



**Securing Web 2.0:
Why Security 1.0 is no longer enough**

An Exploit Prevention Labs Educational White Paper

Exploit Prevention Labs, Inc.

Table of Contents

1	Introduction	3
1.1	What is Web 2.0?	3
1.2	New technologies bring new vulnerabilities	4
1.3	What you'll learn from this paper.....	5
2	Security Issues and Threats	6
2.1	The changing nature of computer security threats.....	6
2.2	How attacks are developed and distributed	6
2.2.1	How hackers discover flaws in software.....	7
2.2.2	Hackers write software to exploit the flaw	7
2.2.3	Malware is created by cybercriminals	8
2.2.4	Payload is distributed via exploit distribution networks	8
2.3	How cybercriminals invade PCs.....	9
2.3.1	Social engineering websites	9
2.3.2	Exploitive websites and drive-by downloads	9
2.3.3	Adware distribution	9
2.3.4	Traditional tools to deliver exploits and payloads.....	10
2.4	How cybercriminals operate.....	10
2.4.1	Steal your money.....	10
2.4.2	Identity theft	10
2.4.3	Ransomware	10
2.4.4	Compromise your eBay account	11
2.4.5	VPN IDs and passwords.....	11
2.4.6	Spambot network recruitment	11
3	Why Traditional Security Tools Can't Protect Web 2.0	12
3.1	Traditional end user security tools	12
3.2	Traditional security tools for web developers.....	12
3.3	Program patches from vendors.....	13
4	Collaborative Threat Monitoring and Prevention: The Web 2.0 Solution	14
5	LinkScanner: The First Effective Web 2.0 Security Solution	16
5.1	Plugging the gap left by conventional online security software	16
5.2	How LinkScanner protects your system.....	16
5.3	Fully automatic operation	18
5.4	Extremely frequent updates	18
5.5	Low impact on your PC	18
6	In Summary	19
7	About Exploit Prevention Labs	20

LinkScanner, LinkScanner Pro, LinkScanner Lite, and Exploit Prevention Labs are trademarks of Exploit Prevention Labs, Incorporated. Other product names are the marks or registered marks of their producing companies.

1 Introduction

1.1 What is Web 2.0?

If you share your photos on *Flickr*, you are an active user of Web 2.0. If you have a *Facebook* or *MySpace* page, download video from *YouTube*, subscribe to *RSS* feeds, or use *Wikipedia*, you're also participating in Web 2.0. Web 2.0 describes a new generation of the web, designed around content created by *users*.

High-tech industry people describe Web 2.0 sites as “collaborative”, “participatory and interactive”, “personalized”, or “community-driven” because these sites enable people to go beyond simply reading content provided by others. People can proactively share their interests and ideas with other site visitors. Blogs, podcasts, dating sites, social and business networks, and mashup sites combining data from multiple sites are all part of Web 2.0. This is in stark contrast to Web 1.0 – still what most sites represent – where the content is created by the site owner and offers little or no opportunity for the site visitor to enter into a dialogue or add their own content. Online banking, e-tail stores, and most corporate web sites are examples of the Web 1.0 world.

"I think one pervasive change is the increasing importance of community. That will come in different forms, with different age groups of people and it will change as the technology evolves. But the notion of multiple people interacting on things -- that will continue forever." - Steve Ballmer, CEO, Microsoft, quoted in *The New York Times*, October 14, 2006

Web 2.0 also let you navigate through sites in different ways that can provide a more participatory experience through rich, interactive text and image displays:

- drop down menus that might appear anywhere on the screen
- fly over or pop-up windows
- rollover images that change when you move the mouse over them
- dynamic scrolling menus

All these features enable you to interact with the web site far more than the click-boxes, buttons, and hyperlinks of the typical Web 1.0 site.

Even if you don't think you're visiting a Web 2.0 web site, you may be viewing a page enhanced with Web 2.0 technologies. Companies are beginning to experiment with next-generation web sites using many of these features; Google is a prime example of a company making heavy use of Web 2.0 features and functions.

Web 2.0 sites are fundamentally about making it easy and convenient for web users to share information and build communities of interest, without the need for those users to have any knowledge of programming or website development.

Web 2.0 sites use powerful new technologies that put more intelligence into the browser, to expand the range of what you can see (and hear) at the site. The most important of these technologies for adding power to the browser is *AJAX*, short for *Asynchronous JavaScript* and *XML*. JavaScript is a programming language that can control functions on your system. XML refers to a group of standards for sharing data among different applications. In this context, “asynchronous” means the web page can automatically download additional information or updates after the page itself has finished loading – a typical example would be a stock ticker or baseball scores. These sites don't need you to click on a refresh button or take any other action to keep the content current, as a Web 1.0 site would.

Both JavaScript and XML were in use before Web 2.0. JavaScript was originally developed by Netscape for their Navigator browser in 1995.¹ XML, or *Extensible Markup Language*, evolved in the late 1990s from earlier industry standards. But they are so important for Web 2.0 sites that, if they hadn't already existed, someone would have had to invent them. The acronym AJAX was first used by a speaker at an industry conference in February, 2005 as an easy-to-remember term for the evolving collection of tools being used to build Web 2.0 sites.²

Other key Web 2.0 technologies include IFRAME links and RSS. IFRAME is a programming technique that allows additional content to be embedded into a document or web page. IFRAMES are often used to display banner ads or information about different topics, or from different web sites, on a single page. RSS, or Really Simple Syndication, is a way for users to get updates automatically from a web site, whenever that site changes. Typical uses include news feeds, weather and traffic reports, blogs, and individual pages on social networking sites like Facebook.

