WatchGuard's 2013 Security Predictions

If 2011 was the year of breaches, 2012 was the year cyber security went mainstream. Hacking and information security (infosec) used to be topics reserved for specialists. And while security professionals have long understood the scope and risk of cyber threats, average computer users and general IT staff didn't – often assuming their organizations weren't big enough targets to worry about. However, recent costly and public security breaches have changed that perspective.

The increased awareness is good news, and much needed. As hacktivists, organized criminals, and even nation-states continue to figure out how to leverage cyber space for fun and profit, their attacks will continue to evolve. So as the cyber arms race continues, please join us in our annual prediction exercise. It is our hope that these predictions will help you prepare your network defenses for a safe and secure 2013.

Malware Enters the Matrix through a Virtual Door

Today, organizations of every size leverage hardware virtualization in some way, whether directly within their own environments or via cloud services, which rely on virtualized environments. Even mobile devices are starting to use virtualization to secure sensitive data in sandboxed, contained environments. While there is nothing wrong with adopting this innovative technology to improve our businesses, most of us have not spent enough time securing virtualized environments.

Cyber attackers are aware of this unbalance, and will definitely exploit it. Already we're seeing malicious code that can recognize when it's running in a virtual system and act accordingly. Last year we had the first real-world instance of malware that actually sought out virtual machines and infected them directly. In 2013, expect to see attackers create even more VM-targeted malware. It will be designed to take advantage of weaknesses found in many virtual environments, while attempting to avoid virtualized automatic threat detection systems.

It's Your Browser - Not Your System - that Malware Is After

Traditional malware tends to infect the OS. Typically, it runs as an executable program, and modifies various boot parameters to ensure it runs every time you turn on your computer. Now, a new type of malware has emerged. Sometimes called Man-in-the-Browser (MitB) malware or browser zombie, it arrives as a malicious browser extension, plugin, helper object, or piece of JavaScript. It doesn't infect your whole system; instead it takes complete control of your browser and runs whenever you surf the web.

Cyber criminals have realized two things:

1. With our increased adoption of cloud services (like online banking) a great deal of personal, private, and sensitive data passes through our web browser.
2. Many antivirus solutions, which are focused on catching more traditional malware, aren't as effective at detecting these browser-based infections.

As a result, we expect to see a steep rise in browser-infecting malware in 2013.

Strike Back Gets a Lot of Lip Service, but Does Little Good

"Strike back" refers to launching a counter-offensive against cyber hackers. This can mean filing lawsuits, launching cyber espionage campaigns to gain intelligence about our adversaries, or even launching cyber attacks (sometimes automatically) against networks we think have attacked us. Most of us can appreciate the frustration of having little or no reparation against those who attack our networks and steal our data. This is why strike back will be a major topic of discussion in the IT security community in 2013, and we even expect to see a few companies create strike back solutions.

However, there's a problem with strike back. The nature of cyber crime makes attribution extremely difficult. Criminals leverage proxy servers to bounce attacks through many systems. They gain control of victim computers and leverage them as malicious zombies in their attacks. Advanced attackers sometimes plant "false flags" into their malware, hoping to trick us into thinking someone else is behind the attack. All the while, these digital attacks bounce through many different countries, making jurisdiction a nightmare. As satisfying as "strike back" may sound, counter-attacking IP addresses we believe have attacked us will – more often than not– just take out some unsuspecting victim's computer, and likely break local laws in the process. In the end, strike back will cause more trouble than it's worth, and probably won't be implemented in most organizations.

We'll Pay for Our Lack of IPv6 Expertise

We find ourselves in a strange dichotomy. On one hand, the IT industry – especially in the US – continues to be slow at intentionally adopting IPv6 into their networks. At the same time, most new devices ship IPv6-aware and can create IPv6 networks on their own, whether or not you're ready. As a result, many IT professionals don't yet have a deep understanding of IPv6's technicalities, yet they have IPv6 traffic and devices on their networks. This also means most administrators haven't implemented any IPv6 security controls.

This is fantastic news for attackers looking to exploit unprotected weaknesses. Next year, expect to see an increase in IPv6-based attacks and IPv6 attack tools. At the very least, we expect a marked increase in IPv6 DDoS attacks and IPv6 device scans.

Android Pick Pockets Try to Empty Mobile Wallets

Three general mobile trends contribute to this prediction:

a) Mobile malware is skyrocketing! Every malware detection vendor agrees they have seen exponentially more mobile malware in 2012. Tablets and smartphones are getting infected, and sensitive data is being stolen. If you download "free" games from unsanctioned mobile markets, you have a high chance of infection.

b) Cyber criminals are targeting Android devices more than any other. This has less to do with the Android platform being less secure than others, and more to do with platform's openness. Google allows Android devices to download, or side-load, applications from anywhere, not just their legitimate Google Play marketplace. You have much more choice and control as a consumer, but it's easier for bad guys to get poisoned software on your mobile device. iOS devices, on the other hand, can only get software that Apple has aggressively vetted. (That said, jailbroken iOS devices are much less secure.)

