very slow. It looks like lots of things are going on and I suspect one of these gangs has taken over my computer. What would I do at that point? What would you recommend the first thing that I should do?

Thomas Raef: Well, the first thing I would do is -- Windows, I am presuming that most people are using a Windows computer, so that's what I'll address. Windows has some files on there, some programs that you can run from a command prompt that can tell you what kind of connections you have to your system.

So the first thing I would do is I would recommend you close all your browser windows. Basically, close all the programs on your system. Because then you know that you shouldn't have any communication going on with your system and anything else at that point. So close down all your programs.

Then open up a command prompt. You can hit start, run, and then you type in CMD - Charlie, Mary, David - and hit okay. It will bring you to a DOS prompt. At that point you can type in netstat, n-e-t-s-t-a-t, then put a space and then dash AN. That will show you a list of all the connections to your system.

There's a column that will be displayed on your screen there called 'foreign addresses', and those foreign addresses are IP addresses that your system is connected to. So if you don't have any programs open and you start to see some IP addresses in there, in that foreign address column, that you don't recognize -- because if you're in a network situation, you are going to have a connection to your server, so you will have some internal connections. Your IP addresses in that foreign address column should not be something outside of your network.

If you do see some connections, then in the far right column it'll show the state. Are they established, are they listening, whatever. If you see established connections and you have no other programs open on your system, then you're definitely, I would say definitely under the control of someone outside.

Anita Campbell: Alright, well I'd like just to take a moment and go back over what you just described here. So you're saying if you suspect that someone has taken over control of your system, and you're using Windows, you go to the 'Start' menu, which usually appears in the bottom tray ...

Thomas Raef: Correct.

Anita Campbell ... of information on your computer and you click that and you click 'Run' and that's when you enter in those commands that you talked about.

Thomas Raef: Well, yes, you would type in the CMD like Charlie-Mary-David, and that will bring you to a command prompt window.

Anita Campbell: Which is basically a dark window?

Thomas Raef: Correct.

Anita Campbell: Is that correct?

Thomas Raef: Yes.

Anita Campbell: For someone who doesn't know what a command prompt window is -- because there are some of us who may not be as aware of it -- that's going to be kind of an ugly looking window. But basically, are you bypassing Windows at this point?

Thomas Raef: Yes, you're into a different area of your computer, yes.

Anita Campbell: When you enter those commands you're going to be able to see these things that you're talking about.

At that point if you see the kinds of things you mentioned that suggest someone has taken over your computer, what should we do at that point? Should we interrupt the Internet connection?

Thomas Raef: Yes, I would. I would disconnect from the internet immediately. If you have an IT person on staff, notify them. You know there are a number of things you should do. Oh, I hear the music in the background so I think we're taking another break here?

Anita Campbell: Yes we are. We'll continue this when we come back. We are going to be back in just a few minutes. We've got a lot more with Thomas Raef, Founder of e-Based Security, on why hackers love small businesses. So do join us after the break. I'm Anita Campbell.

(Radio Break)

Anita Campbell: We're speaking with Tom Raef, Founder of e-Based Security, and a provider of unified threat management systems for small businesses. We're talking about why hackers love small businesses.

Well, just before the break, Tom, you were walking us through the procedure we should follow if we suspect that our system has been compromised in some way by one of these hacking gangs.

You said we should disconnect from the Internet, and then you mentioned if we have an IT person to contact the IT person. That all makes sense. What if we don't have an IT person who works on our business?

Thomas Raef: At some point, you're going to have to enlist the services of an IT person. Microsoft recommends that, depending on how severe the infection is, you really should have your drive basically reloaded from scratch, which means formatting the drive, reloading Windows, and then reinstalling all of your programs, because sometimes they can get in so deep with their malware that cleaning becomes ineffective.

I've had some people that wanted me to clean their system, and they said, "Well, I can't find the CDs anymore for the software that I've got on here," or, "It's old," or whatever. I've spent six hours just trying to clean infections off of somebody's system where hopefully it should take somebody a lot less time just to format the drive and reinstall everything from scratch.

Anita Campbell: Unfortunately, it sounds like having one of those bad situations happen to you is probably the time when you really start thinking seriously about getting an IT person to help you.

Thomas Raef: Yes.

Anita Campbell: What else can people do? I mean, this is great stuff, to advise other small businesses about. But what else should we be doing either to protect ourselves and our computers from getting hacked in the first place or once we've been hacked.

Thomas Raef: There are a couple of other things that you can do. I'm a firm believer in free software. There are some programs -- if they're working out of their home -- there's a program called AVG (Apple, Virginia, Gary) that you can download and it's an antivirus program.

