

A background image showing a person's hand pointing at a laptop screen in a meeting room. Overlaid on the image is a semi-transparent circular gauge with numerical markings from 10 to 70 and a white needle pointing towards the 40 mark.

Threat Management

Web 2.0 Security Threats ↻

↻ Web Threats

A Trend Micro White Paper | April 2007



TABLE OF CONTENTS

Executive Summary	3
Introduction to Web 2.0	3
Web 2.0 Threat Vectors	5
Dangers of Web 2.0: Case Study	5
Multi-Layered Approach	7
In-the-Cloud	7
At the Internet Gateway	8
At the Endpoint	8
Best Practices for Minimizing Web 2.0 Threats	9
Consumers	9
Businesses	9
References	10

EXECUTIVE SUMMARY

While Web 2.0 is an exciting and revolutionary development in online computing, it exposes consumers and businesses to a broader spectrum of Web threats. Web 2.0 technologies, such as asynchronous Javascript and XML (AJAX), expand both the attack surface and the security gaps available to cyber criminals, while the communal interaction premise of Web 2.0 renders users more susceptible to social engineering techniques. These developments challenge security solutions to expand protection beyond the traditional client-server endpoints of online computing. With many more threats unfolding “in the cloud” of the Web, which in the Web 2.0 paradigm is coming to function as a dynamic and exploitable operating system, next-generation security solutions must pay increasing attention to defense mechanisms that secure Web sites. Web reputation technologies, for example, have the potential to be the next frontier of defense against the burgeoning Web 2.0 security threat.

The potential consequences of neglecting Web 2.0 protection are significant: “Ignoring security during the Web 1.0 deployment led to Web site defacement, identity theft and business losses... Web 2.0 mashups that are not done securely will lead to huge openings for new forms of phishing and other attacks,” warns Gartner Group [1]. However, because of the rush to architect Web 2.0 applications to meet demand and the underlying security weaknesses of AJAX, the Web 2.0 ecosystem remains disturbingly vulnerable to attack. Web developers are not sufficiently ameliorating the security problem, leading consultants to warn: “We can’t leave Web security to Web developers.” [2]

This white paper describes the origin, development, and impact of the Web 2.0 security threat; explains why traditional tools, technologies, and development strategies offer insufficient protection against the evolving threat; examines the ability of multi-layered approach and Web reputation technology to secure the Web 2.0 experience; and summarizes best practices for protecting consumers and businesses against the rising tide of Web 2.0 threats.

INTRODUCTION TO WEB 2.0

Web 2.0, a phrase that currently yields 100 million hits on Google, entered the lexicon when Tim O’Reilly of O’Reilly Media coined it for a conference title. At the time, O’Reilly did not advance a rigorous definition of Web 2.0, instead considering it a constellation of tools, attitudes, and practices that treat the Web as a platform, empower users to create and manage content, and transform static Web sites into interactive, service-based application interfaces. More recently, O’Reilly has offered a compact definition of Web 2.0 as “the business revolution in the computer industry caused by the move to the Internet as platform, and the attempt to understand the rules for success on that new platform.” [3]

These various aspects of Web 2.0 illustrate the new freedoms it offers to collaborative communities. In the Web 1.0 era, few users could create code or content outside their personal Web pages, and a handful of editors and developers determined the content of the most popular Web sites of the day. Today, some of the most heavily trafficked sites on the Web—including MySpace, Orkut, Wikipedia, and YouTube—are open to anyone with a browser and the will to participate. A Web that was previously the provenance of information elites has become a global commons.

The media is abuzz with the positive repercussions of Web 2.0, with *Time* Magazine declaring 2006 “The Year of You” and hundreds of millions of users flocking to participate in Web 2.0. In the rush to Web 2.0, however, consumers and businesses have neglected to adequately address the accompanying paradigm shift in security. Consider one of the clouds in O’Reilly’s Web 2.0 map: “hackability.” In Web 2.0 and traditional computer science parlance, this phrase refers to programming fixes into a system, but it has also come to acquire the dark connotation of cyber crime. The “hackability” of Web 2.0 is a boon to the inevitable segment of malware authors and the criminal ecosystem that seize upon new and acute Web 2.0 security vulnerabilities to victimize unsuspecting users (see Table 1). Unfortunately, the convergence of content, code, and community in Web 2.0 offers no less freedom to the criminal than to the ordinary user.

