Quit Bugging Me!
CSI June 2005 Alert
Rebecca Herold, CISSP, CISM, CISA, FLMI
April, 2005

When I find white papers about privacy or security offered on vendor sites I often download them to read later. Around a year or so ago I provided my email address to a security vendor site and received a UNIX security Word document via email zip attachment. I filed it under my UNIX security file folder and forgot about it…that is until I got a friendly email from the vendor a few weeks later asking me if I needed assistance unzipping the file since they saw I had not yet opened it. The vendor had apparently bugged me!

A Creepy Crawly by Any Other Name…

Web bugs, also known as web beacons, web crawlers, and clear GIFs, can be much more invasive than cookies. They are usually designed specifically to be invisible. Surprisingly they have received much less press by privacy groups than I would have expected. However, this may be changing as their use is increasing, particularly by a wider range of businesses.

A web bug is typically a single pixel used to collect information. End-users have basically no control over the web bugs, or even knowledge that they are being used, cannot easily detect them, and cannot turn off web bugs in the same way that they can turn off cookies. Besides within HTML pages, web bugs can also be in Word, Excel, PowerPoint, and other Microsoft files, in addition to being placed within email messages.

Web bugs can collect an amazingly large amount of information for such a tiny little pest. For example, they can collect such data as the:

- End-user's IP address
- URL of the page where the Web bug is located
- Location of the web bug itself
- Time and date the web bug was it was initiated
- Type of browser used to retrieve the web bug
- Previously set cookie values
- Names
- Etc.

Web bugs in the aforementioned Microsoft files allow the document creator to track such activity as:

- Where a file is being read
- How often a file is being read
- When a file is sent to another person or organization
- Detecting and tracking leaks of confidential files from a company network
- Tracking possible copyright infringement
- Tracking the flow of intellectual property
- Monitoring the distribution of a marketing materials, such as a press release
- Tracking the copying of text from one document to a different document.

Microsoft files generally use web bugs to link to an image file that is located on a remote web server. The following are the types of information that could be sent to a remote web server when the file containing the bug is opened:

- The full URL of the web bug image
- The IP address and the host name of the computer requesting the web bug
- A web browser cookie

This image linking allows the remote server to monitor such things as when and where a file is being opened. Because the creator of the document has control of the URL of the document, he or she can put pretty much put any information within this URL. For example, a URL might contain a unique document ID number or the name of the person to whom the document was originally sent. Privacy concerns are heightened when web bugs are used in partnership with cookies. For example, cookies could allow the creator to match up the person who received the Word document to visits to the creator's web site.

Increasingly More Organizations Are Bugging Out

A 2001 Cyveillance study found that 95.94% of pages that contained web bugs also contained a top 50 brand. Companies are increasingly using web bugs for their marketing and customer relationship management (CRM) activities. Much of this activity is not obtrusive, but some question the ethics of using an invisible data-gathering tool without notifying the bugged individual of its existence. As the knowledge of web bugs becomes more widely communicated to consumers, businesses will likely start receiving more questions about if and how they are using web bugs. Organizations need to be aware of the privacy risks and customer concerns of using such secret surveillance tools.

Some organizations are increasingly using web bugs combined with cookies, customer databases, and other information-gathering methods, to identify web site visitors and file recipients, the web sites they visit, and when they visited them. Some organizations use web bugs for many purposes, such as:

- Providing an independent accounting of how many people visit a specific site
- Gathering statistics on browser usage on different places on the Internet
- Monitoring the effectiveness of advertising
- Adding information to a personal profile of the sites a person is visiting
- Determining the banner ads to display based on the accumulated profile
- Counting visitors to sites or gathering other statistical data
- Collecting data about those who visit clients' web pages, such as which ads they click on
- Collecting search terms or personally identifiable information
- Creating on-line traffic reports, advertising, and e-mail auditing
- Personalizing web sites
- Using within text material that accompanies downloaded MP3 music files to track how many times a song is played and on which computer(s)

How Wide Is the Web Bug Infestation?

www.securityspace.com has some interesting statistics on web bug use. It is amazing to see how many sites are using a wide range of web bugs, and also the types of bugs each site uses. Amazon.com appears to be using the widest range; the bugs they use include input, img, iframe, script, frame, area, im, s, i, 1000, image, content, fd3, ifram, cursive, 2000, br, and embed. See the securityspace site for some good descriptions for each of these types.

Another indication of the widespread use of web bugs is the number of websites devoted specifically to tracking and managing the web bugs organizations use; I found 80 different organizations, but there are probably more.

