2010 Security Predictions

by Corey Nachreiner, WatchGuard® Senior Security Analyst, CISSP

At the start of each new year, the WatchGuard LiveSecurity team releases its annual list of Security Predictions, because we know having an idea of what type of threats you can expect in the coming year helps you plan your defenses accordingly. And frankly, it's also kind of fun for us to gaze into an imaginary crystal ball and try to predict the future. This is how I see it.

SOCIAL NETWORKS: THE #1 MALWARE SOURCE – Last year, I predicted that the web was the battleground and social networks would get ugly. Both those predictions proved true. This year's threat is no different – just more specific. Social networks have in fact become so ugly that they will be the #1 source of malware infections. Why? Neilson Online says social networks have become more popular communication tools than email. Also, social networks by their very nature are gathering places, which tends to imply increased levels of trust. Finally, social networks leverage complex, Web 2.0 technologies that can suffer serious security vulnerabilities. When you add those factors together, it's no wonder that social networks will become to malware what email used to be to the virus; the #1 source of infection.

THIRD-PARTY PROGRAMS GET PWNED – OS vendors have fixed most of the obvious flaws so the code in their popular client applications for web browsing and email is more secure, and the patch cycle is well-established – even automatic. So where are the attackers going to turn? Expect them to move on to the next layer of software and target popular third-party apps in 2010, including Adobe Flash, Sun Java, and the ubiquitous Adobe Reader. Hackers realize that, unlike the OS folks, not all third-party software vendors have gotten the security patch cycle down yet. That leaves them with a nice ripe target to exploit. In 2010, I recommend you make a concentrated effort to keep the third-party software on your computer up-to-date; otherwise attackers *will* use these programs against you.

GOVERNMENTS WILL CREATE SECRET ATTACK BOTS – I expect most major governments to secretly build their own botnets for use in cyber-warfare against other countries and malicious entities this year. Furthermore, they will build these botnets by sneaking trojans onto citizens' computers! Sound crazy? Well put on your tinfoil hat and stay with me as I explain my rationale.

The power of botnets scares the bejesus out of governments. They've seen botnets successfully leveraged in cyber-attacks against countries like Estonia and Georgia and they recognize a classic asymmetrical threat (that is, when a single person or entity has way more power than they technically ought to). So where's my proof? It's everywhere, if you look close enough. All through 2009, governments announced their plans to create cyber security attack teams of one sort or another. Countries like the US, China, Russia, the UK, France, Israel, and Korea have all been reported to have instituted cyber warfare programs with the means to launch cyber attacks. While I doubt governments will continue to publicly talk about their military botnets, don't be surprised to hear rumblings about governments launching secret cyber warfare attacks in 2010.

SMART PHONES GET HAMMERED – We might as well call smart phones mini computers. A smart phone is simply a mobile phone that has all kinds of extended PC-like services, such as web browsing, email, and sometimes even word processing. In fact, many of these smart phones run light versions of the same operating systems that we use on our full computers. So why will the increase in smart phones result in a real world mobile phone attacks? Simply put, smart phones increase your phone's attack surface. Now add to this scenario the number of smart phones in use – something you can easily observe when taking any form of public transit these days. Everyone seems to have an iPhone, Blackberry, or Droid in hand. Combine the increasing market share of smart phones with all the attack surfaces they offer, and you have a hacker's dream. I predict that *every* popular smart phone will suffer at least one attack during 2010.

DATA LOSS PREVENTION MAKES BIG GAINS – Headlines in 2009 were full of high-profile data breaches that affected governments, businesses, and schools. They reminded us that sensitive data is our most important asset, yet we tend to spend more time securing our applications, servers, and environments than protecting the actual data itself. This will change in 2010 as technologies that directly protect data – things like local hard drive encryption and DLP (data loss prevention) solutions – are more frequently adopted by SMBs.

WINDOWS 7 SUFFERS CRITICAL ZERO DAY VULNERABILITY – Administrators almost uniformly hated Windows Vista, despite its enhanced security features. On the other hand, people have raved about Windows 7 since its early release candidate was available, even though Microsoft reversed some of Vista's security capabilities. With the hole left by Windows Vista, administrators will adopt Windows 7 in record numbers and this accelerated adoption rate paints a big fat target on the new OS. Between its huge popularity, and slightly decreased security, I expect at least one critical, zero day Windows 7 exploit to surface in the next 12 months. Hackers are already scouring Windows 7, looking for chinks in its armor. My advice: don't let a patch go by.

CLOUD COMPUTING: HALF HAVEN, HALF STORM – By now everyone has heard of the power of the cloud. The cloud can save your business time, money, and resources – heck, it can probably even do your laundry. However, behind this industry buzzword lays some pretty serious security implications. Can you trust cloud vendors to protect your sensitive data? Can we secure virtual environments? How can you comply with security and privacy regulations when your sensitive data resides somewhere in the cloud? In 2010, I expect at least one major cloud service security breach, which will bring some of these security issues to a head.

On the other hand, cloud-based security solutions will thrive in 2010. Despite the potential insecurities posed by cloud computing, security vendors have found ways that they can leverage the cloud to provide more robust and dynamic security services. I predict that most security vendors will have cloud-based security solutions in 2010 that will significantly help protect our networks.

SIGNATURE-ONLY SOLUTIONS CRUMBLE AS MALWARE GOES BALLISTIC – This prediction is simple. New malware variants have grown exponentially over the past three years, and signature-only solutions can't keep up. In 2009, PandaLabs identified over 25 million new malware variants. To put this in perspective, they'd only previously identified 15 million unique variants during their entire 20-year history. This perfectly illustrates why signature-only malware detection solutions will crumble under the pressure of malware in 2010. This doesn't mean signature solutions are worthless, but you need to make sure to combine them with non-signature solutions if you want to survive the malware deluge that's coming.

MAC THREATS DOUBLE – Most Mac fanatics think their platform of choice is bulletproof against malware. Yet, in 2009, Apple fixed hundreds of vulnerabilities in its OS and supporting products and Apple users began to see increased examples of Mac malware (like DNSchanger variants). Making matters worse, Apple's products are making gains in market share. These factors will entice both security researchers and black hats alike to focus more heavily on vulnerabilities in the Mac platform. Mac users won't want to hear it, but expect to see twice as many Mac threats in 2010.

POISONING THE INFORMATION WELL – Over the years, bad guys have discovered many ways to poison the results of popular search engines. They leverage these SEO (search engine optimization) techniques to place their malware links prominently among the results of popular searches. I expect major SEO poisoning attacks to surface in 2010, and I suggest you remain wary of your web search results.

WatchGuard Technologies provides an extensive family of network security products to help you secure your network from zero day threats, prevent unauthorized data from leaving your network, filter spam, block social networking sites, prevent malicious intrusions, integrate in-the-cloud security services, and much more. For more information, contact your reseller or visit us at www.watchguard.com.