WEB 2.0 SECURITY THREATS

Table 1. Web 1.0-Web 2.0 Security Implications

	Web 1.0	Web 2.0	Security Notes
Code	HTML	AJAX	Asynchronous Javascript and XML (AJAX) is a cluster of programming languages designed to make Web pages behave more like applications. HTML-architected Web pages required users to reload Web pages to view new data sets, but AJAX continually exchanges data with the server so that users can enjoy faster responses to their requests. In Google Maps, for example, AJAX enables rapid loading times and heightened user interactivity with the application (e.g., zooming in and out to check current locations). Since AJAX is an amalgam of constantly evolving languages, it creates a larger exploitable attack surface for cyber criminals. AJAX has so far been implicated in XSS and XSRF attacks (see below).
Platform	Browser and Operating System	Web	With Web sites themselves acting as applications, protecting the browser and operating system (OS) does not guarantee security against Web 2.0 threats. Consider mashups, or Web sites that integrate input from disparate sources to create a unified experience. HousingMaps.com, for example, is a mashup of Google Maps and Craigslist. Google Maps handles the visual mapping, while Craigslist provides associated real estate information. Although mashups enable a rich user experience, their aggregation of multiple applications creates more potential points of vulnerability for malware to exploit.
Client Role	Limited	Heavy	Cyber criminals can inject malware directly into Web 2.0 sites and applications. For Web 2.0 hackers, there's "More fun to be had on the front end." [4]
Syndication Model	None	RSS, Atom	Syndication built atop the Atom standard, and employing the Really Simple Syndication (RSS) file format allows publishers of Web logs, or blogs, to automatically distribute posts to a body of subscribers. If a Web 2.0 worm such as the Storm Trojan infiltrates a given blog, syndication is a simple way of distributing the threat to many unsuspecting potential victims.
Peer-to-Peer Model	None	BitTorrent, Napster, etc.	Peer-to-Peer (P2P) is a computing model in which clients connect directly to each other. P2P became popular when Napster first afforded individuals the power to store and share music files from their desktops. P2P remains a central part of the Web 2.0 model. Technologies such as BitTorrent allow users to upload and download large files without built-in security. This increases the risk of inadvertently acquiring ride-along malware.
Content Creation/Editing	Single User	Community	Allowing a user to add content to an online community enables users to target that community with malware. A manifest case is cross-Site Scripting (XSS)—a means of injecting malicious code from one Web site into another. Cross-site reference forgery (XSRF) combines XSS and social engineering techniques.
Completeness	Iterative	Perpetual Beta	Web 2.0 evolves in response to user inputs. Perpetual immaturity means Web 2.0 Web sites will almost always present new weak links for malware to attack.

WEB 2.0 THREAT VECTORS

Exploitation of Web 2.0 security vulnerabilities has already begun. In late 2005, a high-profile Web 2.0 site, MySpace, went offline thanks to the Samy cross-site scripting (XSS) virus. Samy, created by teenage hacker Samy Kamkar, consisted of malicious AJAX code placed in the hacker's MySpace profile. Anyone who subsequently viewed Samy's profile would unknowingly execute the code, which added the user to Samy's friend list and added Samy to the user's friend list. While adding anyone to a friend list normally requires user approval, the AJAX code bypassed human intervention and automated the approval process. The code surreptitiously added Samy to the friend list of any viewer who browsed Samy's page.

The virus was one of the fastest spreading pieces of malware in history, resulting in over 1 million infections in less than a day, and serves a dangerous proof-of-concept for hackers interested in targeting Web 2.0. Samy himself was surprised at how rapidly it spread and believes that the worst is yet to come: "MySpace tries to allow freedom of what users can post...Any similar sites that allow such tailoring or have holes that would allow JavaScript to pass through could easily allow a similar thing to be unleashed, and to possibly cause real harm." [5] Aspiring criminals need only examine Samy's code, which is posted on the Web in its entirety, to duplicate his attack, with potentially greater consequences, on another site.

