

A cloudy future for Web security?

Analyst: Paul Roberts

Sector: Enterprise Software

As the Web has morphed from a single-faceted medium for displaying graphics and text online to a de facto OS and platform for conducting commerce of all kinds, its importance as an attack vector has similarly increased. Countless surveys and studies have shown a migration to the Web by online criminal groups, which has raised the stakes for enterprise IT personnel to defend the Web channel at their organizations. That said, we believe Web threat detection is just the latest challenge in the giant game of 'whack a mole' that is enterprise IT security. That's not to say it isn't a real problem, or that companies selling products that target Web-based threats aren't providing real value to their customers – they are. What we mean is that the Web isn't a paradigm shift in IT security – it's just the latest threat vector, like floppy disks and email before it. Looking down the road, VoIP and mobile devices are waiting to pop their heads out of the mole hole, too.

The Web presents new challenges to security vendors that are not necessarily transferable from previous areas of focus. Unlike email, Web traffic is implicitly trusted by most users, who are far more concerned about latency and slow-loading pages than malicious JavaScript. At the same time, Web users and organizations have embraced the increases in interactivity offered by Web-based applications and Web pages, but often haven't stopped to consider the security of the JavaScript, ActiveX or Flash application they're using. The composite nature of many Web pages makes it difficult to assess the trustworthiness of even well-established websites. Messaging vendors needed to concern themselves only with the integrity of the email message, its origin and its attachments. Web security vendors must reckon with redirection, cross-site scripting, iFrame and SQL inject attacks that may turn even innocent websites (recently, **BusinessWeek's** website was one) into malware-serving rogues.

Secure Web gateway firms like **Blue Coat Systems** (Nasdaq: BCSI), **Websense** (Nasdaq: WBSN) and **Secure Computing** (Nasdaq: SCUR) have offered appliances to filter Web traffic for a decade or more. In recent years, software-as-a-service (SaaS) firms like **MessageLabs**, **ScanSafe** and even newer startups have promised services aimed at cleansing Web traffic for unsuspecting Web surfers, although it is not clear whether enterprises are ready to sign on to Web scanning in the Internet cloud. Given the enormity of the Web security problem, we're left to wonder: Who are the players in the fast-emerging Web security space?

Context

Statistics on Web-borne threats all point to a marked increase in attacks in recent months, and underscore the difficulty of identifying and neutralizing them. For example, data from the first half of 2008 released by Web security vendor Websense showed that 75 percent of the websites serving up malicious code were legitimate sites that had been compromised by hackers. That was a 50 percent increase in the number of legitimate sites implicated in attacks from the second half of 2007. MessageLabs, another vendor in the Web threat detection space, says its scanners identified an average of 3,660 new sites per day in September that were serving malware, including spyware and adware. That was an increase of 23% over the previous month. Also, 45.9% of all Web-based malware it intercepted in September was new.

Potential targets

As **Symantec's** (Nasdaq: SYMC) recent \$695m acquisition of SaaS security firm MessageLabs makes clear, security SaaS is an area of intense interest both to investors and to larger firms looking to diversify. We also think Web security is an area that lends itself to the SaaS model – at least in theory – and see the potential for hybrid services that mix an on-premises appliance with security intelligence, online reputation and scanning services hosted in the Internet cloud. As it stands, there are a slew of companies that sell such technology. While we don't think that means the current leaders in the Web security space – publicly traded firms Blue Coat and Websense – are targets themselves, smaller and well-established Web security outfits may be, especially if they have SaaS platforms or threat intelligence services akin to Secure Computing's Trusted Source that larger vendors can use to bolster detection across their product lines.

