

Internet Threats and Healthcare IT Today

Ian Burke

We are facing new threats today. It is no longer a fight against generic spam and viruses. Today we are facing targeted attacks leveraged against industries, organizations or individuals. This environment changes the fabric of how attacks work today. As spam decreases, phishing attacks are on the rise. While web viruses fade in number, cross-site scripts, cross-site fraud requests, site manipulation and SQL injection are becoming more prevalent. But how does this translate to you on your desktop?

In the average corporation spam is still an issue. It has changed dramatically. In the glory days of spam it was a plague that would hit every mailbox in an organization. Today it is not uncommon for people in the same organization to have different spam experiences. One mailbox may see hundreds of spam hits in a day while another mailbox may not get a single piece of spam. The reason behind this is spam's improved targeting. It is closer to phishing attacks and targeted malicious code attacks. While much of the spam we are still seeing today is junk mail, a good portion of it is intended to gain confidence of the user, to gain information from the user, or to plant code or pull code from the user's system. Spam today has a purpose.

This new face to spam is the tip of what we are seeing. The old school of attackers had viruses as their primary weapon. They loaded them into thumb drives, software distributions, and web sites, anything they could. From a security stand point we simply had to have good anti-virus protection and we were in good shape. There was some concern about the really diligent attacker trying to sneak in from the outside but that was easy to protect against with a firewall. The attacker of today has learned from the lessons of business today and has new tricks that they are employing. When you buy software today you no longer go to a store you go online. Usually you have three sometimes four websites from which to choose. When you need information about something you no longer go to the library, you go to your library's web page or your favorite search engine and query the topic, getting thousands of hits. How do we know these sites we are going to are safe? Attackers have figured out how to clone sites, compromise sites to their own bidding, post sites of their own for malicious use, and to capture traffic going to and from sites. These are only a few of the tricks they have. When an attacker takes control of a site they have the tools to capture your data, plant code on your system, send you to another location, or cause your system to perform in a specific manner. All depending on how aware you are and how willing you are to go along with the attackers wishes. The successful attacker will never let you know that you are on a malicious site. Do you think you could spot it? According to Sophos Labs, the first quarter of 2007 had close to twenty-four thousand new threats identified on the web. Of those seventy percent were on legitimate web sites. White Hat Security recently put out their 2008 website vulnerability report and reported that in their survey sixty-five percent of the sites reviewed had cross-

site scripting vulnerabilities. Many experts feel that these are the most difficult to detect if they can be spotted at all without looking at the code.

We stand out in the crowd. Attackers are after information. They want data that can be profitable to them. Healthcare is all about data. There is an entire law, HIPAA, written specifically about that data. Not only do healthcare organizations possess the data needed for identity theft: social security numbers, names, addresses, age, date of birth; they also have other personal data about health, family, personal history. All of this information has a marketplace from which we need to protect it. Ironically as the guardians of that information you would think we would be experts in the field. We are not. White Hat, again referencing their 2008 security survey, points out that two industry pillars that have more web based vulnerabilities than others are IT and Healthcare. This sword slices two ways. First is the obvious of checking you own applications. But the other is checking our resources. How often are we out searching the web for a technical resource? How often are our nurses searching the web for continuing education material? This report from White Hat is telling us is that we are more susceptible to hitting a site subject to vulnerabilities. Whether using the web for work or play, many of the sites we are hitting may fall into in to Sophos Lab's seventy percent of compromised sites.

We need to know what we are protecting against and how to protect against it. Every year IC3, the Internet Crime Complaint Center, publishes a report on the consensus of the nature of the complaints they received over the past year. Most for 2007 telling was that despite the fact that the number of reported crimes had dropped from 2006 to 2007, the dollar amount of damage had increased. The nature of crime being conducted over the past year fits with what we have been talking about thus far; it is much more personal and lays the ground work for future attacks. The top three types of crime reported to the IC3 were: Auction Fraud, non-delivery, and Confidence Fraud. All of these would involve some exchange of personal information as in the form of a phishing attack. Most would open the opportunity for perpetrating other opportunities onto a system, such as a back door or code injection for bot net harvesting.

Is this is what we are protecting against? If this personal data is what they are harvesting for it would it not be easy to avoid attacks when looking for medical information or technical information on the net. How often do you go to a site and fill in a request form for a white paper? How often do you go to a site and fill out a form for a download? Any of these could be harvesting for an attack. This still does not answer how to defend against the attacker while still sustaining business. I don't know that there is an answer beyond best practice; beyond knowing how to identify bad URL's and suspicious content on web sites. We need to know how to spot when we have been directed away from the site we intended to be working with. Some of the responsibility needs to be placed on the vendors and web hosting facilities as well. With constantly changing web sites, companies need to strive to have a standard corporate look so that surfers know when they are on their page. Smart Internet use combined with sound security practices: intrusion protection on the host and network, firewalls, anti-virus, data loss prevention measures, and encryption in place offers a starting place for fighting the battle against attackers and their goal of getting our data.

References:

1: Grossman, J., "White Hat Website Security Statistics Report", <http://www.whitehatsec.com>, 2008.

2: Richardson, R., "2007 CSI Computer Crime and Security Survey", <http://goCSI.com>, 2007.

3: The National White Collar Crime Center, Bureau of Justice Assistance, Federal Bureau of Investigation, "2007 Internet Crime Report", <http://security4all.blogspot.com>, 2007.

4: <http://www.sophos.com>