The same JavaScript that powers the Web 2.0 experience is, in the hands of cyber criminals, a powerful and automated weapon. The JavaScripted Yamanner worm, for example, spread through Yahoo! Mail without requiring users to actually open a link or attachment—opening the mail was sufficient. Unlike Web 1.0 malware, Web 2.0 threats like Samy and Yamanner no longer require victims to deviate from security best practices by opening unknown attachments, emailing financial details to strangers, etc.

Web 2.0 also offers novel opportunities for traditional viruses to proliferate. For example, the Storm Trojan that infected many users earlier this year spread itself through bulletin board messages, Google links, instant messages (IMs), and the blog comments of infected users. Storm successfully leveraged the multiple vectors offered by Web 2.0 to better proliferate itself.

DANGERS OF WEB 2.0: CASE STUDY

Combining the technical acuity of XSS with older social engineering techniques (i.e., con games intended to trick consumers and businesses into surrendering sensitive data) results in an even more potent emerging threat: cross-site reference forgery (XSRF). XSRF does not require the victim to download or install any software. Merely keeping the XSRF threat page open launches the attack. Consider the following consumer threat scenario, which International Security Partners has successfully modeled and executed.

1. John likes to make new friends on a Web 2.0 social networking site, often chatting with these friends in an open window while he surfs other Web pages. John has a personal profile page on this site with his picture and other personal information.
2. Eliza, a cyber criminal employing a false identity, visits John's profile page and strikes up an online friendship with him. During the course of their chats, Eliza gleans more information about John. They discuss the various ways they use their computers, with John mentioning that he uses the Web for online stock trading. In response to a question from Eliza, he recommends his own broker's online services. Eliza also learns that John is an ardent baseball fan.
3. One day, John and Eliza are chatting while John also has an online brokerage window minimized in his Windows tray. Eliza sends John a link to a breaking sports story. John's favorite baseball player Ois being traded! John clicks on the link and eagerly reads the news.

WEB 2.0 SECURITY THREATS

4. Unbeknownst to John, the sports news Web site is not genuine, but spoofed and malicious. This is a fact easily concealed from John. As one authority notes, "Links can be easily obfuscated so they appear to go elsewhere, and to conceal words that would disclose their obvious function." [6] As John reads the news, the sports Web site launches an XSRF attack that uses iFrames to create a hidden HTML document within the main page. This phantom document employs HTTP request methods such as POST or GET to target John's online brokerage site.
5. The HTML forms, which pirate John's perpetual authentication cookies, appear as if they are coming from John's computer and therefore have the authority to instruct his stockbroker's site to create a new checking account for transfers, to divert his balance there, and to drain it.

Web 2.0's role in this attack is to desensitize John to the possibility that the ubiquitous "friend list" can be a point of entry for criminals, and to provide the code for the attack. Figure 1 illustrates other types of social engineering techniques that threaten consumers.