Here are a few of the firms we think are worth watching in 2009:

MX Logic of Englewood, Colorado, provides email, Web and business continuity services using a SaaS model. The company was founded in 2002 with \$2m in seed money from chairman and CEO John Street. Since then, MX Logic has taken in approximately \$16.5m in two additional rounds from **Adams Street Partners**, **UV Partners**, **River Cities Capital**, **Grayhawk Capital Venture Partners** and **Vista Ventures**. Like other security SaaS vendors, MX Logic OEMs much of its core security functions from third parties, including Symantec's **BrightMail** for its anti-spam capability, **Kaspersky Lab** for antivirus and anti-spyware scanning, and Blue Coat for secure Web gateway functionality. On top of that, the company offers Threat Center, a management platform that combines automated threat rating and correlation with manual analysis by MX Logic employees to spot new attacks. Tools for message archiving and recovery, end-user quarantine and e-discovery (using a custom implementation of the Apache Lucene search engine) are all included. In 2006, MX Logic introduced its Web Defense Service, a Web security and content-filtering option. It also unveiled a message-archiving service targeted at compliance-minded SMBs. It competes mostly with on-premises vendors like **Barracuda Networks** and **Cisco** (Nasdaq: CSCO)/IronPort. In the SaaS space, MX Logic competes mostly with Symantec and **Google** (Nasdaq: GOOG). MX Logic differentiates itself from those vendors with its channel-friendly go-to-market strategy and management tools that it claims make it easier for customers and channel partners to use its technology. The company has 200 employees,

most in North America, as well as 31,000 customers. FY 2008 revenue is estimated to be around \$30m and MX Logic says it is close to profitability, but has not ruled out another funding round. The company declined to give revenue projections for 2009, but says it hopes to expand into markets outside the US and Japan, its two main markets to date.

Atlanta-based **Purewire** was formed in January with \$1.75m raised from the founders: president and chief operating officer Mike Van Bruinisse, chief technical officer Paul Judge and VP of sales Mark Caldwell. All three held senior positions at messaging security vendor **CipherTrust** and then at Secure Computing (following that company's \$264m acquisition of CipherTrust in July 2006), as did Purewire CEO Steve Raber, who held the same position at CipherTrust. A \$2m funding round followed in July. Purewire operates a highly available, multi-tenanted content-scanning service using a network of colocated hosting centers. The company currently has two hosted locations, one each on the East and West Coasts of the US. These servers intercept inbound and outbound Web (HTTP, HTTPS, FTP-over-HTTP) content and scan for malicious content and for adherence to enterprise security policies. Purewire says its secret sauce is Purewire Trust, a technology that allows the company to correlate user reputations against Web reputations or other malicious content. Trust gives it the ability to mine social networks like **MySpace**, **LinkedIn** and **Facebook** and develop online reputations for particular users or networks that go beyond the URL. Purewire also trumpets 'cooperative-caching' technology, which stores copies of safe content on its servers (**Akamai** (Nasdaq: AKAM) does something similar). Customers accessing that content get accelerated delivery, saving cycles to analyze unknown or suspicious content without introducing latency.

As we've noted before, London- and San Mateo, California-based ScanSafe was an early mover in the Web security-as-a-service space. Its founders, brothers Ron and Eldar Tuvey, started in the Web-based advertising market before branching out into Web threat policy management for MessageLabs. The Tuvey brothers launched ScanSafe in the UK in 2004 and in the US in August 2005. The company now does Web- and IM-based security as a service and launched a product for mobile workers dubbed Anywhere+ in January, which Google resells as part of its Google Web Security offering. ScanSafe has raised two rounds of funding to date, totaling \$26m. The company relies on channel sales and licensing agreements for 100% of its revenue, and has some major-league channel partners including Google/**Postini**, **AT&T** (NYSE: T) and **NEC**. ScanSafe sells mostly to small enterprises working with managed security services providers to reach companies with less than 2,000 seats. Large enterprises represent about 10-15% of its customer base, with its biggest customer – an international bank – licensing 70,000 seats. ScanSafe differentiates itself from competitors, including traditional Web security gateways, with its dynamic classification engine, which it claims can make sense of the 'long tail' of inappropriate websites that URL blacklists don't capture. These include porn, gambling and discrimination sites, and ScanSafe says it can accurately spot them the first time out. The company is also testing outbound content control features that will add basic leak protection of keywords and other regular expressions. Those features, targeted at compliance-minded firms, are slated for a December release.

