



LinkScanner Lite™

User Guide

What is LinkScanner Lite?

LinkScanner Lite is a safe searching, safe browsing utility that provides real-time analysis and advice on web site content and behavior safety to protect you against a wide range of online threats, including malicious content, phishing, social engineering and targeted software exploits.

LinkScanner Lite's technology is highly dynamic, enabling it to provide timely, accurate advice without relying on out-dated databases that introduce time-wasting false alarms. Its protection and site ratings are based on an inspection of any requested web page *in its current state*. Using this approach, LinkScanner Lite can provide a timely and accurate analysis of web hyperlinks before you click through to that page to alert you of suspicious activity and notify you of threats to exploit software vulnerabilities and compromise your system.

The dynamic Internet (often called Web 2.0) of integrated RSS feeds, distributed advertising networks, blogs, forums, and wikis demands this level of scrutiny, thanks to a growing trend for sites to present content from multiple sources. Add the serious threat of poisoned web sites and phishing scams to this explosion of user-generated content, and it's clear why it is vital to analyze a web site at the moment you visit. Only then can the true safety of a web page be determined.

LinkScanner Lite performs web site inspections in two ways: **SearchShield** and **QuickScan**.

- With **SearchShield**, LinkScanner Lite inspects search results delivered by Google, Yahoo and MSN to advise you, before you click, the level of trustworthiness you should accord each url and why. **LinkScanner Lite** classifies every inspected site in one of four categories:

Dangerous: This page contains active threats.

Risky: This page contains the potential for active threat delivery.

Questionable: Site ownership or registration is not clear.

Safe: This page contains no active threats..

- With **QuickScan**, LinkScanner Lite enables you to scan any hyperlink by simply right-clicking on the link. Again, the current relative trustworthiness of the site is reported before you click through.

Research: the fuel for online security

Key to a safe Internet experience is timely, accurate information about a site's trustworthiness and the rapid Key to online security is timely, accurate information about a site's trustworthiness and the rapid detection and blocking of malicious web sites and exploits.

The patent-pending Intelligence Network behind LinkScanner Pro is the most extensive and sophisticated research operation of its kind in the world, with high levels of knowledge about new and old threats alike. The architecture is such that update files can be issued several times an hour (the current default is every 15 minutes) without impacting system performance. Plus, an override function allows Exploit Prevention Labs to push an unscheduled update out in the case of a particularly fast-moving threat or zero-day attack.

Rapid deployment is only valuable if the ammunition deployed is of high quality. Exploit Prevention Labs' research brings together four components which together create a combined early warning and "neighborhood watch" system that makes it possible to identify and protect against exploits and zero-day attacks in the wild within minutes of their release.

- **Exploit Intelligence** is an extended network of human researchers, automated probes, honeypots, "hunting pots," and search bots focused on discovering new vulnerabilities and exploit examples.

- The **Reputation Filter** creates an intelligent filter for known and suspected exploit distribution sites.
- **Community Intelligence** is the community of Exploit Prevention Labs users like you who allow information about attempted exploitation of their computers to be collected. This data collection process allows LinkScanner users to serve as an extension of Exploit Prevention Labs' research efforts, providing a virtual Neighborhood Watch for the Web to report new malicious web sites, hyperlinks and exploits back to Exploit Prevention Labs researchers.
- The **Correlation Engine** aggregates intelligence gained through this research, assembles it in real time, and distributes it transparently back to the community, providing exploit-specific protection within minutes of a zero-day exploit discovery.
- **SiteID** 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.

Taken together, Exploit Prevention Labs' multi-faceted research and compact, efficient software provides the most thorough and accurate security protection for web surfers everywhere.

Table of Contents

WHAT IS LINKSCANNER LITE?	2
RESEARCH: THE FUEL FOR ONLINE SECURITY	2
ABOUT THIS GUIDE	5
INSTALLATION AND SETUP	6
SYSTEM REQUIREMENTS	6
INSTALLING LINKSCANNER LITE.....	6
SETUP AND INTERFACE	11
PROGRAM COMPONENTS.....	11
LINKSCANNER LITE MONITOR	11
<i>LinkScanner Lite Console</i>	12
ADVICE, ALERTS, AND ICONS	15
SEARCHSHIELD THREAT INDICATORS	15
UPDATE NOTIFICATIONS	16
USING SEARCHSHIELD	17
USING QUICKSCAN	19
RIGHT-CLICK QUICKSCAN.....	19
CONSOLE QUICKSCAN.....	20
REPAIRING AND UNINSTALLING LINKSCANNER LITE	21
SUPPORT AND DOCUMENTATION RESOURCES	23
RESOURCES AVAILABLE.....	23
<i>Knowledgebase</i>	23
<i>LinkScanner Lite Release History</i>	23
GLOSSARY	24

About this guide

This guide is intended to assist with the installation, operation, and troubleshooting of **LinkScanner Lite**. For help with **LinkScanner Pro**, please download the LinkScanner Pro [Users Guide](#).

- For installation instructions, read the section entitled **Installation and Setup**
- For operational instructions, read the sections entitled **Configuration** and **Alerts and Icons**
- To uninstall the software, read the section entitled **Uninstalling LinkScanner Pro**

If, after consulting this guide, you still have questions or concerns, please visit the frequently asked questions area on our website or contact our helpdesk using the form at <http://www.explabs.com/support/form.asp>

Installation and Setup

This section walks you through the installation of **LinkScanner Lite**.

Please take note of the following requirements before starting the **LinkScanner Lite** installation process:

- You will need to be logged into Windows with an Administrator account or an account that has Administrative privileges. To see if your account has the appropriate privileges, go to **Start | Settings | Control Panel** and double-click on the **Users** category. This will show you all of the user accounts on your machine and what their privileges are.
- We recommend closing all open applications before starting the installation, as your computer will need to be restarted for **LinkScanner Lite** to start protecting your system. This restart is necessary because **LinkScanner Lite** needs to register system files in order to protect your computer from exploits, and it cannot do that until your system goes through the startup process.
- During installation, you will be asked to supply certain personal information for registration purposes. See the privacy statement on our website at <http://www.explabs.com/about/resCenter/privacy.html> for more information about how we use information we collect from our customers.

System Requirements

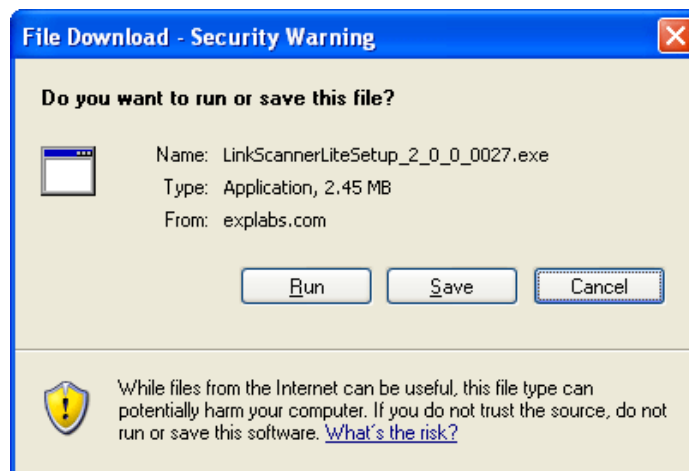
- Pentium 1.2 GHz or faster
- 256 MB RAM
- Microsoft Windows 2000, Windows XP Home, or Windows XP Professional

Note that Internet Explorer 6.0 or later is currently required for full SearchShield and QuickScan support; support for other browsers will be added shortly.