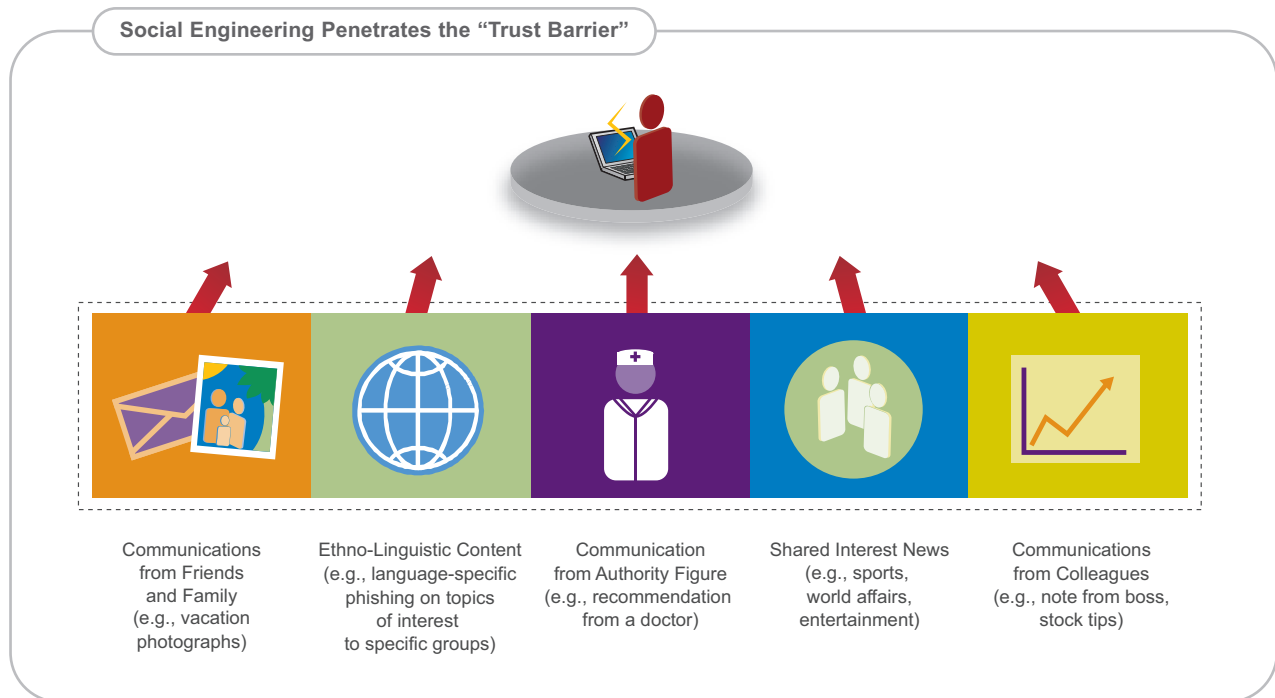


Figure 1. Social engineering principles inform attacks against both groups and individuals, cynically taking advantage of psychology, trust, and vulnerability to penetrate the consumer's "trust barrier" (the natural human skepticism that cyber criminals overcome by associating themselves with trusted groups and compelling content).

In addition to these threats to consumers, the security risks are particularly acute for businesses seeking to turn their traditional applications and Web sites into Web 2.0 experiences for customers and partners. For example, some companies allow customers to blog on their Web sites. As Aberdeen Group cautions, "With this increased accessibility comes increased vulnerability to unwanted intrusions into key business systems, which can result in the theft of key data such as private customer information...to the outright destruction of critical information which can bring a company to a grinding halt." [7]

The loss of customer data and the draining of customer funds, as in John's story, not only damage a brand's reputation but also render the company susceptible to fines and lawsuits. In the eyes of the law, companies may be liable for fraud perpetrated on their Web sites by others. Furthermore, cyber criminals are no doubt examining how to directly exploit the innate vulnerabilities of AJAX in a corporate setting, because AJAX is expanding beyond its consumer-oriented origins. "We are already seeing AJAX at financial institutions, healthcare, and government," notes International Security Partners [8]. This creates possibilities for hackers to drain corporate accounts, access sensitive government information, and otherwise wreak havoc.

MULTI-LAYERED APPROACH

A new approach is needed to address this class of threats – an approach that complements existing techniques already in use by most security savvy enterprises and consumers. The most effective approach employs multiple layers of protection and incorporates a range of protective measures. In addition, the evolving nature of the threat necessitates some form of information sharing mechanism, in which information gathered in one portion of the protection system is used to update information in other layers. This can be accomplished by implementing integrated solutions at three different layers (see Figure 2):

- In-the-cloud: Analyzing Internet data at a data center, for example, before the data even reaches the gateway.
- At the Internet gateway: Analyzing data where the internet connects to a corporate or Internet Service Provider network.
- At the endpoint: Analyzing data on the PC or server.