1.2 New technologies bring new vulnerabilities

“Web 2.0 is causing a splash as it stretches the boundaries of what Web sites can do. But in the rush to add features, security has become an afterthought” – CNet.

Unfortunately, the same technologies that enhance your web experience can all too easily become powerful tools for far less positive activities when they're in the hands of hackers and criminals out for financial gain. If an innocent user can add innocent content to a web site, you can bet that a malicious user can add malicious content.

Just as there are many Web 2.0 site networks devoted to helping users share their ideas, cybercriminals have set up elaborate and far-reaching sites to distribute potentially malicious content. The most common form of malicious content distributed in this way is known as an *exploit*. Exploits are programs designed to take advantage of vulnerabilities in the way personal computers are configured in order to steal electronic assets – online access to your money, identity, trade secrets, and more.

“Globally, cybercrime is now a bigger problem than drug trafficking. “Last year was the first that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over \$105 billion.” – Valerie McNiven, advisor to the US Government.

“Just as users are getting savvier about protecting their personal info from phishers, they are giving up the farm in new ways, such as posting personal details on sites such as MySpace and Facebook. Add the vulnerabilities that have plagued these sites and you have a privacy disaster on your hands.” Top 3 Threats to Personal Privacy, SC Magazine, December, 2006

Ill-intentioned individuals are able to spread exploits by harnessing Web 2.0 tools such as IFRAMEs and cross-site scripting to insert their malicious code into otherwise innocent sites *without the knowledge of the site operators*. In doing so, they are creating highly dynamic and fast-moving *exploit distribution networks* that take advantage of Web 2.0's collaborative nature. So while you're visiting what would appear to be an entirely legitimate site, for example a mortgage broker or a local construction company, your system can be under silent attack from cybercriminals.

These exploit distribution networks are key in enabling cybercriminals to attack large numbers of people rapidly and at very low cost. The ease of putting malicious content onto a legitimate web site and the power of Web 2.0 technologies both contribute to this problem. Also contributing greatly to the overall problem is the payment of commissions to intermediaries for every PC infected with a malware

*“An online banner advertisement that ran on **MySpace.com** and other sites used a Windows security flaw to infect more than a million users with spyware” – Washingtonpost.com July 19, 2006.*

program. Money is a great motivator of human behavior, and such payments ensure widespread distribution of malicious content.

Web sites operated by a smaller business, an individual, or hosted by a regional ISP are often vulnerable to abuse by hackers because the operators don't have the security expertise to adequately protect their sites (and thus their site visitors) against this type of sophisticated attack.

So what does this tell us?

- You cannot protect yourself just by avoiding pornographic, illegal software downloads ("warez"), online gambling, or other disreputable sites
- When you click on a link, you may not end up on the site you thought you would
- You can't trust a site just because a search engine serves it up to you, even in the organic (non-advertising) listings that appear in response to your search

1.3 What you'll learn from this paper

We've created this paper to help you better understand the threats to your system in the Web 2.0 world. You'll learn who's behind these new dangers, how they are created and distributed, and the very real damage that they can cause to your world, online and off. You'll also learn about Exploit Prevention Labs and their products, which provide effective protection against the exploited web.

You'll also become the personification of Web 2.0 – a veritable goldmine of knowledge about how to keep safe online, that you can and should share with your friends, family, colleagues, and online buddies.

2 Security Issues and Threats

2.1 The changing nature of computer security threats

Viruses and worms have been circulating on the Internet since it first opened up for public use almost twenty years ago. Historically, this kind of malware has been created by maladjusted individuals operating under fantasy names – “nyms” - like *DaRkLord* or *aVEngEr*. Such individuals earned recognition and elite status in their sub-culture by proving that they had the skills to discover and exploit a software vulnerability. The faster the spread worldwide, the larger the number of individuals or companies affected, the greater the damage, the greater the status and recognition for the author.

As the Web became the friendly interface for the Internet, making it accessible to anyone and everyone, hackers kept pace by creating new forms of threat that affected the browser or used the browser as the delivery vehicle. We began to have to protect ourselves against spyware, adware, keyloggers, and other stealthier malware programs. And the first mass market cybercriminals began to appear – making use of these new forms of malware to steal passwords and gain access to confidential information.

Unlike real world crimes, there is almost no personal risk during the commission of a cybercrime. There is also almost no risk of prosecution, simply because the physical world’s legal infrastructure is still struggling to find a way to deal with the virtual world of the Internet. An Internet criminal located in any country, using cybercrime servers located anywhere in the world, can commit crimes against anyone, anywhere in the world, at any time of day or night, using automated, anonymous tools.

2.2 How attacks are developed and distributed

A successful attack on your PC requires both an *exploit* and a *payload*. And of course, an effective way of getting the attack delivered to your system. The exploit relies on an opening in your PC based on a flawed design or a programming error.

