Preparing For The Emerging Threats Of HTML5 Content

A DCI (deep content inspection) solution is a must to protect your customers from the wave of threats that will come through this new Web content delivery standard.

By Hongwen Zhang, president and CEO, Wedge Networks

HTML5 has become a necessary transition for organizations in need of a new method for delivering content. Significant social networks and browsers, like Facebook, Google, YouTube and PayPal, have begun the transition to HTML5, not only transforming today's web structure, but also how content is being processed and presented. With HTML5, organizations will benefit from new functionalities that deliver richer media, increased online responsiveness, and allowance for a disconnected operation. However, HTML5 also triggers a common IT headache — security.

HTML5 Vulnerabilities

HTML5 provides a rich, responsive, and standardized Web application environment that enables trends like increased mobile access and dynamic cloud-based applications. Traditional security solutions are unqualified for these new dynamics as the introduction of HTML5 opens the door to new and unique malware passages that use cross-site delivery/communication, broader Javascript capabilities, and WebSocket protocol.

While safer than former versions, the fast uptake of HTML5 still undoubtedly requires a security solution that is able to tackle the new content packaging, transmission protocols and the growing number of malware delivery outlets. Without network protection that is cognizant of HTML5, an organization is defenseless against malicious codes carried through this channel. Forrester Research stated, "Firms are using more consumer-style Web applications… with 84% of firms increasing their use of Web applications." Organizations need to take back control of the Internet and Web infrastructure with a real-time and scalable solution that provides advanced information scanning techniques while enabling high network performance.

Hongwen Zhang

Dr. Hongwen Zhang is president and CEO of Wedge Networks, a provider of remediation-based deep content inspection for high-performance, network-based Web security.

Secure Against HTML5 Threats

To ensure an organization's network is secure without limiting the benefits presented by HTML5, organizations must implement security that is capable of DCI. DCI scans and understands the intent of all Web content (from simple coded threats to advanced malware hidden in large volumes of traffic). This level of inspection helps ensure that security services can detect and remediate malware in motion. A thorough DCI plan will mesh with the network and scan content that is packed in both existing and new standards. Additionally, a DCI solution will ensure the end user is fully secured. As a result, regardless of the end user's location and what they click on, their computing devices are secured.

WebSocket has recently become a powerful and convenient feature for many Web and content developers, these organizations can use WebSocket to transmit data for applications by using any payload without well-formed URL or HTTP headers. Unfortunately, the usefulness of WebSocket concurrently raises a vector for malware transmission. By implementing security capable of conducting DCI to WebSocket payload, the network will be protected against malicious attacks. A DCI solution can extract, scan, and prevent threats found in a WebSocket protocol, securing the transmission of data for any application.

Usability is the most crucial step in selecting a security solution for your network. The solution will allow high performance scanning throughput, prevent bandwidth bottlenecks, and end user latency. A slow and delayed system is inefficient and no longer acceptable in the business world; the purpose of a security solution is to fix problems, not generate new ones.