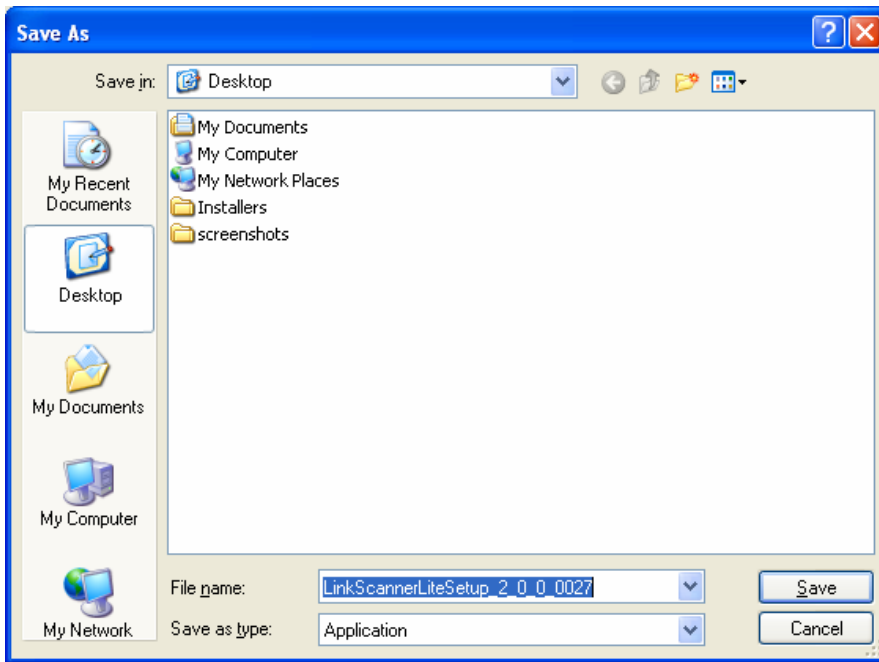
Installing LinkScanner Lite

To download the software, go to <http://www.ExplLabs.com/ss/download.html>

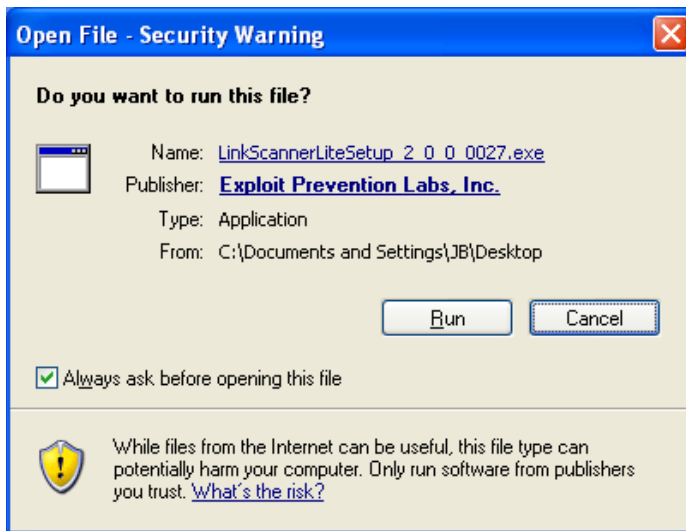
Click the link to display the download box, then click **SAVE**



Accept the default folder suggestion or select a different folder where you would like to save the program. If you are not sure where to save the file, choose **Desktop** from the drop-down list



When the Security Warning screen appears, click the **Run** button to activate the download process.



Once the file has finished downloading, double-click on the **XPL** icon to begin the installation process. You will be presented with a Welcome screen.



Click the **Next** button to start the installation.

Read the License Agreement carefully, as it contains important information. You must accept the License Agreement before you can continue with the installation. To do this, place a checkmark in the box that states “I have read, understand, and accept the license agreement” and click **Next**.

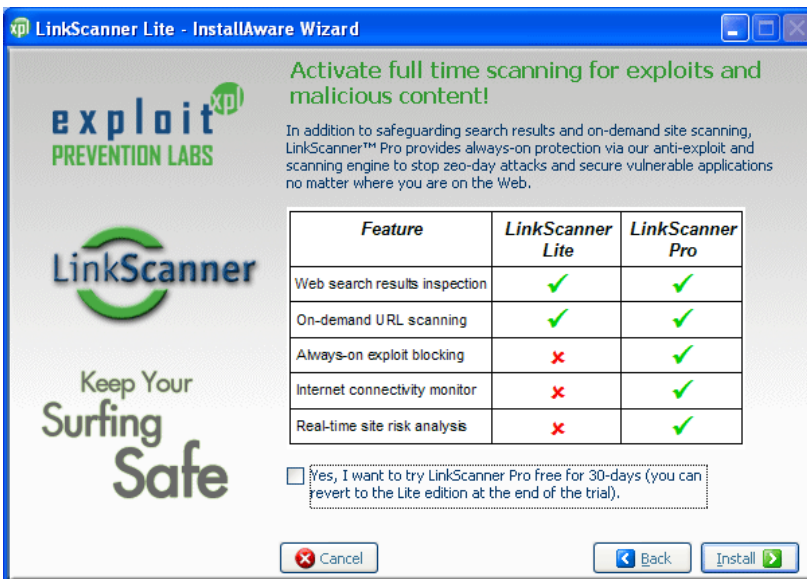


On the registration screen, enter your name and email address. If you do not wish to receive alerts about product updates and customer news, uncheck the box below your email address and click **Next**



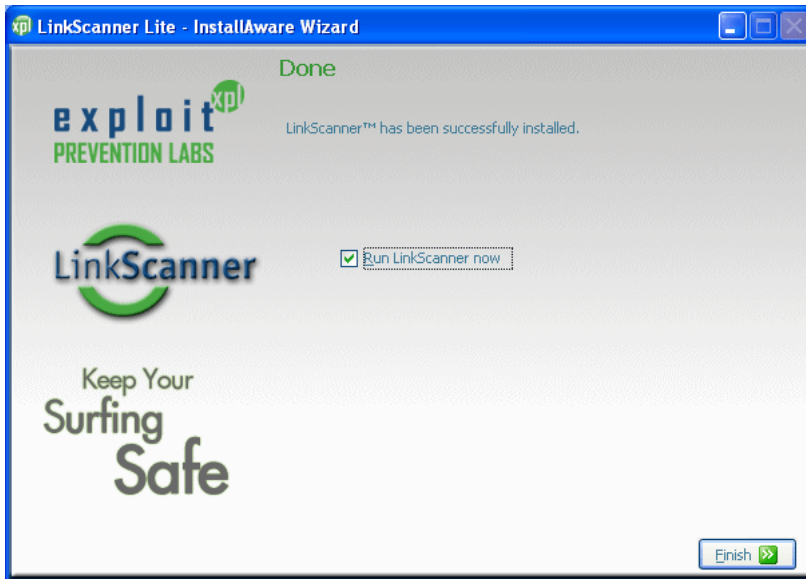
The next screen describes the differences between **LinkScanner Lite** (this free product) and **LinkScanner Pro** (which requires payment of a license fee). You can choose at this point to install a free trial of **LinkScanner Pro** instead of **LinkScanner Lite**. If you do decide to install the trial version of **LinkScanner Pro**, place a checkmark in the box below the table and click next.