You want to be careful because your system could slow down. I've seen some systems that the people have installed six different antivirus and spam blockers and pop-up blockers and everything else. That in itself slows down their system to a crawl. So it kind of becomes self-defeating.

Anita Campbell: All that protection is fighting against each other, huh?

Thomas Raef: Exactly. But another great program, if you go to www.microsoft.com/security, Microsoft offers their Windows Defender program, and it's free. You can download it, install it on your system, and it's a great tool for detecting malware on your system as well.

Anita Campbell: Oh, that's great. That's a free Microsoft tool?

Thomas Raef: Correct. There's one other tool that I would recommend that's free. You can go to a website called www.clamwin.net, and Clam Win is an open source software that you can run on your Windows system. It's an anti-virus program, and they're very diligent about updating their signatures and so forth, and that is free as well. So, you know you can kind of use a mixture.

Anita Campbell: Well, that's good, a good mixture. The first you mentioned, I think it was AVG?

Thomas Raef: Correct.

Anita Campbell: That is at what site? Where can you download that?

Thomas Raef: That's from, www.grisoft.com.

Anita Campbell: OK. That's good. Now, I assume you don't recommend people download just any old free software. It's got to be software that has a reputation for actually being a reliable help, right?

Thomas Raef: Correct. One of the, I'll call it an attack vector to sound very official, but an attack vector for hackers is they will actually hack into a website, change the code on the website so that anybody who visits it gets a pop-up on their screen that says, "Your system may be infected, click here and run this scan on your system."

Well, by you clicking there, it's going to have you download some "anti-malware software", and all it really does is infect your system and gives them remote control of it, and you're none the wiser.

So yes, you do have to use reputable software and software that's recommended directly, that you download directly from a specific website.

Anita Campbell: What else can we do to protect our computers and our systems from all these malware attacks and hacking attacks and so on?

Thomas Raef: You can be diligent about updating your operating system. Do your Microsoft updates. Set it up so that it downloads the updates automatically and then notifies you so that you can install them.

Sometimes it does ask to reboot your system, and you don't want to be in the middle of a long document that you haven't saved, and all of a sudden your system tells you that it's going to reboot because it's applied some updates, and there goes your work!

You do want to have it download the updates, but notify you on when to install them. You need to keep up-to-date. People don't realize there's Microsoft Office update for Word and PowerPoint and Excel, you need to apply those updates as well. You can get those off of Microsoft's site.

You need to update your Adobe Acrobat Reader. There have been vulnerabilities that have been

exploited by sending around infected PDF files, like an Acrobat file, and people don't realize that it's easy to spoof somebody's email address.

A typical scenario would be, I find out who the owner of a company is, and I find out all their employees' email addresses. Well, I spoof the owner's address and send an email to all the employees saying, "Please review this document and let me know your thoughts and comments." Everybody who opens up that file is going to get infected. You need to update all your software on a constant basis.

Anita Campbell: So you really should be scheduling this and setting aside time specifically for it, is what it sounds like to me.

Thomas Raef: Yes. It's something that has to be done, because the software vendors -- Microsoft, Adobe, Macromedia, all the software companies -- they are pretty diligent about catching things once they know that there's a hole in them. So, the least people can do is accept their free downloads and update all their software.

Anita Campbell: Tom, this is a great point, because I think especially a lot of microbusiness owners, those who own very small businesses, or business owners who work out of their homes, may not be setting aside a specific amount of time each week to focus on their computer systems. You know, we do that for our accounting and for other administrative tasks, but what you seem to be suggesting is we should be setting aside times, specifically, and treat this as an important aspect of running our businesses.

Thomas Raef: Correct. Like you said, you take time to do financial planning, tax planning, et cetera. You also need time to do computer planning, and that is protecting your system, because who of us could live without our computer? If a hacker takes it over and crashes it because something that they tried installing didn't work, and it winds up crashing your system; you have to bring in an IT person or take it to an IT person to get it fixed.

You might be down for a couple of days while they get everything rectified. By being diligent about keeping up-to-date on everything, you're taking a huge step, and it's free, I mean, it costs you time, but dollar-wise it's free, it's a huge step towards protecting your systems.

Anita Campbell: Now, where does your company, e-Based Security, come into all of this, Tom? What does your company actually do?

Thomas Raef: What we do is provide a device and a service for small businesses, because we know what's coming in and going out on the Internet. We watch it all day long. The problem is that, as I mentioned before about the command -- the netstat command where we're on that dark

window -- that command is effective for certain types of infections, but there are other types of infections where the hacker's activity won't even show up on there. The only place it would show up would be like on a firewall.

But you could ask for a show of hands, if you could see their hands, who has reviewed their firewall logs in the last six months or a year, and probably nobody's hand is going to go up, because most people don't even know that their firewall even has logs. You need to be diligent about watching your firewall logs as well, and your firewall needs to be properly configured to be able to catch that type of outgoing traffic.

