



THE MALWARE REPORT

The Financial Crisis Spurs Online Banking Attacks

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET LLC

The Malware Report Transcript

Title: The Financial Crisis Spurs Online Banking Attacks.

Episode: 90

Location: http://www.eset.com/podcasts/ESET100608_Online_Banking.mp3

October 9, 2008

[Begin recorded material]

Matt Grant: Hi, this is Matt Grant and you're listening to The Malware Report with Randy Abrams. Hi Randy, thanks for being here.

Randy Abrams: Hi Matt, it's great to be back.

- Matt Grant: I wanted to spend some time today discussing a topic that seems to be on everyone's mind. That's the recent financial crisis that's taking place. I wanted to see if you had any thoughts on how this might affect or is affecting IT spending and IT resources. Have you heard from any of your customers, or anybody in the industry in particular about how this is affecting them so far?
- Randy Abrams: I really haven't heard how it's affecting their IT spending. Obviously if a company is suffering because of the financial crisis they're going to be tightening the belt strings, and security might not be the best place to be making cuts. If a bank is trying to save money, you don't make it easier for the bad guys to take the money that's in the bank.
- Matt Grant: That's a good point. If IT managers are being requested to cut back on spending in these times, is there an area they should look to? Is security one where they should look to cut back resources?
- Randy Abrams: Probably not. It depends on the company, if a company isn't making wise choices about their security profile then perhaps there's ways to decrease spending without decreasing security. If you've got a good IT person and they've made sound choices for their security they're probably not spending too much on it right now. Cutting back would be a net decrease in security which could, in the long run, be very costly for a company.
- Matt Grant: Absolutely. Outside of just the effect that it's having on organizations, I wanted to spend some time to talk about attacks or possible attacks that we might see targeted at consumers and computer users. According to a new survey conducted by iTracks, 61% of U.S. citizens say they have security concerns when it comes to online banking. I would assume that these concerns might increase even more with the recent financial crisis. Is there something that consumers can do to stay safe online, or are there any attacks that are correlated so far with this crisis?

Randy Abrams: Well, currently what we're seeing and what we're going to see a lot more of is attacks designed to play upon the confusion of consumers. We're going to see a lot of mergers, where a couple banks will get together, or acquisitions, where a bank will take over another bank. What happens each time that occurs, even outside of a financial crisis, is the phishing group gets into it. They send out an e-mail saying "this is bank "A", we've acquired bank "B". To convert over to our new system you need to go your account and type in this information. The banks don't do that; that isn't true. What people have to constantly be aware of is that computers lie to you all the time. Just because an e-mail looks like it came from your bank, it doesn't mean it did. If you have any question at all pick up the telephone and call your bank and ask about it.

Matt Grant: You read my mind Randy, I was thinking in particular about Chase purchasing Washington Mutual, and Washington Mutual customers have got to expect some sort of phishing attack from organizations pretending to be Chase. Have we seen that yet? Or should we just expect to see this?

Randy Abrams: I haven't seen an actual Chase/Washington Mutual phish; I would certainly expect to see a lot of them. I don't know how much information Chase has sent out to Washington Mutual customers. We're going to see it, it's going to happen. It's too big of a target for phishers to skip; they're going to attack these people. There will probably be additional IRS related phishing scams around the bailout package too.

Matt Grant: Absolutely. The feds said earlier this week that they were looking to provide as much as 900 billion in short-term loans in the next three months to stressed banks. I'm sure then that consumers will start to see some of those as well. Is there anything that they should be on the lookout for these particular attacks?

Randy Abrams: Not if they're doing things right. If they're doing things right, they're always suspicious of an e-mail that comes from the bank, the IRS, their stock broker, that says "you need to go to this website." If you keep that in mind, you should be able to avoid the phish. It's also good to use an up-to-date and current browser, because the browsers will help identify some of these phishing sites, so if you got suckered into it and clicked on the link, often times the browser can help prevent that page from showing up. It'll tell you that this is a bad site. Additionally, using anti-spam software will actually filter out a lot of these phishing e-mails. And using anti-malware, antivirus software, in many cases will catch these kinds of attacks as well. Use technology, it's useful, but don't rely on it exclusively. Your mind is the best tool you have to prevent yourself from becoming a victim.

Matt Grant: Overall 61% of citizens are concerned when it comes to online banking. Should they be? If they're just visiting the site directly, if they're not clicking on links through an e-mail or falling for what might be a scam, is there a legitimate concern around online banking? Or have we gotten to the point where online banking is pretty secure?

Randy Abrams: The online banking itself is pretty secure if you type the URL in yourself and don't follow it from a link in an e-mail. But, if your computer is not properly secured, you can have a keystroke logging program on there that you don't know about that is capturing the information you type in to log-in to your bank and sending it to a remote attacker. What that survey tells me is that 39% of those surveyed need more education, because they should be concerned about it. I'm not saying don't do it, but if you aren't concerned about it then you probably don't know enough to take proper precautions to keep your computer secure.

Matt Grant: That's great advice for everybody listening Randy, is there anything that you'd leave us with on this topic?

Randy Abrams: I was just reading today about attacks on voters, where people at colleges will get an e-mail or a phone call saying “there’s going to be a big police presence at the voting site, so if you have any warrants for your arrest then you might not want to show up,” and it’s designed to scare people away from voting. Fundamentally, this is the same kind of attack in a non-digital format that phishing is. These kinds of tricks and cons have been with us for a long time, the fact that it happens on a computer in an e-mail isn’t really different. If you learn to understand the fundamentals of the attack then it doesn’t matter if it comes in e-mail; you’ll spot it and be protected.

Matt Grant: Well Randy, that’s great feedback, and it’s definitely sparked my interest on another topic that we’ll be visiting next week on The Malware Report, and that is how dangerous are electronic voting machines that are going to be used in the upcoming election. Randy, thanks again for being here. This has been Matt Grant and you’re listening to The Malware Report.

[End of recorded material]