The trial version of **LinkScanner Pro** will expire after 30 days. At that time, if you choose not to purchase the product, the software installation will revert to **LinkScanner Lite**. For help with **LinkScanner Pro**, download the appropriate [User Guide](#).



If you decide to stay with **LinkScanner Lite**, click Install to start the installation process.

Once the installation process is complete, the **Done** screen appears. Leave checked the box that states **Run LinkScanner now**, and click the **Finish** button.



Setup and Interface

This section explains how the different aspects of **LinkScanner Lite** work.

Program components

You can access the different **LinkScanner Lite** components by going to **Start | Programs | LinkScanner Lite**. (You may have **All Programs** instead of **Programs**, depending on which version of Windows you are running). Highlight **LinkScanner Lite**; a new menu will appear:

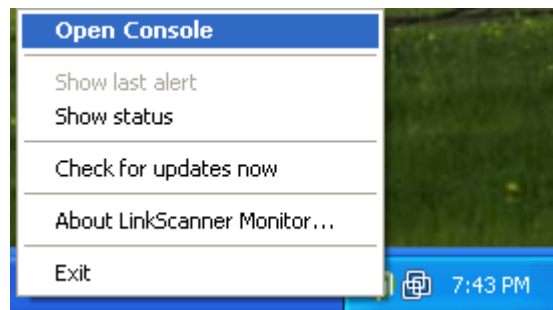
- Select **LinkScanner Lite Console** to customize your installation, view a list of exploits and malicious websites that have been blocked, and check out the latest news from Exploit Prevention Labs. You can also run a **QuickScan** to check the safety of any individual url before you go there.
- Select **Repair or Remove LinkScanner Lite** to either
 - Run a Repair utility to fix any corrupted or missing files
 - Remove **LinkScanner Pro** and all of its components
- Select **Support and Documentation** to visit the Exploit Prevention Labs support website. From this site you can view our Knowledge Base, enter a support request, report a new exploit, and much more.

Once you have installed **LinkScanner Lite**, you will notice a new icon in your system tray, usually along the bottom right hand side of your screen. The icon will look like this.

LinkScanner Lite Monitor

The **LinkScanner Lite Monitor** icon is inserted into your systray at the conclusion of the installation process. Right-click on the icon to display the menu:

- **Open Console** - opens the main Console for **LinkScanner Lite** (see below for more details)
- **Show status** – displays the categories of threat your system is protected against.
- **Check for updates now** – instructs **LinkScanner Lite** to contact the Exploit Prevention Labs update server for the latest updates
- **Exit** - closes the monitor (not recommended, as this will shut down the **LinkScanner Lite** protection)



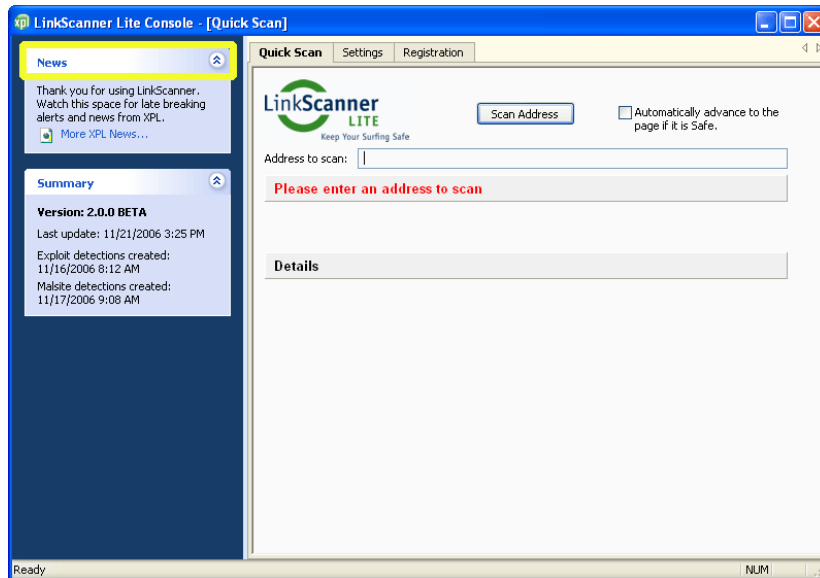
Double-clicking on the **LinkScanner Lite** Monitor icon will open the **Console**.

LinkScanner Lite Console

The Console lets you customize your installation of **LinkScanner Lite** to best fit with the way you use your computer. Right-click on the Monitor icon in the systray and then click on Open Console to open the console. Here's what's available to you from the Console:

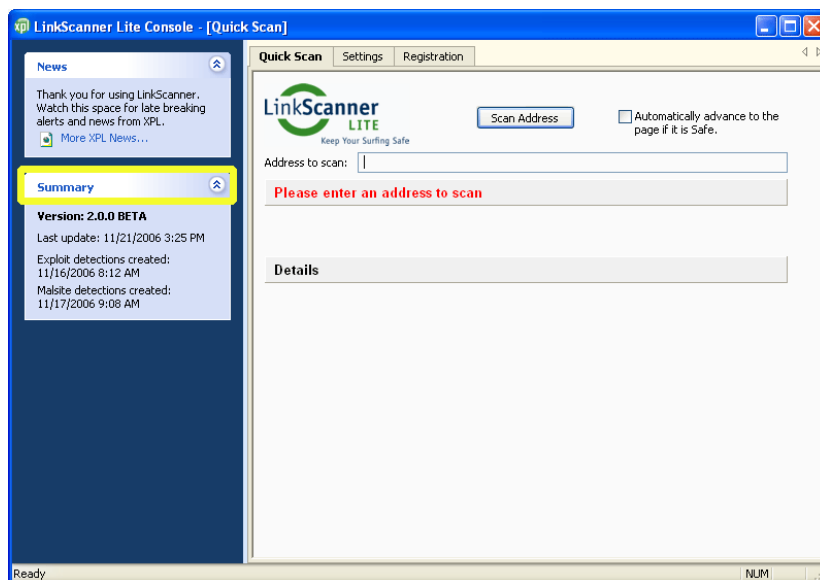
The **News** window is located in the upper left hand side of your screen. Its function is to

- Alert you to increases and/or decreases in global exploit activity
- Provide information on the latest threats and malicious activities
- Link to the Exploit Prevention Labs website for further information