Spammers often use web bugs as a return receipt to verify valid e-mail addresses. Marketing agencies such as DoubleClick also utilize web bugs all over the Internet. When you visit a Web page that contains an advertisement, that advertisement often comes from a different site than the one you visited. However, the URL reference in the web bug's HTML causes your browser to send information about your browser type, source IP address, and other types of information, to the logs of the advertising company's web server, even if you didn't click the ad or visit the site.

Are Web Bugs Against the Law?

There are no enacted laws that I could find that specifically make the use of web bugs (or any of the aliases) illegal. In fact, the U.S. District Court for the District of Massachusetts ruled August 13, 2002, that Pharmatrak Inc. did not violate the federal Wiretap Act, the Stored Communications Act, or the Computer Fraud and Abuse Act in the way that it used cookies and web bugs to collect what may have been considered as personal information about visitors without their consent. Pharmatrak used web bugs to send cookies back to individuals' computers to monitor such things as the length of time a user viewed a pharmaceutical company's web site.

In a similar 2001 case involving electronic cookies used by market profiler DoubleClick, the court held that the web sites affiliated with DoubleClick were parties to the web bug communications and had given sufficient consent for DoubleClick to intercept them, even though the individuals about whom the web bugs applied did not know that their computers were communicating with DoubleClick and that the affiliated web sites appeared to not fully understand the mechanics of DoubleClick's service. The court dismissed the action, indicating they believed that DoubleClick's intentions were neither criminal nor tortious, but "motivated by legitimate business goals."

Call the Exterminator!

How do you feel about web bugs entering your corporate network and tracking your network users' activities? If you use ad- or cookie-blocking software, you may already be able to block web bugs. Programs such as InterMute's AdSubtract and Guidescope's utility offer web bug blocking features. If your web browser blocks third-party cookies or supports the P3P security standard, you may already be blocking web bugs. The Privacy Foundation's Bugnosis utility can be used to warn when a web page you're browsing contains a web bug.

Quit Bugging Me!
CSI June 2005 Alert
Rebecca Herold, CISSP, CISM, CISA, FLMI
April, 2005

Does Your Company Want to Bug People?

Before using web bugs, check to see if the intended use of web bugs violate your posted privacy policy. If not, then you should consider how the use of web bugs could undermine customer loyalty, damage corporate image, reduce your brand value, or otherwise impact your company's bottom line. If you decide based upon these considerations that you still need to use web bugs for marketing, or other business purposes, then seriously consider the following when implementing web bugs:

- Use visible web bugs
- Give notification if invisible web bugs are being used and how they are used
- Give notification if web bug data is transferred to third parties
- Allow your consumers to opt-in to allow web bug use
- If you want to use web bugs on another company's web site, structure the web bug icon (assuming you will make the web bug visible) so that the name of your company is visible. When a user clicks on the icon, display a disclosure that includes things like the type of data the web bug is tracking, how the data is used after it's collected, the companies receiving the data, how web bug data is combined with other data, and if a cookie is used along with the web bug.
- Do not use the web bugs to collect or track sensitive personal information (such as that which is medical, financial, or sexual) or information about children.

Guidelines for use of web bugs were issued in early 2002 by the Network Advertising Initiative (NAI), a group of on-line advertisements network operators. The text of their Web Beacons - Guidelines for Notice and Choice is available at http://www.networkadvertising.org/.

I want to emphasize how you need to be very careful to use web bugs only in accordance with your published web site privacy policy. Be sure to discuss any planned web bug use with your legal counsel to get their opinion and interpretation as it applies specifically to your organization. In fact, you should probably check with your legal counsel to see if they have already given your marketers or web applications area the green light to use web bugs. I have spoken to numerous security and privacy officers over the past year who didn't think their companies were using web bugs, but then were very surprised to found out their lawyers had approved web bug use months earlier based upon the nonexistence of laws expressly prohibiting such use. Your legal counsel may not have considered how such use would impact your privacy policy, or any third party contracts you may have in place, let alone the customer perception impact to your company. Wouldn't it really bug you to find out your company was already using web bugs without your knowledge?

Rebecca Herold, CISSP, CISM, CISA, FLMI is an independent information security, privacy and compliance consultant and can be reached at rebeccaherold@rebeccaherold.com. Rebecca has a B.S. in Math & Computer Science, an M.A. in Computer Science & Education, created "The Privacy Papers," co-authored "The Practical Guide to HIPAA Privacy and Security Compliance," authored "Managing an Information Security and Privacy Awareness and Training Program" and is currently authoring the online privacy governance manager for Information Shield.

