



Security Web 2.0: Open season for attackers?

The Web is quickly becoming a participatory medium – users contributing, communing, and building. The downside of this is a new slew of security threats, explains Blue Coat’s Director of Product Marketing, Sandy Hawke

For a number of years, the Web was a relatively one-dimensional experience characterised by the delivery of static HTML pages in a one-way client-server environment with little direct user involvement. The security threats were and are real. But Web 2.0 is a different animal. Web 2.0 is a participatory client server environment of social networking, bookmarking, media-sharing sites, blogs, wikis, P2P networking, AJAX-generated applications and RSS feeds. A world largely outside the IT department’s control.

The boundary between the trusted network and the Internet is quickly disappearing, leaving the corporate enterprise open to a new generation of threats that make previous ones seem benign. Take email. Several years ago, SMTP was the main vector for viruses and other malicious content. In Web 2.0, SMTP is no longer the carrier for the malicious payload. Instead, email only directs the unsuspecting user to a website, where the more dynamic HTTP can be exploited for nefarious purposes.

Today, many malicious attacks target the browser. Among other techniques, attackers can now manipulate the DNS protocol to mask a malicious website as legitimate in order to gain access to the corporate network via the user’s browser and virtually any information the user can access. A chilling possibility.

Web 2.0 is by definition dynamic, social and collaborative. Users supply the data that make many Web 2.0 applications and services what they are: Google Earth works because users interact with it, MySpace is only as great as the sum of its members, digg.com functions because users share their favourite articles, the blogosphere works because users blog. It is this very collaboration and openness that attackers thrive on. Users today share information in multiple venues – email was once the venue.

In this open environment, monitoring for corporate data leakage and unwanted content becomes a Herculean task. The danger has increased in orders of magnitude. An email leaking corporate information has a limited reach and shelf-life (delete it and it’s gone). But sensitive data leaked into the blogosphere has the potential to do significant, long-term damage. Blogs are stored in searchable archives. Redirects to thousands of websites put data at the fingertips of anyone interested in the information. ►

As always, the challenge is balancing user expectations with corporate security. Users demand unfettered connectivity – email, IM, and video conferencing – and access to Web-based applications. More and more companies are outsourcing their mission-critical data (e.g. CRM systems) to web-based hosting infrastructures. These applications enable organisations to reduce IT administration costs and headaches associated with traditional, locally-hosted applications. But hackers have been quick to exploit vulnerabilities in Web applications.

For example, Web 2.0 has been especially good to phishing attackers. Phishing sites built using Rich Internet Applications (RIAs) appear so legitimate that even seasoned users and early-generation security solutions are fooled. Nomadic attack patterns make it almost impossible to track down the attackers.

Legitimate stand-alone RIAs are powerful because they offload most of processing to the client machine via a client engine that acts as an extension of the user's browser. This client executable can be used as a vector for malicious code. RIAs that use ActiveX plug-ins, a common RIA technique, are especially vulnerable to attack. (89% of browser plug-in vulnerabilities disclosed by Symantec in the first half of 2007 affected ActiveX plug-ins in Internet Explorer.)

Legitimate websites aren't safe any more either. Attackers can (and do) embed executable XML malware on popular sites; in 2006, computer experts found virus code embedded in MySpace pages. Streaming video is the next vector of choice. Imagine the effect of a Trojan horse embedded in one of YouTube's featured videos which, potentially, millions of unsuspecting users would view.

Very recently, the long-running Storm Trojan horse that has infected user machines via SMTP, made the jump to HTTP. Storm backers infected the website for the Republican Party in Wisconsin. Fortunately, the site's owners were able to remove the dangerous code within a few hours. Security experts estimate that as many as two million machines are part of the Storm botnet; its tentacles could reach into the tens of millions with the move to the Web. Blanket-blocking of legitimate sites is not the solution; arguably some of these sites fulfill legitimate business functions for some users.

If you think these problems are all consumer-related, think again. A group of companies in Israel were infected by a Trojan that copied sensitive emails to a group of criminals who then sold the emails to the victim's competitor.

SSL-encrypted websites also pose a threat. Most web security solutions don't inspect the SSL tunnel, which carries the encrypted data point-to-point, making SSL an effective vector for stealing data. Attackers also set up SSL-enabled web servers to appear legitimate to phishing victims. When the user receives an email and clicks through to what he believes to be his banking site, the familiar lock within his web-browser gives him a false sense of security.

SSL is also an effective ways of getting bots and Trojans past a corporate firewall and onto the trusted networks. Once a bot is installed, it forms botnets that use similar SSL sessions to leak sensitive data and other valuable content out of the corporate network. Most content filters and other security products fail to identify these attacks as they occur because they can't view the encrypted data so these sessions are allowed in and out of the network.

What can security professionals do to protect their enterprises?

First they must be able to scan legitimate websites in real-time for executable viruses and other malware. Blanket blocking is not the answer: many legitimate web-based business applications use executables to enrich the user experience. Security professionals must also be able to establish both broad and granular user-based policy controls over P2P applications such as IM and Skype, without hindering user productivity and application performance.

An understanding of phishing techniques is essential. Users should be blocked from posting data to high-risk sites (often defined to include sites previously unknown to block brand-new phishing sites) and sites with invalid SSL certificates. Finally, IT pros should exercise broad protocol control over RTSP, MMS, IM, SSL, and P2P applications so threats can be identified and blocked. Some of the more comprehensive web security solutions offer this level of functionality along with basic messaging, anti-virus and anti-spam filters. The key is to ensure a seamless, unfettered user experience. It's a tall order, but not an impossible one.

How enterprise security threats have evolved

Web 1.0	Web 2.0
Primitive phishing attacks	Evolved phishing attacks; RIAs and other techniques 'legitimise' phishing sites
Email-borne viruses	Email for social engineering, not malicious payload
Corporate data leakage via email	Corporate data leakage on blogs, social networking sites, etc.
Website defacements ('Hactivism')	Website infections (malware inserted into XML tags for financial gain)
'Clear text' malware	Malware 'hidden' within SSL-encrypted traffic