The **Summary** window provides information on the program and its status:

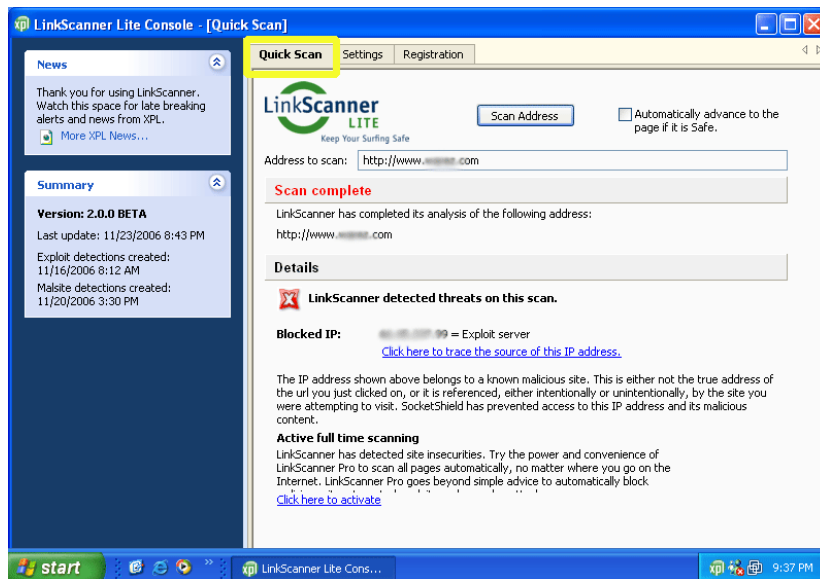
- The currently-running version of **LinkScanner Pro**
- The number of **Exploits** and **Malicious sites** that have been blocked
- The date on which your current **Exploit** and **Malicious sites** detection strings were created.



Each of these windows may be minimized if you do not want to keep this information on continuous display. To do this, just click on the arrows to the right of each heading. To redisplay the information, simply click on the arrows again. These controls are available whenever the Console is open.

On the right side of the screen, you will see six tabs along the top. Click the tab to display the information.

QuickScan allows you to immediately scan any url for site insecurities before you visit. Just enter the url into the **Address to scan** box and click on the **Scan Address** button in the top center of the screen. The time taken to complete a scan will depend on how many links are on the page, as **QuickScan** will scan all the links on that specific page.

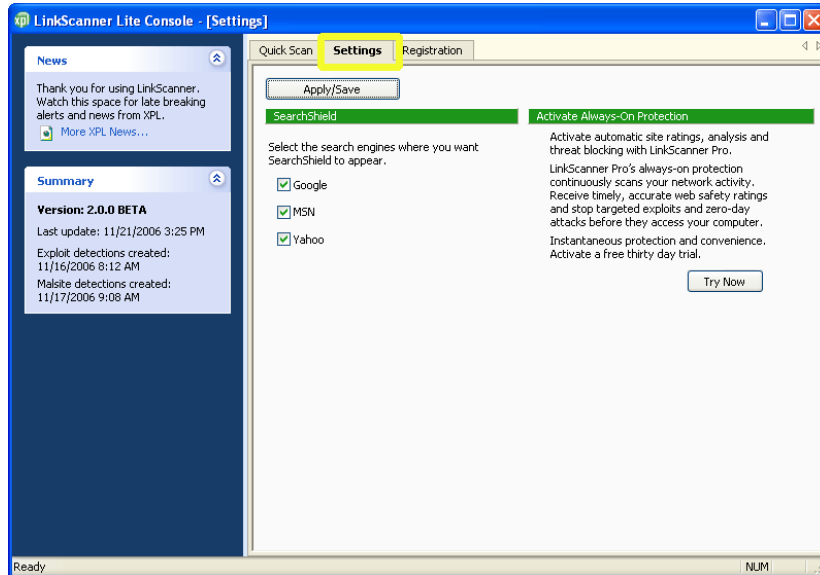


Settings lets you customize how your **LinkScanner Lite** installation operates.

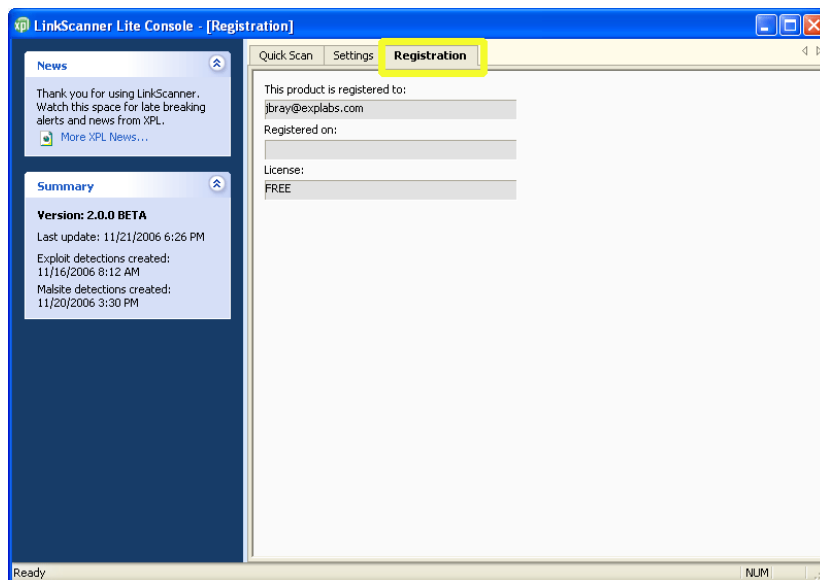
The **SearchShield** section lets you select which search engine(s) you would like to use in conjunction with **LinkScanner Lite**. The options are currently:

- Google
- Yahoo
- MSN

There is also a **Try Now** button that gives you ongoing access to the **LinkScanner Pro** trial if you find at any time that you would prefer the always-on protection of this product.



The **Registration** screen displays the email address you entered when you registered the software, as well as the date it was registered.



Advice, Alerts, and Icons

This section describes the different alert windows that appear when **LinkScanner Pro** notifies you of a suspicious web site or blocks an exploit or malicious site.



The **LinkScanner Pro Monitor** icon is automatically installed in your system tray when the software is installed

SearchShield Threat Indicators

LinkScanner Lite provides information about your search results using a technique called **SearchShield**, which classifies every inspected site in one of four categories.







- Dangerous: This page contains active threats.
- Risky: This page contains the potential for active threat delivery.
- Questionable: Site ownership or registration is not clear.
- Safe: This page contains no active threats.

To determine the status of a website, **LinkScanner Lite** uses three methods of investigation.

Method #	Method Name	Process
1	<i>Realtime Bad List Lookup</i>	Is this site/page one of our known malicious sites/pages?
2	<i>Realtime Paper Trail Evaluation</i>	If it is not on the known bad list, a site is evaluated on the fly using a variety of 'background check' procedures.
3	<i>Realtime Content Inspection</i>	If the site is not on the known bad list and the paper trail is clean, LinkScanner Pro examines the actual page content looking for exploits and other malicious content.