That's all stuff that we do. We put in our appliance; it only lets out traffic that is absolutely necessary for your business to operate. So there's a constant communication between us and the client as to what is necessary. We watch the logs constantly, so we can tell if something is trying to get out that shouldn't, and then we can trace it back. We contact the client and assist them in one way or another of cleaning that system.

We also block all their spam, and sometimes they say, "John Doe tried sending me an email, and it's a file I need." We'll take a look in the logs and say, well, they need to put it in a zip format, or they need to put it in a different format in order for it to come through, because that type of file is typically infected. It's a constant partnership with us and the client so that they stay clean.

Anita Campbell: How much does that kind of a service or that box that you're talking about actually run?

Thomas Raef: The price varies based on the size of the company or the specific application. It starts at just under a thousand dollars, $995, and the monthly service is $179 a month. But like I say we're watching everything coming in and going out so we can stop it in a heartbeat.

Anita Campbell: What is your website address, Tom?

Thomas Raef: It's www.ebasedsecurity.com. That's e-b-a-s-e-d-security.com.

Anita Campbell: I assume you've got all sorts of methods to contact you or others in your company on the site, correct?

Thomas Raef: Correct. We have a toll free number on there, people can email me; we have a variety of ways, yes.

Anita Campbell: Excellent. Thank you so much Tom. This has been very informative and I really

appreciate you coming on the show. You've been a fabulous guest.

Thomas Raef: Thank you very much for the time.

Anita Campbell: Well do stay with us. We will be coming right back for our Today's Trend segment. Today's Trend segment is about pet industry trends. I'm Anita Campbell.

(Radio Break)

Anita Campbell: Well it's time once again for our "Today's Trend" segment. Today's Trend is about trends in the pet industry and how to profit from these trends for new products and services. Yes, I'm talking about those four-legged little creatures that many of us seem to have, or the pet birds or pet fish or pet reptiles or whatever.

Whatever your pet is, you are not alone. Just in the United States alone, there are 69 million homes with pets. So with that many pets, pet-related products and services are a huge business; $38 billion -- that's billion with a B -- dollars a year. With that much money floating around, there's plenty of opportunity for smaller businesses. So, for that reason, every year we call on an expert in the pet industry to come in and predict the trends for the coming year.

Laura Bennett, who is the CEO of Embrace Pet Insurance [http://embracepetinsurance.com], has provided the top ten trends this year. I'd like to talk about just a few of the highlights of her trend predictions -- ones that I think will possibly trigger some ideas for new pet products and services.

- The first trend that she notes is that we can expect to see a lot of growth in unique pet goods. The emphasis there is on ***unique***. She mentions items such as pet deli snacks, toys for pets, luxury items for pets, and convenience accessories such as programmable feeding and watering stations, warming mats and even self-cleaning litter boxes. As she also notes, high-end specialty pet stores are thriving despite all the big-box retail outlet emphasis on pet goods, because it's the high end stores that are providing these ***unique*** pet goods.

- The second trend she mentions is to expect considerable growth in pet ***services***, such as grooming, boarding, pet photography, dog walking, pet sitting. As she notes, more pet owners are paying for these kinds of services, because in some areas of the country, it's becoming socially unacceptable to leave your pet alone during the day, or leave your cat alone over the weekend.

  You can expect to see more pet services, but you can also expect to see pet services banding together in ***partnerships***. For instance, perhaps a breeder and a groomer of pets, getting together and providing services throughout the pet's lifespan. Perhaps a doggie day care facility and pet hotel facility banding together with veterinarians. You can also expect to see pet insurance and pet trusts and pet cremation, burial, memorial services.

- Another area that you can expect to see quite a bit more is ***pet-friendly environments***. These are restaurants, shopping malls, and other places that actually welcome pets. Even hotels, such as the Starwood and Loews hotel chains, are doing more to welcome pets. Some states are even considering laws that will require pets to be accommodated in restaurants.

- You can also expect to see some additional benefits happening in some of the websites online for pets. As Laura notes they are getting better and better. Urban Hound, Waggin' Tails, and PawSpots are some of the ***websites that are attracting communities of pet lovers***.

With all these pet trends there is sure to be an opportunity available for you if you have an interest in this area. So check out the pet industry.

With that I want to thank you very much for joining me on another show. It has been great to have you here with me.

Please do visit our podcast site, where you can be sure to find all the podcasts from our shows. That's at www.smbtrendwire.com. Or visit the main Small Business Trends site for more text-related small business trends information at www.smallbiztrends.com.

Thank you so much. See you next week; I'm Anita Campbell.

* * * * *

www.smbtrendwire.com