ScanSafe makes top web security predictions for 2007 - web threats eclipsing other attacks

Submitted by: Six Degrees Limited
Wednesday, 13 December 2006

For media enquires, contact:
Amanda Hassall or Marcus Edgar
Six Degrees Ltd
amanda.hassall@sixdegreespr.com or marcus.edgar@sixdegreespr.com
+44 (0)1628 480280

ScanSafe makes top web security predictions for 2007
- web threats eclipsing other attacks

Wednesday, December 13, 2006: London – ScanSafe, the leading global provider of Web Security-as-a-Service, today released its top eight web security predictions for 2007.

1. Web extends its lead over email as the threat vector of choice
Perhaps more than any other year, 2006 marked the ascendance of Web threats. In fact, unlike previous years that were marked by mass-mailing worms like MyDoom, Bagle and Sober, 2006 was the year when Web-based threats, most notably the Windows Meta File (WMF) Flaw, took centre stage – eclipsing the email threats.

A recent IDC survey of businesses also supports the notion that Web surfing has surpassed email as a threat vector. It found that up to 30 per cent of companies with 500 or more staff have been infected as a result of Internet surfing, while only 20 to 25 per cent of the same companies experienced viruses and worms from emails.

ScanSafe expects this trend to continue in 2007, with more and more threats moving to the Web.

2. Malware authors continue to target Web 2.0 sites making real-time scanning imperative
As more and more users go online to take advantage of Web 2.0 applications like social-networking sites, blogs, wikis and RSS feeds, malware authors are going to be right behind them. The explosion in the popularity and use of Web 2.0 sites has made them an irresistible target for malware authors. Early signs of this were evident in 2006. In August, the ScanSafe Threat Centre found that up to one in every 600 social-networking pages host malware and in recent weeks malware on Wikipedia, MySpace and YouTube have been exposed.

Web 2.0 user-contributed content means that the content on the thousands of URLs is constantly changing. Unfortunately, many traditional Web filtering solutions rely on URL databases and honeypots and therefore, are not in a position to keep the dynamic content that characterises Web 2.0 sites. In addition, traditional anti-virus solutions that require signatures will be slow to react to zero-day threats – threats that appears before a signature or patch is made available.

“Web 2.0 and the increasing shift toward Web services makes many existing Web filtering and Web-malware solutions ineffective,” says ScanSafe’s Product Manager, Spencer Parker. “The only way to keep up

with the latest Web-threats is to rely on a solution that actually scans the URL in real time every time it is requested versus just comparing it to a dated list of URLs."

And of mounting concern is the potential for abuse of AJAX and Web 2.0 applications. Cross-site scripting worms (XSS), for example that can insert malicious code into dynamically generated Web pages could allow an attacker to change user settings, access account information, poison cookies with malicious code, expose SSL connections and access restricted sites.

3. IM increasingly leveraged by hackers to send SPIM and malware
According to a survey by the ePolicy Institute, 31 per cent of employees use IM at the office, and 78 per cent of those users downloading free IM software from the Internet. However, only 11 per cent of organisations employ IM gateway/management software to monitor, purge, retain, and otherwise control IM risks and use. The same survey found that only 20 per cent of companies surveyed have adopted a policy governing IM use and content.

Spencer Parker, explains: "The threat has shifted from email communications to IM and Web-based applications. IM is too lucrative a target for malware authors to overlook. We expect to see a meaningful increase in spam over IM, or SPIM, as well as malware targeting IM in 2007."

4. Continued pressure on service providers to deliver clean bandwidth – including HTTP traffic
On November 28, the European Commission called for ISPs and regulators to do more in cracking down on spam, spyware and other malware. Regulators and others have long called for ISPs to take a more active role in providing clean bandwidth, in much the same way that water companies are required to provide clean water. ScanSafe anticipates that in 2007, ISPs will take a more active role pushing security into "the cloud" in an effort to deliver clean bandwidth.

"We believe 2007 is the year that more and more ISPs begin to push security solutions out into the cloud. We anticipate more and more ISPs will partner with managed security service providers to deliver clean bandwidth."