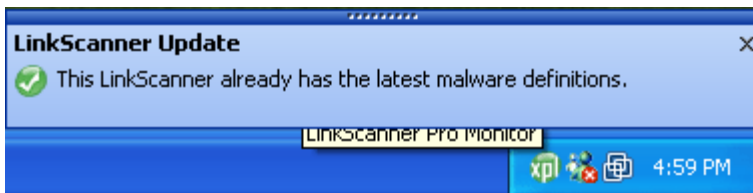
Once all three methods have been applied to the selected url, one of the four threat indicator icons is applied to that url; The table over the page shows what each icon represents and an explanation of what the risk level means.

After performing a search using Google, Yahoo or MSN, SearchShield will display these icons as appropriate alongside each of the search results.

Symbol	aRisk Level	Explanation
	Safe	Safe and free from exploits, phishing, social engineering and other threats.
	Questionable	There is a very limited chance the page may contain harmful content. You should be wary if the site/page is unknown to you or it involves online purchasing or login information of any kind.
	Risky	There is a reasonable chance that the page contains links to harmful content. You should not go there unless you have previous experience with the page/site and should carefully consider what personal information, if any, you share with the owner.
	Dangerous!!!	The site has been set up to deliver exploits without user knowledge or permission and/or is a known phishing, social engineering or other malicious site. LinkScanner Pro prevents you from accessing this site and, if any direct exploit threat is present, blocks that code from entering the computer.
	Unknown	LinkScanner Pro was unable to scan this page. This could be because the page is no longer there, is malformed, is not an actual webpage (PDF, MP3 or the like). It could also be the result of an unexpected error in LinkScanner Pro when scanning the page.
	Animated Clock Image	This rating symbol means that LinkScanner Pro is scanning the page

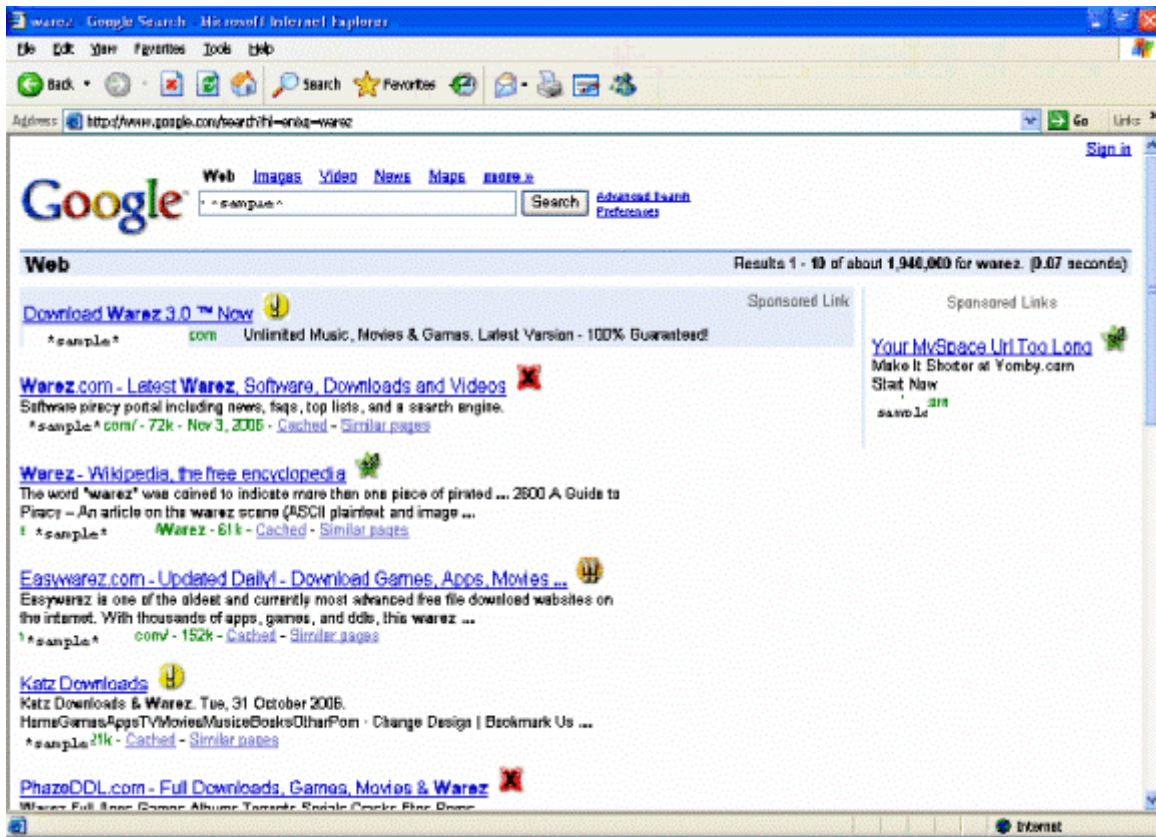
Update Notifications

LinkScanner Lite will also notify you every time an **update** has been downloaded. Updates include new malware definitions, as well as any program updates that may be available.