⊕ **In-the-Cloud.** At this level, one way to foil these hackers is to evaluate the legitimacy of the Web sites through which they operate. However, static URL filtering, which generally involves periodic updates to a list of "known bad" URLs, is not responsive enough to identify threats that can spread, via XSS, XSRF, syndication, or other means, to otherwise "good" sites. Powerful AJAX code and the freedom to post it on any site renders quaint the Web 1.0-era distinction between legitimate sites and sites with malicious content. Under these circumstances, only a more comprehensive check of the reputation of a Web site before allowing user access can properly identify malicious sites. This "Web reputation" check still involves a URL filtering database; however, the addition of approximately 5000 new domains per day means that additional measures are needed to complement this important element (see Figure 3).

Advanced Web reputation services do not assume the existence of a fixed number of "bad" sites, but instead dynamically compile, monitor, and assess a comprehensive list of registered domain names—a list that today exceeds 300 million in Trend Micro's reputation database. Based on the domain name list, advanced Web reputation checking technologies employ methods of examining domain name registrant information—public information necessary to register an IP address—to determine the legitimacy of a Web site. Information such as who registered the site and where the site is hosted, when monitored over a period of time, can yield telling information about the stability of a particular domain. For example, frequent change of location may indicate that a site is not safe, as cyber criminals often change the physical locations of IP addresses to evade detection. Also, new sites that are drawing inordinately high numbers of 'hits' raise red flags, as such activity is a signal that a virus may be drawing traffic to a particular site. Other indicators, such as geographical location, yield key information about the stability, or legitimacy, of a particular site and should also be considered when evaluating a site. Of course, determining the reputation of a Web site also includes checking the site against other databases of known phishing, pharming, or otherwise malicious URLs.

