



The Security Implications of Web 2.0

Table of Contents

Executive Summary	3
What is Web 2.0?	3
What's in store for Web 2.0	4
Web 2.0 Exposes New Vulnerabilities	4
Entirely new vulnerabilities	4
"Pull" replaces "push"	4
Polymorphism complicates defenses	6
Web 2.0 vulnerabilities	6
Solution: Web 2.0 Countermeasures	7
Protect consumer information	7
Protect business information	8
McAfee Protects Against Web 2.0 Vulnerabilities	9
About McAfee	10

Executive Summary

The collaborative benefits of new Web 2.0 technologies have fueled rapid growth in online consumer markets and now are being adopted by businesses worldwide.

Like most emerging technologies, Web 2.0 brings new types of attack vectors. Hackers are targeting the vulnerabilities brought by Web 2.0 with new and time-tested attack techniques that are proven to trick users or steal information, enabling online fraud or corporate data theft. They are also taking advantage of on-the-fly combinations of untested content that are being dynamically assembled in ad networks, social networking sites, blogs, and collaborative applications. More and more, threats include multiple paths—combinations like email, compromised web content, and a Twitter tweet—and multiple stages to avoid any individual defense.

Countermeasures include a mix of changed business processes, user awareness, and technical safeguards to mitigate and defend against attacks.

Web 2.0 defenses start with validating all data and executable code downloaded from Web 2.0 applications. All downloads from Web 2.0 websites, or within Web 2.0 applications, should be checked for malware. Educating users about the risk posed by the new threats greatly reduces exposure to Web 2.0 vulnerabilities.

McAfee leads the market in providing solutions to defend against Web 2.0 threats. Our on-demand family of cloud-based defenses and our scalable on-premises gateways reduce the risk of conducting business online, allowing companies to realize the efficiency gains and increase in collaboration offered by Web 2.0 technologies.

What is Web 2.0?

The term “Web 2.0” entered popular use in 2004 when technology publisher Tim O’Reilly used it to explain how new technologies were being used on the Internet. At the inaugural O’Reilly Media Web 2.0 Conference, O’Reilly was describing the rapid movement away from static pages and websites to enhanced browsers and dynamic content. In this seminal session, O’Reilly was credited with permanently linking Web 2.0 to the “Web as platform” phrase.¹

Wikipedia defines Web 2.0 as “the use of World Wide Web technology and web design that aim to enhance creativity, communications, secure information sharing, collaboration and functionality of the web.”

Web 2.0 technical evolutions have added new types of dynamic applications and content, more robust messaging, and new browser standards with extensions for dynamic client applications.

Wikipedia goes on to say, “The differing, yet complementary approaches of such elements provide Web 2.0 sites with information storage, creation, and dissemination challenges and capabilities that go beyond what the public formerly expected in the environment of the so-called ‘Web 1.0’.”²

The popularity of Web 2.0 applications has fueled rapid growth in hosted software-as-a-service applications, such as Salesforce.com; social networking sites, such as Facebook, Twitter, and LinkedIn; video-sharing sites like YouTube; and collaborative wikis and blogs—both public and private. Social networking, video sharing, and collaboration sites leverage many of the same technologies, with applets and Web 2.0 applications on each network. Facebook estimates its platform has 500,000 applications in active use by its 400 million users.³

“Criminal toolkits are evolving rapidly to use new technologies that increase the sophistication of the attack—leaving even more users blind to the risks. Malware authors love following the social networking buzz and hot spots of activity.”