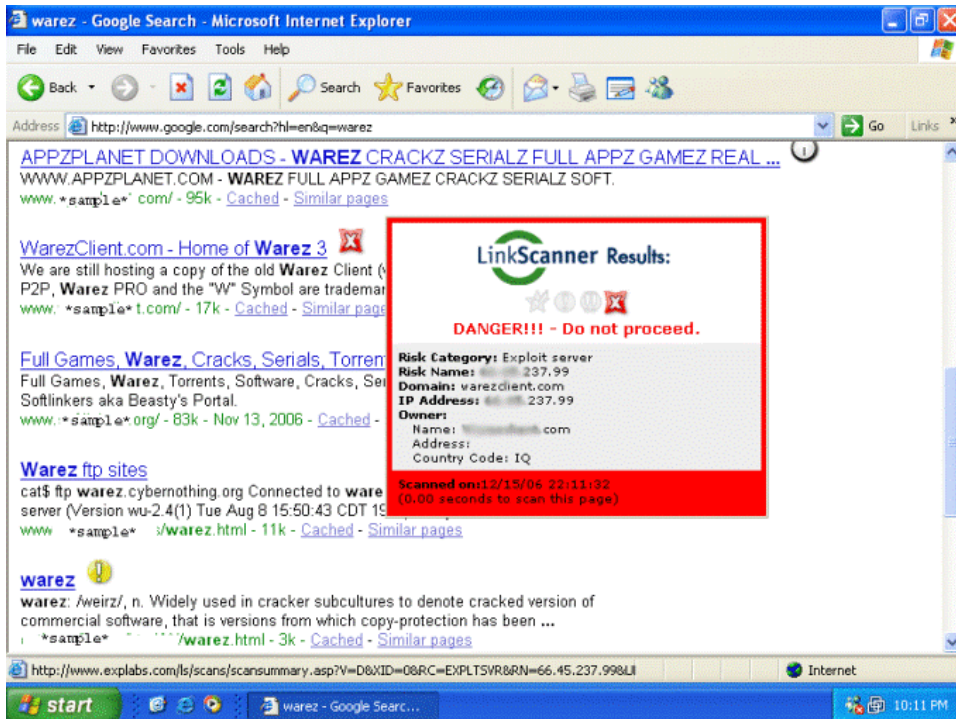


Using SearchShield

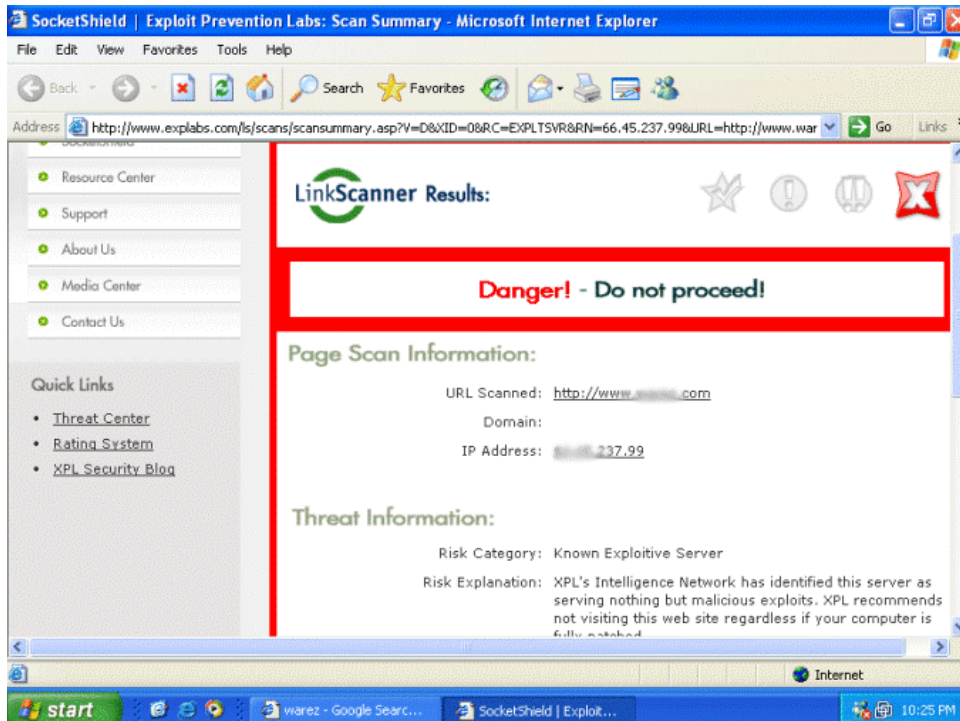
This section describes how **LinkScanner Lite's SearchShield** technology inspects and reports on search engine results. For the purposes of demonstration, Google results are used here.



As well as displaying an icon to represent the url's relative trustworthiness, SearchShield also provides additional information about the site and why that particular rating was assigned. You can see this additional information by hovering over the icon.



For each result, you can click on the icon, to get more in-depth information:

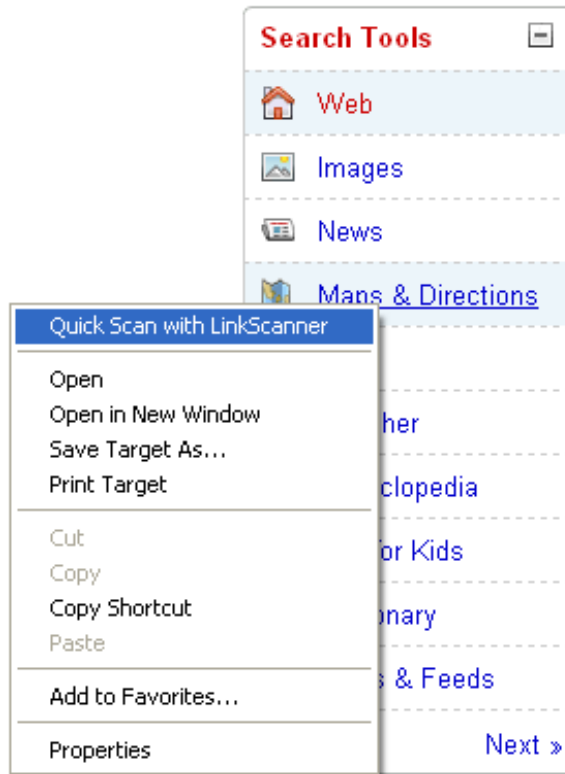


Using QuickScan

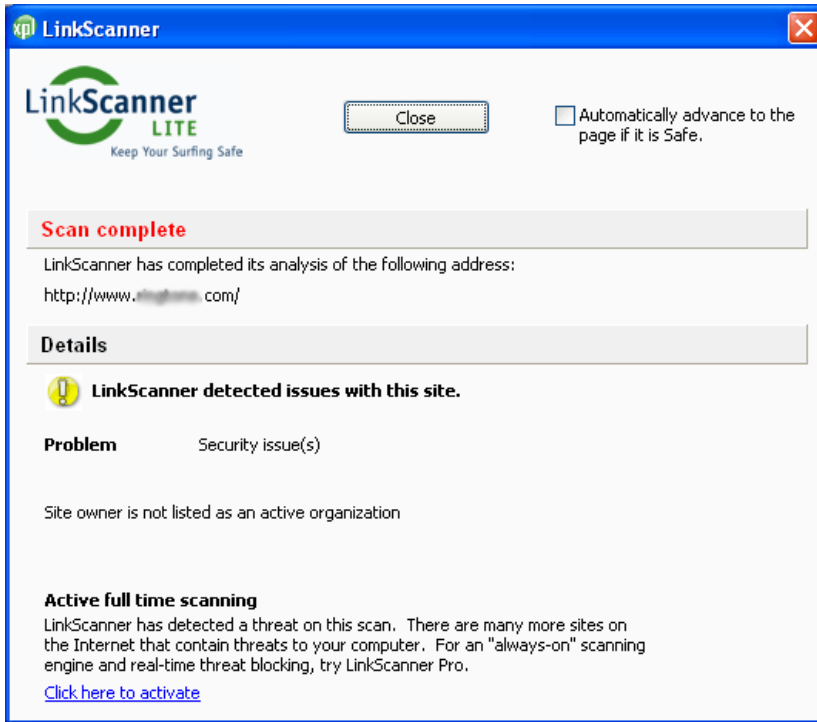
LinkScanner Lite's **QuickScan** gives you the ability to pre-scan any url to obtain a site trustworthiness report. **QuickScan** is great when you're browsing the web and for verifying links forwarded by friends, in blogs or other forums. There are two simple ways to **QuickScan** a link.

Right-click QuickScan

The easiest way to check a link quickly before visiting that page is to right-click on the link and select **QuickScan with LinkScanner**. This will give you a full report on the trustworthiness of the site.