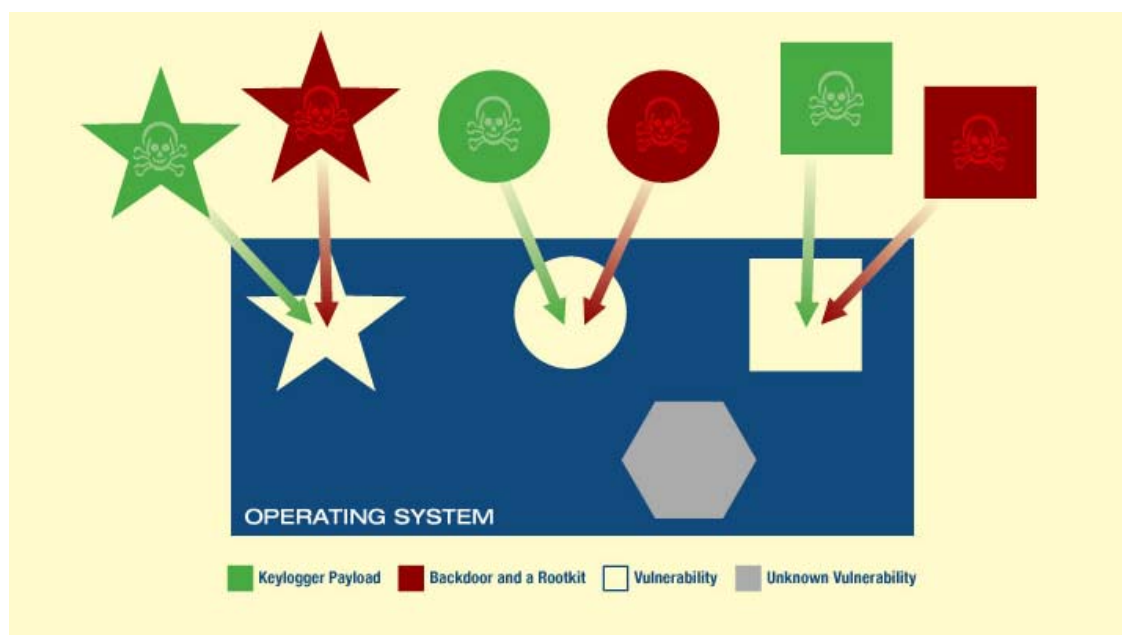


Figure 1: How exploit attacks are developed and distributed

- The exploit is the “delivery vehicle”
- The payload is the “cargo” carried by the delivery vehicle, that is, the malware program designed to steal your confidential information or your personal data and send it off to a web site or server operated by a cybercriminal
- The exploit distribution network is the means by which the malware accesses the websites users are likely to visit

If software were perfectly designed and programmed without any flaws or errors that could be exploited, with built-in security that detected all attempts to compromise your sensitive information and financial assets, the security problem would be a lot smaller. The hacker must have an exploit that he can use to target a flaw or error. Without an available exploit, it would be very difficult for a hacker to deliver his malware payload to your PC.

In the real world of complex software with more features than any one person will ever use, and frequent version releases with hundreds of new features developed under tight deadlines, design flaws and programming errors are unfortunately inevitable. AJAX, for example, is designed to operate in the background. But it has a serious design flaw – there is no built-in way to verify that those actions have a legitimate purpose.

Any software that doesn't validate input can be vulnerable to a buffer overflow. With a buffer overflow, the hacker can overwrite part of the code of the target program with his own code. This would enable him to take control of your system, either to do damage directly, e.g. erase all your files, or to install additional malware. Of course, no software engineer deliberately writes software which is prone to buffer overflows. Testing during development is supposed to identify all such flaws so that they can be fixed before the software is released. But if, as so often happens, the testing procedures fail to catch the buffer overflow (or other program errors), the software will be released with errors. Errors that can and will be discovered by hackers and cybercriminals.

2.2.1 How hackers discover flaws in software

Hackers discover software flaws in a variety of ways.

- Many hackers work hard to discover software vulnerabilities. They share this knowledge through underground web sites and mailing lists for the status among their peers.
- These days, hackers may be in the pay of cybercriminals, or marketing and selling the exploits they have developed rather than simply publishing their discoveries. So software companies may not become aware of vulnerabilities in their code until a new exploit hits.
- Ironically, whenever a software company issues a patch to correct a software flaw, it is like erecting a huge billboard that says, “Hackers, LOOK HERE!” Hackers can examine the patch and figure out what flaw is being fixed – and how. If they didn't know about the flaw before, they do now. This information serves as their guide to writing a program to exploit that flaw. The hackers are relying on the fact that most users don't update their systems until well after the patches are released - if ever.

“eWeek has confirmed the flaw ... on a fully patched version of Windows XP SP2 running IE 6.0. There are at least three sites hosting the malicious executables, which are being served up on a rotational basis.” eWeek, September 19, 2006.

2.2.2 Hackers write software to exploit the flaw

Once a flaw has been discovered, a hacker will often write a “proof of concept” exploit, a form of beta testing, hacker-style, to see whether the newly discovered flaw is indeed real and widespread (ie, worth exploiting). Only later on is the same exploit used for actual cybercrimes.

Hackers rely on users not updating their systems promptly when patches are issued. It makes their life so much easier when it comes to distributing exploits. Hackers and cybercriminals can cut and paste from existing exploit programs to create their own. Since many of these people don't have the ability to actually discover flaws and write their own exploits, they are sometimes derisively known as "script kiddies."

While the true breed of elite hackers may not respect script kiddies, they have no problem making money by selling them easy-to-use tools. *WebAttacker* is an interesting example of a tool designed (and priced) for script kiddies. Developed and sold over the web by a group of Russians, it is designed to enable individuals to easily create malicious web code to download any kind of malware onto an unsuspecting user's PC. WebAttacker looks professional and polished – it even offers support and update services, just like many other software development tools – and costs just a few hundred dollars.