—2010 Threat Predictions

McAfee Labs, http://www.mcafee.com/us/local_content/reports/7985rpt_labs_threat-predict_0110_fnl_lores.pdf

¹ <http://oreilly.com/web2/archive/what-is-web-2.0.html>

² Wikipedia, http://en.wikipedia.org/wiki/Web_2.0

³ As of March 29, 2010, <http://www.facebook.com/press/info.php?statistics>

What's in store for Web 2.0

Web 2.0 in consumer applications and markets has posted accelerated triple-digit growth based on an advertising-driven business model.⁴ Web 2.0 delivers consumer services via the Web, and not with traditional licensed software. A “build once, deploy broadly” service model is helping to fulfill the Web 2.0 vision of mass customization to provide targeted services for a large number of small web communities and niche markets.⁵

Globalization and the tight economy are spurring adoption in the enterprise market. Salesforce.com's cloud collaboration platform, Chatter, and the maturing Google Apps are the kind of cost-effective, ubiquitous innovations that will make it increasingly difficult for enterprises to avoid Web 2.0 applications in their ecosystems.

Security and anti-spam defenses also benefit from the collaborative elements of Web 2.0 by countering user perceptions that updates to anti-virus software are slow or incomplete. Increasingly, users and their protective tools are reporting the spam and malware they encounter to community and reputation networks. Each new malware report helps to speed the development of countermeasures to combat rapidly propagated polymorphic malware.⁶

The unique capabilities and needs of mobile users and wireless platforms will further drive the evolution of Web 2.0 technologies and usage. We can already foresee the possibilities with applications on the iPhone and the Android and the success of e-readers and netbook devices.

Web 2.0 Exposes New Vulnerabilities

Many new technologies—perhaps most—are deployed in the marketplace before security is proven and mature. Web 2.0 is no exception, having exposed vulnerabilities before users were armed with sufficient countermeasures.

Entirely new vulnerabilities

Web 2.0 relies on a more robust user experience, with rich content and processes linked to web servers through application programming interfaces (APIs). Many Web 2.0 services rely on Java and Flash-based client applications, with a variety of scripts bringing more life and interactivity to browser-based interactions. Other advanced browser capabilities use Dynamic HTML (DHTML) services in a client browser or make use of service-oriented architectures (SOA) for a broadly deployed service model.

Web 2.0 attack vectors are different, although they borrow many attack concepts from Web 1.0. Web 1.0 was victimized by “push” model threat propagation and static attack code distributed via email as well as network-based denial of service attacks. Static attack code did not change much, so security vendors had the ability to develop reliable anti-virus signatures and malware defenses. To get malware installed, users needed to click on an executable or consciously allow a file to install. Educating users not to click on attachments and recommending that they scan email for malicious content were relatively effective ways to block malware distribution.

“Pull” replaces “push”

In contrast, Web 2.0 uses the “pull” model of malware distribution to target the more robust and capable Web 2.0 browser-based clients. Pull-based malware infections are downloaded unwittingly into clients or injected (“drive-by”) into browsers or websites. Once downloaded or injected into a vulnerable client or website, they are ready to be executed without the end user's knowledge or explicit permission. Simply visiting a web page enables the infection, so user education has limited effect. Websites distributing malware can be legitimate sites that have been compromised by injected or uploaded malware or bogus hacker websites masquerading as innocent ones. As of summer 2009, a new infected webpage was being discovered every 3.6 seconds.⁷

⁴ Nielsen/NetRatings, 2006, <http://www.mediapost.com/publications/index.cfm?fuseaction=Articles.san&s=50754&Nid=24887&p=380828>

⁵ “The Long Tail”, Wired, Chris Anderson, Oct. 2004, <http://www.wired.com/wired/archive/12.10/tail.html>

⁶ See McAfee® Global Threat Intelligence white papers at http://www.mcafee.com/us/mcafee_labs/gti.html.