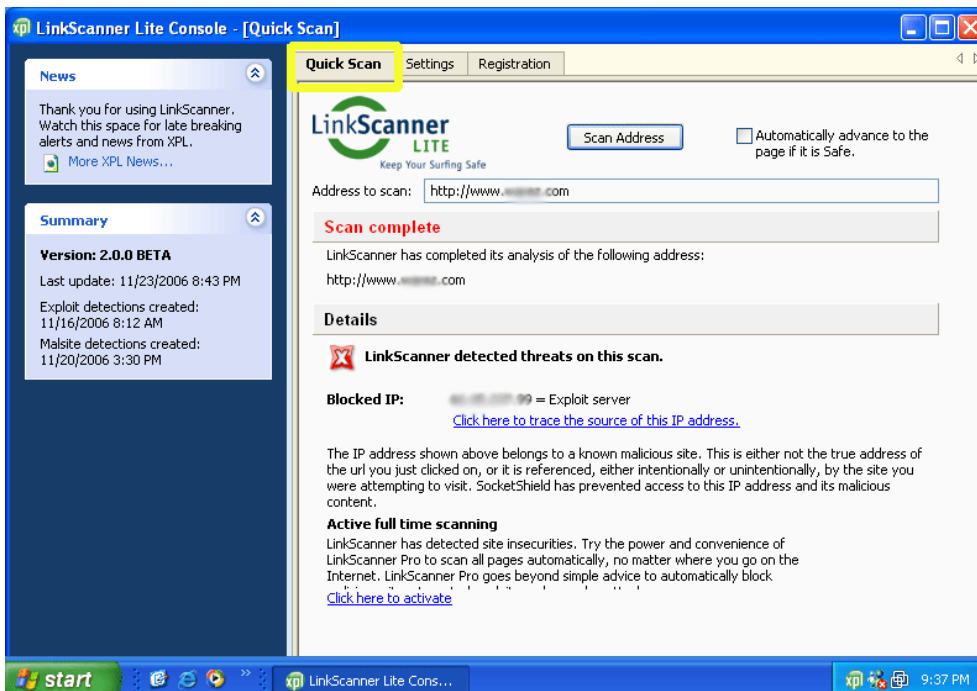


When a **QuickScan** is completed, a window showing the site safety rating is displayed. You can choose to be directed automatically to any link that results in a Safe rating by checking the box in the upper right corner. Leave it unchecked to always see the site report first.



Console QuickScan

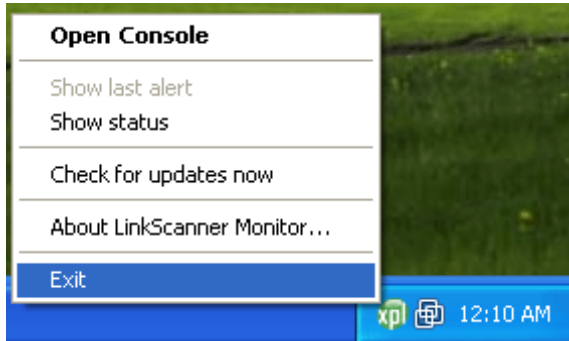
The second way to perform a **QuickScan** is to open the **LinkScanner Lite Console** and select the **QuickScan** tab. Enter a url into the **Address to scan** box and click **Scan Address**



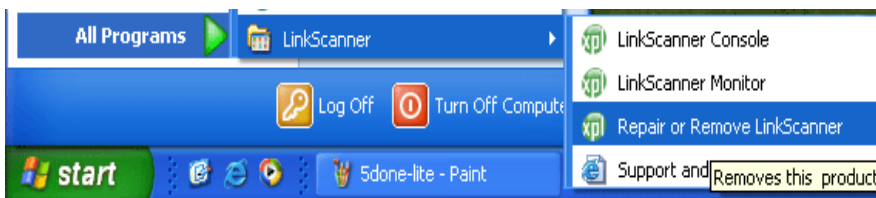
Repairing and Uninstalling LinkScanner Lite

Before commencing any uninstall process, make sure to close any open or running applications; a reboot is required to complete the uninstall.

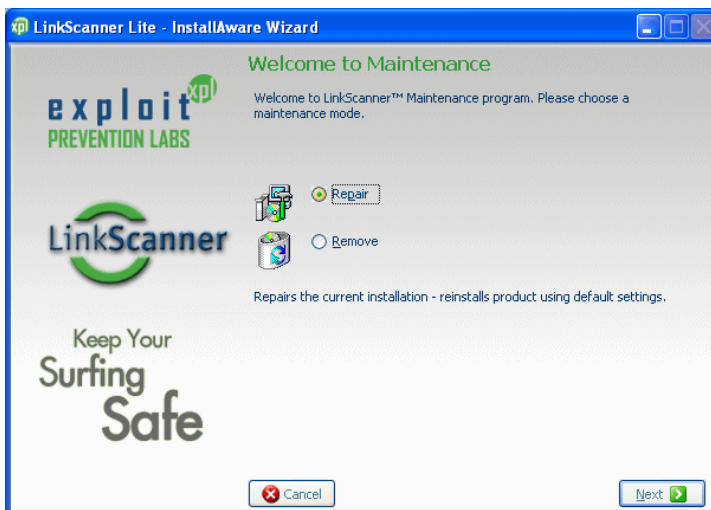
1. Shut down **LinkScanner Lite** by right-clicking on the **Monitor** icon in the system tray and choosing **Exit** from the available options.



2. Click **Start | Programs | LinkScanner Lite | Repair or Remove LinkScanner Lite** to activate **LinkScanner Lite's Maintenance Mode**.



3. Click **Repair** to fix the current **LinkScanner Pro** installation if it is not functioning properly.

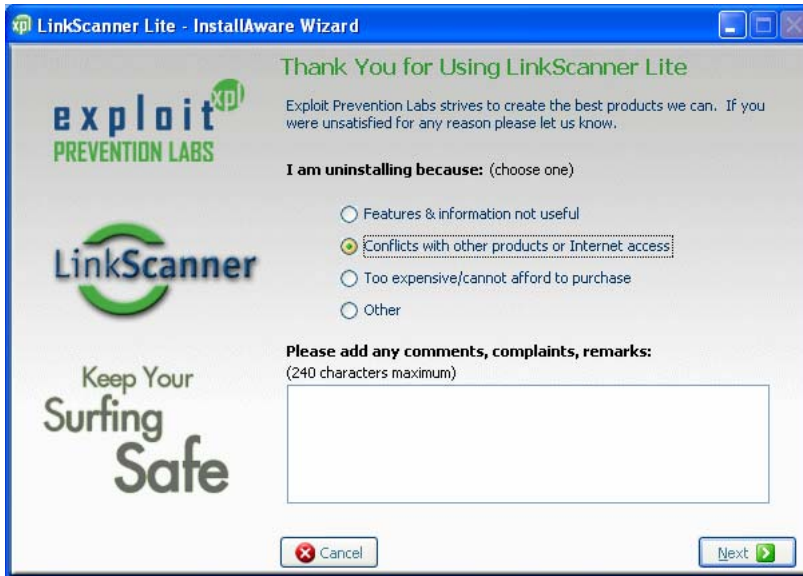


OR

Click **Remove** to uninstall all **LinkScanner Lite** components from your system.

