2011 Security Predictions
Compiled by Corey Nachreiner, WatchGuard® Senior Security Analyst, CISSP

2011 will be a year like no other. Expect to see a wider array of network threats and a repositioning of IT priorities. The good news is that new security tools will deliver greater levels of protection than ever before. Here’s what WatchGuard’s team of security analysts see on the threat landscape for the coming year.

THE CYBERWAR IS ON! – Last year we warned that government or state-sponsored digital attacks – aka cyberwars – were coming. In 2011, we believe cyberwar skirmishes will occur almost daily, whether the average citizen is aware of them or not.

Many believe the Stuxnet worm is a perfect example of a politically-motivated attack, likely created by a state-funded team of hackers. The amazingly advanced, highly targeted worm primarily infected Iranian uranium manufacturing facilities with the sole purpose of quietly disrupting the uranium enrichment process. Furthermore, recent political document leaks also suggest the headline-grabbing Aurora attack on Google was orchestrated by China’s Politburo. For every attack you hear about, remember there are likely others that are so incredibly sophisticated, they remain undetected.

“APT” IS ACRONYM OF THE YEAR – Heard anyone mention “APT” (advanced persistent threat) yet? You will in 2011. Think of APTs as the doomsday malware that security researchers have always been worried about. Although there is no single, standard definition, APTs have these things in common:

- They apply the most advanced attack, infection, and malware propagation techniques known – in fact, they often employ techniques the industry hasn’t become aware of yet.
- APTs are designed to stay hidden within a victim network or host for a long period of time – typically by using strong rootkit technology, cleaning logs, and slow, quiet Command and Control channels.
- They tend to have a specific, targeted goal in mind. For instance, they might be designed to slowly steal intellectual property from a specific business.

In reality, APT is just a new way to say very advanced malware attack; so our prediction has two parts. First, we expect security experts to jump on the term and over-use it throughout 2011. That said, we do expect to see many more treacherous attacks this year that fit the APT category.

VOIP ATTACKS BECOME THE NORM – Because VoIP leverages relatively new technologies that haven’t been fully explored from a security perspective, researchers have warned that attackers would begin targeting VoIP solutions. In 2011, we expect to see full-force VoIP attacks.

Just in the last few months, VoIP scans and attacks have increased significantly. Some of this has to do with the public availability of VoIP attack tools, such as SIPVicious. Moving forward, brute-force and directory traversal class attacks against VoIP servers will be as common as they previously have been against email servers.
PERIMETERS SHRINK AND HARDEN – This prediction actually comes from some SANS security people, but we whole-heartedly agree. Many security researchers have rightly pointed out that our networks have become more mobile, and that we need protection outside our perimeter to help ward off threats to mobile resources. While that’s true, it doesn’t mean that the perimeter disappears. In fact, we expect to see organizations concentrate their perimeter security around the assets that matter most – their data – which means we will concentrate primary perimeter defenses around our data centers.

CARS HACKED IN 2011 – Hackers are always trying to find unexpected ways to infiltrate computing devices, successfully infecting network printers, routers, and even gaming consoles with malware. Cars are no exception. In fact, lately cars have become more “connected” than the average computer – with built-in Bluetooth, 3G internet, GPS, OnStar, and dashboard computers. This doesn’t even take into account the actual internal computers that our cars use to run. Security researchers have definitely noticed this and are writing about various security issues affecting car electronics.

We expect more attackers to get into the car hacking game, which is especially worrisome if you consider the potential for physical harm via a car attack/hack.

FACEBOOK DANGERS MAKE US NOSTALGIC FOR MALICIOUS .EXE ATTACHMENTS – Remember when email attachments were the biggest threat we faced? Most of the malware infecting our computers arrived as an executable attachment that proxy firewalls could outright block. Now most attacks come from the web. And one site poses the largest risk of all – Facebook.

When you combine Facebook’s culture of trust, the many potential technical security issues (Web 2.0, API, etc), and its 500 million users, you have a huge and attractive playground for computer attackers and social engineers.

We believe links on Facebook will become the common threat vector that attachments in email were years ago.

MANUFACTURER-DELIVERED MALWARE KEEPS GROWING – It used to be you could buy a laptop, a storage device, or even an electronic picture frame and expect the thing to be malware-free. No more!

Through 2010, there have been reports of many popular products arriving with infections out-of-the-box. In some cases, big companies have even embarrassed themselves by handing out such infected devices at well known security conferences...Oops!

Next year, we expect this “manufacturer-delivered malware” trend to get even worse. No one has proven whether or not these manufacturer infections are accidental or intentional. Considering where some of the gear is made, and the increase in political cyberwar, one could easily argue the latter. In any case, we plan to malware-scan all of our new electronic purchases in 2011, and we recommend you do the same.
DLP FOR INTELLECTUAL PROPERTY PROTECTION, NOT JUST COMPLIANCE – Many countries are shifting toward creating more and more digital products rather than manufacturing physical things. In order to ensure a strong economy, we need to find ways to protect these digital assets. Unfortunately, by its very nature, a digital product is hard to protect. It’s easy to make perfect copies of digital assets. Same with “ideas” or intellectual property, once it’s out, anyone can use it.

With the shift from physical to digital production, as well as the economic crisis, we believe governments will get much more involved in protecting intellectual property this year. New laws and regulations will force more organizations to implement stronger IP protection, and we’ll see new security technologies crop up to help keep our data or IP from being stolen, or used in an unauthorized fashion. In 2011, expect to employ even better data loss prevention mechanisms than you already do.

DETECTION TAKES A FRONT SEAT – When implementing security controls, most organizations focus more on protection and prevention than on detection and analysis technologies. This will change in 2011.

As increasingly advanced threats surface, administrators will realize that even the best prevention technologies cannot stop malware from entering the network through a simple user mistake, or a tiny hole in the security infrastructure. This realization will help them recognize that it is just as important to be able to detect and analyze a threat that has already entered the network, as it is to try and prevent it from entering. As such, technologies will become very popular in 2011 that can:

a. Increase network visibility
b. Help identify threats already infecting your network
c. Correlate all aspects of a network attack
d. Help with forensics

ONLINE ‘EXPLOIT STORES’ DELIVER MALWARE AS A SERVICE (MAAS) – We live in a world of software convenience. Need a new app to get traffic updates on your phone? No problem. Just log onto the app store and download it in seconds. Want to watch the latest DVD release immediately? Great. Go to Microsoft’s Zune store and stream a copy for a marginal price. Today, if you need a commercial software product, you can have it in seconds. We expect the same will happen for attack software in 2011.

Over the years – as hacking has become more organized and criminal – the hacker underground has already started mimicking commercial markets by releasing pre-packaged, black-market exploit kits. You can already buy web attack kits, pre-packaged botnets, and ready-to-go malware from underground websites and forums. You can even buy service contracts to get the latest zero day threats. In 2011, we think the criminal underground will take this a step further by creating a convenient “app store” for malware. Script kiddies are one PayPal click away from their own botnet.

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.

©2011 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, and LiveSecurity are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part. No. WGCE66723_011111