WEB 2.0 SECURITY THREATS

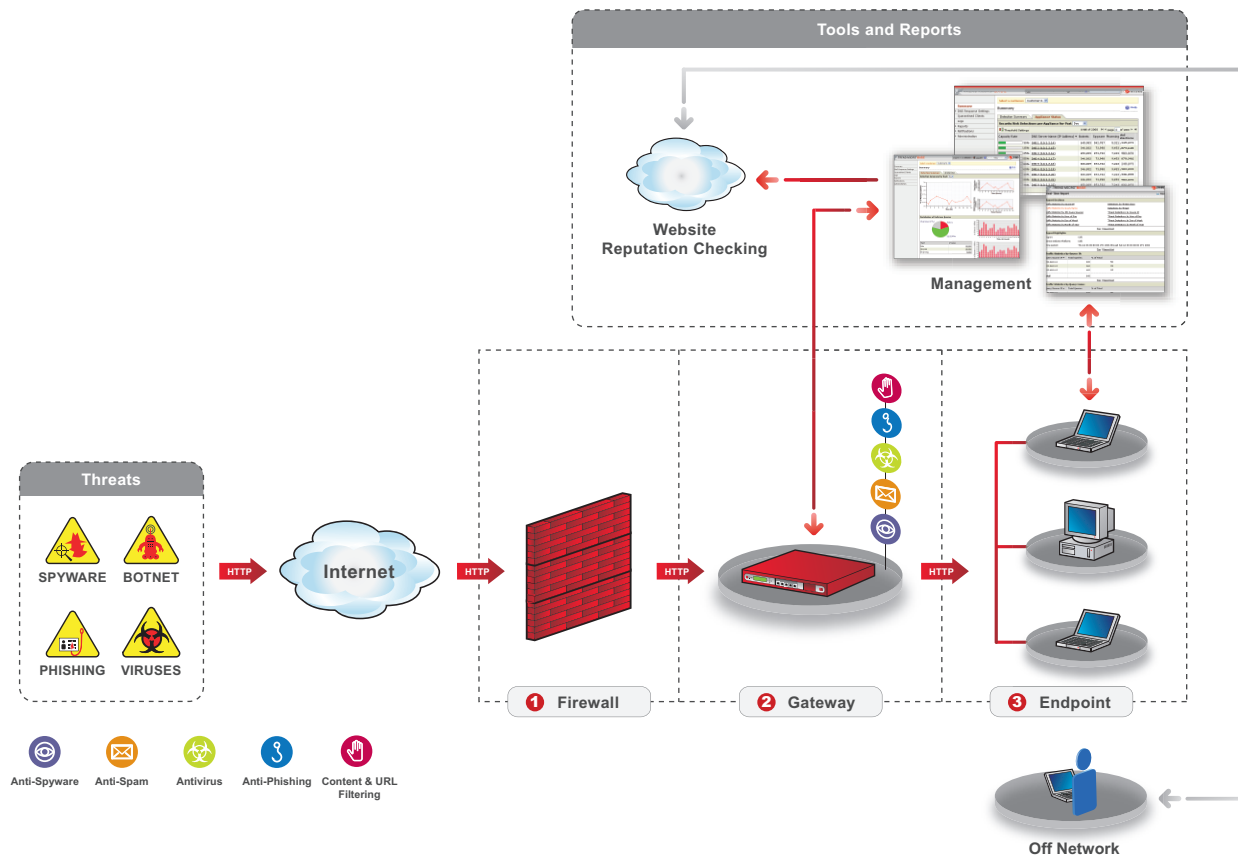


Figure 2. A multi-layered approach is needed to protect against the broad range of Web threats.

- ➔ **At the Internet Gateway.** Performed via software or a hardware appliance, Internet gateway capabilities should include file checking and behavior analysis. The file checking function essentially checks the “reputation” of each file before permitting the user to download it. To do this, a data crawl of each file at the Web site and an assessment of each file’s reputation are periodically performed to establish and maintain a database of file reputation. This file checking is needed, in addition to the Web reputation function in-the-cloud, because cyber criminals can easily move individual files with malicious content from one Web site to another.
- ➔ **At the Endpoint.** Endpoint-based (i.e., client-based) prevention should consist of URL filtering, Web site reputation capabilities, and use of a “restore point.” A restore point is saved prior to Web surfing. If abnormal activity is detected after downloading a file or browsing the Internet, the machine can be returned to its previous state. Other prevention options should include establishing a “virtual environment” for the user to surf the Web; in this arrangement, Web threats reach only the virtual environment and do not penetrate the user’s actual environment. Clean up capabilities also must reside at the endpoint and should include methods for visiting computers. Total recovery is also needed in cases when cleanup is not feasible due to a rootkit infection, for example.