Make your selection and click **Next**.

4. If you are uninstalling the program, please help us to serve you better in future by letting us know why you have chosen to uninstall **LinkScanner Lite**. Click **Next** to start the uninstall process.



5. The processing screen is displayed while **LinkScanner Lite** is removing its components from your system.



6. When the uninstaller has completed, click **Finish**.

Support and Documentation Resources

LinkScanner Lite documentation and support can be accessed in two ways:

- Go to **Start | Programs | LinkScanner | Support and Documentation**
- Go to the support area of our website at <http://explabs.com/support/index.html>

Resources Available

Knowledgebase

Search the online knowledgebase for answers to frequently asked questions, installation tips, information about exploits and more. You can perform a search by Article Number, Title, or Text of Article, or you can browse the articles via the drop-down menu at the bottom of the page.

LinkScanner Lite Release History

Learn about the latest product releases and fixes – you may be experiencing problems that have been fixed in a more recent version of the software and simply need to update.

Glossary

Here you'll find definitions of terms used to describe the threats and problems addressed by the LinkScanner product family. The glossary is also reproduced at the end of this document for your convenience.

Online Support

If you're unable to locate an answer to your question or concern, you can complete a simple online form to request assistance from our technical support team. Please provide as much detail as possible.

Report a New Exploit

If you believe your computer has been infected by an exploit that **LinkScanner Lite** has not detected, or that you have found a web site you believe is delivering new exploit code, please send the details, including any urls and a description of how you found the site/exploit, in an email to research@explabs.com. Please include your contact information so our researchers can get back to you with any questions they may have.

Glossary

Ad Server - Some Internet advertising networks occasionally (either knowingly or unknowingly) present advertising banners or text that point to or contain **exploits** or other malicious code. Such servers are identified by XPL's **Intelligence Network** as having served up such malicious code in the past.

Community Intelligence - A network of **LinkScanner** users who allow information about attempted exploitation of their computers to be transferred to **Exploit Prevention Labs** as part of the **Intelligence Network**.

Correlation Engine - Aggregates intelligence from the **Community Intelligence** and **Exploit Intelligence** networks and the **Reputation Filter**, assembles it in real time and distributes it to **LinkScanner** users.

Crack Server – A server that offers up tools and technologies that enable others to hack or crack into legitimate servers. Crack servers occasionally also serve up **exploits**.

Crimeware - **Exploits** and other **malware** programs that seek to extort money or other assets with portable value from the owner or user of an unpatched computer on behalf of a third party.

Drive-by Download - The downloading of one or more **malware** programs triggered by a user simply visiting a particular website; the user has no knowledge of the download taking place.

Exploit - A program that takes advantage of a **risk window** to take control of, damage, or remove information from an unpatched computer.

Exploit Distributor - A web page, usually displaying seemingly innocuous content, which also contains exploit code and is used to deliver **drive-by downloads**. Operators of **Exploit Distributor** pages are often paid a commission by the operator of the **exploit server** for each download they deliver.

Exploit Intelligence - An extended network of human researchers and automated probes, honeypots, and search bots focused on discovering new vulnerabilities and exploit examples for the purpose of preventing them from accessing users' computers.

Exploit Prevention Labs - the developer of the **LinkScanner** software and its associated **Intelligence Network**.

Exploit Server - A server operated by a developer or owner of **exploit** code for the sole purpose of distributing that exploit to a wide audience, usually via a network of exploit distributors.

i-frame – A one-pixel-square html command used to embed an html page from anywhere seamlessly within any other web page. Often used by some exploiters – known as **i-framers** – to hide exploit code on otherwise-innocent websites.

i-framers - Gangs of cybercriminals, such as CoolWebSearch, who use an **i-frame** (typically one pixel high, and one pixel wide, and thus invisible to the naked eye) to reach out to a **malicious site**, and serve up **exploits**.

Intelligence Network - **Exploit Prevention Labs'** patent-pending combination of research techniques comprising the **Community Intelligence** and **Exploit Intelligence** networks, the **Reputation Filter**, and the **Correlation Engine** used by **LinkScanner** to protect computers.

Keyloggers - A **malware** program that captures all keystrokes entered on a computer keyboard and delivers them to a third party; keyloggers are often, but not always, used by **exploits** and other **crimeware**.

Known Suspect ISP – A server identified by XPL's **Intelligence Network** as belonging to a known malicious Internet Service Provider. It is likely that all servers hosted by that ISP are malicious.

LinkScanner - A software program that protects computers by pre-scanning websites for malicious code and monitoring traffic for exploits identified through the **Exploit Prevention Labs' Intelligence Network** and closing the socket when an exploit is detected so that it cannot enter the user's machine.

Malicious site – A malicious site is any website to overtly or (more often) covertly deliver **malware** to a user's computer, usually by means of a drive-by download through the user's browser or a phishing attempt through the user's email client.

Malware – Malware is an umbrella term used to describe any software program designed to have a negative or destructive effect (payload). Malware includes viruses, worms, Trojan horses, spyware, adware, rootkits, and keyloggers, as well as more generic labels such as **crimeware** and **exploits** which may comprise several types of malware.

QuickScan – A function of LinkScanner that enables users to pre-scan any hyperlink. It's particularly useful for verifying links encountered during browsing or forwarded by friends, in blogs or other forums.

Phishing Site - Phishing sites give every appearance of being a legitimate site – usually a financial services site such as a bank or other financial institution - of which a user may be a member and have a signon. Many such sites even steal or point back to images on the misrepresented institution's website in order to look as authentic as possible. Such pages are actually gathering users' signon information for malicious purposes, including identity and monetary theft. Phishing is a specific type of **social engineering**.

Reputation Filter - Exploit Prevention Labs' proprietary technology which creates an intelligent filter for known and suspected exploit distributor sites.

Risk window - The period of time between the announcement of a **vulnerability** and the provision of a patch by the vendor. The average length of a risk window is currently 56 days.

Rootkits - A set of software tools intended to conceal running processes, files or system data, which helps an intruder maintain access to a system without the user's knowledge, often via some kind of 'back door' into the system. Rootkits are most frequently distributed via **drive-by download** and require high levels of technical expertise to remove safely.

SearchShield – A function of LinkScanner that inspects and advises users on the current safety level of search results from Google, Yahoo and MSN before clicking through to them. Each search result is classified into one of four categories: Safe, Questionable, Risky, and Dangerous, and each result is flagged with the appropriate icon.

Social Engineering - A social engineering site is any site that uses manipulative language, graphics or other content to trick a user into doing something that results in either giving away private and confidential information or downloading a program that grants the criminal high-level access to the user's computer for nefarious purposes.

Socket - A socket in the context of Internet security is the standard application programming interface (API) for sending and receiving data across the Internet, making it the point of entry into a user's system for any downloaded code.

Vulnerability - A weakness in an operating system or application that can be exploited by hackers and other criminals to distribute **crimeware**.