2.2.3 Malware is created by cybercriminals

Once the vehicle has been established, it's time to plug in the payload, which might be:

- A browser toolbar
- Spyware
- A keylogger
- Ad-serving programs (to collect money for distributing ads)
- A back-door program that can turn your PC into a zombie or bot to send spam

In many instances, multiple payloads will be wrapped up in a rootkit that effectively hides all the malware from the operating system as well as traditional anti-virus/anti-malware programs, giving you a false sense of security about the security status of your PC.

Once the exploit has been written with a payload of malware, the cybercriminals can then release it to the world.

2.2.4 Payload is distributed via exploit distribution networks

Cybercriminals use exploit distribution networks to ensure that their malware get widespread exposure quickly. These networks tend to be dynamic, changing their IP addresses frequently to avoid detection, which makes it extremely difficult for the perpetrators to be tracked down. Such approaches might include:

- Upload content to Web 2.0 sites such as blogs, social sites, etc.
- Poison legitimate web sites with hacked IFRAMEs. An IFRAME is a way to embed one HTML document, such as a banner ad, inside another on a web page. However, instead of an actual document, a malicious JavaScript program can be substituted. When you view the affected web page, that malicious JavaScript could automatically download a program (a "drive-by download") or redirect your browser to a site that delivers the drive-by download.
- Infect banner ads so that every time you click on an ad, your system is being silently attacked, Web 2.0 style
- Pay adware distributors (see below) for every copy downloaded onto a user's PC
- Sell the exploits via "Vulnerability Auctions" or on web sites specifically designed for this purpose³
- Infect the copy of a web page stored on a cache server - a server designed to reduce network traffic and improve performance (for example, Akamai). Because these servers are not updated frequently, a stored copy of a bad web page may be sent out to users long after the actual page has been cleaned up or the site taken down

2.3 How cybercriminals invade PCs

There are many ways in which cybercriminals can invade your PC. Most require that your computer downloads some code that exploits a vulnerability in your system and installs malware, as shown in Figure 2 below. These downloads are designed to occur without any action on your part.

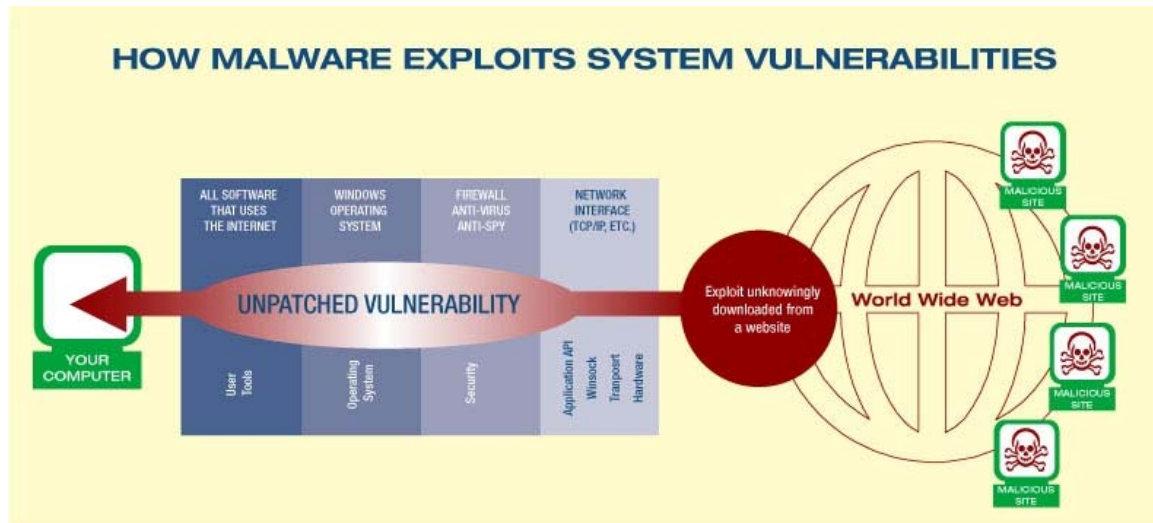


Figure 2. How malicious software gets into your PC by exploiting an unpatched vulnerability.

2.3.1 Social engineering websites

“Social engineering” is a recently-coined term used to describe a range of subterfuges that hackers use to obtain information from people who would not give up this information if they understood the true motivation of the person asking for the information. Account IDs and passwords are a common target. If you visit a web site that offers downloads of movies or music, but which actually contains hidden malware, you are being subjected to a social engineering attack.

Phishing and its close relative, *spearfishing*, (targeting just one group or organization) are forms of social engineering delivered by email or instant messaging.

2.3.2 Exploitive websites and drive-by downloads

The online experience that is most responsible for users’ increasing mistrust of the Internet is the *drive-by download*. Drive-by downloads occur when you visit a website and, while you are innocently reading the content, the site’s web server is busy installing malicious software on your system in the background, with little or no warning, and certainly without your permission. The result can be anything from a whole slew of new and unwanted programs and pop up ads to a keylogger, a back door, ad-serving programs, and a rootkit that effectively hides the other programs from the your traditional security tools. Such sites are at the heart of an effective exploit distribution network.

2.3.3 Adware distribution

Advertising and affiliate programs designed to increase the distribution of banner advertisements and adware programs installed on users’ PCs may be unwitting - or perhaps witting -distributors of exploits.

