



WatchGuard Unveils Top 10 Security Predictions for 2011

Sydney, 17 January 2011 - WatchGuard Technologies, a global leader of business security solutions, has unveiled the following top ten security predictions for 2011:

10) "APT" Becomes Security Acronym of the Year Heard of "APTs" (advanced persistent threats) yet? You will in 2011. 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
- 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.
- In reality, APT is just a new way to say very advanced malware attack; so this prediction has two parts. First, WatchGuard expects security experts to jump on the term and over-use it throughout 2011. Secondly, WatchGuard expects to see many more treacherous attacks this year that fit the APT category.

9) Cyberwar Escalates Cyberwar skirmishes will occur almost daily. 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. Government, infrastructure and financials will need to be hardened to handle the next onslaught of web attacks.

8) VoIP Attacks Grow In 2011, WatchGuard expects 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.

7) Perimeters Shrink and Harden Many security researchers have rightly pointed out that networks have become more mobile, and that businesses need protection outside the perimeter to help ward off threats to mobile resources. While that's true, it doesn't mean that the perimeter disappears. In fact, WatchGuard expects to see organisations concentrate their perimeter around the assets that matter most - data - that results in concentrating primary perimeter defences around data centres.

6) Cars Hacked in 2011 Hackers are always trying to find new ways to infiltrate computing devices, cars are no exception. Because cars have become more "connected" than the average computer - with built-in Bluetooth, 3G internet, GPS, OnStar, and dashboard computers - WatchGuard expects more attackers to get into the car hacking game, which is especially worrisome considering the potential for physical harm via a car attack/hack.

5) Facebook and Other Social Media Become Lead Threat Vectors Remember when email attachments were the biggest threat businesses faced? Most of the malware infecting PCs 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, computer attackers and social engineers have a huge and attractive playground. WatchGuard believes links on Facebook will become the most common threat vector, similar to how attachments in email were years ago.

4) Manufacturer-Delivered Malware Keeps Growing It used to be that one 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. This year, WatchGuard expects this "manufacturer-delivered malware" trend to get even worse. WatchGuard recommends that businesses scan all of our new electronic purchases before connecting to any corporate networks.

3) DLP for Intellectual Property Protection WatchGuard believes that governments around the world will become more involved in protecting intellectual property this year. New laws and regulations will force more organisations to implement stronger IP protection, resulting in new security technologies to help keep data and IP from being stolen or used in an unauthorised manner. In 2011, expect to employ even better data loss prevention mechanisms than those currently available.

2) Detection Becomes a Priority When implementing security controls, most organisation focus more on protection and prevention than on detection and analysis. This will change in 2011. As increasingly advanced threats surface, administrators will realise that even the best prevention technologies cannot stop malware from entering the network. This realisation will help them recognise that it is just as important to be able to detect and analyse a threat that has already entered the network, as it is to prevent it from entering. As such, technologies will become very popular in 2011 that can:

- a. Increase network visibility
- b. Identify threats already infecting business networks
- c. Correlate aspects of a network attack
- d. Help with forensics

1) Malware as a Service (MaaS) Over the years, as hacking has become more organised and criminally controlled, the hacker underground has started to mimic commercial markets by releasing pre-packaged, black-market exploit kits. One can already buy web attack kits, pre-packaged botnets, and ready-to-go malware from underground web sites and forums. For 2011, WatchGuard predicts that the criminal underground will take this a step further by creating a convenient "app store" for malware, which means that script kiddies will be just one click away from instantly unleashing their own botnet."2011 stands to be a dynamic year for network security as criminals and hackers take threats to new levels," said Eric Arrestad, Vice President at WatchGuard Technologies. "Given how new threats are constantly evolving, WatchGuard remains ever vigilant in staying one step ahead of these threats, which gives our customers unparalleled protection for their networks, applications and data."

About WatchGuard Technologies, Inc.

Since 1996, WatchGuard Technologies, Inc. has been the advanced technology leader of business security solutions, providing mission-critical protection to hundreds of thousands of businesses worldwide. The WatchGuard family of wired and wireless unified threat management appliances, messaging, content security and SSL VPN remote access solutions provide extensible network, application and data protection, as well as unparalleled network visibility, management and control. WatchGuard products are backed by WatchGuard LiveSecurity Service, an innovative support, maintenance, and education program. WatchGuard is headquartered in Seattle and has offices serving North America, Europe, Asia Pacific, and Latin America. To learn more, visit www.watchguard.com