⁷ <http://www.scmagazineus.com/every-36-seconds-a-website-is-infected/article/140414/>

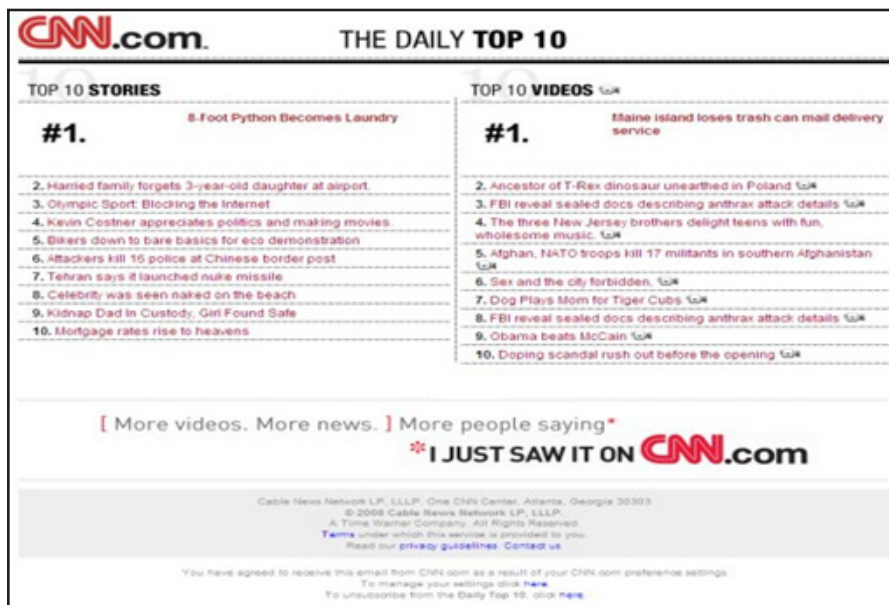


Figure 1. Fake news and tabloid headline emails attempt to lure unsuspecting users to a fake CNN website, which is an example of a hacker malware injection exploit. The systems of site visitors are injected with malware when downloading an updated video player that visitors are made to believe is required. Hackers exploit the trust given to popular, reputable brands to lure visitors.

Fraudulent websites are targeting burgeoning use of Web 2.0 services and online consumer spending. Keyloggers, applications that capture your keystrokes and forward them to cybercriminals, are popular because they can acquire user passwords, account numbers, and other identification. Since 33 percent of Internet users use the same password for every site they visit,⁸ a single theft can enable access to bank accounts, personal information, gaming site credits, and other real and virtual assets.

Unsuspecting site visitors often are lured to bogus or compromised sites by phishing, pharming, or well-crafted social engineering exploits. Phishing exploits send the victim a message either via email, IM, or potentially a Twitter “tweet.” Some messages appear official, with instructions to click on a link in the email or tweet to receive important information at a (compromised) website. Pharming uses an infected server, router, or compromised local DNS to redirect the user’s browser to a malicious fake website.

The traditional purpose of phishing and pharming attacks in Web 1.0 was to steal critical login information or personal identity data for fraud and identity theft. With the increase in compromised legitimate websites, these attacks have become even more dangerous because the systems of passive users can get infected with malware—no overt action is required and detection is less likely.

Social networking sites make this dynamic even more challenging, as recipients get links from people they trust or have “friended” online. They are far more likely to click on a link in a tweet when it is sent from someone they know.

One survey reported that 57 percent of social networking users receive spam.⁹ When the user clicks the link, their system will be attacked with the intention of stealing credentials, stealing data, and taking over the computer for use in a botnet—a network of compromised machines that distributes malware and spam to other users. By reusing personal and corporate hosts, spammers and cybercriminals need no capital investment, maintain highly resilient networks of devices, and distance themselves from any accountability.

⁸ http://security.cronline.com/news/one_password_still_fits_all_for_web_users_100309

⁹ As presented by Graham Cluley, Sophos, RSA Conference, March 5, 2010

Polymorphism complicates defenses

Malware injected or downloaded directly into a user’s browser from both malicious and legitimate websites is an increasingly popular type of polymorphic exploit. “Polymorphism” refers to the ability of some code to change in real time. When used in malware, it allows exploit code to escape signature detections because it is impossible to deploy signatures for exploits that have not yet been seen.

