2013 Security Predictions

While cybercriminals are often opportunistic, we believe that in 2013 the ready availability of testing platforms— some with money back guarantees from their sponsors—make it all the more likely malware will continue to slip through single-tier traditional security systems. As a result we believe we will see more attacks where attackers hold long-term, high impact access to businesses. In response, a renewed focus on layered security and detection across the entire threat lifecycle, not just the point of initial entry, is likely to be a significant theme in the coming year. We also think the following five trends will factor into the IT security landscape in 2013.

Basic web server mistakes

In 2012 we saw an increase in SQL injection hacks of web servers and databases to steal large volumes of user names and passwords. Targets have ranged from small to large enterprises with motives both political and financial. With the uptick in these kinds of credential-based extractions, IT professionals will need to pay equal attention to protecting both their computers as well as their web server environment.

More "irreversible" malware

In 2012 we saw a surge in popularity and quality of ransomware malware, which encrypts your data and holds it for ransom. The availability of public key cryptography and clever command and control mechanisms has made it exceptionally hard, if not impossible to reverse the damage. Over the coming year we expect to see more attacks which, for IT professionals, will place a greater focus on behavioral protection mechanisms as well as system hardening and backup/restore procedures.

Attack toolkits with premium features

Over the past 12 months we have observed significant investment by cybercriminals in toolkits like the Blackhole exploit kit. They've built in features such as scriptable web services, APIs, malware quality assurance platforms, anti-forensics, slick reporting interfaces, and self protection mechanisms. In the coming year we will likely see a continued evolution in the maturation of these kits replete with premium features that appear to make access to high quality malicious code even simpler and comprehensive.

Better exploit mitigation

Even as the number of vulnerabilities appeared to increase in 2012—including every Java plugin released for the past eight years—exploiting them became more difficult as operating systems modernized and hardened. The ready availability of DEP, ASLR, sandboxing, more restricted mobile platforms and new trusted boot mechanisms (among others) made exploitation more challenging. While we're not expecting exploits to simply disappear, we could see this decrease in vulnerability exploits offset by a sharp rise in social engineering attacks across a wide array of platforms.

Integration, privacy and security challenges

In the past year mobile devices and applications like social media became more integrated. New technologies—like near field communication (NFC) being integrated in to these platforms—and increasingly creative use of GPS to connect our digital and physical lives means that there are new opportunities for cybercriminals to compromise our security or privacy. This trend is identifiable not just for mobile devices, but computing in general. In the coming year watch for new examples of attacks built on these technologies.

The last word

Security really is about more than Microsoft. The PC remains the biggest target for malicious code today, yet criminals have created effective fake antivirus attacks for the Mac. Malware creators are also targeting mobile devices as we experience a whole new set of operating systems with different security models and attack vectors. Our efforts must focus on protecting and empowering end users—no matter what platform, device, or operating system they choose.