Rather than focusing broadly on Web threat detection, **Trusteer's** Rapport product focuses narrowly on securing high-value Web sessions and transactions by thwarting malicious programs such as root kits that are plaguing customers in its key verticals: online banking

and brokerage, healthcare and retail. Founded by executives from **Imperva**, **NetScreen** and **Cyota**, the Tel Aviv-based company offers a lightweight agent, Rapport Desktop, that runs deep in the OS at the software-interrupt level. Trusteer claims this allows its software to load prior to even sophisticated key loggers and root kits running at the OS-kernel level. From its vantage point in the OS, Rapport can secure online sessions in two ways. It can be the first in line to control critical OS functions, allowing it to block API calls that malicious programs like key loggers and screen scrapers use to sniff information from Web sessions. Second, the company controls key functions in the OS that do encryption and decryption, allowing it (in theory) to ensure end-to-end encryption of data in Web sessions – from keystroke to delivery to the customer site, with cached Web session data encrypted, as well. On the back end, Trusteer leverages hosted intelligence services to analyze legitimate and illegitimate Web pages. The company relies on a combination of automated scanning and manual reviews of websites as well as reputation blacklists, IP address verification, and so on. A hosted management application, Rapport Management Application, is used to pass updates and configuration changes down to installed desktop agents. Trusteer recently secured a \$6m series B funding round from **U.S. Venture Partners**.

Webroot Software is a privately held anti-malware firm based in Boulder, Colorado. Founded in 1997, the company was an early provider of anti-spyware technology to consumers and small businesses with its Spy Sweeper product. The company has 300 employees worldwide. Closely held since its inception in February 2005, Webroot accepted its first outside investment of \$108m from a syndicate of leading technology venture capital firms that included **Technology Crossover Ventures**, **Accel Partners** and **Mayfield**. After focusing on the consumer and enterprise spyware market, Webroot has aggressively expanded into the security SaaS market, picking up SaaS vendor **Email Systems** in December 2007 and unveiling a new Web security offering with basic Web content filtering and policy management in June. A fuller version of its SaaS-based Web security product is in beta now and will add deep content inspection on inbound and outbound Web traffic, as well as traffic shaping and routing. This will involve the introduction of Web content acceleration technology based on the Gzip open source compression technology and a modified Web proxy that will accelerate content transfers between the Web server and browser. The company claims sales of \$125m in FY 2007. It says SaaS business now accounts for 25-30% of all sales, with Web security around 25-30% of all SaaS sales.

Zscaler is another early-stage startup addressing the Web security problem. The Santa Clara, California-based company says it has built an Akamai-like network of processing gateways and management servers, dubbed 'central authorities,' to serve customers globally. Web traffic leaving a customer's firewall is redirected through the nearest Zscaler processing gateway, a multi-tenanted Web proxy hosted at datacenters globally. Once there, security policies, managed from the central authorities, are applied to that traffic. Malicious or noncompliant traffic is filtered, blocked or redirected. Similarly, on the inbound side, Web traffic is routed through the processing gateway and scanned before arriving on the customer's network. Like other Web security products, Zscaler can identify malicious or suspicious Web URLs and spot malicious code hidden within various types of Web traffic (HTTP, HTTPS and FTP) as well as attacks buried in mobile code like JavaScript and ActiveX. Web traffic and events are logged and then passed on to the nearest central authority, where they are correlated and stored. The company OEMs most of its threat-detection components from third parties and uses multiple engines and threat-intelligence

feeds for malware, botnet and phishing website detection. Zscaler sells services in four main areas: security, management, compliance and analysis. Customers pay on a per-user-per-month basis, taking into account both the number of users and the types of functionality they desire. Prices range from \$0.50-3 per seat per month.