Polymorphic attack code keeps malware signatures one step behind, reducing the effectiveness of this traditional, often primary, defensive layer. To combat this type of threat, host machines must be reinforced with protections such as intrusion prevention systems that block installation of malware and keyloggers. Host and network based malware detection need to step up their games by adding behavioral, reputation, and real-time risk assessment. These advanced tools can proactively block suspicious content based on attributes such as website age, link reputations, the behavior of the code, and other factors, rather than waiting for a formal signature to be released.

Web 2.0 vulnerabilities

Web 2.0 brings new properties that enable new collaborative functionality and enhancements. Desirable Web 2.0 attributes that have been widely deployed in consumer Internet markets include:

- Enhanced usability for complex web applications
- Simplicity with openness that hides complexity from users
- Collaboration from communities of content contributors
- Web services for rapid delivery of applications
- Third-party content reuse for quick and scalable application “mashups,” which combine code from various sources

But the dynamic properties of Web 2.0 and its enhanced functionality create the security liabilities now being exploited. Like much new technology, Web 2.0 has been deployed before security concerns were fully understood and technologies—along with their interactions—fully tested. Third-party software of any type greatly increases exposure to Web 2.0 vulnerabilities and the corresponding attack risk. User-generated and dynamically aggregated content make it almost impossible to fully predict the potential software interactions and behaviors which is how commercial software has traditionally been tested.

Web 2.0 Property	Benefit	Security Weakness
Openness	Simplicity for advanced collaboration and content integration	Collaboration and third-party content can be major attack vectors
Community	Shared community information speeds communications and idea interchange	Exposes valuable personal information that can be used in social engineering attacks or can create physical security risks
Collaboration	Blogs and wikis quickly share ideas, advance thinking and policies	Blogs and wikis have been quickly compromised to distribute spam and malware
Third-Party Content	Content re-use for quick and scalable mashups and integrations	Weak security assurances for third-party content may add vulnerabilities to otherwise secure applications
Web Services	Rapid integration of new and advanced functionality	APIs for executable code and automated business processes often have weak security and invite attack

Figure 2. Comparing Web 2.0 benefits with matching security vulnerabilities.

Solution: Web 2.0 Countermeasures

Countermeasures can be added to secure Web 2.0 enhancements. A combination of technical safeguards and business processes can reduce or remediate vulnerabilities to allow safe and effective use of Web 2.0 features.

Protect consumer information

The openness and collaboration in Web 2.0 bring a heightened awareness of sensitive personal information. Every user of a Web 2.0 service now must assume information criminals are watching to steal personal information. Consumers must become stewards of their personally identifiable information and safeguard its use in Web 2.0 sites and applications to avoid becoming victims of identity theft, fraud and other criminal activities. Here are some of the things they can do to avoid becoming victims:

- *Validate all websites*—Reputation and trust services give users a gauge to measure the risk of known websites and their Web 2.0 services. Security vendors and anti-malware services are adding support for risk evaluation and reputation services that make it more difficult to hijack or redirect traffic to bogus websites lurking to inject malware.¹⁰ New industry standards, such as the extended validation secure sockets layer (SSL) certificates, authenticate valid websites and provide a simple visual indicator of reputation and risk within the browser navigation bar (red, yellow, and green). Buyer should beware and ensure the websites they visit are who and what they claim to be.
- *Pay special attention to unfamiliar websites*—All users of the web should apply extra caution when visiting unfamiliar websites. Consumers and enterprise users can take advantage of free risk and reputation services on the web to check a website's bona fides.¹¹ They should look for anything suspicious in the website address in the browser navigation bar before clicking. It's best to err on the side of caution by never visiting an unfamiliar website or downloading anything from one or use any service until the site is proven trustworthy.
- *Use risk reporting tools*—Every user of a Web 2.0 service should become aware of the fraud risks that come with misuse of personal information or identity theft. Web 2.0 can provide tools to mitigate the risk of identity theft, such as Google Alerts or credit monitoring services that report on activities about you.
- *Look for stronger user authentication*—New user-centric, or claims-based, authentication tools based on the OpenID industry standard are entering the marketplace. These new tools strengthen user authentication beyond simple passwords and user IDs. Reputable websites and services are beginning to deploy these. Registering to use these new authentication tools will help to protect user identities on the Internet.
- *Defend against clickjacking*—Clickjacking is one of the most dangerous and troubling security problems on the web. In this attack, two layers appear on a site, one visible, one transparent, and users inadvertently interact with the transparent layer that has malicious intent. Login credentials for a bank account, for example, can be captured by the second layer. New countermeasures, such as NoScript with ClearClick for the Firefox Web browser, reduce the clickjacking risk. Users can take other countermeasures to limit clickjacking risk, such as minimizing cookie persistence by logging out of applications and using a dedicated browser for each website visited.