People are increasingly using mobile devices for online payments, and even as a second token of authentication (SMS) in more secure payment interactions. More importantly, many vendors, including Google, are starting to launch Mobile Wallets, which use NFC and other technologies to basically attach credit cards to your mobile phone; allowing you to swipe your mobile phone to make payments. Researchers and attackers alike have already started looking into technical weaknesses that may allow attackers to pilfer money from these Mobile Wallets.

Based on these three factors, we expect to at least see one vulnerability, even if just a proof-of-concept, that allows attackers to steal money from Android devices. If you're adopting a BYOD policy at your organization, this is another factor you may want to consider.

An Exploit Sold on the "Vulnerability Market" Becomes the Next APT

Vulnerability markets or auctions are a worrisome new trend in information security. Some so-called "security" companies are selling zero day software vulnerabilities to the highest bidder, while NOT disclosing them to the vulnerable vendor. The only motivation for this seems to be greed. Artificially inflating the value of vulnerabilities does nothing to help secure the victims who use that software, and selling exploits to the highest bidder without disclosing them just puts tools into the hands of potentially evil actors who obviously want to leverage them in cyber attacks.

They claim to "vet" their customers, and only sell to NATO governments and legitimate companies. However, it's easy to imagine exceptions if the price is right. Even selling vulnerabilities to a government without disclosing them allows the government to potentially leverage the flaws against citizens. These vulnerability auction houses threaten everyone's information and network security, and should be considered black markets. At the very least, these organizations are encouraging and aiding the escalation of cyber espionage between nation-states.

Though it will be hard to prove, we expect one of these auctioned off zero day exploits to show up in some majors targeted attack this year.

Finally! Important Cyber Security-related Legislation Becomes Law

It's clear that the US government is very concerned about cyber security (as are other governments). According to some, adding the term "cyber" to your project is the best way to get funding in Washington D.C. right now. For the past few years, the government has been trying to pass various cyber security bills that give the president and other government agencies some control over what happens in the event of cyber attack on US infrastructure. The government also wants more cooperation among private infrastructure organizations and US intelligence agencies. At the same time, many are looking for the government to enact more detailed cyber crimes laws, which may help us better prosecute digital crimes. Finally, some organizations are lobbying for tougher digital IP enforcement, which privacy advocates often oppose. These differing issues seem to be what is making it difficult for the US to pass new cyber legislation, yet this is all coming to a head.

In 2013, you should expect the US government to pass at least one new cyber security act, and it will likely affect some private organizations.

A Cyber Attack Results in a Human Death

Consider the world we live in. Every day our lives become more and more dependent on computing devices. They're embedded in the infrastructure that provides us with energy, water, and easy access to finances. They're in our cars, our phones, our TVs, and even our medical devices. What's more, we're actively trying to connect all these devices to one another.

Now add the fact that we often treat security as an afterthought with technology. We design innovative technical systems to do something cool and useful, but forget to take into account how malicious actors might misuse them. As a result, we are finding some of our most critical systems suffer from fundamental vulnerabilities, and don't even leverage basic defenses.

Then add the human factor. We live in a world where criminals, hactivists, and even nation-states are actively launching cyber attacks. Computer malware has destroyed physical equipment; proving digital attacks can have real-world impact. Recently a researcher even showed how to wirelessly deliver an 830 volt shock to an insecure pacemaker. In short, digitally dealt death is not only possible, it's plausible.

We'd like to think humans are inherently good, and even if these sorts of life-threatening digital attacks are possible, no one would hate someone enough to exploit them. Yet we live in a politically charged world, and history shows us that nations tend to leverage any weapons they can. We hope we're wrong, but perhaps 2013 will deliver the first ever cyber casualty.

Conclusion

If you take anything away from our yearly security predictions, we hope it's the realization that as computer and network attacks continue to evolve, so too must your defenses. Here's another timely tip. According to many sources, the great majority of security breaches are due to misconfiguration of security controls, not the lack of them. In 2013, WatchGuard will continue focusing on improving our defenses, and in making our technology even more manageable and easy to use, so you have the latest protections *and* know how to use them effectively.

WatchGuard Technologies provides an extensive family of network security products to help you secure your network from advanced attacks, stop sensitive data from leaving the network, block social networking sites, prevent malicious intrusions, integrate in-the-cloud security services, and much more – all with unprecedented visibility into network security activity. For more information, contact your reseller or visit us at **www.watchguard.com**.