Potential acquirers

Clearly, major platform providers like Google and **Microsoft** (Nasdaq: MSFT) are among the companies most likely to shop for Web security startups as they look to shore up security concerns around ever-expanding SaaS-based offerings (Google Apps, Office Live, etc.) to SMEs and larger enterprises. As it stands, many of these providers are uncommitted on Web security. We expect that to change.

We've noted that Google has been slowly building its Web security portfolio, with the acquisition of anti-spam firm Postini and browser security startup **GreenBorder Technologies**. Meanwhile, it has also begun to offer SaaS-based Web security, dubbed Web Security for Enterprises, through OEM partner ScanSafe (a relationship inherited from Postini). Picking up ScanSafe would seem to be a no-brainer, but Google's failure to do so yet makes us wonder whether it has other plans – perhaps to build an offering of its own that leverages its position as Ground Zero for the Web and its massive hosting infrastructure. Still, we think Google will move on the Web security space sooner rather than later, and may open its bulging purse to jumpstart things.

Microsoft has a string of security acquisitions under its belt, but just one in the SaaS space: **Frontbridge Technologies** in 2005 (now Exchange Hosted Services). But development of the Frontbridge platform has moved along at a glacial pace. With a growing suite of Microsoft Online Services (which now comprise Exchange Online, SharePoint Online, Office Communications Online and Office Live Meeting) and its newly announced Azure common services platform, it stands to reason that Microsoft will need to bolster its Web security story with an offering that it can plug into Azure and package for enterprise customers wary of Web-based threats and the security of Web services, as Google already has done. Look for Microsoft to make a move in the Web security space, perhaps with a technology-focused acquisition of an early-stage Web security SaaS player.

The same could be said for **IBM** (NYSE: IBM), which has been bolstering its suite of SaaS-based collaboration and productivity tools, including its Bluehouse project management, networking and Web-conferencing tool.

Cisco seems to have hammered down its Web security story, for now. The company just announced new versions of its IronPort S-Series Web security gateways, which it claims are twice as fast as previous S-Series products, adding three new S-Series appliances: the S660 for large enterprises, the S360 for midsize companies and the S160 for SMEs. The company says multicore processing doubles the appliance's scanning performance, allowing the devices to parcel out the scanning of Web content in a way that reduces latency. While S-Series is targeted for on-premises deployments, Cisco has also suggested that managed offerings are possible, either through a partner or by way of an acquisition of a managed services player.

Finally, we consider incumbent security vendors the next group of likely acquirers. Indeed, Symantec and **McAfee's** (NYSE: MFE) recent acquisitions suggest that a wave of Web security consolidation may be cresting.

What will second-tier vendors do? **Sophos** says it's happy with its endpoint and gateway strategy, and it doesn't see SaaS as a big part of its product mix in the near future. Other competitors, including **Panda Security**, **F-Secure** (FRA: DTV.F) and Kaspersky Lab, are more open, especially if it provides access to SMEs in the US. Panda, for example, has already released targeted services for the online banking community that look and sound similar to what a company like Trusteer offers; meanwhile, Trend, McAfee and others are integrating online threat intelligence services more closely with their endpoint agents in an effort to shorten response times. Look for companies that don't already have a strong story at the gateway to pursue SaaS-based offerings as an opportunity to broaden their appeal to SMEs and the midmarket, while also gaining a valuable platform that they can build on further down the road.

About The 451 Group

The 451 Group is a technology industry analyst company focused on the business of enterprise IT innovation. The company's analysts provide critical and timely emerging-technology insight to clients at vendor, investor, services and end-user organizations – insight that aids both strategic and tactical decision making for competitive advantage.

The 451 Group is headquartered in New York, with offices in key locations, including San Francisco, London and Boston. The company also operates Tier 1 Research – an independent division of The 451 Group – which analyzes the financial and industry implications of developments impacting public and private companies within the IT, communications and Internet sectors.

For additional information on the company or to apply for trial access to its services, go to: www.the451group.com