Annual crime complaints reported to IC3 have increased 667.8% when comparing data from the 2001 annual report with 2009

Total dollar loss from referred cases \$559.7 million, up from \$264.6 m in 2008

In addition to FBI scams, popular scam trends for 2009 included hitman scams, astrological reading frauds, economic scams, job site scams, and fake pop-up ads for antivirus software

--Source: 2009 Internet Crime Report, Internet Crime Complaint Center, http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

¹⁰ McAfee SiteAdvisor is a free testing and reputation service available to anyone: <http://www.siteadvisor.com/>

¹¹ <http://www.siteadvisor.com/>

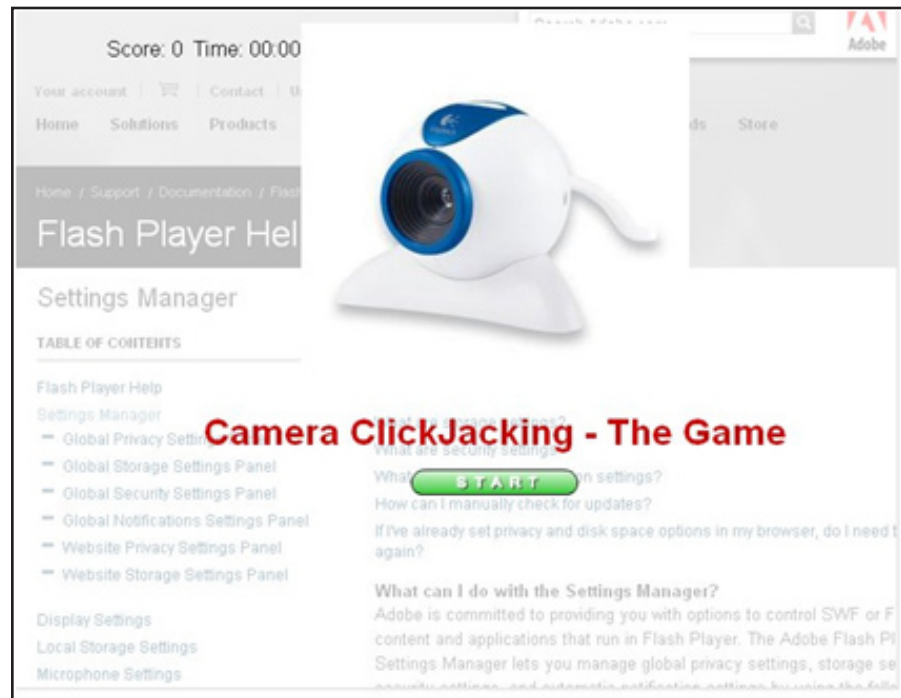


Figure 3. This is an example of an opaque overlay clickjacking exploit. The malicious opaque hacker frame is most visible, superimposed above a legitimate website or application. An unsuspecting user clicking on the camera game overlay actually is executing a command on a vulnerable application hidden beneath.

Protect Business Information

Web 2.0 deployed as Enterprise 2.0 presents business with a double-edged sword, promising greater productivity but increased security risk. The enterprise must implement defenses and processes to protect sensitive collaboration, project, and community information.