5. Zero-Day threats continue to grow, making the need for real-time Web scanning critical
ScanSafe reported zero-day threats accounted for between 10 -15 per cent of all threats it blocked in 2006. And 2006, the Windows Meta File (WMF) flaw, discovered in December 2005 was quickly exploited by hackers, underscore the increasing importance of the zero-day. For example, between December 30, 2005 and January 3, 2006, ScanSafe reported that the percentage of customers subjected to exposure to the WMF vulnerability increased from 6 per cent to 15 per cent.

Again, in September hackers were quickly able to exploit a Vector Mark-up Language (VML) vulnerability discovered in Microsoft's OS. Within days, the vulnerability resulted in exploits, including malware hosted on porn sites as well email lures driving users to compromised sites, including one Web page masquerading as a seemingly benign Yahoo! greeting card. This VML example is further evidence that hackers and malware authors are quick to take advantage of vulnerabilities to seed what are called zero-hour exploits – threats that appear before a patch or anti-virus signature becomes available.

"The day and age of solely relying on signature-based protection to provide protection from Web-based

threats is over. The sophistication of threats and the pace at which new vulnerabilities are exploited demands a multi-layered approach that supplements anti-virus signatures with heuristics and real-time scanning that detect zero-hour threats and deliver protection from them in the critical hours between the emergence of the threat the release of an anti-virus signature."

6. The death of the perimeter: remote and roaming users pose significant challenges to traditional notions of perimeter security

2006 was riddled with stories of security breaches resulting from mobile devices. Even more concerning is that according to the Business Performance Management Forum, 40 per cent of enterprises do not have policies to secure mobile devices and that IDC expects that the number of global mobile employees will grow beyond 878 million by 2009.

IT managers can no longer rely on out-dated notions of perimeter security, because there is no perimeter. Expect malware authors to continue to take advantage of improperly secured PCs of remote and roaming users.

7. VOIP emerges as a real threat vector

ScanSafe believes that in 2007, companies will begin to open up SIP gateways and make them accessible on the Internet. While this will result in lower costs for telephony, it will also open companies up to a wide variety of threats that are not necessarily being contemplated because many companies still don't perceive a VoIP phone as a "computer". The result is that both VOIP devices and servers will be subject to the same to same type of vulnerabilities as any other computer including denial of service attacks, theft of service, fraud and phishing attacks.

8. Vista and IE7

No list of 2007 Web security predictions would be complete without a reference to Vista and IE7.

Will Vista improve security for consumers? Probably. But it's less certain that it will do the same for corporate users because Vista will probably not see widespread deployment in enterprises in 2007 (Gartner) and because it is not designed for centralised management or reporting, meaning corporate users will remain the weakest link in the chain.

We saw a similar pattern when Microsoft released a "personal firewall" in Windows XP. While it certainly did help to protect users, it was not the panacea that some predicted would lead to the death of 3rd party security providers.

While Vista can block malware at the system level, it won't necessarily stop users from installing malware. Given the barrage of warnings and pop-ups, we expect that many users will simply disable the most relevant security features of Vista, negating any potential security benefit. In addition, any malware that leverages social engineering will likely trick users into installing it.

The net result for IT managers will simply be an increase in support calls and no meaningful decline in Web threats.

About ScanSafe

ScanSafe is the leading global provider of Web Security-as-a-Service, ensuring a safe and productive Internet environment for businesses. The easy-to-use service requires no hardware and delivers real-time, complete protection from the latest Web threats. ScanSafe's solutions keep viruses and spyware off corporate networks and allow businesses to control and secure the use of the Web and instant messaging applications.

Powered by its proactive Outbreak Intelligence heuristic technology, ScanSafe processes more than five billion Web requests and blocks 10 million threats each month for customers including Rothschild, Condé Nast and BMW.

Since pioneering the market for Web Security-as-a-Service, ScanSafe continues to deliver innovative Web security solutions, including the introduction of Scandoo - the world's first free secure Internet search tool that classifies search results based on the presence of malware and unwanted content.

With offices in London and San Mateo, California, ScanSafe is privately owned and financed by Benchmark Capital. The company received the 2006 Info Security Global Product Excellence Award for Best Managed Security Service, and was named one of Red Herring's Top 100 Technology companies. For more information, visit www.scansafe.com.