2.3.4 Traditional tools to deliver exploits and payloads

The increasing popularity of web-based attacks doesn't mean that cybercriminals have stopped using traditional methods of malware delivery like:

- Email attachments – viruses and worms
- Phishing emails
- Peer-to-peer file sharing
- Port scans from the Internet to discover unprotected entry points to your system

2.4 How cybercriminals operate

Cybercriminals aim to install a variety of malware on your system using one or more of the above approaches. Regardless of the method, the goal is always the same: steal information that will enable them to defraud you or someone close to you.

It is very important to understand that SSL security (usually represented by a small padlock icon in your browser) cannot protect you against these types of attack. SSL works by encrypting the data as it leaves your browser on its way to an ecommerce or other secure server, so that no one can snoop on that data as it moves over the Internet. But cybercriminals aren't snooping on your data as it passes over the Internet. That approach is so 1990s. They are taking it right from your system.

2.4.1 Steal your money

Cybercriminals can drain your savings and checking accounts⁴, make purchases with your credit cards, and loot hundreds of thousands of dollars from your investment and retirement accounts⁵. *All your assets are potentially at risk from cybercriminals.*

2.4.2 Identity theft

Cybercriminals can use your social security number, mother's maiden name, driver's license number, and other confidential information to purchase cars with a loan, open new credit card accounts, and even apply for a second mortgage on your house.

It can take literally years, consuming thousands of hours of effort and large legal fees, to untangle yourself from these actions and clean up your credit rating.

2.4.3 Ransomware

A particularly obnoxious form of theft involves installing a bogus spyware program like *SpySheriff* without your knowledge on your PC. Once active, this program will constantly flash up warnings that your PC is infected with spyware, which it is. To "fix" the problems, you have to purchase this program for about \$50.

This is extortion, simply put, since the problem you are fixing was created by the *SpySheriff* author. You are paying a "ransom" to get back the free unfettered use of your PC. And of course, you used your credit card to pay for this program, exposing yourself to credit card fraud.

"Identity thieves are manipulating a feature in Apple Computer's embedded QuickTime player ...exploiting the JavaScript support in QuickTime and targeting a MySpace vulnerability to lure users to phishing sites. The double-barreled attack is replacing legitimate links on users' MySpace profiles with links to malicious sites cleverly masked to look legitimate.

"Once a user's MySpace profile is infected-by viewing a malicious embedded QuickTime video-that profile is modified in two ways [according to security researchers]. The links in the user's page are replaced with links to a phishing site, and a copy of the malicious QuickTime video is embedded into the user's site.

"Any other users who visit this newly infected profile may have their own profile infected as well.

"The flaw [allows attackers] ...to steal [user IDs and passwords] when the target is unexpectedly redirected to the attacker's site." – eWeek, December 4th, 2006

A variant of this crime involves a cybercriminal encrypting some important data files on your PC. News reports have quoted a \$200 payoff to retrieve use of your data files.

2.4.4 Compromise your eBay account

A cybercriminal who hijacks your eBay account can trade on your reputation to get bids on fraudulent sales for expensive items such as high-end digital cameras, often requiring an untraceable Western Union money transfer for payment. The resulting negative feedback can ruin your eBay business.

2.4.5 VPN IDs and passwords

If you work from home or travel for your company, you probably use a VPN to access the corporate network. If a cybercriminal can steal your login ID and password, he can gain access to your company's confidential financial, customer, and trade secret information.

2.4.6 Spambot network recruitment

In addition to stealing your confidential information, cybercriminals try to gain control of PCs for use as a spambot or zombie. In the cybercriminal world, there are specialists who build up networks of zombie computers; these networks are rented or sold on underground web sites to criminals who use them to send out spam or overwhelm and shut down business sites with "denial of service" attacks.

3 Why Traditional Security Tools Can't Protect Web 2.0

3.1 Traditional end user security tools

As important and essential as traditional security tools such as anti-virus, anti-spyware, and firewalls are, they cannot protect your or your system against Web 2.0 threats. Firewalls cannot stop exploits because exploits enter within the trusted communications stream of the user's browser connection. Anti-virus and anti-spyware applications can't protect against exploits because they must wait for the malware code to hit the hard disk in order to detect it, and by that time most exploits have already executed their payload. Patch management systems can't distribute a patch until the application vendor releases it. And patching as a general practice, while critical, often fails because it relies on users taking action of their own volition.

Protection Process	Anti-Virus	Anti-Spyware	Firewall
Stops zero-day exploits from installing rootkits and other malware via drive-by-downloads .	NO	NO	NO
Blocks known bad websites before they can infect your PC.	NO	NO	NO
Scans and removes viruses and other malware after they have gained access to your PC.	YES	NO	NO
Blocks programs that you have not authorized to access the Internet.	NO	NO	YES
Scans and removes spyware and other malware after they are on your PC.	NO	YES	NO

Table 1: Key shortcomings of traditional security tools

Traditional security tools cannot protect against:

- Drive by downloads
- Social engineering web sites
- Malware that has not yet landed on your PC

To deal specifically with Web 2.0 security risks, you could use an advisory website or service that provides lists of known bad sites and URLs. In principle you should be safe if you always check a new URL against such lists before going to a new site. Except that these services rely on whether a site was good or bad the last time they looked at it, which might have been six months ago. And as we've already noted, the dynamic nature of both Web 2.0 sites and exploit distribution networks pretty much guarantees that this advice is likely to be unreliable or out-of-date at best.