Businesses also are vulnerable to employees shopping online from work, checking personal email, such as Gmail, or updating LinkedIn or Facebook. Enterprise teams should adjust their security practices to include additional steps:

- *Use commercial tools to keep malicious content out*—Implement automated email and web technologies to block malicious content in email, spam, social networks, and websites. Real-time content inspection and dynamically maintained reputation technologies can block unknown content that signature-based detections will miss. Adding host intrusion prevention systems to critical systems prevents their compromise.
- *Validate and escape all inputs*—Businesses should assume that all data that has been input into or downloaded from Web 2.0 applications and services is suspicious. They should treat all sources as untrusted and validate all downloaded information and applications. Many new application security standards, processes, and countermeasures are available to ease the validation task for collaborative blogs and wikis, as well as video and web services (see www.OWASP.org).
- *Limit untrusted data*—Web 2.0 applications and services present an opportunity to revisit the company's policies and procedures regarding the passing of untrusted data to a trusted zone. Many of these policies originally were developed for static Web 1.0 forms-based data input. Updating these for the new risks posed by Web 2.0 is a critical part of risk assessment.

- *Deploy clickjacking defenses*—Using JavaScript can defeat the possibility of the content layer of websites or application being overlaid. It's important to check to see if code is currently running as the top active layer. If not, it should be made the top layer. Businesses should strictly enforce policies that limit Java applications to a secure browser sandbox and re-authentication for functionality likely to be abused.
- *Secure, then deploy*—Revisiting the software development lifecycle (SDLC) and tightening security when adding Web 2.0 features makes applications secure with the Web 2.0 countermeasures before deployment. Prior to deploying service-oriented architectures, the security impact of web services should be evaluated. Web services privacy standards such as the Platform for Privacy Preferences (P3P) are gaining popularity. Enterprises should review all privacy and security standards prior to starting development. Standards may have conflicts, which may lead to confusion and lengthen development estimates.
- *Add authorization*—Authentication is a coarse-grained access control that verifies users' claimed identities and establishes who they are. Enterprises should consider adding policies and procedures with finer-grained authorization controls to complement authentication and access.
- *Logging and correlations*—The actions taken by users as they transit Web 2.0 applications and services provide a critical audit trail. Web 2.0 exploits typically seek to elevate privileges and transit from untrusted to trusted applications. A forensics audit trail captures who did what, when and where. When properly correlated, the audit trail recreates the history of any suspicious activities.
- *Monitoring*—User behavior during a session or across multiple sessions can quickly reveal malevolent intent. Identifying and isolating suspicious actions can stop exploits in their tracks, preventing data leakage and embarrassing disclosures.

McAfee Protects Against Web 2.0 Vulnerabilities

Web 2.0 offers enormous potential for benefit and risk to your organization. Safe and effective use of Web 2.0 technologies directly affect the bottom line of the enterprise, offering increased efficiency for employees, business partners, suppliers, distributors, consultants and others, while providing business agility for changing economic conditions.

McAfee offers online threat services that can help you realize the secure and rapid adoption of Web 2.0 tools and methods. McAfee® Security SaaS is designed to deliver enterprise-grade service and performance, without enterprise-level complexity and cost. All of these award-winning services benefit from McAfee Global Threat Intelligence, which powers the groundbreaking McAfee threat technologies, including McAfee Artemis™ technology and McAfee TrustedSource™ service. Continually tuned threat protection is distributed throughout the McAfee portfolio of endpoint and network security products and services.

McAfee Security SaaS delivers a complete endpoint, email and web protection and vulnerability management portfolio. It leverages the power of cloud computing to save your IT department time, effort, and costs. McAfee Security SaaS is the most comprehensive security solution available in the cloud from a single vendor—the leader in security software. Between our dedicated security experts and the enormous visibility we have into global threats, McAfee can consistently provide the fastest response to new outbreaks. Our services are easy to set up and administer, available with one integrated console and backed by 24/7 live customer support. Learn more at www.mcafee.com/saas.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. <http://www.mcafee.com>