WEB 2.0 SECURITY THREATS

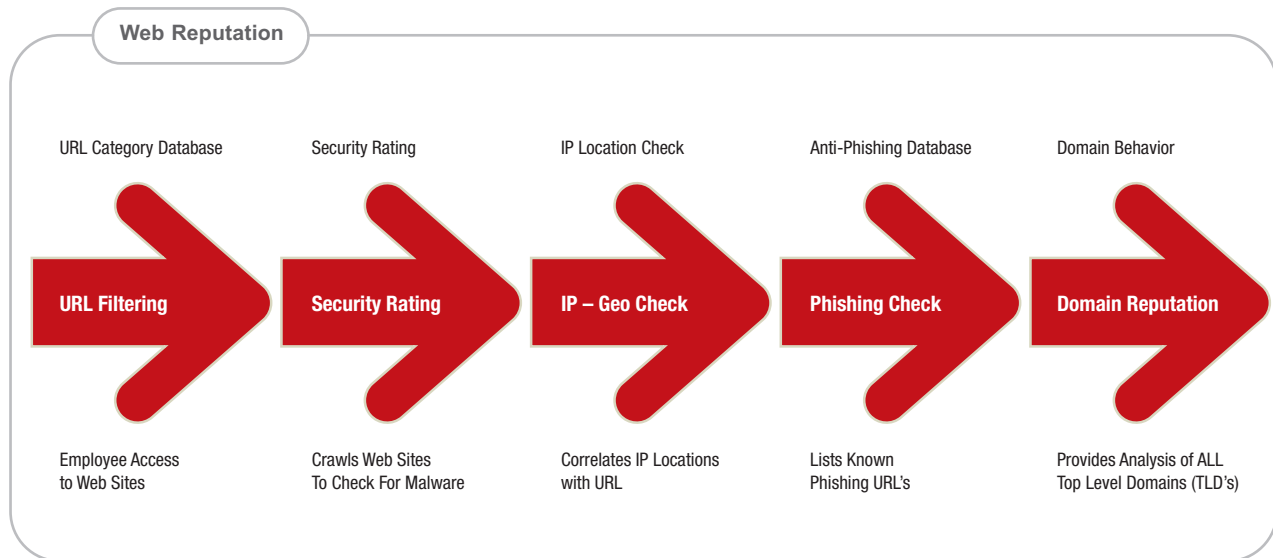


Figure 3. In the cloud, the key is to check the “reputation” of each Web site via a comprehensive set of steps.

BEST PRACTICES FOR MINIMIZING WEB 2.0 THREATS

Consumers. Consumers can optimize protection against these Web security threats by carefully selecting ISPs and security providers that incorporate the following best practices into their products and services:

- Deploy Web 2.0 threat protection software on the PC, along with conventional antivirus and antispyware protection.
- Secure the router/wireless network, and be aware that a third-party network (e.g., at a coffee shop or airport) may not be as secure as the home or office network.
- Select an ISP or security vendor that installs security software to address Web 2.0 threats in the cloud and ensures that background Web reputation checking is active during all online sessions.
- In conducting financial transactions online, make certain that the Web site does not employ perpetual cookies that can open the door to XSRF attack. In case of doubt, ask the financial entity directly about its Web site’s cookies.
- Be aware that Trojans and other malware can appear not only in email links but also as blog comments and other code embedded on user pages.
- Adopt an attitude of caution to other individuals encountered when browsing Web 2.0 sites. Cyber criminals can adopt online identities and stalk potential victims for months before striking.

Businesses. Businesses can increase protection against Web threats by adopting the following measures. In some cases, this may involve selecting the appropriate ISP and security provider.

- Adopt Web reputation technology to protect against Web 2.0 threats in the cloud while simultaneously guarding against conventional gateway- and client-level threats.
- Educate employees about Web 2.0 threats, especially since employees commonly work from home using their laptop computers and occasionally use them for personal purposes.

WEB 2.0 SECURITY THREATS

- Weigh the XSRF, XSS, and viral consequences of allowing employees to browse Web 2.0 sites on company computers.
- Ensure that deployed Web reputation technology transcends Web 1.0-era good/bad static URL filtering by applying weighted scores to URLs.
- Embrace the concept of Web reputation as a service that can be delivered to different security applications on demand.

REFERENCES

1. Pescatore, John. 2006. Web 2.0 needs security 101. Gartner, http://www.gartner.com/DisplayDocument?ref=g_search&id=498199.
2. Stamos, Alex and Lackey, Zane. 2006. Breaking AJAX Web applications: vulnerabilities 2.0 in Web 2.0. Black Hat Japan Conference, October 5, 2006, <http://www.blackhat.com/presentations/bh-jp-06/BH-JP-06-Stamos-Lackey.pdf>
3. O'Reilly, Tim. 2006. Web 2.0 compact definition: trying again, http://radar.oreilly.com/archives/2006/12/web_20_compact.html.
4. Stamos and Lackey, <http://www.blackhat.com/presentations/bh-jp-06/BH-JP-06-Stamos-Lackey.pdf>
5. Lenssen, Philipp. 2005. Samy, their hero, <http://blog.outter-court.com/archive/2005-10-14-n81.html>
6. Burns, Jesse. 2005. Cross-site reference forgery, http://www.isecpartners.com/documents/XSRF_Paper.pdf
7. Patel, Mounil. 2006. Customer and private data protection strategies: the application security benchmark. Aberdeen Group, <http://callcenterinfo.tmcnet.com/whitepapers/articles/3335-customer-private-data-protection-strategies-application-security-benchmark.html>
8. Stamos and Lackey, <http://www.blackhat.com/presentations/bh-jp-06/BH-JP-06-Stamos-Lackey.pdf>

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014
USA toll free: 1+800-228-5651
phone: 1+408-257-1500
fax: 1+408-257-2003
www.trendmicro.com