3.2 Traditional security tools for web developers

Web developers have "crawler" tools that scan their web sites for security weaknesses. These tools work reasonable well for Web 1.0 sites, where the site owner controls all the content. But with Web 2.0, anyone could be supplying content. If the site includes links pointing to JavaScript that uses AJAX programs to bring in data via XML, the crawler program will miss malicious content being pulled in.⁶

Thus, even a security-conscious Web 2.0 site operator can't always be sure that the site is 100% free of malicious content.

3.3 Program patches from vendors

Program patches, once deployed, are an effective way to stop exploits from taking advantage of vulnerabilities in your system. However, the average time for a patch to be written, tested to ensure that it works properly and doesn't cause unintended side effects, is currently 56 days.

Realistically, the number of vulnerabilities is too large for a patch to be written for each and every one. Vendor software engineers have to set priorities for patch development. There is always the risk that a "low priority" vulnerability gets exploited to spread new malware.

And of course, patches are only effective if they are installed ...

4 Collaborative Threat Monitoring and Prevention: The Web 2.0 Solution

The combination of increasing popularity of Web 2.0 web sites, and the growth of the cybercrime, means that you can no longer rely on traditional tools to protect yourself; the tools aren't designed to cope with the dynamic nature of these threats.

And you can no longer rely on a well-known and trusted web site to keep its content 100% safe.

Exploit Prevention Labs (XPL) has developed a unique approach to security that tracks threat patterns, can determine in real time whether a web site has been exploited, and can deliver protection to your computer within minutes of a new exploit being detected. The company has been able to do this by leveraging the spirit of community that is driving the evolution of Web 2.0.

The Exploit Intelligence Network is in effect an early warning system that uses a combination of automated software programs and human researchers for monitoring both existing known threats and new ones as soon as they first appear, literally within minutes of release. This information is augmented by reports from XPL customers, creating the cyber equivalent of "Neighborhood Watch". In this case, the neighborhood is the global web, but the principle is the same: more people watching leads to improved security.

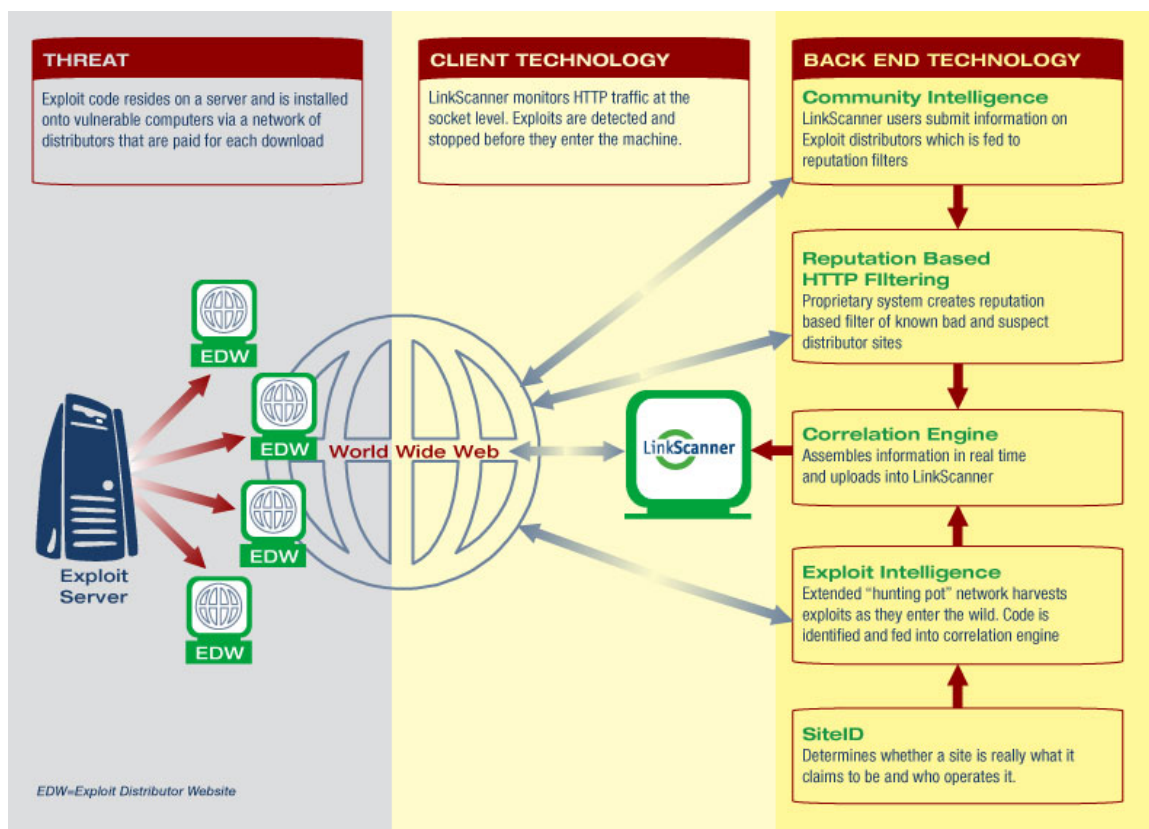


Figure 3: The Exploit Intelligence Network

Exploit Prevention Labs' research network comprises:

- A network of hunting pots or nodes all over the world that actively monitor known cybercriminal sites
- Human monitoring of security and hacker mailing lists
- The community of XPL software users who allow information about attempted exploitation of their computers to be collected.
- A reputation filter to identify known and suspected exploit distribution sites
- SiteID, a tool that digs beneath the surface of any site's publicly-stated ownership to determine whether the site is really operated by the person or entity who claims to own it

A *Correlation Engine* aggregates the intelligence gained through this research, assembles it in real time, and distributes it transparently back to the XPL product user community, providing exploit-specific protection in minutes.

