WatchGuard Notes Top Online Threats Relating to the 2010 World Cup

Online threats relating to the 2010 World Cup increasing

Sydney, 10 June 1010 – WatchGuard, a global leader of business security solutions, sees an explosive growth of online threats relating to the 2010 FIFA World Cup, which runs in South Africa from June 11 to July 11. As a precautionary note, IT administrators should be aware of these World Cup related threats and take appropriate action to mitigate their effects.

Key threat findings:

Spam – WatchGuard sees a global increase in spam using “World Cup” as part of the spam theme. In addition to traditional marketing spam, WatchGuard also sees an increase of malicious spam – spam with pernicious payloads, such as spyware, or spam that lures users to malware-laden websites.

Spear Phishing – Unlike spam, spear phishing attacks are directly targeted to small populations with socially engineered messages in order to entice their victims to open an executable or click to a site that harbors malware. Here, WatchGuard sees a multitude of spear phishing threats targeting 2010 World Cup ticket holders and related World Cup businesses.

PDF attacks – Recently, vulnerabilities associated with PDF documents have surfaced. Administrators may want to consider using PDF file blocking features for the next 30 days, or until a patch is issued, in order to protect against these new “zero-day” threats.

SEO Poisoning – Search engine optimisation (SEO) threats have allowed malicious websites to be highly ranked in search strings relating to the World Cup. As poisoned websites, they pack a malware punch. This can be defeated by administrators using up to date gateway anti-virus and intrusion prevention solutions.

Loss of productivity – Administrators may want to use traffic shaping tools and other forms of content filtering to limit or eliminate access to World Cup related sites and online content.

Social networks – Lastly, WatchGuard warns of malware that may be propagated through popular social networks. Content filtering and file blocking solutions should be tuned to reduce threats related to social networks and the World Cup.

“Cybercriminals are always looking at new ways to lure businesses and people into dangerous places, and often they use major events as tools to snare their victims,” said Scott Robertson, Regional Director ANZ, WatchGuard Technologies.

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 http://www.watchguard.com/