These methods have been in use for long enough that the company can almost guarantee to detect new exploits within minutes of their first appearance in the wild. The information collected this way feeds a testing methodology that confirms the exploit, determines the payload, identifies signatures (a digital "fingerprint" that is unique to that exploit) and variants, and deploys that information to the XPL update server, which sends it out to all users.

5 LinkScanner: The First Effective Web 2.0 Security Solution

LinkScanner is a Windows application that provides real-time, automatic protection against malicious web sites, drive-by downloads and other crimeware exploits, delivered behind the scenes, so that users can enjoy safe surfing all the time.

5.1 *Plugging the gap left by conventional online security software*

Conventional safe surfing applications, which judge web site safety based on historical data, are recognized as delivering results that can be up to 50% inaccurate. LinkScanner's real-time approach delivers definitive information about the threats present on any web site at the only time that matters – when you're about to click through to that site.

Exploit Prevention Labs' own research shows that only a relatively small number of exploit delivery vehicles is used by cybercriminals to attack systems, But do not be lulled into a false sense of security because there are nowhere near as many current exploits as current viruses. Speed and scale of distribution is what matters on the web, and each new exploit can be distributed to tens of thousands of websites in just a few minutes.

Rather than taking the traditional approach of the anti-virus and anti-spyware companies of identifying and blocking each individual item of malware, Exploit Prevention Labs' technology prevents the cybercrime from happening in the first place, focusing on blocking the criminal over the crime.

In addition to providing more effective security than site advisory services, LinkScanner provides a critical layer of security that complements the defenses provided by traditional security solutions.

“The exploit was developed by a single group and sold to hundreds of criminal gangs with the understanding that they would not deploy until a specified date. This is an unprecedented level of cooperation exhibited by these bad guys. ... (T)hey also used an ... exploit against the Linux utility cPanel to install their VML exploits on hundreds of unsuspecting mom and pop web servers which then infected anyone browsing to those web sites⁷.” - Roger Thompson, Chief Technology Officer of XPL

5.2 *How LinkScanner protects your system*

LinkScanner technology is highly dynamic, enabling it to react quickly and effectively to protect computers without introducing time-wasting false alarms or out-dated databases. Its protection and site ratings are based on a current inspection of the web site, its content and the data stream entering your computer. Using this approach, LinkScanner can provide a timely and accurate analysis of every web site and alert you of suspicious activity or block attempts to exploit software vulnerabilities and compromise your computer.

- **Always-on expanded threat blocking** – Protects you against exploits, hacked web sites, phishing, social engineering, malicious lure sites, and adware server attacks
- **Real-time site risk analysis** – Gives you up-to-the-second advice on how safe it is to visit a site
- **Internet connectivity monitor** – Displays all programs sending and receiving data on your network
- **Web search results inspection** – Tells you which search results sites are safe, dangerous and why

- **On-demand URL scanning** – Lets you check any individual url for site insecurities before you go there

The best way to demonstrate this is to let the LinkScanner Pro software speak for itself. The following screen is what you'd see if you were to attempt to visit a site that's been exploited by cybercriminals.

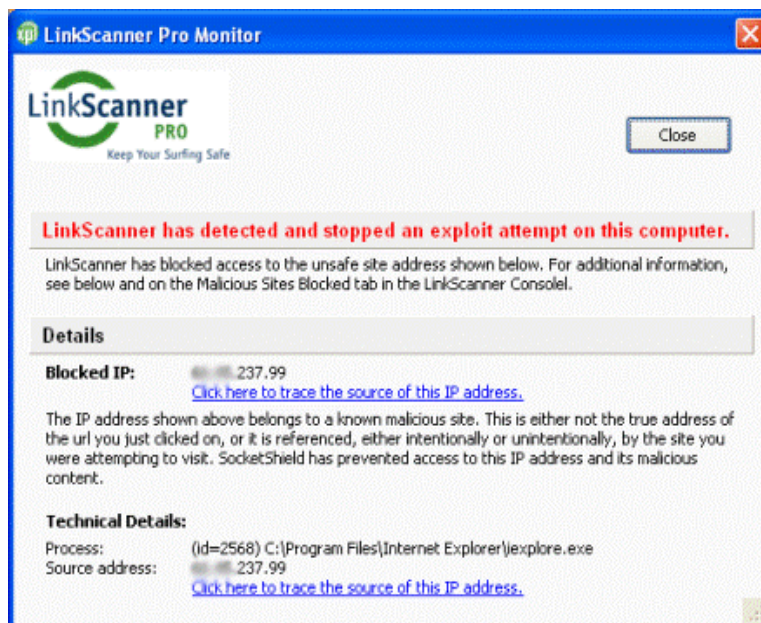


Figure 4: LinkScanner automatically blocks a bad site from infecting your PC.

Web 2.0 demands this scrutiny because of the growing trend to assemble content from multiple sources, and at the last second. Add the serious threat of hacked web sites and phishing scams to the explosion of user-generated content, and you can see why it is imperative to analyze a web site at the moment you visit. Only then can the true safety of a web site or page be determined.



Figure 5: LinkScanner identifies any threats in the results of a Google, Yahoo or MSN search.

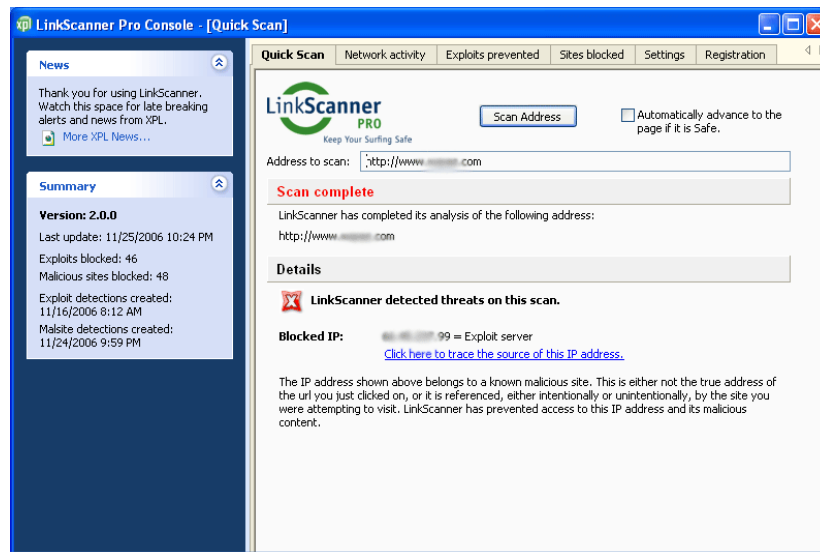


Figure 6: Detailed LinkScanner information on the threat(s) found

5.3 Fully automatic operation

LinkScanner operation is 100% automatic, once the program is installed. You don't have to become a security expert or spend all your free time reading "security advisories. The only action required from you is to click on the CLOSE button of an Alert window.

5.4 Extremely frequent updates

Every 15 minutes, the program queries the XPL servers to see if there is an updated set of exploit signatures, malsite addresses or software. If an update is available, the program downloads and activates it immediately. This frequent update process is essential because of the dynamic, fast-moving nature of exploit distribution networks.

5.5 Low impact on your PC

After you install LinkScanner, you won't notice any change in performance, as LinkScanner uses very little disk space and memory. The URL scanning process itself is very efficient, and displays results almost immediately.

6 In Summary

The Web 2.0 world is quite different from Web 1.0. But as we've seen, it's important to remember that the same technology that makes Web 2.0 so engaging and exciting to use also creates significant opportunities for cybercriminals to attack your system in new and sophisticated ways.

Traditional security tools were not designed with these new risks in mind, and so you should not rely on them to protect you in a Web 2.0 world. You need protection that uses the collaborative spirit of Web 2.0 to deliver real-time protection against today's dynamic threats. Only LinkScanner from XPL can give you that protection in an effective, reliable, and easy-to-use form.

LinkScanner comes in two versions: LinkScanner Lite and LinkScanner Pro:

Feature	Lite	Pro
Web search results inspection Automatically inspects all search results from major search engines for exploits and displays advice. (<i>Internet Explorer only</i>)	✓	✓
Real-time site risk analysis Immediate, up to date analysis of any html web page for exploits and other risk factors.	Manual	Automatic
Always-on exploit blocking Blocks drive-by downloads "in-the-stream" before they infect your PC.	-	✓
Expanded threat detection Continuous updating protects against the latest vulnerability exploits, including zero-day attacks.	Manual	Automatic
Exploit Intelligence Network Patent-pending dynamic hunting-pot research network, enhanced with real-world user data.	✓	✓
Internet connectivity monitor Tracks and displays active Internet-using processes on your PC.	-	✓
Alert reporting and logging Full details of threat detection and site blocking activities.	-	✓

LinkScanner Lite is free of charge; LinkScanner Pro costs \$29.95 or less.

So visit www.explabs.com today to download the version that's right for you and start surfing with confidence, knowing that attacks are stopped before they can ever reach your PC.

7 About Exploit Prevention Labs

Founded by information security veterans Bob Bales and Roger Thompson in 2005, Exploit Prevention Labs develops the LinkScanner family of safe surfing software and services. LinkScanner Pro, LinkScanner Lite and LinkScanner Online provide patent-pending protection against malicious web sites and web-based exploits during the critical risk window between the announcement of a security vulnerability and the provision of a patch by the vendor. A Software Development Kit (SDK) is also available to enable third party vendors to incorporate Exploit Prevention Labs' technology in their own applications and services. More information about Exploit Prevention Labs and LinkScanner may be found on the company's website at <http://www.explabs.com>.

¹ www.wikipedia.org/javascript#history.

² "Ajax: A New Approach to Web Applications",
<http://www.adaptivepath.com/publications/essays/archives/000385.php>

³ "Web Security Trends Report," Finjan Malicious Code Research Center, Q2 2006. pdf file,
www.finjan.com

⁴ Tom Costello, "Crooks Clean Out Couple's Online Bank Account," msnbc.com, December 14, 2005

⁵ Eric Dash, "E*Trade offers to Reimburse Any Victims of Online Fraud", New York Times Online, January 18, 2006.

⁶ "Hacking Web 2.0 Applications with FireFox, Shreerah Shah, October 11, 2006,
www.securityfocus.com/infocus/1879/1